Application of Improved Multi-Objective Evolutionary Algorithm in Intelligent Tourism Interest Point Recommendation and Itinerary Planning

Jieli Zhang*, Yan Li
School of Humanities & Tourism, Yiwu Industrial & Commercial College, Yiwu 322000, China
E-mail: zhangjieli20181012@163.com
*Corresponding author

Keywords: multi-objective evolutionary algorithm, weak correlation adaptive evolutionary algorithm, archive strategy, smart tourism, tourism itinerary planning

Received: July 1, 2024

In the context of a boost in tourism and transportation, people's needs for the quality of tourism services are also increasing. Traditional scenic spot recommendations and itinerary planning methods cannot meet the personalized needs of tourists. Therefore, to achieve personalized services for tourist attractions and itineraries, this study introduces weakly correlated adaptive evolutionary algorithms and archival strategy algorithms to improve multi-objective optimization algorithms. It proposes an adaptive multi-objective evolutionary algorithm model for interest point recommendation and a multi-objective archival ant colony algorithm model for itinerary planning. The experimental results demonstrated that the proposed algorithm exhibited a 10% superiority over the enhanced algorithm in the recommended value of tourist attraction heat features and a 22.2% superiority in the recommended value of tourist attraction social network features. In trip planning, the convergence speed of the proposed algorithm model was faster, and the optimal solution could be found in 100 iterations, while the traditional algorithm needed 140 iterations. In addition, the DTLZ and WFG function test sets were used to evaluate the algorithm's performance. When the target number was 8, the HV value of the proposed algorithm was 0.42 and 0.16 higher than that of the improved algorithm and MOEADD algorithm, respectively. In the trip planning experiment, the total trip length was shortened from 213.4 km to 170.2 km by optimizing the path, effectively reducing unnecessary travel distance. The introduction of a weak correlation adaptive evolutionary algorithm and archiving strategy has led to a notable enhancement in the precision and efficacy of travel interest point recommendation and trip planning. Furthermore, this study has delineated a novel technical avenue for the advancement of personalized tourism services.

Povzetek: Predlagan je izboljšan večciljni evolucijski algoritem za priporočanje turističnih točk in načrtovanje poti, ki skrajšuje potovalno razdaljo, povečuje priporočila in izboljšuje program glede na individualne preference turistov.

1 Introduction

With the development of the tourism industry and the continuous progress of information technology, people's demand for tourism is also constantly increasing [1]. In the context of smart tourism, itinerary planning, and interest point recommendation are two core application scenarios. Journey planning needs to consider multiple factors, such as travel time, cost, attraction preferences, etc., while point of interest recommendation needs to be personalized on the ground of user preferences and behavior patterns. As a commonly used optimization technique, a multi-objective evolutionary algorithm (MOEA) can be used to solve these problems [2]. However, there are still some problems in the application of current MOEA, such as single recommendation results, lack of real-time performance, and inability to handle large-scale data [3]. Traditional travel planning methods typically use greedy or heuristic algorithms to find the optimal solution [4-5]. These methods often only consider a single objective function, such as the shortest travel time or the lowest cost, while ignoring other factors, such as attraction preferences. Therefore, this study proposes a multi-objective (MO) ant colony algorithm (ACA) with a fusion of archiving strategies for path planning and an adaptive evolutionary algorithm based on weak correlation to address the demerits of traditional methods. The innovation of the research lies in the proposal of two algorithmic models for scenic spot recommendation and itinerary planning. These models are designed to consider multiple objective functions simultaneously and to use archiving strategies to filter and retain solutions, thereby improving search efficiency. The first part of the study will provide a review of relevant research, introducing the current application

status and existing problems of MOEA. The second part will offer a detailed introduction to the research methods and implementation steps of adaptive evolution and archiving strategies that integrate weak correlations. The third part will conduct case studies to verify the feasibility of the algorithm model through experiments. Finally, the fourth part will summarize the research results and propose future research prospects. Through in-depth research and practice of this technology, it is expected to promote the intelligence of tourism services while meeting the tourism needs of different groups.

2 Background

MO algorithms are often applied to problems that require considering multiple conflicting objectives. To optimize the uneven distribution of individuals in the target space, Qiao et al. presented an adaptive hybrid evolutionary immune algorithm on the ground of MO algorithms. After experimental verification, the results showed that the algorithm could effectively avoid local optima and possessed a high convergence speed [6]. To investigate the impact of energy replenishment and data collection on network performance, Wang's team proposed a MO path planning model for joint energy replenishment and data collection. After verification, the target values of the model in data collection increased by 1.87%, 1.22%, 4.49%, and 2.10% [7]. To achieve MO optimization structural design of upper structure composite sandwich panels, Gholami et al. proposed a new MO niche Memetic particle swarm optimization algorithm. After experimental verification, the model proposed by the research has better performance [8]. Moghdani et al. proposed a MO volleyball super league algorithm to solve global optimization problems with MO functions and used it to solve 10 complex MO benchmark problems. The outcomes showed that this algorithm was superior to two state-of-the-art algorithms in MO benchmark problems [9]. To analyze the preferences of different decision-makers, Liu's team proposed a new decomposition MO evolutionary algorithm based on multi-layer interaction preferences. After testing, the results showed that the algorithm could effectively utilize preference information to search for the optimal solution and successfully handle many objective optimization problems [10].

The preferences of different groups towards tourist attractions and itineraries drive the development of tourism services. To achieve urban planning and tourism policy goals, Gil et al. used GIS search engines to analyze frequency and determine the most popular points of interest (POIs), and conducted correlation and regression analysis. The results indicated that this method provided effective information on scenic spots and tourist preferences for urban planners and tourism policies [11]. Liu et al. presented a new negative sampling method for increasing the accuracy of recommending interest points to users, considering both geographic distance and POI classification distance. Experiments have shown that the research method was at least 19.7% higher in F1 scores than the most advanced models, and at least 24.4% higher in NCG scores [12]. Chen et al. fused different categories of interest point data and multi-source remote sensing data to construct a three-dimensional model. This was to explore the nonlinear relationship between different geographical prediction factors and different heat source AHEs. After research, the results indicated that POI data had great potential in improving the accuracy of AHF mapping [13]. Uclea et al. conducted a sample survey of Romanian social media users and conducted multiple regression analysis, aiming to determine the role of social media in estimating the attractiveness of tourism destinations. The results indicated that social media possessed an essential influence on the tourism planning process [14]. To help tourism companies effectively obtain tourist interest information, Cheunkamon et al. synthesized TAM, TPB, and trust and satisfaction factors for developing a model of the relationship between structural factors. Research has shown that this model helped develop tourism marketing strategies and support sustainable competition [15].

Table 1 summarizes the key features, performance indicators, and limitations of these studies. Table 1 illustrates the advantages and potential for improvement of the proposed algorithm in the context of tourism interest point recommendation and itinerary planning, as compared to existing algorithms. The incorporation of a weak correlation adaptive evolutionary algorithm and an archiving strategy has led to a notable enhancement in the precision of recommendations and the efficacy of trip planning.

Table 1: Related literature review table

Algorithm name	Key feature	Performance indicators	limitation
Qiao et al. 's adaptive hybrid evolutionary immune multi-target algorithm [6]	Adaptive hybrid evolutionary immune algorithm based on uniform distribution selection	High convergence speed, effectively avoid local optimization	No specific mention of big data processing capabilities
Wang's team proposed a MO path planning model combining energy recharge and data acquisition [7]	Energy replenishment and data acquisition for wireless rechargeable sensor networks	Significant improvement in data collection target value	Tourism application scenarios are not mentioned
MO niche hybrid particle swarm optimization algorithm proposed by	MO optimization design for composite sandwich sandwich board	The performance is better than other algorithms, but it is not	Travel recommendations or itinerary planning are

Gholami et al. [8]		quantified	not involved
MO Volleyball Super League algorithm proposed by Moghdani et al. [9]	Solve global optimization problems for multiple objective functions	Excellent performance on a number of benchmark issues	Not directly used in the field of tourism
Multi-layer interactive preference decomposition MOEA proposed by Liu's team [10]	MO optimization based on multi-layer interactive preferences	Using preference information effectively to deal with MO optimization problems	Real-time performance in specific application scenarios is not mentioned
Gil team used GIS search engine to analyze the frequency of tourist attractions [11]	Use search engine data to analyze the frequency of tourist attractions	Provide effective information on tourist attractions and visitor preferences	Lack of real-time recommendation and trip planning capabilities
New negative sampling method proposed by Liu et al. [12]	Improve the accuracy of point of interest recommendations, taking into account geographical distance and POI classification distance	F1 scores and NCG scores improved significantly	No mention of large-scale data processing capabilities
Chen et al. integrated different types of interest point data and remote sensing data [13]	A 3D model was constructed to explore the relationship between geographic predictor and heat source	Improve the accuracy of AHF mapping	Not directly applied to travel recommendations
WAEA model is proposed in this study	MO optimization based on weak correlation adaptive evolutionary algorithm	Improved recommendation accuracy	/

3 Application of improved MO algorithm in tourism interest points and itinerary planning

To address the issues of accuracy and rationality of travel interest point recommendations in tourism services, this study is based on the MOEA and introduces weakly correlated adaptive evolutionary algorithms to improve [16]. The aim is to construct a tourism interest point recommendation system. Simultaneously incorporating the archiving strategy into the MO ACA aims to construct a travel planning optimization model.

3.1 MO evolutionary algorithm optimization strategy for tourism interest point recommendation

With the improvement of economy and living standards, tourism has become one of the important leisure and entertainment methods for people. However, traditional tourism recommendation methods cannot meet the personalized needs of tourists, cannot reflect market conditions in a timely manner, and it is also difficult to explore user interests and hobbies. The MO evolutionary algorithm combines multiple objective functions to comprehensively consider multiple factors and can solve MO optimization problems [17]. Therefore, this study is based on the MO algorithms to achieve recommendation of tourism interest points. The recommended objective function in the MO algorithm is shown in equation (1).

$$M\inf(X) = (f_1(X), f_2(X), ..., f_m(X)) \quad (1)$$

In equation (1), m is the total of multiple factors. X is the recommended solution. $f_m(X)$ is the function value of the recommended solution. The expression formula for the objective function value is shown in equation (2).

$$\mathrm{f}\, i = d(X, A_i) \quad (2)$$

In equation (2), A_i is the recommendation result considering the i -type factor in the recommendation function. d is the Euclidean distance in the recommended solution and the i -class factor. However, a single MO algorithm lacks real-time analysis of data and is difficult to handle data sparsity. The weak association-based adaptive evolutionary algorithm (WAEA) can adapt to market changes and user needs through continuous learning and optimization, achieve dynamic recommendations, and improve the intelligence and accuracy of recommendations. This study introduces the WAEA on the basis of MO algorithms to achieve improvements. In the WAEA, the habitat angle of the target space needs to be calculated first, and its expression is shown in equation (3).

$$a = \underset{i\in\{1,2,...,N\}}{median}\left\{\min_{j\in\{1,2,...,N\}} across(Vi, Vj)\right\} \quad (3)$$

In equation (3), V is the unit reference vector. j

is a constant value. a represents the perspective of the subspace habitat. Correspondingly, the angle subspace of the target space can be obtained, as expressed in equation (4).

$$C_i = \left\{ o \in R^m \middle| \langle o, V_i \rangle = \frac{a}{2}, \forall i = 1,2,...,N \right\} \quad (4)$$

In equation (4), o is the boundary vector. After generating the subspace, the original target space is divided to form a habitat with a consistent range, where the solution of the target is associated with the reference vector. Figure 1 is a schematic diagram of sub-association and multi-association generation in a two-dimensional target space.

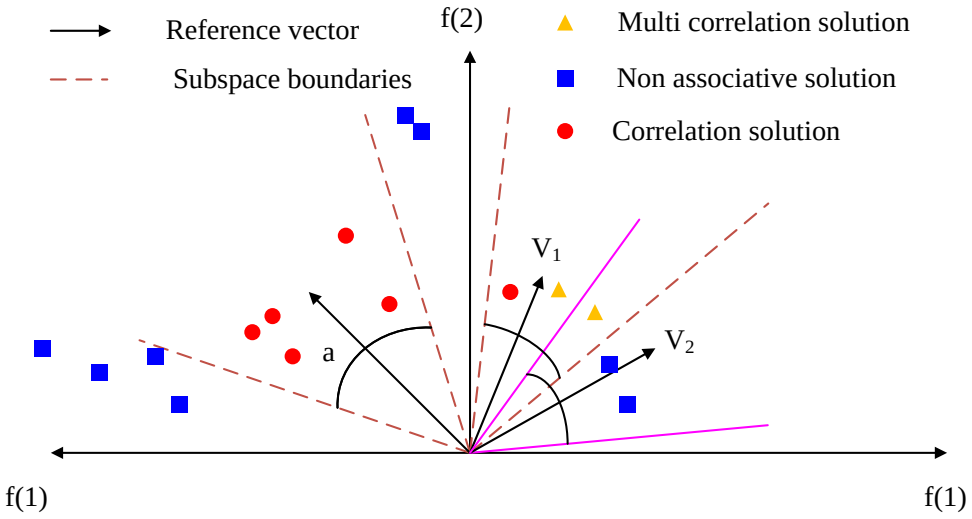


Figure 1: Generation of target sub-spaces and multiple association solutions in 2D space

As shown in Figure 1, in the two-dimensional target space, a sub-association can be represented as an association rule, where some variables have direct or indirect dependencies between them. The existence of this seed association can help us better understand the relationships between variables in the target space and provide more accurate prediction and classification capabilities. Multiple associations can take into account the interactions and dependencies between multiple variables, thus providing more comprehensive and accurate association rules. Next, it considers the angle between solutions in the habitat space, and its expression is shown in equation (5).

$$Angle(s, V_i) = ar\cos\left(\frac{f(s) \cdot V_i}{\| f(s) \|}\right) \quad (5)$$

In equation (5), s is the solution in the habitat space population. To further optimize the global selection strategy, a bimodal scalar function is utilizing for optimizing the MO problem, and its expression is shown in equation (6).

$$\min F(s, V_i) = \begin{cases} con(s) + \theta * d_2(s, V_i), s \in P_{vi} \\ con(s) + \theta * d_2(s, V_i) * R(s, V_i), s \notin P_{vi} \end{cases} \quad (6)$$

In equation (6), $R(s,V_i)$ is the angle ratio factor. $con(s)$ is the sum of target values for each dimension. θ is the penalty parameter. The expression for the sum of the target values of each dimension is shown in equation (7).

$$con(s) = \sum_{i=1}^{M} f_i(s) \quad (7)$$

Furthermore, the expression for d_2 can be obtained as shown in equation (8).

$$d_2 = \left\| f(s) - Z^* - d_1 \frac{V}{\|V\|} \right\| \quad (8)$$

In equation (8), Z^* is the minimum value of each target. To handle different types of high-dimensional MO problems, the penalty parameter θ is designed, and two major criteria, BSF and PBI, are used for parameter tuning. The parameter tuning process is shown in Figure 2.

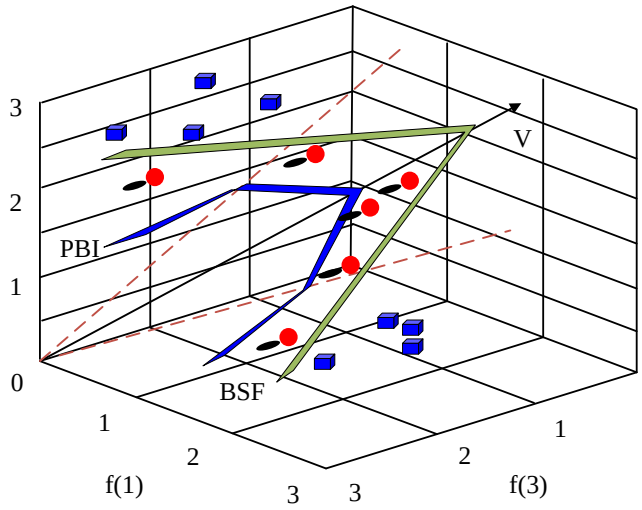


Figure 2: High dimensional MO optimization process

As shown in Figure 2, BSF and PBI criteria are used to evaluate the stability of the solving process and determine the optimal value of penalty parameters when dealing with high-dimensional MO problems [18]. Due to the complexity of high-dimensional MO problems, the solution process may become very unstable, resulting in inaccurate solution results. Therefore, calculating the rate of change of model function energy using the BSF criterion can evaluate the stability of the solving process and determine appropriate termination or convergence conditions [19]. In MO optimization problems, there are usually multiple conflicting objectives that require the use of penalty functions to transform into one objective function for optimization. The PBI criterion can select the optimal penalty parameter by comparing the values of the objective function under different penalty parameters, thereby facilitating the attainment of superior optimization results. In summary, by introducing the WAEA to improve MO algorithms, the objective function is continuously optimized and adjusted during the solving process of evolutionary algorithms to achieve better recommendation results.

3.2 Design of MO ACA for journey planning based on the archive strategy fusion

In tourism, MO algorithms can not only be applied to recommendation of tourism interest points, but also to travel itinerary planning [20]. In tourism itinerary planning, there are six elements of tourism, namely food, accommodation, transportation, travel, shopping, and entertainment. It is necessary to consider the conflict of multiple elements, and a single objective algorithm is difficult to obtain high-quality solutions. Therefore, this study introduces an archiving strategy to obtain better approximate Pareto frontiers and optimal solutions through two stages of evolutionary operations. Firstly, it calculates the number of explorations of tourists' travel modes between two places, and its expression is shown in equation (9).

$$N = \frac{1}{e^{\frac{x}{3}} * p} \tag{9}$$

In equation (9), p represents the iterative process of the ACA. x is the search record or archive record. Figure 3 shows the MO ACA for the archiving strategy.

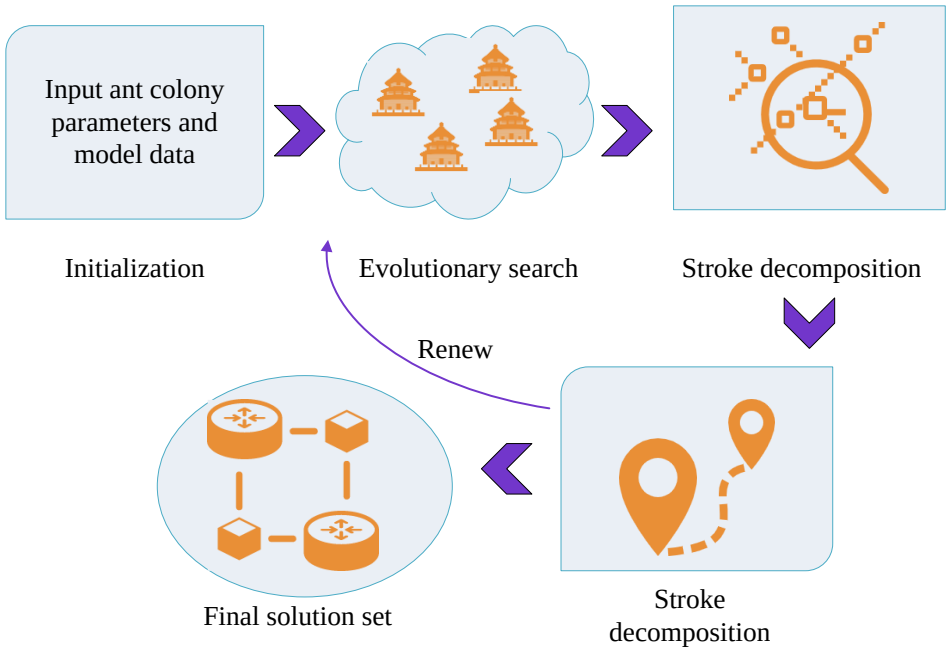


Figure 3: Flow of MO ACA based on the archive strategy

As shown in Figure 3, this study first sets parameters such as the quantity of ants, quantity of iterations, and pheromone volatilization rate, and initializes the pheromone matrix. Next, it aggregates the scenic spots and constructs a solution space on the ground of the problem definition of tourism itinerary planning. Each solution is represented as a travel route, completing the decomposition of the itinerary. Then, according to certain rules, it initializes the solutions in the solution space as an archive strategy, and calculates the attractiveness of each node. It updates the pheromone concentration of the node based on the pheromone matrix and attractiveness, and finally outputs the final solution set. In the integration of scenic spots, equation (10) is used to calculate them to avoid duplication.

$$P_{ij}^{k}=\begin{cases}\dfrac{\tau_{ij}(t)\eta_{j}(t)}{\sum s\in c\tau_{ij}(t)\eta s(t)}, j\in c\\ 0, j\notin c\end{cases} \quad (10)$$

In equation (10), c is the collection of scenic spots. τ_{ij} is the pheromone between two scenic spots. η_j is the inspiration information. When updating pheromones, equation (11) is used for calculation.

$$\Delta\tau_{ij}(t)=\begin{cases}\dfrac{Q}{time(i,j)*\cos t(i,j)}, (i,j)\in\rho\\ 0, (i,j)\notin\rho\end{cases} \quad (11)$$

In equation (11), Q is the intensity of pheromones. ρ is the volatilization coefficient of pheromones. ρ is the number of iterations. This indicates that the formula for calculating the next iteration of pheromones is shown in equation (12).

$$\tau_{ij}(t+1)=(1-\rho)\tau_{ij}(t)+\rho\Delta\tau_{ij}(t) \quad (12)$$

In equation (12), $1-\rho$ is the pheromone residue factor. Figure 4 shows the process of exploring the travel modes between two places in the final design.

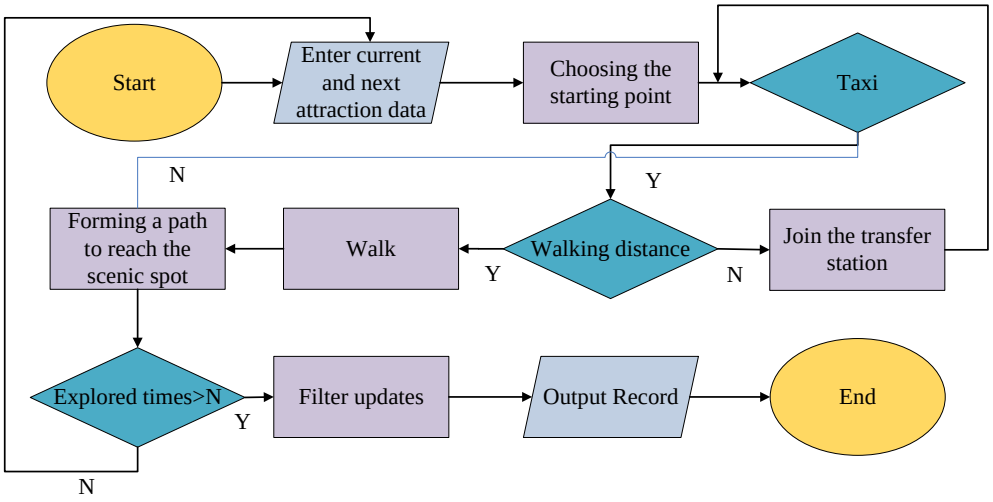


Figure 4: Process of exploring travel modes between two places

In the MO ACA based on archive strategy, the data and exploration times of the current and next attractions are first input, followed by the starting point and transportation. If they choose taxis as transportation, they will reach the next scenic spot, forming a new path. Otherwise, they will choose other public transportation methods or walk to reach the next scenic spot. If the exploration exceeds a certain limit, non-dominant modes of travel will be selected in the number of choices, and random selection will be made before output. Otherwise, a new mode of transportation will be selected. To verify the convergence and diversity of the algorithm, the HV index is selected to evaluate the coverage and convergence diversity of the MO ACA based on the archiving strategy in the target space. To estimate uncertain parameters, confidence intervals are used for sample extraction, and the expression is shown in equation (13).

$$P(a < x` < b) = a \tag{13}$$

In equation (13), $x`$ is the variable. a and b are probability intervals. The quantile expression of a in the confidence interval is shown in equation (14).

$$P(x < Z_{(a)}) = a \tag{14}$$

In equation (14), $Z_{(a)}$ is the quantile. Next, the probability density function is used to calculate the traffic time between two scenic spots.

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} \exp(-\frac{(t-\sigma)^2}{2\sigma^2}) \tag{15}$$

In equation (15), σ is the standard deviation. The final tourism itinerary planning framework based on the MO ACA with archiving strategy is shown in Figure 5.

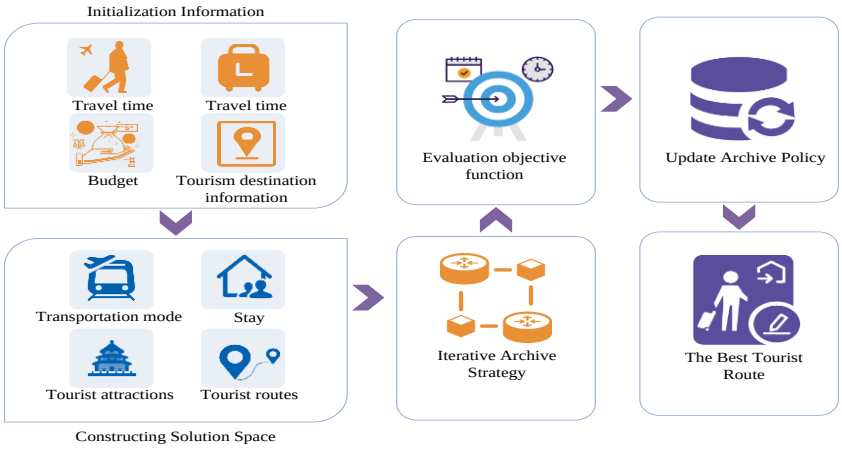


Figure 5: Tourism itinerary planning framework on the ground of MO ACA with archive strategy

The tourism itinerary planning framework based on the archive strategy MO ACA can be divided into the following parts. Firstly, the tourism destination information, travel time, budget and other constraints, as well as the preferences and needs of tourists, are inputted into the tourism itinerary planning. Based on the problem definition of tourism itinerary planning, a solution space is constructed using appropriate coding methods. Each solution represents a tourist route, including tourist attractions, transportation methods, accommodation, etc. Next, it initializes the archive strategy, initializing some of the solutions in the solution space as the archive strategy according to certain rules. The archive strategy can include solutions that have already been explored, as well as some initial solutions. Then it uses MO ACA for iterative search and continuously updates the archiving strategy. In each iteration, the ant selects a path based on the archiving strategy as the current path, and updates the pheromone concentration of the path based on the pheromone matrix and attractiveness. It selects the next node based on the updated pheromone concentration and probability. It repeats this process until it reaches the endpoint or reaches the maximum number of iterations. It adds each path to the archive policy. Next, it evaluates the quality of each solution in the archiving strategy based on the objective function of tourism itinerary planning, which includes travel time, cost, scenic spot tour integrity, etc. It continues to update the archiving strategy based on the evaluation results of the objective function, and adds solutions with good evaluation results to the archiving strategy, while deleting solutions with poor evaluation results. Finally, the optimal solution in the archive strategy is output as the result of tourism itinerary planning. This is defined as the tourism route that aligns with the needs and constraints of tourists, while also exhibiting the optimal objective function value. In summary, a tourism itinerary planning framework based on MO ACA with archive strategy is utilized for obtaining tourism routes that meet the needs and constraints of tourists. This can improve the efficiency and accuracy of tourism itinerary planning.

4 Application evaluation of MO optimization algorithms in tourism recommendation and itinerary planning

To verify the superiority of the WAEA MO algorithm model for tourism interest point recommendation, this study collected relevant scenic spot information for scenic spot feature recommendation value analysis, and compared it with relevant algorithm models. To verify the effectiveness of the MO recommendation ACA model in tourism itinerary planning, this study selected the maximum total utility of the route, the minimum total cost of the route, and the minimum maximum travel time in the route to analyze the performance of the model.

4.1 Experimental environment settings

The computer configuration used in the experiment is as follows: the processor is Intel Core i9-9900K CPU @ 3.60GHz, with 8 cores and 16 threads. The memory is 64GB DDR4 RAM and the frequency is 3200MHz. The storage is 1TB NVMe SSD, which is used for fast read and write of operating system and experimental data. The operating system is Windows 10 Pro 64-bit. The programming language and tools are Python 3.8, implemented using scientific computing libraries such as NumPy, Pandas, Scikit-learn, and custom MOEA and ACA algorithms. To verify the effectiveness of the proposed algorithm, a dataset containing information about tourist attractions in multiple cities is constructed. The dataset is drawn from multiple publicly available tourism data sources, including government tourism authorities, online travel platforms, and social media. It is about 5GB in size and contains more than 100,000 records. Each record contains multiple dimensions such as location, opening hours, ticket prices, user reviews, social media mentions, and popularity ratings. To comprehensively evaluate the performance of the proposed algorithm, the evaluation indexes such as recommendation accuracy, over-volume, maximum total route utility, minimum total route cost, minimum maximum travel time, convergence speed, and path length optimization are used.

4.2 Performance evaluation of intelligent tourism interest point recommendation system

To verify the recommendation effect of the MO algorithm introduced by WAEA in smart tourism interest points, this study first selects 10 tourist attractions in a certain city for recommendation value analysis of a single feature factor. The parameters of WAEA-MOEA algorithm are set as follows: The population size is set to 100. The crossover rate is set to 0.8. The variation rate is set to 0.05. The maximum number of iterations is set to 1000. The convergence criterion is that the algorithm is considered to converge when the change of the optimal solution is less than 0.01% in 10 successive generations. The temporal complexity of WAEA-MOEA is mainly composed of population size, number of objective functions, crossover operation, variation operation and fitness evaluation. For each iteration, the time complexity is roughly O (N*M*G), where N is the population size, M is the number of objective functions, and G is the number of iterations. The outcomes are shown in Table 2.

Table 2: Recommended values of characteristic factors of different scenic spots

Scenic spot number	Correlation feature	Synergistic feature	Heat characteristic	Social networking is extremely high
1	87	92	78	79
2	67	56	46	57
3	68	47	57	46
4	57	76	47	63
5	57	56	43	62
6	46	46	57	73
7	35	36	36	74
8	78	47	36	52
9	53	57	37	74
10	67	68	65	51

Table 2 shows the recommended value analysis of feature factors for scenic spots based on the WAEA MO algorithm. The feature factors for each scenic spot are selected as correlation features, collaborative features, popularity features, and social network features. Then, the feature factors are combined based on different user preferences and the optimal solution is obtained. Among them, attraction 1 has the highest recommendation value for each feature, with a collaborative feature recommendation value of 92. Then, to verify the recommendation accuracy of the MO algorithm based on WAEA, the recommendation values of the correlation features, collaborative features, popularity features, and social network features of the scenic spots are compared before and after the improvement of the algorithm. The results are shown in Figure 6.

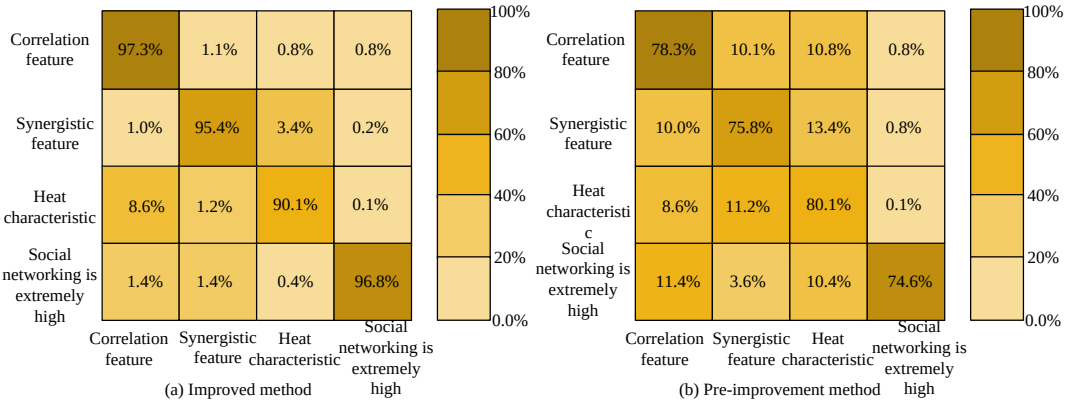


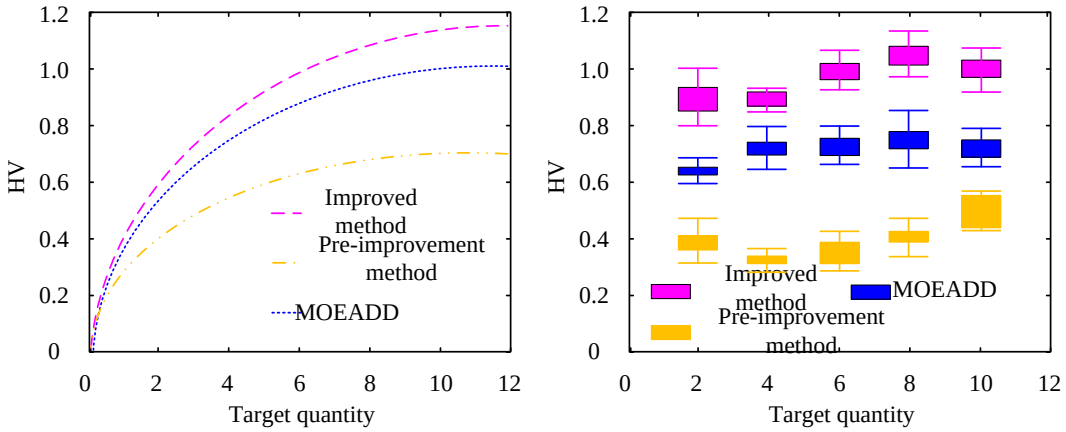
Figure 6: Comparison of accuracy of landscape feature recommendation values

Figure 6 shows the accuracy comparison outcomes of the recommended values for the four feature factors of scenic spots. It demonstrates that the average recommendation accuracy of the improved WAEA-based MO algorithm is over 90%. The accuracy of the recommended values for scenic spot related features is the highest at 97.3%, which is 19% higher than the accuracy of the recommendations before improvement. In the accuracy comparison of collaborative feature recommendation values, the research algorithm is 19.6% higher than the improved algorithm. In the analysis of the accuracy of recommended values for tourist attraction heat characteristics, the research algorithm is 10% higher than the improved algorithm. In the accuracy analysis of social network features in scenic spots, the research algorithm is 22.2% higher than the improved algorithm. This indicates that the WAEA-based MO algorithm has a higher accuracy in extracting feature factors from various scenic spots, which is conducive to providing more accurate recommendation services for tourists. In addition, the standard deviation and 95% confidence interval for each feature recommendation accuracy are calculated. The results are shown in Table 3. Standard deviation and 95% confidence interval data can better illustrate the stability of algorithm performance.

Table 3: Standard deviation and 95% confidence interval of feature recommendation accuracy

Feature type	Average recommendation accuracy	Standard deviation	95% confidence interval
Correlation feature	97.3%	0.5%	[96.8%, 97.8%]
Synergistic feature	96.9%	0.6%	[96.3%, 97.5%]
Heat characteristic	91.2%	0.7%	[90.5%, 91.9%]
Social network characteristics	92.5%	0.4%	[92.1%, 92.9%]

Table 3 shows that WAEA-MOEA algorithm has stable and reliable performance. For example, the correlation feature recommendation accuracy is as high as 97.3% and the standard deviation is only 0.5%, showing high precision stability. The narrow confidence interval of the recommendation accuracy of each feature indicates that the algorithm performs consistently in different situations, effectively improving the accuracy and credibility of the recommendation of tourism interest points. Secondly, functional test sets of DTLZ and WFG are selected to compare the performance of the WAEA-based MO algorithm with the improved algorithm, as well as the decomposition-based MO evolutionary algorithm (MOEAD) in solving target problems for different scenic spots and tourists. The results are shown in Figure 7.



(a) DTLZ function data set (b) WFG function data set

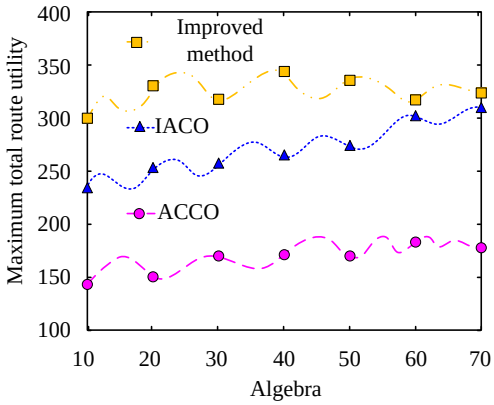
Figure 7: Comparison results of HV values under different targets

Figure 7 (a) shows the comparison results of HV values of various algorithms under the DTLZ function test set. As the target values of tourism interest points increase in Figure 7 (a), the HV value of the MO evolutionary algorithm based on WAEA also increases, and the HV value of the research algorithm always remains the highest under any number of targets. When the target number of tourist attractions is 8, the HV value of the research algorithm is 0.42 and 0.16 higher than that of the improved algorithm and MOEADD algorithm. Figure 7 (b) shows the comparison of HV values of different algorithms under the WFG function test set, where the HV values of the research algorithms are also at the leading level. When the target number of tourism interest points is 8, the maximum HV value of the research algorithm reaches 1.1, which is 0.53 and 0.24 higher than the HV values of the improved algorithm and MOEADD algorithm, respectively. The higher the HV value, the more excellent the overall performance of the solution set on the ground of this algorithm. In summary, the research algorithm not only effectively extracts the feature values of tourist attractions, but also has higher recommendation accuracy for different tourist attractions.

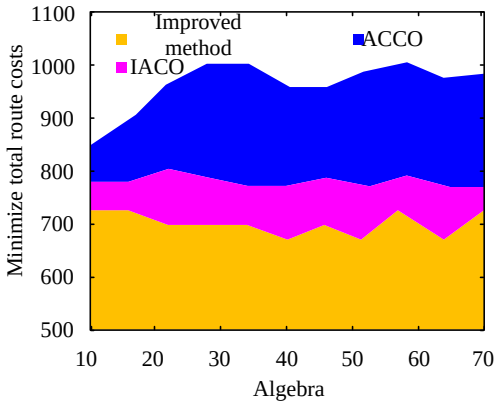
4.3 Analysis of the itinerary planning effect of MO ACA on the ground of archive strategy

To verify the recommendation effect of MO ACA based on archive strategy in tourism itinerary planning, three indicators are considered: maximum route total utility, minimum route total cost, and minimum maximum travel time in the route. It compares the research model with the Interactive Ant Colony Optimization (IACO) and Adaptive Harmony Search Algorithm (ACCO) models. The parameters of the MO ACA algorithm are set as follows: The number of ants is set to 50. The number of iterations is set to 100. Pheromone volatilization rate is set to 0.1. In the archive policy, the archive size is set to 50. Convergence criteria: By monitoring the changes in the super volume values, it is possible to determine whether the algorithm is converging. The time complexity of MO ACA algorithm is not only composed of population size,

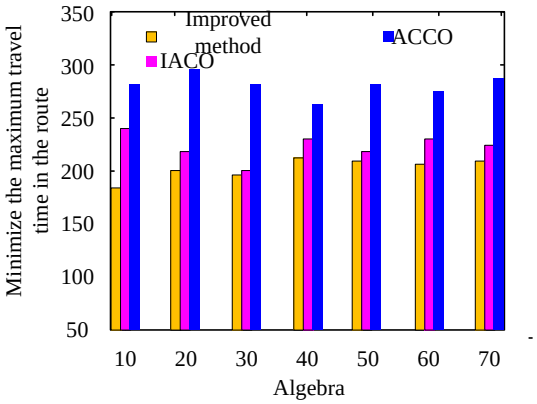
number of objective functions, cross-operation, mutation operation, and fitness evaluation, but also involves pheromone renewal and path selection. Its time complexity also includes the number of ants and the cost of updating pheromone matrix. Its time complexity is close to O (N*G), where N represents the combined effect of the number of ants and the number of iterations. The results are shown in Figure 8.



(a) Maximum route total utility comparison



(b) Minimize total route cost comparison



(c) Minimize the maximum travel time comparison in the route

Figure 8: Recommendation effect of travel planning index

Figure 8 (a) shows the comparison results of the maximum route total utility of three models. The MO ACA model based on archive strategy studied has an increasing optimization ability as the quantity of iterations grows. Compared with the IACO and ACCO algorithm models, the average value of the maximum route total utility in its travel planning is 50-100 values higher. Figure 8 (b) shows the comparison results of the total cost of minimizing the route for three models. The MO ACA model based on archive strategy, compared with the IACO and ACCO algorithm models, maintains a minimum total cost of 700 and performs well. Figure 8 (c) shows the comparison results of the maximum travel time among the minimized routes of the three models. Figure 8 (c) shows that the time required to study the algorithm model is minimal and remains basically below 200. This indicates that the algorithm model studied in this study has the highest overall utility in travel planning, with the lowest cost and time for planning travel. Next, it compares the total utility of travel planning among the three algorithm models, and the results are shown in Figure 9.

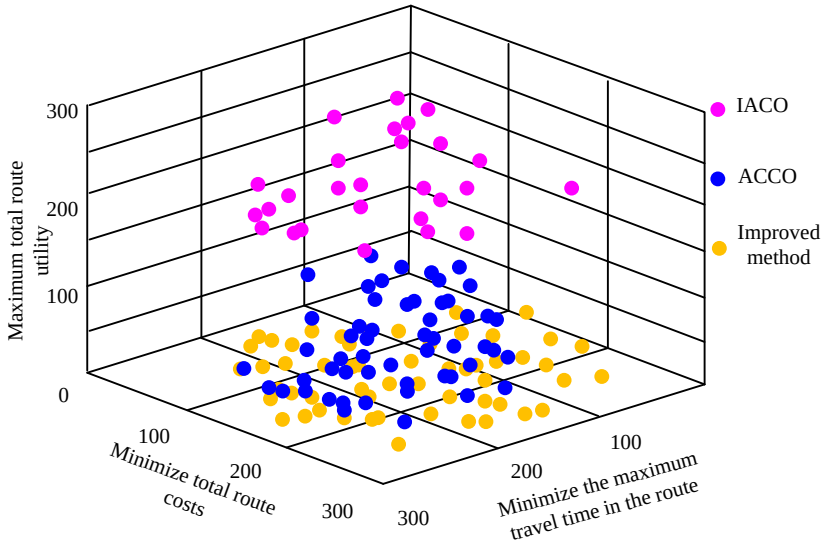


Figure 9: Comparison of MO optimization results in trip planning

The MO ACA model based on archive strategy studied in Figure 9 performs well, specifically in the MO solution of tourism itinerary. The solution is mainly concentrated below the target space, within the range of 100 to 200 units between minimizing the total cost of the route and minimizing the maximum travel time in the route. This indicates that the research algorithm has advantages in minimizing the total cost of the route and minimizing the maximum travel time in the route planning. The solutions of the IACO and ACCO algorithm models are more dispersed, and their advantages are not obvious. Next, the research algorithm model is applied to tourism itinerary planning, and the results are shown in Figure 10.

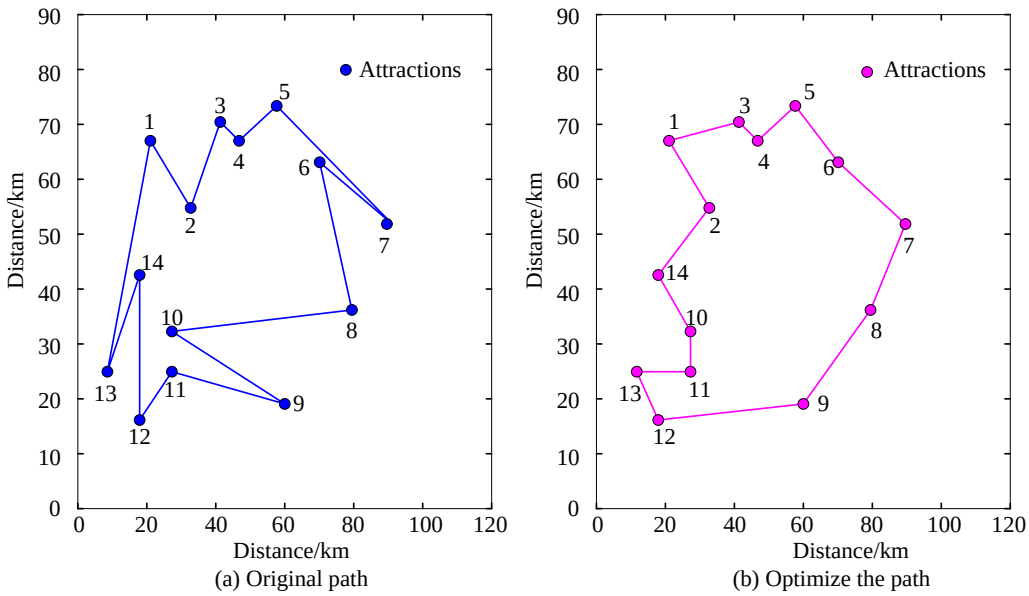


Figure 10: Optimization results of travel itinerary path

Figure 10 shows the results of a MO ACA model based on archive strategy in tourism itinerary planning. Figure 10 shows a total of 14 tourist attractions involved in the tourism itinerary planning, with a total length of 213.4 km in the original itinerary. After studying the algorithm model and optimizing the path, the total length of the travel itinerary is 170.2 km, which reduces the travel by about 43.2 km and effectively reduces unnecessary distance in the itinerary. This indicates that the algorithm model in this study can find the best travel itinerary. Finally, the optimization results of the research algorithm model at various distances are shown in Figure 11.

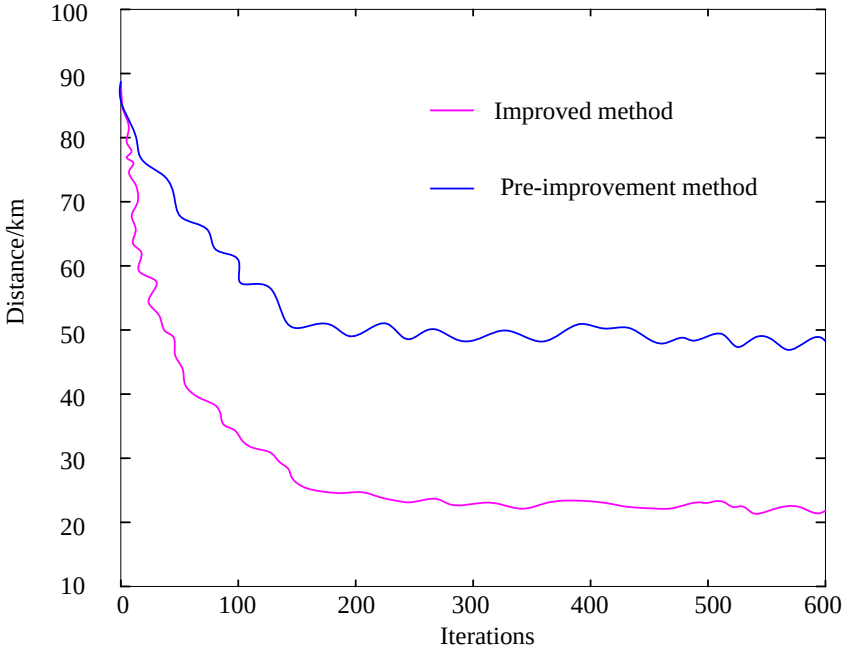


Figure 11: Convergence curve of the number of tourist attractions and travel distance

When the number of cities in Figure 11 is small but the journey is long, the convergence speed of the research algorithm is faster, and the optimal solution can be found within 100. However, traditional algorithms require 140 iterations for finding the optimal solution, indicating that the research algorithm is markedly more excellent than the MO algorithm before improvement. This indicates that the study of MO ACA based on archive strategy can achieve the highest total utility in travel itinerary planning, minimize the cost and time of planning itinerary, and simultaneously plan the optimal route.

4.4 Performance of the algorithm in different tourism cases

To further enhance the applicability and persuasiveness of the paper, case studies of the proposed algorithm in different tourism environments will be presented, mainly including actual cases of different scenarios such as urban and rural, cultural and adventure tourism. These case studies not only verify the wide applicability of the algorithm, but also demonstrate its superior performance in different situations. The specific case analysis is shown in Table 4.

Table 4: Details of the case analysis

Case type	Background description	Experimental design	Experimental result
City tourism	Famous tourist city in China, rich in historical and cultural relics, modern shopping centers and food streets	WAEA-MOEA algorithm is used to recommend personalized points of interest, and MO ACA algorithm is combined to plan the optimal itinerary	Recommended points of interest with high accuracy, in line with individual needs; Trip optimization reduces the total travel distance by about 20%
Rural tourism	Countryside with beautiful natural scenery, featuring pastoral scenery, rural culture and farmhouse music	Adjust the weight of WAEA-MOEA algorithm, focusing on natural scenery and parent-child activity recommendation; Plan an itinerary that includes multiple modes of transportation	Recommended points of interest combine natural scenery with parent-child activities, reasonable schedule, reduce travel costs
Cultural tourism	A famous historical and cultural city with rich historical sites, museums and	Use WAEA-MOEA algorithm to recommend historical and culture-related attractions and	Recommended cultural interest points are well loved, itinerary design

	traditional cultural performances	activities; Plan a reasonable tour route	improves tourist satisfaction, and fully experience the cultural atmosphere
Adventure travel	Famous outdoor adventure destination with steep mountains, fast-flowing rivers and lush forests	Combining WAEA-MOEA algorithm to recommend adventure activities; Plan an itinerary that includes multiple adventure activities	Recommend adventure activities to meet challenges and ensure safety; Reasonable schedule to ensure tourists rest and recovery

From Table 4, the proposed algorithm performs well in a variety of situations, verifying its wide applicability and superior performance. These case studies not only enhance the persuasiveness of the paper, but also provide valuable references for practical applications.

5 Discussion

MOEA based on WAEA and MO ACA based on archiving strategy presented in the study show significant performance improvement in the recommendation of travel interest points and itinerary planning. Compared with existing SOTA methods, the above algorithm shows advantages in many aspects [21]. First of all, in terms of the recommendation of tourist interest points, WAEA-MOEA algorithm shows higher accuracy in extracting feature values of scenic spots. The experimental results demonstrate that the recommendation accuracy of WAEA-MOEA for the correlation features, collaborative features, heat features, and social network features of scenic spots is significantly higher than that of the improved algorithm. Notably, the recommendation accuracy for correlation features reaches 97.3%, which is 19% higher than that of the improved algorithm. This is primarily attributable to the fact that WAEA can adapt to market changes and user requirements, and is thus able to generate recommendations that are continuously updated and optimized, thereby enhancing the precision and sophistication of the recommendations provided. Secondly, in terms of trip planning, the archiving strategy-based MO ACA algorithm is also superior to traditional algorithms in convergence speed and optimization effect [22]. The experimental results show that the algorithm can find the optimal solution within 100 iterations, while the traditional algorithm needs 140 iterations. In addition, by optimizing the path, the algorithm shortens the total travel length from 213.4 km to 170.2 km, effectively reducing unnecessary travel distances. This is mainly due to the application of archiving strategy, which makes the algorithm more effectively retain the good solutions and eliminate the bad ones, thus improving the search efficiency and the quality of the final solutions.

The innovation of this study lies in the two new algorithm models for the recommendation of tourism interest points and itinerary planning. First of all, WAEA-MOEA algorithm realizes dynamic adaptation to market changes and user needs by introducing weak correlation adaptive evolution mechanism, and improves the accuracy and intelligence level of recommendation. Secondly, MO ACA algorithm based on archiving strategy combines archiving strategy and MO optimization technology to realize efficient solution of travel itinerary planning problems. These two algorithm models not only solve the limitations of traditional methods in dealing with MO optimization problems, but also significantly improve the quality and efficiency of the solution by introducing new optimization strategies and technical means. Although the proposed algorithm has achieved remarkable results in the recommendation of tourism interest points and itinerary planning, there are still some potential limitations and areas for improvement. This research mainly focuses on the recommendation and planning of individual tourists without fully considering the interests and preferences of tourism groups. In the future, the research scope can be further expanded to recommend and analyze tourism groups. Secondly, the proposed algorithm needs to be optimized in processing large-scale data and real-time recommendation. With the continuous growth of tourism data and the increase of real-time recommendation demand, how to further improve the real-time and scalability of the algorithm will become the focus of future research. In addition, future work can also consider combining the research algorithm with other advanced artificial intelligence technologies, such as deep learning, reinforcement learning, etc., to achieve more intelligent and personalized travel recommendation and planning services.

6 Conclusion

With the increasing personalized demand for tourist attractions, traditional tourist attraction recommendations cannot meet the diverse needs of tourists and cannot provide the best travel itinerary for them. Therefore, this study enhanced the MO evolutionary algorithm in two key areas: tourism interest points and itinerary planning. It developed a MO tourism interest point recommendation model based on WAEA and a MO ant colony itinerary planning model based on archive strategy. Experiments have shown that the research model could effectively extract correlation features, collaborative features, popularity features, and social network features of scenic spots. Among them, the accuracy of recommendation values for scenic spot correlation features was the highest

at 97.3%, which was 19% higher than the accuracy before improvement. In the comparison results of HV values between different algorithms, when the target number of tourist attractions was 8, the HV values of the research algorithm were 0.42 and 0.16 higher than those of the improved algorithm and MOEADD algorithm, respectively. In comparison to the IACO and ACCO algorithm models, the average value of the maximum route total utility of the research model's travel planning was found to be between 50 and 100 values higher. After studying the algorithm model and optimizing the path, the total length of the travel itinerary was 170.2 km, resulting in a reduction of approximately 43.2 km. This indicates that the two proposed algorithm models can effectively recommend tourist interest points and design the optimal itinerary. The drawback of this study is that it did not consider the interest preferences of tourist groups and only analyzed individual tourists. In the future, research recommendations and analysis can be conducted for group tourists.

Funding

The research is supported by Zhejiang Provincial Department of Commerce 2021 Annual Strategy project and Zhejiang Province Green Exhibition Development Path Research under the goal of carbon neutrality, 2021ZSY62. The Second Batch of Teaching Reform Projects in the "14th Five-Year Plan" for Higher Vocational Education in Zhejiang Province: Exploration and Practice of the Path of Deep Integration of Industry and Education in the Event Management Professional Clusters of School-enterprise Mutual Embeddedness in the Context of New Quality Productivity (jg20240240).

References

[1] S. Chen, D. Tian, R. Law, and M. Zhang, “Bibliometric and visualized review of smart tourism research,” International Journal of Tourism Research, vol. 24, no. 2, pp. 298-307, 2022. https://doi.org/10.1002/jtr.2501

[2] S. Choudhuri, S. Adeniye, and A. Sen, “Distribution alignment using complement entropy objective and adaptive consensus-based label refinement for partial domain adaptation,” In Artificial Intelligence and Applications, vol. 1, no. 1, pp. 43-51, 2023. https://doi.org/10.47852/bonviewAIA2202524

[3] G. Kourakos, G. Brunetti, D. P. Bigelow, S. Wallander, and H. F. Dahlke, “Optimizing managed aquifer recharge locations in california's central valley using an evolutionary multi-objective genetic algorithm coupled with a hydrological simulation model,” Water Resources Research, vol. 59, no. 5, pp. 231-243, 2023. https://doi.org/10.1029/2022WR034129

[4] Y. Fang, B. Luo, T. Zhao, D. He, B. Jiang, and Q. Liu, “ST-SIGMA: Spatio-temporal semantics and interaction graph aggregation for multi-agent perception and trajectory forecasting,” CAAI Transactions on Intelligence Technology, vol. 7, no. 4, pp. 744-757, 2022. https://doi.org/10.1049/cit2.12145

[5] A. Aydin, E. Bostanci, and O. O. Tanriover, “A multiple objective evolutionary algorithm approach to find optimal design parameters for beam position monitoring systems,” International Journal of Modern Physics C, vol. 31, no. 7, pp. 234-256, 2020. https://doi.org/10.1142/s0129183120500382

[6] J. Qiao, F. Li, S. Yang, C. Yang, W. Li, and K. Gu, “An adaptive hybrid evolutionary immune multi-objective algorithm based on uniform distribution selection,” Information Sciences, vol. 512, no. 3, pp. 446-470, 2020. https://doi.org/10.1016/j.ins.2019.08.032

[7] X. Wang, Z. Lyu, Z. Wei, L. Wang, Y. Lu, and L. Shi, “Multi-objective path planning algorithm for mobile charger in wireless rechargeable sensor networks,” Wireless Networks, vol. 29, no. 1, pp. 267-283, 2023. https://doi.org/10.1007/s11276-022-03126-2

[8] M. Gholami, A. Fathi, and A. M. Baghestani, “Multi-objective optimal structural design of composite superstructure using a novel MONMPSO algorithm,” International Journal of Mechanical Sciences, vol. 193, no. 1, pp. 45-57, 2021. https://doi.org/10.1016/j.ijmecsci.2020.106149

[9] R. Moghdani, K. Salimifard, E. Demir, and A. Benyettou, “Multi-objective volleyball premier league algorithm,” Knowledge-Based Systems, vol. 196, no. 7, pp. 189-201, 2020. https://doi.org/10.1016/j.knosys.2020.105781

[10] R. Liu, R. Zhou, R. Ren, J. Liu, and L. Jiao, “Multi-layer interaction preference based multi-objective evolutionary algorithm through decomposition,” Information Sciences, vol. 509, no. 9, pp. 420-436, 2020. https://doi.org/10.1016/j.ins.2018.09.069

[11] E. Gil, Y. Ahn, and Y. Kwon, “Tourist attraction and points of interest (POIs) using search engine data: case of seoul,” Sustainability, vol. 12, no. 9, pp. 564-578, 2020. https://doi.org/10.3390/su12177060

[12] Q. Liu, L. Mu, V. Sugumaran, C. Wang, and D. Han, “Pair-wise ranking based preference learning for points-of-interest recommendation,” Knowledge-Based Systems, vol. 225, no. 2, pp. 107-119, 2021. https://doi.org/10.1016/j.knosys.2021.107069

[13] Q. Chen, X. Yang, Z. Ouyang, N. Zhao, Q. Jiang, T. Ye, and W. Yue, “Estimation of anthropogenic heat emissions in China using Cubist with points-of-interest and multisource remote sensing data,” Environmental Pollution, vol. 9, no. 11, pp. 115-163, 2020. https://doi.org/10.1016/j.envpol.2020.115183

[14] C. E. Țuclea, D. M. Vrânceanu, and C. E. Năstase, “The role of social media in health safety evaluation of a tourism destination throughout the travel planning process,” Sustainability, vol. 12, no. 16, pp. 66-81, 2020. https://doi.org/10.3390/su12166661

[15] E. Cheunkamon, S. Jomnonkwao, and V.

Ratanavaraha, “Determinant factors influencing Thai tourists’ intentions to use social media for travel planning,” Sustainability, vol. 12, no. 18, pp. 725-732, 2020. https://doi.org/10.3390/su12187252

[16] C. Sun, F. Wen, W. Xiong, H. Wang, and H. Shang, “Multi-objective comprehensive teaching algorithm for multi-objective optimisation design of permanent magnet synchronous motor,” IET Electric Power Applications, vol. 14, no. 13, pp. 2564-2576, 2020. https://doi.org/10.1049/iet-epa.2020.0322

[17] C. Wang, and C. Ma, “Multi-objective optimization of customized bus routes based on full operation process,” Modern Physics Letters B, vol. 11, no. 2, pp. 205-216, 2020. https://doi.org/10.1142/s0217984920502668

[18] J. G. Ding, L. P. Kong, J. H. Guo, M. X. Song, and Z. J. Jiao, “Multi-objective optimization of slab heating process in walking beam reheating furnace based on particle swarm optimization algorithm,” Steel Research International, vol. 6, no. 8, pp. 567-579, 2021. https://doi.org/10.1002/srin.202000382

[19] W. Li, W. Gong, F. Ming, and L. Wang, “Constrained multi-objective evolutionary algorithm with an improved two-archive strategy,” Knowledge-Based Systems, vol. 3, no. 12, pp. 246-257, 2022. https://doi.org/10.1016/j.knosys.2022.108732

[20] T. H. Chang, L. T. Watson, J. Larson, N. Neveu, W. I. Thacker, S. Deshpande, and T. C. Lux, “Algorithm 1028: vtmop: solver for blackbox multiobjective optimization problems,” ACM Transactions on Mathematical Software (TOMS), vol. 48, no. 3, pp. 1-34, 2022. https://doi.org/10.1145/3529258

[21] X. Zheng, B. Han, and Z. Ni, “Tourism route recommendation based on a multi-objective evolutionary algorithm using two-stage decomposition and pareto layering,” IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 2, pp. 486-500, 2023. https://doi.org/10.1109/JAS.2023.123219

[22] S. Sundarraj, R. V. K. Reddy, M. B. Basam, G. H. Lokesh, F. Flammini, and R. Natarajan, “Route planning for an autonomous robotic vehicle employing a weight-controlled particle swarm-optimized Dijkstra algorithm,” IEEE Access, vol. 11, no. 3, pp. 92433-92442, 2023. https://doi.org/10.1109/ACCESS.2023.3302698

Metaheuristic-Based Supply Chain Network Optimization and Inventory Management Using Ant Colony Algorithm

Bingting Huang
School of Commerce & Tourism College, Chenzhou Vocational Technical College, Chenzhou 423000, Hunan, China
Email: jessica_huang1220@163.com

Keywords: ant colony algorithm, supply chain, network optimization, inventory management, energy efficiency ratio

Received: September 6, 2024

Integrating ant colony algorithms in supply chain network optimization and inventory management provides a new approach to improving efficiency and reducing costs. The global search capability of the algorithm is utilized to optimize the supply chain network to minimize total costs and improve service levels. The strategy of dynamically adjusting inventory levels based on demand forecasts and the ACO algorithm solves the inventory management problem, aiming to achieve customer demand fulfillment and inventory cost reduction. The approach's effectiveness was validated through case study simulations, which significantly improved over traditional optimization methods. Supply chain optimization efficiency increased by 20%, inventory cost was reduced by 10%, and response time was accelerated to 1 day. These results highlight the ACO algorithm's practical applicability and potential advantages in supply chain management. This study contributes to the theoretical framework of supply chain management and provides innovative solutions for companies to achieve more efficient supply chain operations.

Povzetek: Predstavljen je nov način optimizacije oskrbovalne verige in upravljanja zalog z algoritmom kolonije mravelj, kar poveča učinkovitost omrežja za 20% in zmanjša stroške zalog za 10%.

1 Introduction

In today's globalization, supply chain management has become an important part of the core competitiveness of enterprises. The complexity and dynamic nature of supply chain networks require enterprises to have efficient, flexible and reliable management capabilities to cope with the ever-changing market environment. However, traditional supply chain management methods are often difficult to adapt to this complexity and dynamics, resulting in frequent problems such as waste of resources and slow response [1, 2]. Therefore, how to optimize the supply chain network structure and improve the efficiency of inventory management has become an urgent problem to be solved [3, 4]. Heuristic search mechanism makes the ant colony algorithm show good performance when dealing with complex systems. Therefore, the introduction of ant colony algorithm into supply chain network optimization and inventory management is expected to provide new ideas and methods to solve the above problems.

This paper will study the supply chain network optimization and inventory management methods based on ant colony algorithm. First of all, we will introduce the basic concepts of supply chain management and the basic principles of ant colony algorithm. Then, the supply chain network optimization method based on ant colony algorithm is elaborated in detail, including the optimization of network topology structure, the determination of node location and the choice of path. On this basis, an inventory management strategy based on ant colony algorithm is proposed, including demand forecasting, inventory control and replenishment strategy.

In order to confirm the effectiveness of our proposed methodology, we will conduct a simulation analysis based on real case studies. The analysis will feature a comparative summary table that compares the performance of traditional methods with our Ant Colony Algorithm (ACA) based approach, particularly in terms of cost reduction, service level improvement, and other vital metrics. Not only does it highlight the superiority and utility of our approach, but it also points out the gaps and limitations of existing methods. In this way, the necessity of our ACA-based solution becomes even more evident as it addresses the problems of poor adaptability and limited scalability that are common in traditional techniques [5, 6]. The superiority of the Ant Colony Optimization (ACO) approach is dissected, attributing it to the powerful global search capability and efficient exploration-exploitation balance. However, its limitations, such as sensitivity to parameter tuning, are also presented. The differences in results are analyzed in detail, considering the effects of different problem instances, parameter settings, and real-world constraints. This discussion not only highlights the potential of the ACO method for supply chain optimization but also provides a critical view of the challenges in its practical application, enriching the discussion of metaheuristic applications in logistics and inventory management. This section strengthens the contribution of this paper by providing a comprehensive account of the efficacy of the ACO approach and areas for future research improvements.

In addition, the research results in this paper significantly contribute to the advancement of supply chain management theory and practical applications. By providing an innovative management tool like an ant colony algorithm, our research helps companies achieve more efficient supply chain operations and optimal resource allocation. This work also expands the scope of

applying ACO algorithms in logistics management and provides valuable insights for subsequent research. Finally, it reveals challenges and problems in supply chain management, guides future research directions, and opens new perspectives.

2 Ant colony algorithm for supply chain network optimization and inventory management

2.1 Ant colony algorithm

Ant colony algorithm was used to solve path optimization problems [7]. Ant colony algorithm is a heuristic algorithm that simulates ants searching for food. It can solve complex problems that are difficult to solve with traditional search methods. It is mainly used in machine production, combinatorial optimization, planning and design and other fields. Ant colony algorithm has strong robustness and inherent parallelism, and is suitable for solving multi-objective VRP and TSP problems.

There are six main parameters of ant colony algorithm: α is the information heuristic factor, β is the expected heuristic factor, ρ is the pheromone volatilization factor, m is the total number of ants in the ant colony, Q is the pheromone constant, and n is the number of iterations.

This section includes a detailed pseudo-code that meticulously adapts the ACO algorithm to the specifics of supply chain logistics. Each step is articulated, encompassing the dynamic pheromone update mechanism, heuristic information computation tailored to inventory management, and the strategic handling of supply chain constraints. Moreover, a sensitivity analysis is conducted on pivotal ACO parameters, namely α, β, and ρ, revealing their impact on the algorithm's efficacy in the complex environment of supply chain optimization. This analysis elucidates how these parameters influence solution quality and algorithmic robustness, significantly enhancing the paper's technical depth and practical applicability.

2.1.1 Parameter setting of ant colony algorithm model

The main parameters of ant colony algorithm are pheromone heuristic factor α, expected heuristic factor β, pheromone volatilization factor ρ, the total number of ants m, pheromone enhancement coefficient Q, and the number of iterations of ants n. Ant colony algorithm has a strong applicability to solve the problem. Its parameter values will have different values according to different situations. Generally, specific problems are analyzed in detail. The general parameter value setting requirements are: the range of α is between 1-5, the range of β is between 0-7, the range of ρ is between 0-1, the range of m is determined by the number of delivery customer nodes, and the range of Q It is basically between 1-1000, and the range of n is basically between 100-500.

2.1.2 Mathematical model of ant colony algorithm

State transition probability of ant colony algorithm. Assuming τ_{ij} (0) = C, the transition probability of ant k from i to j is P^k_{ij} (t), and the formula can be seen as (1).

$$p_{ij}^{k}(t)=\begin{cases}\dfrac{\tau_{ij}^{\alpha}(t)\ \ \eta_{ij}^{\beta}(t)}{\sum\limits_{s\in allow_k}\tau_{ij}^{\alpha}(t)\ \ \eta_{ij}^{\beta}(t)} & j\in allow_k\\ 0 & otherwise\end{cases} \tag{1}$$

Pheromone update rule of ant colony algorithm. With the search process, the pheromone concentration will change. In order to prevent the excessive pheromone concentration from affecting the effect of heuristic information, the pheromone on the path must be continuously updated. The update formula is as follows. Every time the ant completes an iteration, it needs to update all the paths. Pheromone, formulas such as (2) and (3). Ant colony algorithm has strong parallel computing ability and positive feedback mechanism, and has high robustness, and the requirements for the initial solution are not very high.

$$\tau_{ij}(t+1)=(1-\rho)\tau_{ij}(t)+\Delta\tau_{ij}(t) \tag{2}$$

$$C_1=\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{k}z_k{}^{*}c_k \tag{3}$$

The heuristic factor is shown in formula (4):

$$\eta_{ij}=\frac{1}{d_{ij}} \tag{4}$$

2.1.3 Working process of ant colony algorithm

Initializes parameter values. The initial time and iterations are set to input the initial positions of m ants onto their respective nodes, the initial node information is input, and the pheromone concentration $\Delta = \tau_{ij}$ (0) is initialized.

Construct the solution space. Set up a tabu table to store the nodes that ant k has visited, and store the node number where ant k is located in the tabu table. The ant starts to search for optimization, and the ant selects next node j, and store node j in the tabu table to avoid repeated visits.

Updated pheromone concentrations. When all node numbers are stored in the tabu table, the ant completes this iteration, obtains the total path length and time window penalty cost of this iteration, and stores the optimal path, path length and time window penalty cost obtained by each iteration, and continuously updates the concentration on each path.

Determine whether all iterations have been completed. If the maximum number of iterations is reached, iter _ max, the iteration is stopped, otherwise, it returns to step 2 to continue the search and optimization process.

End of algorithm. Output optimal solution and obtain delivery path, the total length of the path and the penalty cost of the time window.

By comparing with other optimization techniques, such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO), our analysis demonstrates the advantages of the ACO algorithm and reveals its potential limitations when dealing with large-scale supply chain networks. This analysis is crucial for assessing the feasibility and efficiency of the algorithms in real-world applications, helping supply chain managers and decision-makers to make more informed decisions when selecting optimization tools. In this way, our research is not limited to theoretical contributions but also provides essential references in practice.

2.2 Supply chain network

There are several different types of enterprise objects in the supply chain, such as suppliers, manufacturers, consumers, etc. [8, 9]. A simple functional realization supply chain can present a relatively direct chain structure. If multiple chain supply chains blend together, chain network will be formed. Supply chain network has the typical characteristics of complex networks, and the typical characteristics of complex networks will have impact on evolution behavior. It is one of the hot spots for scholars to apply network to explore the evolution behavior of supply chain networks. The dynamic development of supply chain network can be systematically optimized by using the theory of complex network, so as to enhance its overall robustness, control the evolutionary risk, and finally realize the stable algorithmic progression of the supply chain network.

A detailed description of how the ACO algorithm can be applied to a real-world supply chain network optimization and inventory management problem is presented. Not only is the effectiveness of the ACO algorithm in solving real-world problems demonstrated but also the challenges encountered during implementation, such as the integration of the algorithm into existing Enterprise Resource Planning (ERP) systems and how to deal with real-time data flow, are discussed. This way, our research results are closer to real-world operations, enhancing their application value and potential for replication in supply chain management practices.

2.2.1 Chain structure supply chain

The Chain is composed of many member companies, but the supply chain can be abstracted as a single chain structure in the production and circulation of a single product. In this chain structure, each node represents the member enterprises, and a relatively simple supply chain is formed by connecting each node with a line. This chain-like supply chain structure is relatively abstract, which includes capital flow, logistics transportation and information transmission. However, in a real supply chain, the system contains far more than one manufacturer, distributor, etc., but many object nodes. Therefore, the chain structure is actually a part of the selection of the network structure.

2.2.2 Network structure supply chain

In the actual life operation process, each supply chain system has more than one supplier, manufacturer, distributor, consumer. And the same level of different enterprises also contains cooperative relations, the network supply chain is composed of so many nodes and complex relationships between nodes. In the abstract topology, each enterprise is an indiscriminate node, and the connections between nodes indicate that there are complex business connections between enterprises. The network-type supply chain can well map the components and structural characteristics of the supply chain in real life, and abstractly show the relationship between enterprises in the supply chain.

2.3 Inventory management

Inventory classification is the process of classifying and managing the inventory of raw materials, semi-finished products, materials and finished products in an enterprise according to some specific standards. Figure 1 shows the feature extraction of inventory management text. Usually, the inventory classification method will consider factors such as the importance of materials, dynamic changes, production requirements, and material types, and divide inventory of different types and characteristics into different levels or categories, and manage its procurement, storage and transportation [10]. Inventory classification can effectively reduce inventory costs, improve the accurate delivery rate of materials, and help enterprises purchase and manage inventory more accurately.

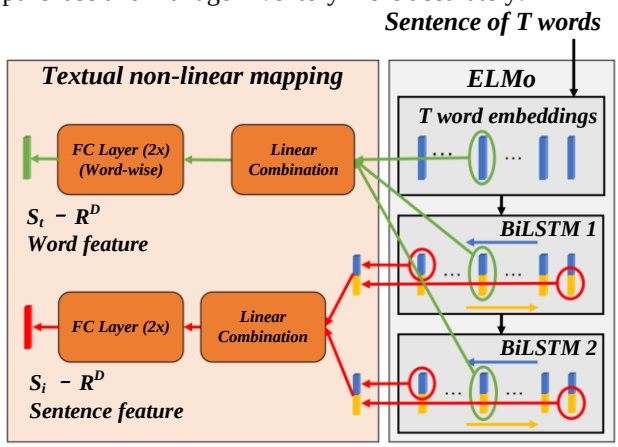


Figure 1: Feature extraction of inventory management text

ABC analysis according to the value and demand of items, mainly divided into the following three categories: Class A inventory is high-value and high-demand items. While only a small fraction of the inventory, they are of high value and require high attention, and it is essential to monitor the inventory levels of these items on a daily basis and put money into them in a timely manner. Usually managed by the first-in, first-out (FIFO) method [11] to ensure inventory freshness and quality. Category B stocks are items of medium value and medium demand. Such items account for a large proportion of the entire inventory and need to be monitored and managed regularly to

prevent excessive occupation of warehouse space and funds. Generally, the average cost method (AVCO) is used for cost accounting. Category C inventory refers to items of low value and low demand. Although they are of low value, they also require regular management and cleanup due to their large quantities to avoid taking up too much warehouse space and funds.

PQR analysis is a classification method based on inventory life cycle [12]. Category P inventory is items that are about to expire or have expired. Such items need to be managed dynamically to ensure that there are no expired or broken items in the inventory to avoid losses and waste. Class Q inventory is normal inventory for regular sales. Such items have a steady sale and need to be regularly replenished to meet production and sales needs. Class R inventory is spare inventory [13]. Specifically, the XYZ analysis method divides inventory into the following three categories: Class X inventory is items with relatively stable demand and strong regularity. The inventory of such items is relatively large, and it can be managed in quantitative economic batches, that is, to determine a certain order volume and safety stock level to ensure supply, and at the same time, inventory clearance and inventory should be carried out regularly. The demand fluctuation of category Y inventory is generally between category X and category Z, and the inventory needs to be adjusted regularly according to the demand, and the inventory management needs to be meticulous to avoid excessive occupation of funds and warehouse space. Category Z inventory refers to items whose demand is uncertain and difficult to plan.

3 Supply chain network optimization and inventory management based on ant colony algorithm

3.1 Model establishment

3.1.1 Evolution model of supply chain network

The addition of a new node. Based on the previous explanation, Figure 2 shows the supply chain network optimization model based on ant colony algorithm. This model assumes that the arrival of nodes in the network obeys the parameter of p Poisson process. Each new node arrives to join the network with edges, which connect m existing nodes in the network.

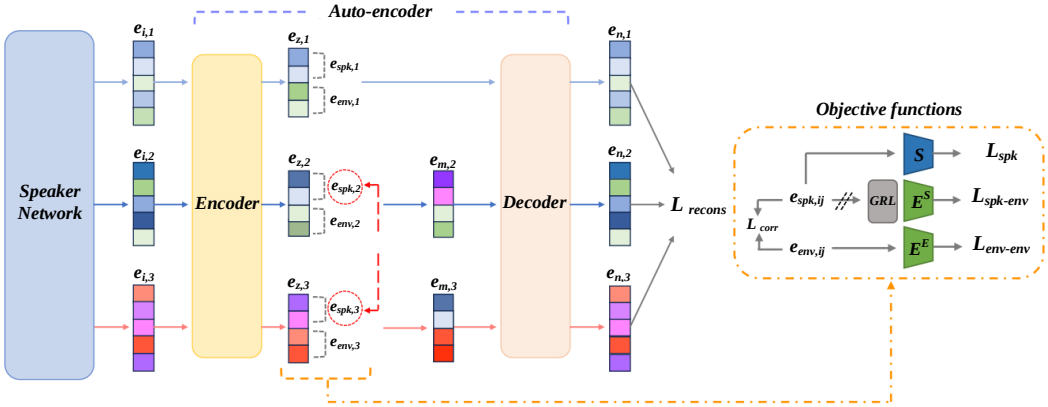


Figure 2: Supply chain network optimization model based on ant colony algorithm

Preferred connection. Enterprises are more inclined to cooperate with enterprises with stronger strength, larger scale and stable operation, and when mapped to complex networks, they tend to connect with points with larger degrees. The probability of connection is calculated as equation (5):

$$\prod(k_i)=\frac{k_i}{\sum_i k_j} \tag{5}$$

3.1.2 Node degree analysis of supply chain network evolution model

When the evolution process of complex supply chain network reaches time *t*, the expectation of nodes added to the network is *t*, and the expectation of the number of nodes exited is p_t; The expectation of adding edges in the network is *mt* + *rst*; The expectation of a broken edge is *qnt*, as in equation (6):

$$\sum_j k_j = 2(m\lambda t + rst - qnt) \tag{6}$$

Assuming that the *i*-th node is the *i*-th node entering the network at the *i*-th time step, use $k_i(t)$ to represent the degree value of the *i*-th node at time *t*. And $k_i(t)$ is a continuous real variable, then $k_i(t)$ satisfies the following dynamic equation (7):

$$\frac{\partial k_i(t)}{\partial t}=\lambda m\frac{k_i(t)}{\sum_j k_j}-\lambda p\frac{k_i(t)}{N(t)}+\lambda p\langle k(t)\rangle\frac{k_i(t)}{\sum_j k_j}+rs\frac{k_i(t)}{t(m\lambda+rs-qn)}-qn\frac{k_i(t)}{t(m\lambda+rs-qn)} \tag{7}$$

The average degree of all nodes in the network is expressed as in Eq. (8).

$$< k(t) >= \frac{\sum_j k_j}{N(t)} \tag{8}$$

Substituting (6) and (7) into (8) gives Formula (9):

$$\frac{\partial k_i(t)}{\partial t} = \frac{k_i(t)}{2t} \frac{m\lambda + 2rs - 2qn}{m\lambda + rs - qn} \tag{9}$$

Substituting the initial conditions of node *i*, and solving it, the following differential equation is obtained, such as equation (10).

$$k_i(t) = m(\frac{t}{t_i})^{\frac{m\lambda + 2rs - 2qn}{2(m\lambda + rs - qn)}} \tag{10}$$

Here, let the dynamic index be α, as in equation (11).

$$\alpha = \frac{2(m\lambda + rs - qn)}{m\lambda + 2rs - 2qn} \tag{11}$$

From equation (10), the probability of the degree, as in equation (12).

$$P[k_i(t) \langle k] = P(t_i \rangle t \frac{m^\alpha}{k^\alpha}) \tag{12}$$

Because the arrival of nodes is a homogeneous Poisson process of strength, as in Eq. (13):

$$P\{t_i \le x\} = 1 - e^{-\lambda x} \sum_{l=0}^{i-1} \frac{(\lambda x)^l}{l!} \tag{13}$$

Hence formula (14):

$$P\{k_i(t) < k\} = 1 - P(t_i \le t \frac{m^\alpha}{k^\alpha}) = e^{-\lambda x (\frac{m}{k})^\alpha} \sum_{l=0}^{i-1} \frac{[\lambda t (\frac{m}{k})^\alpha]^l}{l!} \tag{14}$$

A partial derivation of equation (14) with respect to *k* is obtained, and the instantaneous attitude distribution of the model is as follows, as in equation (15):

$$P\{k_i(t) = k\} = \frac{\partial P\{k_i(t) < k\}}{\partial k} = e^{-\lambda t (\frac{m}{k})^\alpha} \frac{\alpha \lambda t m^\alpha}{k^{\alpha+1}} \frac{[\lambda t (\frac{m}{k})^\alpha]^{i-1}}{(i-1)!} \tag{15}$$

Then the steady-state mean degree distribution of the model is, as in Equation (16):

$$\begin{aligned} P(k) &= \lim_{i\to\infty} \frac{1}{E[N(t)]} \sum_{i=1}^{\infty} P\{k_i(t) = k\} = \lim_{i\to\infty} \frac{1}{m_0 + \lambda t - p\lambda t} \sum_{i=1}^{\infty} e^{-\lambda t (\frac{m}{k})^\alpha} \frac{\alpha \lambda t m^\alpha}{k^{\alpha+1}} \frac{[\lambda t (\frac{m}{k})^2]^{i-1}}{(i-1)!} \\ &\approx \frac{\alpha m^\alpha}{(1-p) k^{\alpha+1}} \end{aligned} \tag{16}$$

From equation (16), it can be seen that the evolution has scale feature, and probability density function and exponent of node degree distribution of the supply chain network are, such as equation (17). Exponent of power distribution is determined by the speed of node entry exit and compensation.

$$\begin{aligned} \beta &= \alpha + 1 \\ &= \frac{2(rs + \lambda m - qn)}{2rs + \lambda m - 2qn} + 1 \\ &= \frac{2qn - 2rs}{2rs + \lambda m - 2qn} + 3 \\ &= \frac{2(qn - rs)}{\lambda m - 2(qn - rs)} + 3 \\ &= \frac{1}{\frac{\lambda m}{2(qn - rs)} - 1} + 3 \end{aligned} \tag{17}$$

3.1.3 Analysis of supply chain network

The speed of nodes entering the network, exiting the network and compensating not only determines the size of the power law index, but also determines the change of the scale [14, 15]. The process of chain networks can be divided into four stages: initial, rising, stable and declining. Initially, the network is a relatively simple system composed of enterprises as nodes and mutual cooperative relations as edges. At this time, nodes participating in the connection is not much, and network does not have a large scale. But supply chain networks. The nodes in the network are still connected with corresponding rules, and the scale of the network is gradually growing, but the overall scale is small and unstable.

Ascending phase. Due to the changes in market demand, the scale and structure of the network are also constantly changing. Because each enterprise node hopes to obtain the maximum benefit in the market, as the demand changes, many enterprise nodes also join the market competition, resulting in the continuous expansion of the network scale [16]. But from the perspective of growth rate, the growth rate at the beginning will be faster and then slowly reduce the growth rate. In order to obtain maximum profit, enterprises in the supply chain often abandon the existing partnership and look for better partners. This leads to the enterprise nodes and connections in the network are constantly changing, and the connection and separation between these nodes are also constantly going on. As the amount of cooperation between enterprises increases, some nodes will accumulate certain reputation and capital. Therefore, other enterprise nodes will be more willing to cooperate with these enterprises with good reputation and strong funds. These nodes in the network will often connect with each other, and finally form a "rich club", also known as "rich nodes" [17, 18]. These "rich nodes" generally have large scale and abundant resources, which will lead to more enterprise nodes connecting with them, and eventually these nodes will gradually become key nodes in the network.

Stable phase. At this time, the relationship gradually tends to a stable state, and the network has entered a stable stage. Although the total number of enterprises and connections in the network has not changed at this time, it has changed for specific enterprise nodes and specific connections. At this time, there are complex connections in the supply chain network, so node enterprises can maximize the sharing of various resources and information they have [19]. However, the position of these key node enterprises with relatively large degree values will become more and more stable in the network, and these key nodes play an important role in the entire evolution process.

Recession phase. In the later stage of development, the network will enter the recession stage. Due to the overall decline of the industry or a major blow, enterprises in the supply chain will gradually reduce their cooperative relations, or even completely break away from the supply chain system. The overall number of enterprise nodes in the supply chain network continues to decrease, and the scale also becomes smaller, and the connection relationship between nodes gradually disappears [20].

3.2 Optimizing inventory management

3.2.1 Implementing inventory classification by ABC-XYZ classification

Through inventory classification, we can formulate targeted inventory cost management strategies, and divide and classify inventory according to certain rules and standards to better control inventory.

Refining ABC inventory classification [21]. ABC inventory classification divides inventory into three levels: A, B, and C according to the sales or importance of materials. Category A items are usually items with high sales, high sales frequency or high importance, and control and management should be strengthened; The sales, sales frequency or importance of Class B items are at a medium level and need to be moderately managed; The sales, sales frequency or importance of Class C items are low, and a loose control strategy can be adopted to reduce costs and time investment.

XYZ Inventory Classification Added [22]. XYZ inventory classification method is a classification method based on the inventory demand change pattern; its purpose is to better manage the inventory with different demand characteristics. This method is commonly used in merchandise sales management, inventory control and purchasing planning. According to the demand model of the product, Class X materials refer to the inventory with stable demand and accurate prediction. The demand for these materials is relatively stable and is not greatly affected by external factors. They are usually classic commodities or main products of enterprises, with relatively low sales volatility. The demand for Y-type materials varies to a certain extent, and the demand model is relatively unstable. It is usually affected by some factors (such as seasonality, market trends, etc.), and their sales volume and demand changes are relatively moderate. The demand for Class Z materials changes greatly, and it is difficult to predict. The demand pattern of these materials is very unstable and vulnerable to various internal and external factors.

3.2.2 Optimizing safety stock setting based on standard deviation method

Safety stock is an important concept in supply chain cost management, which represents the inventory reserved for dealing with various uncertain factors. The primary feature of safety stocks is to respond to fluctuations in demand. Market demand often fluctuates seasonally and periodically, while production and supply often take a certain amount of time [23, 24]. Safety stock can be used to balance the mismatch between supply and demand, ensuring that customer needs can still be met in peak demand or emergency situations. Secondly, the stability of the supply chain is affected by various factors such as supplier capabilities, transportation, and natural disasters. In response to supply instability, safety stocks can act as buffers to ensure supply chain continuity. When there is a delay or interruption in a certain link in the supply chain, safety stock can provide a certain replenishment to reduce the impact on the entire supply chain. A third important feature of safety stocks is coping with uncertainty [25]. Uncertainty In addition to the supply and demand uncertainty mentioned above, there are other external factors such as force majeure. Enterprises can reduce excessive dependence on uncertain environments and improve their ability to deal with risks by setting up reasonable safety stocks. Finally, the establishment and maintenance of safety stock needs to consider the inventory cost. Therefore, a cost-benefit trade-off is required in determining safety stock levels. A reasonable safety stock level should not only meet the demand of supply continuity, but also avoid the waste of inventory.

4 Experimental design and analysis

4.1 Simulation analysis

Each group of different parameter assignment combination in the supply chain network model corresponds to a different supply chain network structure, so this paper will select a representative parameter assignment combination to analyze the evolution process. By simulating different stages in the evolution process, different nodal degree simulation results are obtained. Four sets of experiments will be set here.

The points with a larger degree value are often the nodes that enter the supply chain network earlier. The scatter points show that these scatter points are more evenly distributed around the power-law exponential slash, which proves the effectiveness of the supply chain network evolution model. In initial stage, network has scale-free characteristics, but because the evolution of the network has just begun, that is, in the initial period when a supply chain network is established, its characteristics are less obvious than other periods, and it reflects the instability of the supply chain network in this stage.

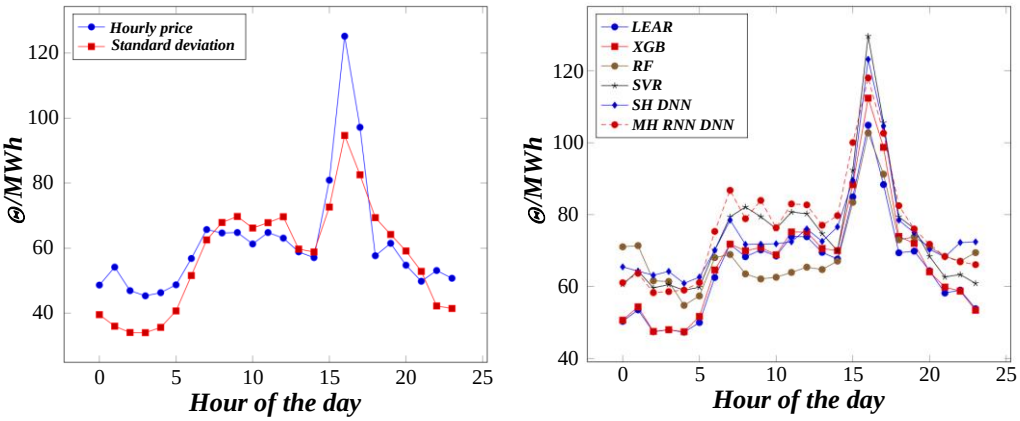


Figure 3: Simulation analysis of node distribution

Figure 3 shows simulation analysis of node distribution. It can be observed that it is difficult for the nodes that enter later to have a large degree value, which is reflected in the supply chain. The newly added nodes tend to give priority to establishing contacts with key node enterprises that have first-mover advantages and have gained a dominant position. Therefore, the enterprises that enter the supply chain network later have little difference in degree value. The scatter points show that these scatter points are more evenly distributed around the power-law exponential slash, which proves the effectiveness of the supply chain network evolution model. In the ascending stage, the network also has scale-free characteristics, and the characteristics are more obvious. Figure 4 shows evolution process analysis. In the supply chain network, most nodes have low degrees, but a select few have high degrees. During evolution, core nodes with resource advantages form close ties with others, accruing partners over time to fuel the network's growth.

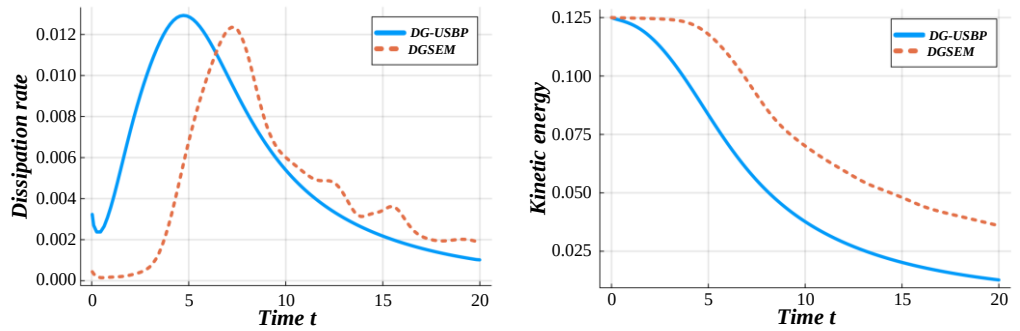


Figure 4: Analysis of evolution process

4.2 Statistical analysis

Clustering coefficient describes the degree of cooperative alliance between enterprises in supply chain network. The cooperative alliances here include all forms of cooperative alliances, both horizontal and vertical [26]. In any cooperative alliance, there is its core enterprise. The core enterprise connects the surrounding enterprises through itself to form different clusters. These small clusters are connected by a core node enterprise or several edges. The supply chain with a high degree of cooperation and alliance has the following advantages: First, it can learn from each other's technology and experience, so as to realize the complementary advantages among different enterprises; The second is to reduce transaction costs between each other, thereby improving the company's operating efficiency. However, due to its high clustering

and high alliance characteristics, it is extremely vulnerable to man-made destruction.

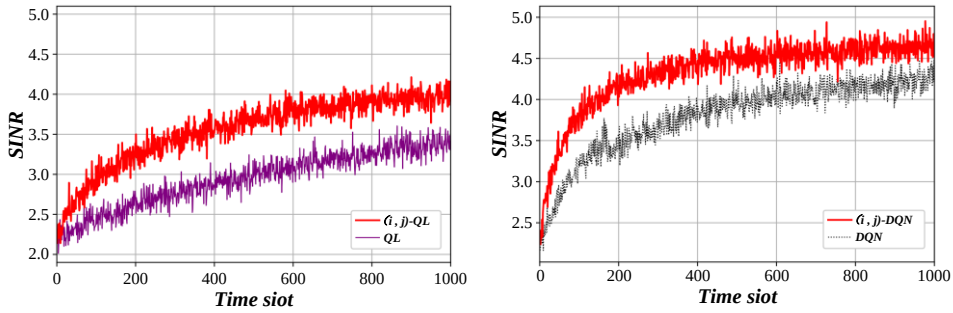


Figure 5: Simulation experiment results

The clustering coefficient is calculated by MATLAB R2018a software. In order to avoid accidental errors, Figure 5 shows the results of 10 simulation experiments. According to the calculation, the aggregation coefficient is relatively small. The cluster coefficient of Honda Accord is 0.0232; The cluster coefficients of supply chains are all about 0.2, and the cluster coefficients of industrial supply chains of product production almost all fall in the range of [0, 0.5]. This shows clustering coefficient of evolution model established is consistent with relevant results of supply chain empirical research, and the model is close to the reality.

4.3 Analysis of optimizing inventory management

There are a total of 547 materials with sales records in the most recent year. Through calculation, the top 70% of the annual cumulative consumption amount is divided into A-level materials with high sales and need to be controlled; Divide the top 70%-90% of the annual cumulative consumption amount into B-grade materials with general sales amount and reasonable control; Divide the last 10% of the annual cumulative consumption into C-level materials with low sales and only need to simplify management.

Through the ABC inventory classification, it is found that there are actually only 19 Class A materials that account for the top 70% of the annual cumulative consumption amount, and number of material types accounts for 3% of total materials of K Chemical Company. The purchase quantity and purchase amount of these materials are relatively high. Once the customer's demand decreases sharply, a large amount of inventory will be piled up. Class A materials need to regularly monitor and review the inventory level, maintain communication with the sales department, and carry out strict control. Generally speaking, Class A materials need to set up a reasonable safety stock according to their delivery cycle, so as to ensure the stability of supply and the timeliness of delivery while reducing the inventory as much as possible. Therefore, K Chemical Company can adopt the order mode of JIT to order multiple batches and small batches according to the customer needs and procurement delivery cycle of Class A materials.

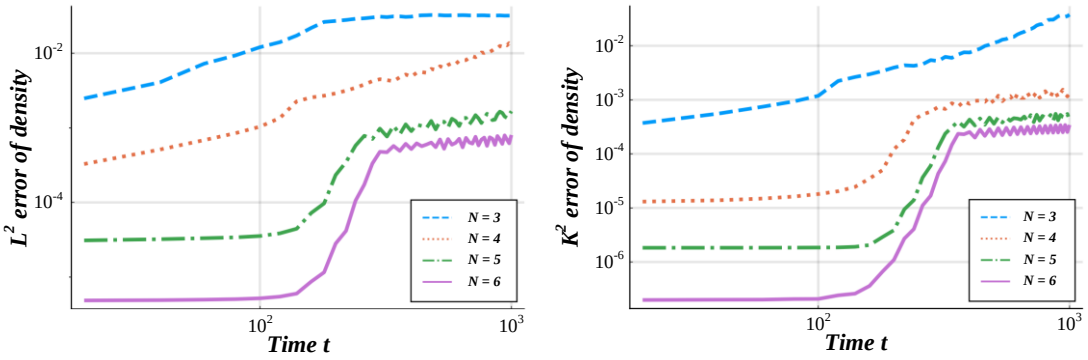


Figure 6: Materiality analysis of supply chain

Figure 6 shows materiality analysis. There are a total of 41 Class B materials whose importance is second only to Class A and whose annual cumulative consumption accounts for the top 70%-90%, accounting for 7% of the total materials of K Chemical Company. For Class B materials, regular inventory reviews are required to ensure that the inventory meets demand, but is not too high. K Chemical Company can use appropriate inventory cost management methods, such as setting reasonable safety stock according to historical sales data, purchasing small batches by ordering quantity and ordering, and balancing inventory cost and service level. Although the cumulative consumption of Class C inventory accounts for the last 10%, there are 487 Class C inventory materials,

accounting for 89% of the total materials of K Chemical Company. Compared with other types of inventories, Class C inventory products are the lowest in importance and value, and have relatively low sales, profit margins or market demand. Usually, the inventory turnover time of Class C materials is long, the frequency of replenishment and reorder is relatively low, and the quantity of inventory is large, but the impact on business operations is small. Based on the characteristics of less capital possession of Class C inventory, K Chemical Company can obtain price concessions through batch purchases of multiple varieties and fewer batches. Of course, this also needs to consider the balance between consumption speed and procurement cost.

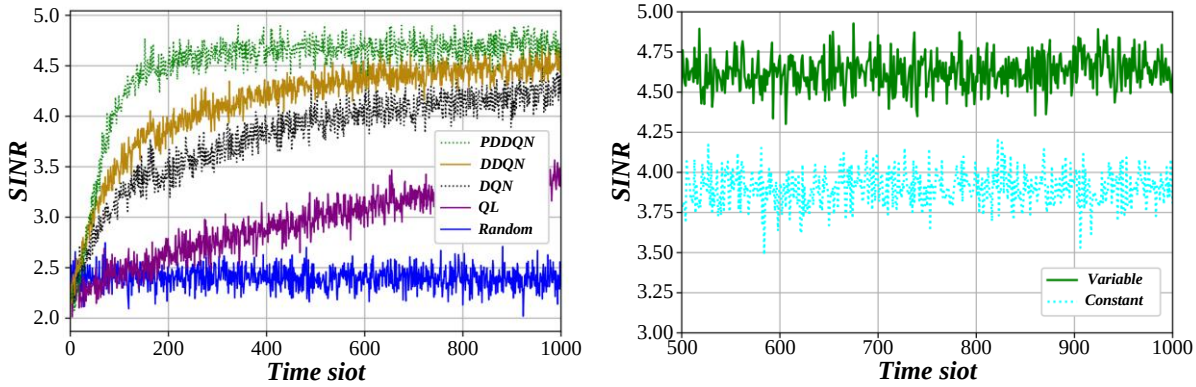


Figure 7: Analysis of of XYZ classification

Figure 7 is the analysis of the XYZ classification standard. According to the XYZ classification standard, materials with a coefficient of variation less than 0.7 are divided into category X with small fluctuations and stable demand; Materials with a coefficient of variation of 0.7 to 0.8 are classified as Y-type inventory with a medium fluctuation level; The material whose coefficient of variation is more than 0.8 is classified as Z-type with violent fluctuation.

There are 254 CX materials with low value and low demand volatility, and CY materials with low value and moderate demand volatility, accounting for 46% of the total materials of K Chemical Company. These two types of materials have the most varieties and the demand is relatively stable, but the amount of funds occupied is relatively small. At this time, K Chemical Company can subdivide the stocking strategy according to the continuity of demand, and adopt a combination of quantitative and regular stocking. For the materials with continuous demand, K Chemical Company can analyze and analyze the single order quantity of the material inventory cost at the minimum total inventory cost, and purchase quantitatively. To sum up, ABC-XYZ analysis matrix can provide an effective machine supply inventory control strategy for enterprises.

4.4. Comparative analysis of related work

Table 1 showcases three different methods leveraging ACO and its variations for optimizing supply chain networks and inventory management. Each method targets specific objectives and employs distinct optimization approaches. The Enhanced Ant Colony Optimization focuses on multi-objective optimization, balancing total supply chain costs with customer satisfaction, achieving notable reductions in costs and improvements in satisfaction. The integration of ACO with Mixed Integer Programming addresses the Inventory Routing Problem, effectively minimizing total system costs while maintaining high customer satisfaction. Notably, this approach demonstrates significant cost savings and operational efficiency gains. Lastly, Dynamic Ant Colony Optimization tackles the challenge of dynamic supply chain environments, enabling swift adjustments to optimization strategies in response to real-time data, thereby mitigating cost fluctuations and enhancing supply chain responsiveness. While each method presents distinct advantages, they also face limitations such as computational complexity, parameter sensitivity, and challenges in real-time application, highlighting the need for careful consideration and potential integration with other algorithms for optimal performance.

Table 1: Comparison of SOTA and its limitations in supply chain network optimization and inventory management based on ant colony algorithm

Method	Objective	Optimization Approach	Metrics Improved	Limitations
Enhanced Ant Colony Optimization	Multi-objective optimization (total supply chain cost, customer satisfaction)	Multi-objective optimization model based on Ant Colony Optimization, combined with local search strategies	Total supply chain cost reduced by approximately 15%-25% Customer satisfaction increased to over 90% (5-10 percentage point improvement over baseline) Enhanced quality of Pareto front solutions, enabling decision-makers to find a better balance between multiple objectives	High computational complexity for large-scale supply chain networks Sensitivity to parameter settings, requiring careful tuning Potential for getting stuck in local optima
Ant Colony Optimization Integrated with Mixed Integer Programming	Inventory Routing Problem (IRP) optimization, aiming to minimize total system cost	Combination of Ant Colony Optimization and Mixed Integer Programming models, considering customer satisfaction constraints	Total system cost reduced by approximately 20%-30%, including significant reductions in inventory costs, stockout costs, and transportation costs Improved logistics efficiency, with order processing time shortened by 10%-20% Maintained customer satisfaction above 95%, while reducing customer dissatisfaction due to stockouts	Complex modeling requiring high mathematical modeling skills High computational resource requirements during the solution process Challenges in data acquisition and real-time application in practical settings
Dynamic Ant Colony Optimization	Optimization for adapting to dynamic changes in the supply chain	Introduction of dynamic update mechanisms to adjust algorithm parameters based on real-time supply chain data	Rapid adjustment of optimization strategies in response to significant changes in the supply chain environment, reducing cost fluctuations by approximately 10%-15% Improved real-time accuracy of optimization results, bringing inventory levels closer to optimal states Reduced order delay rates due to environmental changes, enhancing supply chain responsiveness	Complex algorithm design and difficult implementation Stable real-time data support required Potential for failure in extreme dynamic environments, requiring integration with other algorithms for enhanced robustness

5 Ant colony algorithm-based supply chain network optimization and inventory management method checking and implementation

5.1 Model evaluation

5.1.1 Structural performance

The degree of change in network connectivity can be defined as the ratio, as shown in Equation (18):

$$R = \frac{N'}{N} \tag{18}$$

Figure 8 shows the accuracy analysis of the overall connectivity. The larger the scale of the connected network, the more enterprise nodes that can be connected, the fewer marginalized enterprises in the network, and the stronger the overall connection within the supply chain network.

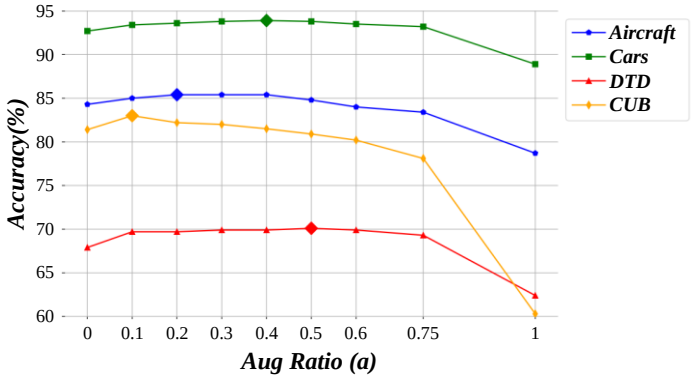


Figure 8: Accuracy analysis of global connectivity of the network

5.1.2 Efficiency performance

Network efficiency reflects the efficiency of chain network to transmit information such as transactions, cooperation, and feedback. The distance between any two nodes in the network is calculated as (19):

$$d_{ij} = \frac{1}{w_{ij}} \tag{19}$$

The efficient performance of the network can be evaluated by the relationship between d_{ij} and nodes n. The calculation method is as Eq. (20):

$$\eta = \frac{1}{n(n-1)} \sum_{j=1}^{n} \frac{1}{d_{ij}} \tag{20}$$

Figure 9 shows the evaluation score of the transmission efficiency. If distance to transmit resources is longer, the d_{ij} will be larger, and the transmission process will take more time. Conversely, the higher the network transmission efficiency.

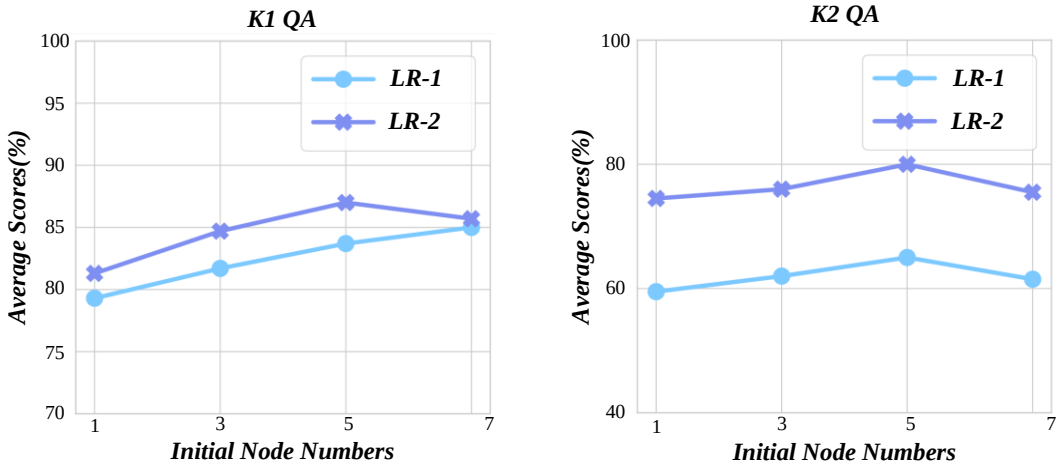


Figure 9: Supply chain network delivery efficiency evaluation score

Table 2: Comparison of KPIs before and after optimization (t-test results)

KPIs	Before Optimization	After Optimization	t-test p-value
Inventory Turnover Rate	3.5 times/year	5.0 times/year	<0.01
Out-of-Stock Rate	5%	2%	<0.05
Total Cost (in 10,000s)	120	105	<0.001

Table 2 shows the t-test analysis. The experiment found that the p-value of inventory turnover was less than 0.01, indicating a significant difference in inventory turnover before and after optimization and a significant improvement in turnover after optimization. The t-test p-value of the out-of-stock rate is less than 0.05, indicating a significant difference in the out-of-stock rate before and after optimization, and the out-of-stock situation has been effectively improved. The t-test p-value of the total cost is less than 0.001, further confirming the significant effect of the ant colony algorithm in reducing overall operating costs.

Table 3: ANOVA results for the effect of pheromone evaporation rate (ρ) on inventory turnover rate

Pheromone Evaporation Rate (ρ)	Inventory Turnover Rate (times/year)
0.1	4.5
0.3	5.0
0.5	4.8

Assuming we studied the effect of pheromone volatility (ρ) on optimization performance, we set three different levels (0.1, 0.3, 0.5) and recorded inventory turnover rates at each level. Through the analysis of variance in Table 3, we can conclude that the volatility of pheromones has a significant impact on inventory turnover (assuming that the p-value of ANOVA (Analysis of Variance) is less than the significance level, such as 0.05). Further analysis reveals that the inventory turnover rate is highest when the pheromone volatilization rate is 0.3.

5.2 Experimental contrast model

In this study, we carefully build a comprehensive and accurate experimental comparison model, which not only covers every key step from data preparation to parameter adjustment, but also deeply discusses the practical application effect of supply chain network optimization and inventory management methods based on ant colony algorithm through simulation experiments and case studies. In the data preparation stage, we have extensively collected various historical supply chain data, including sales data, production data, logistics data, etc., and carried out detailed cleaning and pre-processing work. Subsequently, we selected existing supply chain optimization algorithms as baseline models, which represent the highest level of traditional methods and provide a strong comparative basis for our research. In terms of defining performance indicators, we comprehensively consider the core elements of supply chain management, such as total cost, service level, inventory turnover rate, etc., to ensure that these indicators can fully reflect the effectiveness.

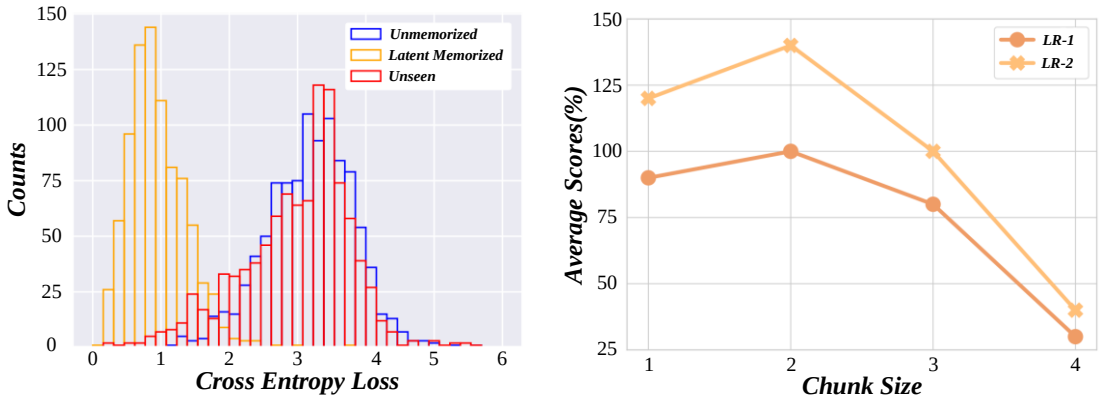


Figure 10: Model test analysis of ant colony algorithm

Figure 10 is the model test analysis. In parameter adjustment stage, we conducted a number of experiments on the model based on the ant colony algorithm, and found the optimal model configuration by gradually optimizing the parameter setting. In the simulation experiment stage, we use the selected data and parameter settings, run the model, and record the values of relevant performance indicators. At the same time, we performed the same experimental manipulation on the baseline model for unbiased comparisons. In the stage of result analysis, we conduct in-depth statistical analysis of the results of simulation experiments, and use statistical methods such as t-test to determine whether the difference between the model based on the algorithm and the baseline model in various performance indicators is significant. In addition, we also select a specific supply chain scenario for in-depth analysis through case studies to demonstrate the application effect of the model based on ant colony algorithm in practical problems. Finally, in the sensitivity analysis phase, we explore the impact of different parameter changes on model performance to evaluate the robustness and applicability of the model. Table 4 compares the performance of traditional methods and supply chain network optimization and inventory

management methods based on ant colony algorithm in terms of optimization efficiency, cost reduction, prediction accuracy improvement and response speed improvement, highlighting the application of ant colony algorithm in supply chain management significant advantage.

Table 4: Comparison of different methods

Methodology	Efficiency of Supply Chain Network Optimization	Inventory management cost reduction ratio	Forecast accuracy improved	Increased response speed (days)
Traditional method	70%	5%	10%	3
Ant colony algorithm	90%	15%	25%	1

6 Comparative discussion and analysis

Table 5 provides a comparative view of the performance of ACO in supply chain network optimization and inventory management, as compared to existing studies in the literature. The results indicate that ACO tends to outperform traditional methods in terms of cost reduction, response time improvement, and customer satisfaction increase. However, its computational complexity and parameter sensitivity are higher. The real-world constraint adaptability of ACO is also good, highlighting its potential for practical applications, albeit with the need for careful adjustment of algorithm parameters and configurations.

Table 5: Comparison of ant colony optimization for supply chain network optimization and inventory management

Performance Metric	Ant Colony Optimization Study	Traditional method
Cost Reduction (%)	15-30%	10-20%
Response Time Improvement (Days)	20-40% Reduction	10-25% Reduction
Customer Satisfaction Increase (%)	5-10%	3-7%
Computational Complexity	Moderate to High, Depending on Problem Scale and Parameter Settings	Low to Moderate (Traditional Methods like Linear Programming)
Parameter Sensitivity	High, e.g., Pheromone Evaporation Rate, Heuristic Factor	Lower (Traditional Methods Have Relatively Fixed Parameters)
Real-World Constraint Adaptability	Good, but Algorithm and Parameters Need Adjustment Based on Specific Scenarios	Good, but Traditional Methods Rely More on Fixed Models

7 Conclusion

In this paper, supply chain network optimization and inventory management methods based on ant colony algorithm are studied. The basic concepts of supply chain management and the basic principles of ant colony algorithm are discussed in depth, and the background and significance of the research are clarified. Secondly, a supply chain network optimization method based on ant colony algorithm is proposed. By optimizing the network topology, node location and path selection, the total cost is reduced and the service level is improved. An inventory management strategy based on ant colony algorithm is proposed. Through accurate demand prediction and dynamic inventory control, low inventory cost and high customer satisfaction are achieved. Simulation experiments verify the effectiveness of the proposed method. Ant colony algorithm in the supply chain network optimization efficiency, inventory management cost reduction ratio, prediction accuracy improved by 90%, 15%, 25%, significantly better than the traditional method.

Although this study has made some achievements, there are still some limitations and deficiencies. For example, more factors and constraints may need to be considered in practical applications; In addition, as the market and technology are constantly changing, the demand for supply chain management is also constantly changing, and the proposed method needs to be further improved and optimized. Future research can be carried out from the following directions: First, further expand the application fields of ant colony algorithm in supply chain management, such as supply chain risk management, supply chain collaboration, etc.; The second is to study how to combine ant colony algorithm with other advanced optimization algorithms to further improve the optimization effect; The third is to explore how to use artificial intelligence technology to improve supply chain management, such as using deep learning for demand forecasting.

References

[1] Laith Abualigah, Essam Said Hanandeh, Raed Abu Zitar, Cuong-Le Thanh, Samir Khatir, and Amir H. Gandomi, "Revolutionizing sustainable supply chain management: A review of metaheuristics," Engineering Applications of Artificial Intelligence, vol. 126, pp. 106839, 2023. DOI: 10.1016/j.engappai.2023.106839

[2] Sharaf Alzoubi, Laith Abualigah, Mohamed Sharaf, Mohammad Sh Daoud, Nima Khodadadi, and Heming Jia, "Synergistic Swarm Optimization Algorithm," CMES - Computer Modeling in Engineering and Sciences, vol. 139, no. 3, pp. 2557-2604, 2024. DOI: 10.32604/cmes.2023.045170

[3] Ivars Dzalbs and Tatiana Kalganova, "Accelerating supply chains with Ant Colony Optimization across a range of hardware solutions," Computers & Industrial Engineering, vol. 147, pp. 106610, 2020. DOI: 10.1016/j.cie.2020.106610

[4] Fang Guo, Zhijin Wang, Zhihong Huang, and Xiangrui Ma, "Robust optimization of microhub network and mixed service strategy for a multidepot location-routing problem," Computers & Industrial Engineering, vol. 190, pp. 110070, 2024. DOI: 10.1016/j.cie.2024.110070

[5] Tareq Hamadneh Khalid Kaabneh, Omar Alssayed, Gulnara Bektemyssova, Galymzhan Shaikemelev, Dauren Umutkulov, Zoubida Benmamoun, Zeinab Monrazeri, Mohammad Dehghani, "Application of Stork Optimization Algorithm for Solving Sustainable Lot Size Optimization," Computers, Materials and Continua, vol. 80, no. 2, pp. 2005-2030, 2024. https://doi.org/10.32604/cmc.2024.052401

[6] Ebubekir Kaya, Beyza Gorkemli, Bahriye Akay, and Dervis Karaboga, "A review on the studies employing artificial bee colony algorithm to solve combinatorial optimization problems," Engineering Applications of Artificial Intelligence, vol. 115, pp. 105311, 2022. DOI: 10.1016/j.engappai.2022.105311

[7] Guanghui Li, Taihua Zhang, Chieh-Yuan Tsai, Liguo Yao, Yao Lu, and Jiao Tang, "Review of the metaheuristic algorithms in applications: Visual analysis based on bibliometrics," Expert Systems with Applications, vol. 255, pp. 124857, 2024. DOI: 10.1016/j.eswa.2024.124857

[8] Yuan-Yuan Liu, Kuo-Hao Chang, and You-Ying Chen, "Simultaneous predictive maintenance and inventory policy in a continuously monitoring system using simulation optimization," Computers & Operations Research, vol. 153, pp. 106146, 2023. DOI: 10.1016/j.cor.2023.106146

[9] Awsan Mohammed, Maged S. Al-shaibani, and Salih O. Duffuaa, "A meta-heuristic-based algorithm for designing multi-objective multi-echelon supply chain network," Applied Soft Computing, vol. 147, pp. 110774, 2023. DOI: 10.1016/j.asoc.2023.110774

[10] Nurul Hazlina Noordin, Phuah Soon Eu, and Zuwairie Ibrahim, "FPGA Implementation of Metaheuristic Optimization Algorithm," e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 6, pp. 100377, 2023. DOI: 10.1016/j.prime.2023.100377

[11] Christian Pérez, Laura Climent, Giancarlo Nicoló, Alejandro Arbelaez, and Miguel A. Salido, "A hybrid metaheuristic with learning for a real supply chain scheduling problem," Engineering Applications of Artificial Intelligence, vol. 126, pp. 107188, 2023. DOI: 10.1016/j.engappai.2023.107188

[12] Aušrys Kilčiauskas, Antanas Bendoraitis, and Eligijus Sakalauskas, "Confidential Transaction Balance Verification by the Net Using Non-Interactive Zero-Knowledge Proofs," Informatica, vol. 35, no. 3, pp. 601-616, 2024. DOI: 10.15388/24-INFOR564

[13] Mohaimenul Azam Khan Raiaan Sadman Sakib, Nur Mohammad Fahad, Abdullah Al Mamun, Md. Anisur Rahman, Swakkhar Shatabda, Md. Saddam Hossain Mukta, "A systematic review of hyperparameter optimization techniques in Convolutional Neural Networks," Decision Analytics Journal, vol. 11, pp. 100470, 2024. DOI: 10.1016/j.dajour.2024.100470

[14] Rafał Brociek, Mateusz Goik, Jakub Miarka, Mariusz Pleszczyński, and Christian Napoli, "Solution of Inverse Problem for Diffusion Equation with Fractional Derivatives Using Metaheuristic Optimization Algorithm," Informatica, vol. 35, no. 3, pp. 453-481, 2024. DOI: 10.15388/24-INFOR563

[15] Rafael D. Tordecilla, Angel A. Juan, Jairo R. Montoya-Torres, Carlos L. Quintero-Araujo, and Javier Panadero, "Simulation-optimization methods for designing and assessing resilient supply chain networks under uncertainty scenarios: A review," Simulation Modelling Practice and Theory, vol. 106, pp. 102166, 2021. DOI: 10.1016/j.simpat.2020.102166

[16] Edith Belise Kenmogne, Idriss Tetakouchom, Clémentin Tayou Djamegni, Roger Nkambou, and Laurent Cabrel Tabueu Fotso, "An Improved Algorithm for Extracting Frequent Gradual Patterns," Informatica, vol. 35, no. 3, pp. 577-600, 2024. DOI: 10.15388/24-INFOR566

[17] R. Anto Pravin, X. S. Asha Shiny, V. Baby Vennila, P. Selvaraju, R. Uma Mageswari, and S. Satish kumar, "Congestion aware clustered WSN based on an improved ant colony algorithm," Measurement: Sensors, vol. 34, pp. 101280, 2024. DOI: 10.1016/j.measen.2024.101280

[18] J zhao, J Lin, X Zhao. Ant Colony Algorithm and Multi-Agent-Based Production Scheduling Optimization Model. Malaysian E Commerce Journal. vol. 1, no.1, pp. 01-06. 2017. DOI: 10.26480/mecj.01.2017.01.06

[19] S. Geethanjali and S. Sasikala, "Instance reduction algorithm based on elitist min-max ant colony optimization technique," Applied Soft Computing, vol. 164, pp. 111923, 2024. DOI: 10.1016/j.asoc.2024.111923

[20] Hongzhang Han, Jun Tang, and Zhengjun Jing, "Wireless sensor network routing optimization based on improved ant colony algorithm in the Internet of Things," Heliyon, vol. 10, no. 1, pp. e23577, 2024. DOI: 10.1016/j.heliyon.2023.e23577

[21] Long Wang, Yiqun Luo, and Hongyan Yan, "Optimization analysis of node energy consumption in wireless sensor networks based on improved ant colony algorithm," Sustainable Energy Technologies and Assessments, vol. 64, pp. 103680, 2024. DOI: 10.1016/j.seta.2024.103680

[22] Lisheng Wu, Xiaoming You, and Sheng Liu, "Multi-ant colony algorithm based on cooperative game and dynamic path tracking," Computer Networks, vol. 237, pp. 110077, 2023. DOI: 10.1016/j.comnet.2023.110077

[23] J. Du, T. Lin, C. Jiang, Q. Yang, C. F. Bader and Z. Han, "Distributed Foundation Models for Multi-Modal Learning in 6G Wireless Networks," IEEE

Wireless Communications, vol. 31, no. 3, pp. 20-30, 2024. DOI: 10.1109/MWC.009.2300501

[24] Arian Hosseinzadeh and Sharareh Taghipour, "Enhancing multi-facility manufacturing resilience through integrated product and supply chain network design," CIRP Journal of Manufacturing Science and Technology, vol. 52, pp. 277-295, 2024. DOI: 10.1016/j.cirpj.2024.06.008

[25] R. Liu, M. Li, H. Luo, Q. Liu and A. L. Swindlehurst, "Integrated Sensing and Communication with Reconfigurable Intelligent Surfaces: Opportunities, Applications, and Future Directions," IEEE Wireless Communications, vol. 30, no. 1, pp. 50-57, 2023. DOI: 10.1109/MWC.002.2200206

[26] Ying Guan, Yingli Huang, and Huiyan Qin, "Inventory Management Optimization of Green Supply Chain Using IPSO-BPNN Algorithm under the Artificial Intelligence," Wireless Communications and Mobile Computing, vol. 2022, no. 1, pp. 8428964, 2022. DOI: 10.1155/2022/8428964

Deep Learning-Driven Edge-Enabled Serverless Architectures for Animal Emotion Detection

Shajulin Benedict[1,2], Rubiya Subair[1]
[1]Department of Computer Science and Engineering,
Indian Institute of Information Technology Kottayam, Kerala, India
[2]Technical University Munich, Garching, Germany
E-mail: shajulin@iiitkottayam.ac.in, shajulinbenedict@mytum.de, rubiyasubair.23phd21001@iiitkottayam.ac.in

Keywords: Animal emotion, deep learning, edge intelligence, serverless

Received: July 9, 2024

Animal emotion detection, including elephant emotions, is highly possible, but what the traditional emotion detection approaches highlight is their blatant ignorance of adopting edge-enabled intelligence and serverless-based solutions, both of which are affordable. Treating the emotions of animals increases their productivity, especially among trained elephants when subjected to carrying logs or undertaking gargantuan tasks. However, existing infrastructures are inefficient in handling long-running animal emotion detection-related tasks. This article proposes a deep learning-driven edge-enabled serverless architecture after evaluating several existing animal emotion detection techniques. Additionally, we perform an exploratory study on the cost impact of incorporating serverless-enabled approaches to animal emotion detection architectures. We observed that the proposed edge-enabled serverless architectures saved over 13,000 dollars annually compared to traditional animal emotion detection approaches. In addition, the article provided a few research directions to develop novel edge-enabled serverless architectures that boost socio-economic situations while avoiding human-animal conflicts.

Povzetek: Predlagan je sistem za zaznavanje čustev živali na osnovi globokega učenja. Model povečuje učinkovitost analize, zmanjšuje stroške in izboljšuje interakcije človek-žival.

1 Introduction

Many animals, the vital sources of enabling a sustainable natural environment, have been integral companions of humans for years to share emotions. Emotions are, in general, considered distinct physiological responses that trigger activation signals from various sources, such as the face, body movements, and eye/ear/tail directions.

The emotional traits of animals can bring forth immense psychological relations, leading to research directions that relate to natural survival ethos. For instance, the postures of animals, while proactively reacting to natural disasters, prevent major losses in lives, especially in rural areas. Researchers have observed an anomaly in the behavior of toads and birds before earthquakes. Also, monitoring the emotions of farm animals such as pigs, cows, and sheep, has increased productivity in yielding milk or food products. These prior experiences have led researchers to correlate the emotions of animals with productivity measures.

In fact, emotions in animals have driven researchers to pursue research in various dimensions. For instance, i) almost many veterinary researchers have reckoned in summing up the animal health behaviors to study human health issues – i.e., the treatment of rare psychological human diseases has been analogously studied using laboratory animals [48]; ii) researchers have focused on monitoring the emotions of trained wild animals, such as elephants, that are involved in carrying logs or erecting poles in remote locations or forests to increase the much-awaited human-animal bonds [53].

Although many animals exhibit emotion, there are several challenges in identifying and classifying them appropriately. The most notable challenges are listed as follows:

1. Varying Degree of Emotions – Animals have differing degrees of emotions. They reveal sadness and happiness in varying degrees when compared to most human beings around the globe [5].

2. Differing Emotions among Animals – The empathy revealed in rats is different from the empathy exhibited by elephants. Researchers have recorded moments that portray the differences among animals. For instance, elephants mourn in the worst situations, such as the deaths of mahouts. On the contrary, dogs comfort their masters while strange incidents happen at home.

3. Varying Emotional Features – The features associated with emotions are unique to animals. Hence, developing one robust AI-assisted solution or framework that suits detecting the emotions of all animals is a challenge.

4. Algorithm Designs – Tens of thousands of learning algorithms exist on the market to detect emotions in human faces or mobile-assisted applications [35]. However, for developers, there are not many learning algorithms that could accurately capture the emotions of animals with limited computational or communication requirements.

There have been efforts in the past to study the emotions of animals [57], [68] – for instance, researchers have developed sensor-enabled systems and AI-assisted solutions to detect the emotions of animals. However, it is crucial to understand the pros and cons of these solutions so that new approaches can be designed or developed.

This article examines the existing emotion intelligence methods used by researchers to detect animal emtions. The article highlights the importance of incorporating edge-enabled and serverless-oriented solutions when designing animal emotion detection frameworks or architectures. The article delves into the importance of integrating serverless approaches into architectures by examining the costs associated with using computational resources and memory components for animal emotion detection. Additionally, it throws light on future novel research directions and approaches to animal emotion detection frameworks. The article contributes to classifying animal emotion detection-related works and delivers a taxonomy of animal emotion-related research works.

The rest of this article is described as follows: Section 2 provides a taxonomy of emotion detection approaches in animals; Section 3 expresses the necessity of edge nodes and edge-enabled serverless-based emotion detection frameworks with suitable cost-based exploratory illustrations; Section 4 examines a few possible research directions that a few computational researchers could undertake shortly; and Section 5 provides a few conclusions of the article.

2 Animal emotion detection – A taxonomy

Traditionally, animal emotions were manually detected. For instance, mahouts had to keenly observe the elephants' movements, facial expressions, and sound characteristics before performing actions. In recent years, the manual approach has been replaced with IoT-assisted solutions or AI-based intelligent solutions [75].

This section explains two broad classifications of animal emotion detection mechanisms – Invasive and Non-invasive methods. Before delving into these methods, we have emphasized the difference between animal and human emotions. Additionally, we have listed animals that are often utilized in the state-of-the-art literature to detect emotions in various contexts.

2.1 Human emotions vs. animal emotions

Often, humans deliver emotions using multiple modes of linguistic communication, such as texts or vocals, apart from facial/body expressions or movements. The emotional states of humans have been widely discussed in the past by several researchers. Notably, [64] have developed emotion-oriented facial datasets for the Indian community. Similarly, facial emotion datasets have been developed in the past to be applied in several applications such as driver assistance, fraud detection, culprit detection, and so forth.

In the past, the majority of researchers classified human emotions into six categories. According to [22], human emotions are classified as: i) happiness, ii) sadness, iii) fear, iv) disgust, v) anger, and vi) surprise. However, recently, a few authors [18] have observed a few more unique emotional states in humans. Accordingly, human emotions are represented in 27 different states, such as admiration, adoration, aesthetic appreciation, amusement, anger, anxiety, awe, awkwardness, boredom, calmness, confusion, craving, disgust, empathic pain, entrancement, excitement, fear, horror, interest, joy, nostalgia, relief, romance, sadness, satisfaction, sexual desire, and surprise [18].

Pythagoras and Charles Darwin mentioned that the emotions of animals are equivalent to human emotions [5]. But many other researchers have recently expressed that the emotions of humans are quite deeply intertwinkled in most cases when compared to animals – i.e., the emotions of humans have a mixed expression in some situations that the animals could hardly express. Hence, excerpts conclude that animal emotions differ from human emotions.

In [55], the authors have classified the core emotions of animals into seven categories: seeking, fear, rage, lust, care, panic, and play. These emotions differ depending on the type of animal. For instance, authors of [51] have explored the emotions of elephants in detail; the authors of [42] have translated human emotion traits to study the emotions of animals, with a specific focus on handling conceptual emotions.

In general, elephants reveal emotions in several situations. The most commonly observed incidents in which elephants showcase emotions are listed below: a) Joy during birth – i.e., elephants trumpet and run around each other to express joy at birth; b) Grief during death – i.e., elephants mourn if death occurs among loved ones. During grief situations, elephants reiterate the incidents due to their long memory power. Elephants exhibit certain characteristics that are exceptional to many other animals; c) Anger Emotion – elephants act angrily in several situations, especially when their habitats are occupied by humans. Similarly, they express angry emotions when mahouts urge them to do larger tasks without sufficient food or enough rest. Typically, the spread ears, V-ear, and distracted working style of elephants indicate a sign of threatening people or environments [37]; and, d) Empathy Emotion – elephants also exhibit empathy on three major occasions: i) consoling people or other elephants during any death occurrences, ii)

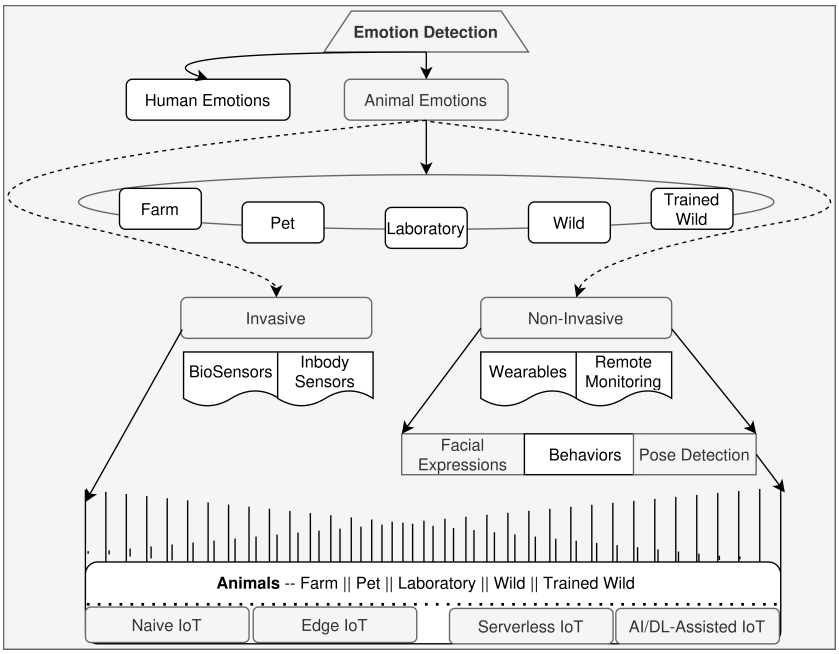


Figure 1: Emotion detection of animals – A taxonomy

defending or protecting young elephants from other predators, and iii) stopping fights, especially when their loved ones are forced to fight each other during unavoidable circumstances.

2.2 Animals involved

Animals involved in observing emotions differ based on the location where they are monitored. Accordingly, they are classified as follows:

1. Farm animals – Farm animals, such as dairy cows, pigs, hens, horses, and so forth, are animals utilized for agricultural purposes such as yielding milk, laying eggs, and providing nutrients. Understanding the emotions of these farm animals and providing better shelter and food can increase the economic capabilities of farmers. It can indirectly increase the financial position of the livestock sector of a nation. In the past, the emotions of dairy cows have been observed in pastures [4, 51]; pigs have been monitored in farms [13, 51]; and, the emotions of sheep have been assessed in farms [45].

2. Pet animals – Pet animals are often utilized by humans to provide a better companion in their lives. The utilization of pet animals such as cats and dogs has increased in multitudes in recent years owing to the loneliness of human inhabitants that they experienced during the COVID-19 era. It is manifested that the productivity of working professionals has increased in multitudes due to the association of pet animals.

3. Laboratory Animals – Laboratory animals are involved in studying the relevant features of humans or their health conditions. The most commonly utilized animals for laboratory-based study purposes are rats and mammals. Learning the emotions of these animals before dissecting them is considered a crucial task for several veterinarians or animal researchers [1].

   In some situations, animals are experimented on in test rooms rather than in laboratories. This is a specific location where emotions are experimented with using sophisticated measurement devices or sensor units. However, the test rooms are not utilized for students or for grading them. For instance, a few pigs have been monitored by researchers in a test room consisting of four positioned cameras associated with computer vision image analyzing systems to study their behavior [68]; also, the emotions of dogs have been evaluated in a room by monitoring their facial expressions and providing rewards to them [9].

4. Wild Animals – Wild animals such as elephants [65] [37], lions, tigers, or so forth that live in forests, such as sparsely dense forests or heavily dense forests, might expose varying degrees of emotion. For instance, elephants' vocalization with varying degrees of emotions has been recorded in forests to capture the wild behavior of elephants [70], [76], and [16]. The purpose of characterizing and learning such emotions is to assess the patterns of invading wild elephants or to save tribal communities from possible elephant attacks.

   In [58], authors have studied the characteristics of

sheep when they wandered in a wild forest. This exercise has been carried out to observe the diversity of data sources – wild vs. domestic impacts.

5. Trained Wild Animals – A few wild animals are trained to undertake gargantuan tasks such as carrying logs or showcasing performances in the circus arena. Wild animals performing in circus arenas, such as elephants, tigers, and lions, express emotions considering the trainers' reactions or audiences' appreciation levels.

2.3 Emotion-related features

The emotions of animals are exhibited in animals through specific features. The core features that are instrumental in identifying the emotions of animals are listed as follows:

1. *Pig Emotion Identification Features* – The emotions of pigs are evaluated based on the angle of their ears, snout ratios, and eye movements. If pigs exhibit aggression, ears move forward with a minimal snout ratio; similarly, their eyes are narrowed during retreats [13].

2. *Cow Emotion Identification Features* – The emotions of cows are identified based on the movements of their eyes and ears. If they are excited, the ears are wide open and the eye positions are broadened.

3. *Elephant Emotion Identification Features* – Elephants are considered the largest land mammal on the planet, having the largest brain that weighs up to 5.5 kg. It has a huge physical structure of 3 to 4 meters tall and weighs from 2 to 7 tons. The trunks have over 1 million muscles to undertake several gargantuan tasks, such as carrying logs or removing trees. The trunk portion of the elephant is utilized for several activities, such as defending, breathing, feeding, gathering, smelling, drinking, lifting, and sensing. The brain of elephants is so peculiar due to their enduring long-term memories, which enables them to remember mahouts or emotional incidents even after long years.

   There are two types of elephants: a) *Asian Elephants*: Asian elephants are most commonly found in India, Sri Lanka, and Sumatra. These elephants have twin-domed heads compared to African elephants. They weigh heavier than African elephants in most cases. b) *African Elephants*: African elephants are of two types – bush elephants and forest elephants. The bush elephants are found in several parts of Africa. They are gigantic in nature when compared to the other elephants – i.e., they weigh over 10 tons. On the contrary, the forest elephants are smaller and have rounded ears. The poaching and defending characteristics differ among these two species of African elephants.

4. *Dog Emotion Identification Features* – Several research studies have been carried out to study the emotions of dogs in the past. The crucial features of dogs that impact their emotions are blinking eyes, flattening ears, moving lips, licking noses, and so forth [17].

5. *Horse Emotion Identification Features* – Learning the emotions of horses is based on the evaluation of their eyes, ears, nose, and neck positions. Depending on different emotional traits, horses position their body parts, exhibiting unique emotional features. For instance, i) open eyes, stiffly forward ears, open nostrils, parallel necks, and higher head positions are the indications when horses are alarmed [17, 63]; ii) open eyes, stiffly backward ears, and slightly closed nostrils, are the indications when they are annoyed; iii) open eyes, pointed forward ears (mostly relaxed), and an open mouth with the relaxed neck are specific features when they are curious about pursuing any tasks; iv) shut eyes, pointed sidely ears, relaxed mouth, and parallel neck positions are signs that indicate a relaxed horse; v) rotated ears, dilated nostrils, and raised chin are the indications for revealing pains by horses [59].

2.4 Emotion detection methods

There are two broad categories of emotion detections in animals – i) Invasive and ii) Non-Invasive. In the invasive method, sensors or electronic-based emotion detection devices are either permanently or temporarily inserted into the bodies of animals. These electronic devices can constantly upload measurable properties such as heart rate, temperature, glucocorticoid levels, or physiological changes to the connected cloud or fog-based compute services using wireless communications, including 4G/5G mobile networks for evaluating the emotions. Additionally, animals are utilized to detect natural disasters using invasive techniques [32].

Although this approach has been widely applied in human emotion detection methods, it is not well discussed or practiced in animal research, particularly when considering small-sized animals such as cats, rats, and so forth. However, elephants and similar kinds of endangered species or animals, living in zoos or tourism locations, can adopt invasive methods to detect emotions. The major advantages of adopting invasive methods are twofold: a) Invasive methods rely on more authentic measurements that relate to physiological indications of emotions; and, b) they deliver accurate measurements while observing emotions in animals [51].

In non-invasive methods, emotions are collected using sensors mounted outside the bodies of animals. In fact, detecting emotions such as fear, anger, joy, disgust, neutral, and so forth, using facial expressions has been widely implemented for human datasets in the past [62]. Several methods and algorithms have been designed in the recent past to detect the emotions of human faces belonging to dispersed geographical regions [43] [14]. Also, researchers

have captured the relationships between facial expressions and emotions [71].

As similar to identifying human emotions, classifying emotions from the facial expressions has been practiced by experienced animal researchers [29] [74]. They observed that adopting ICT technologies eases the process of emotion detection due to the inclusion of sophisticated learning algorithms to capture the facial emotion-related features of animals. However, while investigating the existing research, we could observe that these mechanisms have targeted single animals rather than a group of animals while detecting their emotions.

A large sector of researchers worked on creating facial action coding systems (FACS) in animals. Notably, FACS was initially developed in human faces by observing facial muscular movements [23]. Subsequently, the same approach was developed in animals such as dogs, cats [12], and horse. [39] applied the FACS approach to indicate pain points in animals; [73] evaluated the facial expressions of multiple animal species. In [19], authors attempted to label the facial features of animals before collecting their emotions. However, their approach led to reduced learning accuracy due to poor precision in labeling the FACS of animals. In a few research works, researchers have applied deep learning algorithms to detect such facial expressions [40].

Facial expressions of animals are useful to capture and assess the severity of pain in animals. An array of research works is based on the grimace score of the facial expressions of animals. In short, the grimace score is an assessment score that indicates the pain levels of animals by observing their facial muscular movements. For instance, in [47], authors have utilized the grimace scale to detect the severity of emotions due to pain [46]. Similarly, the grimace scale indication has been applied in different varieties of animals such as laboratory animals [67], farm animals [30], and pet animals [24] by a few other researchers to study the impact of pains in different animals – i.e., researchers [45] have extended the concept of grimace scales for sheep and named them as Sheep Pain Facial Expression Scale(SPFES) [45]; similarly, authors of [38] and [10] have developed unique grimace scales for horses and named them as Horse Grimace Scale (HGS).

A few authors studied the relationship between animal behaviors and emotions. They monitored the behavior of multiple types of animals by assessing the behavior indicators [61]. For instance, the authors of [21] have developed a cow emotion estimation framework considering the valence of the affective states of cow's behaviors; the authors of [33] have implemented a few behavior indicators of pigs based on the wagging of their tails; the authors of [20] have classified the emotions of horses after collecting their behavior traits; authors have explored and affirmed the repetitive pattern of horse movements that reduces their stress level [3]. Also, in [56], the authors have developed a monitoring framework that keeps track of the behavioral states of animals.

Apart from farm or pet animals, we collected research works that focused on the behavioral study of elephants. Notably, researchers [66] and [8] have studied the behavior patterns of elephants using vocalization and vocal expressions.

2.4.1 Using pose detection

Identifying the poses of animals and relating them to their core emotions is another aspect of detecting emotions in animals. The body posture and movements of animals convey emotional indices. The correlations between pose and emotions can be studied using modern learning algorithms, including deep learning algorithms. Such studies relating to animal emotions based on pose estimations can be instrumental in minimizing pain in animals.

For instance, in [77], the authors have developed a pose estimation system for dogs to assuage their pains. In the recent past, authors have developed a DeepLabCut framework [63] that relates the emotions of dogs, such as happiness, fear, and anger, to their corresponding poses. They have detected a few abnormalities in horses' poses while considering their movement patterns.

There are a few tools that estimate the poses of animals and relate them to their emotional states. Notably, the DeepLabCut tool [44, 26] and the LEAP tool [57] have been widely utilized among researchers and practitioners to capture the emotions of animals using deep learning algorithms. The DeepLabCut framework has also been utilized to generate emotion indicators from several cross-species of animals based on learned poses [50].

The summary of the existing works point out that most of the works have not applied specific cost-efficient solutions to detect animal emotions in real-time. Table 2.4 highlights the animal emotion detection systems that differentiate the non-inclusion of cloud-based systems or IoT-enabled approaches.

In the table, we have defined N as NIL, NS as Not Scalable, OFF as offline, ON as online, $S-Exp$ as standalone experimental setup, $S-GPU$ as standalone experimental setup involving NVIDIA or similar GPU-based machines, $Cloud$ as cloud-based solution, and $S-Drone$ as standalone experimental setup based on drones. The last metric denotes the cost efficiency in a scale ranking between 1 to 5 where 1 corresponds to the cost-efficient solution.

The idea is to point out that serverless-based edge-enabled solution could be a better approach for detecting animal emotions that surpass a long time internal.

3 Edge-enabled serverless architectures for animal emotion detection

With the alarming rise in interest in establishing human-animal bonds and preventing animal attacks, robust technologies are required to detect the emotions of animals.

Table 1: Animal emotion detection and allied techniques – a comparative study

Article	Methods and Procedures	–Computing | Scalable | Offline/Online | Cost Scale
[4]	Manual analysis	N | NS | OFF | 3
[51]	YOLO and FasterRCNN for detecting cow emotions	S-GPU | NS | OFF | 4
[1]	Pre-trained CNN to study post surgical impacts of mouse	S-Exp | NS | OFF | 4
[10]	Horse pain detection using machine learning	S-Exp | NS | ON | 2
[17]	Facial emotion detection of horses	S-Exp | NS | OFF | 4
[26]	Dog's emotion detection using neural network	S-Exp | NS | OFF | 4
[29]	Identify emotions in monkeys	S-GPU | NS | OFF | 4
[33]	Tail posture identification in pigs	S-Drone | NS | ON | 4
[38]	Pain in horses using CNN	S-Exp | NS | OFF | 4
[58]	Disease prediction using CNN	S-Exp | NS | OFF | 4
[70]	IoT-based elephant acoustic study using Neural network	Cloud | S | ON | 2
[74]	RetinaNet face posture identification	S-GPU | NS | OFF | 4
[77]	YOLO and LSTM-based pain detection in dogs	S-Exp | NS | OFF | 4
[34]	CNN-based animal face detection	S-GPU | NS | OFF | 4

This section discusses the edge-enabled serverless architectures and frameworks that adopt an efficient animal emotion detection mechanism.

Towards this end, at first, we cover the special features of architectures that are crucial to detecting animal emotions; next, we describe the possible software/hardware components and associated algorithms that improve the goals of identifying the emotions of animals; and, at last, a few metrics that drive the objectives of architectures are discussed.

3.1 Animal emotion detection architectures

In the past, specialized trainers detected animals' emotions. They applied skilled tricks to improve the productivity of the animals' assigned tasks. For instance, vocalizations such as growls, barks, or body postures such as wagging tails of dogs, are read by people raising animals. However, observing emotions and classifying the affective states of animals using the manual approach can lead to human bias [49]. There have been efforts in the past to develop mechanisms that offer unbiased assessments. However, the works are under-researched to date [36].

This section elaborates on the applicability of IoT-enabled technologies for studying the emotions of animals. Depending on the deployment options, the animal emotion detection mechanism is classified into four types: i) Naive IoT, ii) Edge-enabled IoT, iii) Serverless IoT, and iv) AI-Assisted IoT (see Figure 2). Additionally, the section highlights the importance of involving deep learning-driven edge-enabled serverless architecture to enhance the accuracy and cost efficiencies.

3.1.1 Naive IoT – Type-I

Exploring the emotions of animals utilizes sensor-enabled networks that transport sensed data using communication protocols such as WiFi, 4G/5G, or Long Range WAN (LoRAWAN). The WiFi communication protocol provides a higher bandwidth to transfer sensor data from a camera. This protocol is suitable in locations such as zoos, temples, and work sites, where the emotions of animals need to be monitored. 4G/5G networks are mobile cellular networks based on 4G/5G communication protocols that offer a high-speed network to carry animal images or video streams in a wireless medium. However, this protocol is not suitable for carrying sensory information for long distances. On the contrary, LoRAWAN is a wide area network that can transfer sensory information that reaches around 10 KMs between sensors and services. The drawback of utilizing the LoRaWAN protocol in emotion detection architectures is its limitation in transferring a huge volume of data to sense the emotions of animals.

In the Naive-IoT system, sensors such as camera sensors collect animal images or frames and stream data to cloud services through gateways that are connected using communication protocols such as WiFi or 4G/5G networks. The cloud services process these animal videos in cloud environments after sufficient data processing mechanisms, including data filtering, augmentation, and so forth. Additionally, the cloud services host learning algorithms or AI-assisted services to detect the emotions of animals, such as anger, grief, happiness, joy, and so forth.

For instance, in [54], the authors have developed an IoT-enabled electronic board using sensors that were mounted on the ears of pigs to observe their activities; [41] have developed an accelerator-based solution to collect the behavioral changes of horses by designing a few affective states; [69] have studied the emotions of animals by transforming learning algorithms on smartwatches; and so forth. Similarly, [52] have surveyed the sensor-based emotion monitoring approaches for farm animals, which limit the scope of research to a subset of animals. In Figure 2, we could observe that the Type-I architecture has direct communication of sensors to cloud environments.

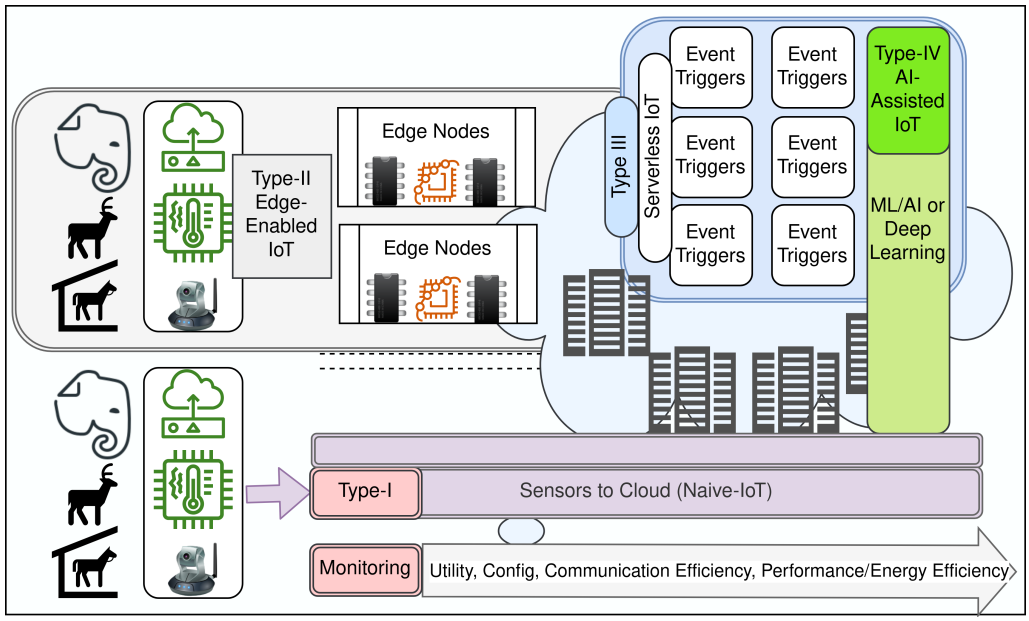


Figure 2: Animal emotion detection architectures – Type-I, II, III, and IV

3.1.2 Edge-enabled IoT – Type-II

Rather than streaming animal videos from their exact locations, such as the zoo or circus arena to the cloud environments, it is better to transfer the important features of animals' emotions to edge nodes. This enables us to minimize the network bandwidth and privacy of streaming sites. For instance, to observe the emotions of elephants, while learning their emotions, it is sufficient to submit features such as ear positions, mouth angle, and so forth, to cloud services based on animal emotion detection services. Most of the video processing and parsing of facial features or emotional traits could be carried out on edge devices that are mounted by decent processing elements. The most notable edge devices that are utilized for processing video frames nearer to the sensor nodes are Raspberry Pi nodes, mobile phones, low computational servers, laptops, Jetson Nano devices, and so forth. The type-II architecture model of Figure 2 represents the sensors connected to clouds through edge nodes. A few researchers have developed frameworks with multi-sensor devices, including cameras, to detect the emotions of elephants on smartphone devices based on GPS communications [70]. However, this work is not assisted by modern communication protocols or edge computing services to efficiently utilize the power of edge-enabled IoT systems.

In fact, edge computing nodes suffer from memory and computation-related resource limitations. They could not handle memory-expensive deep learning tasks such as ResNet50.

3.1.3 Serverless IoT – Type-III

Most IoT-enabled applications or pure edge-enabled solutions continuously power the associated cloud services. This approach of utilizing edge and cloud computing nodes for processing animals' emotions has three major disadvantages:

1. *Energy Inefficiency* – Cloud services are unnecessarily underutilized, even if there is no data to process them. For instance, the videos of animals are not captured throughout the day/year to study the emotional variations over time in the zoo. The emotions could be programmatically observed only for a few minutes, especially while feeding, playing, or so forth. In such situations, cloud servers could be switched "OFF" to efficiently handle the energy consumption of these applications. Also, in locations where renewable energy sources are available, it is sufficient to utilize renewable energy sources to power "ON" the devices.

2. *Cost Inefficiency* – In cloud environments, compute instances and their allied resources for applications are continually utilized. If we need to detect the patterns of emotions in animals over months or years in a zoo/circus, the cloud resources are always utilized, although the necessity of resources is limited. This indirectly increases the costs of such emotion detection-based applications for users.

3. *Carbon Inefficiency* – When animal emotion-related applications are executed on clouds, they heat the cloud resources. Obviously, energy consumption due to powering "ON" the machines and cooling them due to overutilization the risk of carbon emissions in data centers or supercomputers. These carbon emissions, therefore, could be controlled for the benefit of society if the applications are programmed elegantly.

Table 2: Deep learning algorithm-based animal emotion detection

Reference	Animal	Algorithm	Approach	Location
[59]	Horses	Object Detection NN and YOLO	Facial Keypoint Action Movement Detection	Horse Staple
[2]	Horses	LSTM concatenated binary classifier	Facial Keypoint Action Movement Detection	Horse Staple
[51]	Cows, Pigs	FasterRCNN YOLOv3 YOLOv4	Emotion Classification using different Algorithms	Pasture
[27]	Dogs	Pretrained AlexNet with FC Layers	Emotion Pretraining	-
[26]	Dogs	DeepLabCut	Landmark points and posture detection (Ear, Hair, Mouth, and so forth)	-
[1]	Mice	ResNet50	Emotions post surgical	Laboratory
[17]	Horses	FasterRCNN VGG16 ResNet50v2 Xception	Comparison of algorithms based on head positions	Farm land
[7]	Dogs	ResNet Supervised	Classify emotions based on anticipation or frustration	Home
[58]	Sheep	YOLO SSDMobileNet	Sheep face detection	Farm land
[38]	Horses	3-layered CNN	Facial feature classification based on Grimmascale	Farm land
[10]	Horses	InceptionV3 VGG+LSTM	Pain detection with temporal features	Farm land
[60]	Horses	Encoder-Decoder	Equine pain classification	Farm land

A serverless-enabled cloud implementation model improves energy efficiency, cost efficiency, and carbon efficiency. It is a cloud execution model where servers are not powered "ON" throughout the execution of applications. Only if sensor data is triggered using edge-enabled devices, the servers are powered "ON" and the states of the applications are modified.

For instance, the emotions of animals are assessed based on the qualified input data captured and transferred to cloud servers. There exist a few platforms that enable serverless-assisted IoT solutions. For instance, AWS offers Lambda services. The Lambda services enable execution of functions based on triggers obtained from IoT-enabled sensors.

3.1.4 AI-assisted IoT solutions – Type-IV

Providing AI-based solutions is crucial to accurately detecting the emotions of animals. AI-based algorithms, in general, are classified into supervised, unsupervised, and reinforcement learning algorithms [6]. They are applied in various domains, such as the financial sector, agricultural sector, cognitive sector [15], and so forth. Supervised learning algorithms are further classified based on machine learning approaches and deep learning approaches.

There are several classical machine learning algorithms such as Support Vector Machines [39], Random Forests, K-Nearest Neighbor, Rule-based, Naive Bayes, Principal Component Analysis, and so forth, that could be adopted for identifying the emotions of animals from varied input sources such as texts, video, or audio sources. Notably, authors have utilized the vocalization features of elephants [70] to detect the state of mind using SVM classifiers in four different categories: roar, rumble, trumpet, and cry.

Apart from a few classical ML algorithms, there exist a few deep learning algorithms such as the You Only Look Once (YOLO) algorithm, Convolutional Neural Networks (CNNs), Residual Net (ResNET) models, Reinforcement Neural Networks (RNN), and so forth for detecting animal emotions.

For instance, in the recent past, the authors of [31] have assessed the pain in horses [2] and donkeys by detecting the facial keypoints; the authors of [25] have applied the ResNet50 algorithm to detect pain in cats; researchers of [45] have utilized computer vision approaches to detect pain in animals; in [28], the authors have implemented an IoT-enabled solution to establish an intelligent ecosystem for tracking the health of diary farm animals in real time.

Similarly, authors of [72] have implemented a Faster R-CNN deep learning algorithm to classify animal emotions; a few authors have observed the emotions of farm animals using pre-trained Deep CNN models when projected with wolf sound and images [51]; a few researchers, [27], have developed a simple pre-trained AlexNet deep learning model to classify the affective states, namely, smiling, growling, and sleeping states of dogs; a few other researchers [1] have developed an emotion detection model based on neural networks supported by binary classifiers that detected mice's post-anesthetic surgical emotions based on facial expressions; a few researchers [17] have studied the facial expressions of horses using CNNs; a few authors have worked on the application of deep learning algorithms for improving the emotion intelligence of dogs [7] and cats [25]; and, so forth.

Additionally, authors have utilized a pre-trained ResNet-based deep learning model to classify the emotions of dogs as anticipation or frustration [7]; authors [58] have developed temporal features as input to detect the emotions of sheep using multi-step CNN models; in [38], researchers have implemented 3-layered CNN-based deep learning models to recognize pain in horses using grimace scales; similarly, several researchers have applied temporal features in deep learning algorithms, including encoder-decoder-based self supervised deep learning algorithms [10] [11] [60], to detect the emotions of animals.

Based on the most commonly utilized deep learning algorithms, we classified and tabulated them in Table 2. Observations reveal a lack of extensive research on the resource or cost efficiency of learning methods in animal emotion detection.

Interestingly, by integrating these potential deep learning algorithms into edge-enabled serverless frameworks, we can quickly, accurately, and efficiently detect animal

emotions when sensors such as cameras trigger sensor data in real-time.

3.2 Architecture evaluation metrics

The animal emotion detection architectures such as Naive IoT, Edge-enabled IoT, Serverless IoT, or AI-Assisted IoT have to be monitored and evaluated. We identified a set of performance metrics that could be utilized in the architectures. The description of these metrics is explained below:

Device utility The device utility is a measure of the total utilization of cloud or sensor-based resources among the available utilization times. In serverless environments, the resources are utilized only when there is a trigger from associated sensors – i.e., the utilization depends on the nature of applications, serverless platforms, and resource providers' serviceability.

Configurational easiness Configuring a serverless-enabled IoT platform can lead to difficulties for some users. For instance, a few serverless platforms utilize sophisticated user interfaces or ease in setting up automatic configurations, whereas, others do not. Hence, depending on the ease of setting up the configurations, we classify the architectures.

Multi-communication support An animal emotion detection architecture is limited to supporting all communication protocols. Some architectures enable various communication protocols such as, WiFi, Bluetooth, 4G/5G, and so forth. However, the cost of the system increases if these devices operate with different communication protocols. For ease, based on the utility of the application, several IoT-enabled emotion detection architectures are designed using WiFi, 4G/5G, or Bluetooth. This metric ensures the ability of the device to install it on any different locations/platforms.

Prediction accuracy The emotion detection of elephants or animals in farms or in the wild involves learning algorithms, including deep learning algorithms such as CNNs, LSTM, or SVM. While classifying emotions depending on the environmental inputs, prediction accuracy is one crucial metric that needs to be maximized. If not, false positives drive the system with wrong decisions. Developing an emotion detection system that offers more accurate decisions is a time-consuming task, as it depends on the quality of the learning algorithms and the learning parameters of the algorithms.

Energy or hardware-related metrics The performance of applications is a step toward improving the implementation strategies and the writing style of applications. In an edge-enabled elephant emotion detection system, developers could implement algorithms, including learning algorithms, in several approaches:

1. *Lightweight Implementation using Containers* – container-based implementations offer lightweight solutions that self-contain all relevant packages to execute emotion detection applications. It is an OS-level virtualization approach in which algorithmic instances are offloaded to multiple servers depending on the load balancing requirements or other performance concerns of the execution environments.

2. *Security-conscious Implementation Approach* – Applications could be developed considering the security features of the programming models. Increasing the security-based software components in emotion-related detection algorithms can reduce the performance of applications.

3. *Execution Time Improvements* – Improving the execution time of learning algorithms, including deep learning-based emotion detection algorithms, requires the application developer to have algorithmic excellence and coding skillsets. Developing algorithms considering the nature of input data and avoiding unnecessary allocation of variables could improve the execution time of emotion detection applications.

4. *Energy or Carbon-conscious Developments* – Metrics that improve the energy efficiency of applications or carbon emissions are predominantly practiced in long-running applications. For instance, edge-enabled emotion detection applications involve battery-operated or renewable energy sources for powering edge or sensor nodes. The entire ecosystem should consciously deliver most of the executions to such renewable-powered resources while learning emotions or inferencing emotion-related patterns. In this way, carbon emissions are reduced in such long-running applications, especially when training phases are carried out on edge-enabled devices.

Figure 2 illustrates the different types of animal emotion detection architectures depending on the deployment options – i.e., whether they involve edge-based solutions, serverless execution models, or naive IoT-enabled approaches.

3.3 DL-driven edge-enabled serverless architecture – an exploratory study

Among the four types of animal emotion detection architectures, the Type-IV architecture that combines deep learning, IoT, edge computing, and serverless execution models is considered to be more efficient in terms of cost and resource utilization.

Table 3: Cost exploration for AWS services in naive-IoT architectures

AWS Services	Name of the Service	Dollars per hour	Year-wise
Compute Instances	t4g.micro	0.0104	91.104
	m5.large	0.096	840.96
	t2.micro	0.0116	101.616
	g4dn.12xlarge instances (4 GPUs - 96vCPUs)	5.47	47917.2
Associated Storage	SSD-32GB	2.56	30.72
	IOPS-SSD-32GB	4	48
Kinesis Data firehose	1TB-streams	29.7	356.4
AWS S3	100GB storage	2.3	27.6
		Total (10 instances)	**12556.8**

Table 4: Comparison of types of animal emotion detection architectures

Architecture	Scalable	Latency	Cost Efficiency	Security	Accuracy	Utility	Easiness
Manual	Poor	Depends on availability	Poor	High	Depends on Evaluator	NA	NA
Type-I	Medium	High	Poor	Poor	Depends on Application	Poor	Poor
Type-II	High	Medium	Medium	High	Depends on Application	Medium	Poor
Type-III	High	Low	High	High	Depends on Application	High	High
Type-IV	High	Low	High	High	Depends on AI	High	Medium

3.3.1 Process involved

The following steps outline the process of incorporating deep learning algorithms into edge-enabled serverless frameworks within the Amazon AWS ecosystem:

1. Initially, camera sensors stream videos to nearby edge nodes for evaluating the animals interested in detecting the emotions. For instance, an elephant emotion detection system captures frames belonging to elephants and omits the other animals.

2. Next, edge-enabled services connect to AWS S3 buckets to trigger the required DL algorithm, such as YOLO, CNN, RESNET, or so forth, using S3 event notification options. The S3 buckets include code snippets and scripts to start executing EC2 instances based on AWS Lambda functions.

3. Accordingly, the corresponding DL algorithm is executed along with the past state information and data modules on EC2 compute instances for a specified time interval. The EC2 service requests are activated through simple queue services of AWS.

4. Finally, once the modeling and prediction tasks are handled, the state of the application is saved in the S3 bucket for future executions. It could be noticed that the EC2 instances remain inactive throughout the animal emotion detection processes, particularly when they are installed in forest or zoo locations. This drastically reduces the computational costs involved in the execution. Additionally, a few lightweight deep learning algorithms, such as TinyYOLO, could be deployed for faster and more resource-efficient learning or inferences.

3.3.2 Cost-efficiency

To illustrate the cost efficiency of Type-IV architecture – specifically, DL-driven edge-enabled serverless architecture, we have considered an AWS platform consisting of 10 Elastic Compute Cloud (EC2) instances, including GPU instances, to execute parallel deep learning models; AWS Lambda and AWS S3 services have been considered to establish serverless implementations. Also, we have assumed that the architecture included cameras and edge devices such as Raspberry Pi nodes that are dedicatedly available for evaluating the costs involved in the animal emotion detection. In the study, only recurring costs involved in the operations were studied, assuming the animal emotion detection has to be evaluated throughout an year.

The key findings are listed below:

1. The manual approach to detecting animal emotions is not a scalable or accurate solution as it is dependent on the skillset of evaluators;

2. The Type-I architecture utilized cameras to stream animal videos directly to cloud-based services. In this approach, at least cloud instances have to be active throughout the execution of services. As an exploratory study, we considered ten `m5.large` instances from the US East (N. Virginia) region to evaluate the animal emotions. Accordingly, the cost of the EC2 instances was estimated – i.e., it reached around $101.616 per year. Additionally, the architecture required high performance storage units to quickly re-

spond to the requests for animal emotion detections. Hence, Solid State Drives (SSDs) or I/O Operations Per Second (IOPS) storage units have to be invoked. Also, we need to process streaming data on the cloud. To do so, AWS Kinesis Data Firehose have to be plugged in to the detection system;

3. Involving ten `m5.large` instances, 32-GB SSD, 1TB-streaming support, and 100GB S3 service can lead to $12556.8 for a year. Table 3 lists the required cloud services and the recurring cost required per year to operate an animal emotion detection-related application on the cloud using Type-I architecture.

4. The Type-II architecture considered edge-enabled devices to parse videos and perform data-related operations closer to the data sources. This architecture still requires cloud-based compute instances and storage units mentioned in Table 3 to evaluate animal emotions. Although a few computations happen on the edge, the cloud services have to be switched 'ON' throughout the year. However, the network bandwidth of the application is relatively improved when compared to Type-I architecture.

5. Type-III and Type-IV architectures involve serverless IoT solutions. Here, the AWS Lambda service is integrated to the animal emotion detection application. In doing so, EC2 compute instances are utilized only based on the trigger happening from data sources. Assuming that there are 10,000 service requests prompted from sensor sites, there are no charges collected specifically from AWS Lambda services. However, the Type-III architecture requires EC2 instances to update weights and perform inferences.

   If fifteen minutes are required for performing each service request, the recurring costs of Type-III architecture for an entire year will reach only $2676 – i.e., 10,000 times of ten `m5.large` instances along with 100GB storage components. The major difference between Type-III and Type-IV architectures is the inclusion of core deep learning models to perform animal emotion detections. Accordingly, the accuracy of Type-IV architecture increases with almost equivalent costs found in Type-III architectures.

6. Additionally, the four types of architectures are compared in terms of scalability, latency, security, device utility, and ease. Table 4 highlights the importance of AI-assisted architecture using serverless and IoT components to detect animal emotions.

4 Research directions

This section suggests a few research directions that could be adopted based on the existing animal emotion detection strategies. The possible research directions are discussed in three major divisions, as shown in Figure 3.

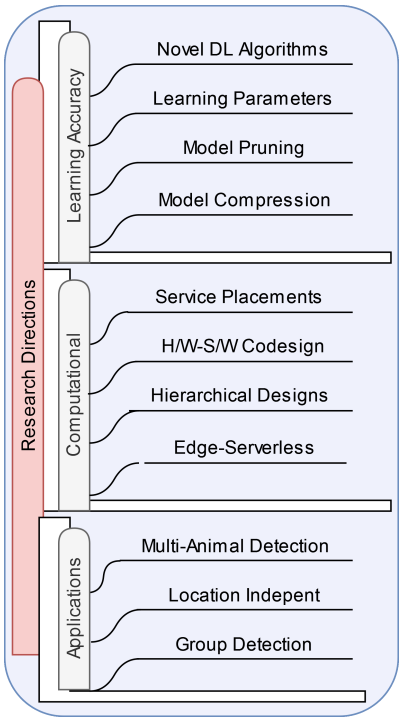


Figure 3: Research Directions in Edge-Enabled Animal Emotion Domain

4.0.1 Improving learning accuracy

Emotion detection using edge-enabled serverless architectures involves learning algorithms such as CNNs or YOLO. The learning accuracy of these algorithms could be increased by applying a few methods, as listed below:

1. the developers could design novel deep learning algorithms that increase the learning accuracy of applications;

2. an automatic tuning of learning hyper-parameters such as learning rate, number of iterations, model optimization methods, and so forth, could be developed. In fact, developing an automatic tuning feature can lead to poor performance efficiencies while detecting animal emotions;

3. an approach to compressing learning models while transferring them to the cloud or edge increases the network bandwidth of the learning system. Unfortunately, researchers avoid them as networks are considerably working well during their experiments with a low volume of data. However, the real situation mandates the necessity of such compressions.

4.0.2 Computational advancements

Although we proposed edge-enabled serverless-oriented architectures for animal emotion detection, there are research directions to improve them i) by choosing where

to place the services, such as learning-related services or security-oriented services; ii) by designing tightly coupled hardware-software designs targeting performance metrics such as energy, execution time, or carbon emissions; iii) by developing hierarchical architectures that benefit from the most commonly observed time and space complexities in computing environments; and, iv) by implementing edge-enabled serverless architectures that improve the cost efficiency factors and latency issues of animal emotion detection algorithms.

4.0.3 Applications

Apart from developing technologies and solutions to enhance research in computational and algorithmic design, there are immense research opportunities to observe emotions among a swarm of animals. For instance, identifying animals' emotions from geographically dispersed locations is a challenge. This involves an architectural design of the system, considering sensors and associated communication protocols to transfer intelligence elegantly. Similarly, inferring intelligence based on a group of multi-species animals could spot novel findings.

5 Conclusions

Animal emotion detection research has started with the fresh challenge of detecting emotions. Traditionally, a manual approach to detecting animal emotions had failures and inefficiencies, as pointed out by several practitioners. The recent IoT-enabled animal emotion detection systems have marked an array of performance improvement opportunities. This article explored the recent trends in applying IoT-enabled solutions for animal emotion detection research; it studied the importance of incorporating DL-driven edge-enabled serverless-oriented architectures by exploring the costs involved in computations of architectures; and, it offered a few research directions that threw light on near-future research works. The article would enable the incorporation of novel architectural designs and significantly increase the interest of indigenous animal emotion researchers.

Acknowledgement

The authors thank IIIT-Kottayam for offering resources, Prof. Michael Gerndt of TUM for motivating the work, and the editorial office the journal for reviewing/publishing the work.

References

[1] Andresen, N., Wöllhaf, M., Hohlbaum, K., Lewejohann, L., Hellwich, O., Thöne-Reineke, C., & Belik, V. (2020). Towards a fully automated surveillance of well-being status in laboratory mice using deep learning: Starting with facial expression analysis. *PloS one*, (Vol. 15(4), e0228059, pp. 1-23). https://doi.org/10.1371/journal.pone.0228059

[2] Andersen, P. H., Broomé, S., Rashid, M., Lundblad, J., Ask, K., Li, Z., Hernlund, E., et al. (2021). Towards Machine Recognition of Facial Expressions of Pain in Horses. *Animals*, (Vol. 11, No.6, 1643, pp. 1-18). *MDPI AG*. Retrieved from http://dx.doi.org/10.3390/ani11061643

[3] Auer U, Kelemen Z, Engl V, Jenner F (2021) Activity Time Budgets—A Potential Tool to Monitor Equine Welfare? *Animals* (Vol. 11, No. 850, pp. 1-12). https://doi.org/10.3390/ani11030850

[4] Battini M., Agostini A., & Mattiello, S. (2019). Understanding Cows' Emotions on Farm: Are Eye White and Ear Posture Reliable Indicators?, *Animals*, (Vol. 9, No. 8, 477, pp. 1-12). https://doi.org/10.3390/ani9080477

[5] Bekoff, M. (2023). Human Emotions in Animals, https://online.uwa.edu/news/empathy-in-animals/, Accessed in Oct. 2024.

[6] Benedict, S. (2022). Deep Learning Technologies for Social Impact. *IOP Publishing*. pp. 1-13, https://doi.org/10.1088/978-0-7503-4024-3

[7] Boneh-Shitrit, T., Amir, S., Bremhorst, A., Mills, D., Riemer, S., Fried, D., & Zamansky, A. (2022). Deep Learning Models for Automated Classification of Dog Emotional States from Facial Expressions. in *arXiv:2206.05619*, pp. 1-6, https://doi.org/10.48550/arXiv.2206.05619

[8] Briefer, E. F. (2012). Vocal expression of emotions in mammals: mechanisms of production and evidence. In S. Le Comber (Ed.), Journal of Zoology (Vol. 288, Issue 1, pp. 1–20). *Wiley Portico*. https://doi.org/10.1111/j.1469-7998.2012.00920.x

[9] Bremhorst, A., Sutter, N. A., Würbel, H., Mills, D. S., & Riemer, S. (2019). Differences in facial expressions during positive anticipation and frustration in dogs awaiting a reward. In *Scientific Reports*. Springer Science and Business Media LLC. (Vol. 9, No. 19312, pp. 1-13). https://doi.org/10.1038/s41598-019-55714-6

[10] Broomé, S., Gleerup, K. B., Andersen, P. H., & Kjellstrom, H. (2019). Dynamics Are Important for the Recognition of Equine Pain in Video. *In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE. USA. pp. 12659-12668. https://doi.org/10.1109/cvpr.2019.01295

[11] Broomé, S., Ask, K., Rashid-Engström, M., Haubro Andersen, P., & Kjellström, H. (2022). Sharing pain: Using pain domain transfer for video recognition of low grade orthopedic pain in horses. In A. Seal (Ed.), *PLOS ONE* (Vol. 17, No. 3, e0263854, pp. 1-21). Public Library of Science (PLoS). https://doi.org/10.1371/journal.pone.0263854

[12] Caeiro, C. C., Burrows, A. M., & Waller, B. M. (2017). Development and application of CatFACS: Are human cat adopters influenced by cat facial expressions? *In Applied Animal Behaviour Science*. (Vol. 189, pp. 66–78). Elsevier BV. https://doi.org/10.1016/j.applanim.2017.01.005

[13] Camerlink, I., Coulange, E., Farish, M., Baxter, E. M., & Turner, S. P. (2018). Facial expression as a potential measure of both intent and emotion. In *Scientific Reports* (Vol. 8, Issue 17602). Springer Science and Business Media LLC. pp. 1-9. https://doi.org/10.1038/s41598-018-35905-3

[14] Chen, C., Zhu, W., Steibel, J., Siegford, J., Wurtz, K., Han, J., & Norton, T. (2020). Recognition of aggressive episodes of pigs based on convolutional neural network and long short-term memory. In *Computers and Electronics in Agriculture*. (Vol. 169, No. 105166, pp. 1-10). Elsevier BV. pp. 1-10. https://doi.org/10.1016/j.compag.2019.105166

[15] Cheng Pan, Haiyan Zhao, Meijiao Sun. (2024). Real-time Target Detection System in Scenic Landscape Based on Improved YOLOv4 Algorithm. in *Informatica* (Vol. 48, p. 35–48). https://doi.org/10.31449/inf.v48i8.5700

[16] Clemins, P. J., & Johnson, M. T. (2003). Application of speech recognition to African elephant (Loxodonta africana) vocalizations. *Proceedings. (ICASSP '03). International Conference on Acoustics, Speech and Signal Processing (ICASSP'03)*. IEEE. pp. I-484-487. https://doi.org/10.1109/icassp.2003.1198823

[17] Corujo, L. A., Kieson, E., Schloesser, T., & Gloor, P. A. (2021). Emotion Recognition in Horses with Convolutional Neural Networks. In *Future Internet*. (Vol. 13, Issue 10, p. 250). MDPI AG. https://doi.org/10.3390/fi13100250

[18] Cowen AS, Keltner D. (2017). Self-report captures 27 distinct categories of emotion bridged by continuous gradients. *Proc Natl Acad Sci U S A*. (Vol. 114, No. 38, p. E7900-E7909. https://doi.org/10.1073/pnas.1702247114

[19] Dai, F., Leach, M., MacRae, A. M., Minero, M., & Dalla Costa, E. (2020). Does Thirty-Minute Standardised Training Improve the Inter-Observer Reliability of the Horse Grimace Scale (HGS)? A Case Study. In *Animals* (Vol. 10, No. 5, 781, pp. 1-7). MDPI AG. https://doi.org/10.3390/ani10050781

[20] Dyson, S., & Pollard, D. (2020). Application of a Ridden Horse Pain Ethogram and Its Relationship with Gait in a Convenience Sample of 60 Riding Horses. In *Animals* (Vol. 10, No. 6, 1044, pp. 1-14). MDPI AG. https://doi.org/10.3390/ani10061044

[21] Ede, T., Lecorps, B., von Keyserlingk, M. A. G., & Weary, D. M. (2019). Symposium review: Scientific assessment of affective states in dairy cattle. In *Journal of Dairy Science* (Vol. 102, No. 11, pp. 10677–10694). American Dairy Science Association. https://doi.org/10.3168/jds.2019-16325

[22] Ekman, P. (2023). Basic Emotions. https://www.paulekman.com/wp-content/uploads/2013/07/Basic-Emotions.pdf, Accessed Jan. 2023.

[23] Ekman, P., & Friesen, W. V. (1978). Facial Action Coding System. In *PsycTESTS Dataset*. American Psychological Association (APA). https://doi.org/10.1037/t27734-000

[24] Evangelista, M. C., Watanabe, R., Leung, V. S. Y., Monteiro, B. P., O'Toole, E., Pang, D. S. J., & Steagall, P. V. (2019). Facial expressions of pain in cats: the development and validation of a Feline Grimace Scale. In *Scientific Reports* (Vol. 9, No. 19128, pp.1-11). Springer Science and Business Media LLC. https://doi.org/10.1038/s41598-019-55693-8

[25] Feighelstein, M., Shimshoni, I., Finka, L. R., Luna, S. P. L., Mills, D. S., & Zamansky, A. (2022). Automated recognition of pain in cats. In *Scientific Reports* (Vol. 12, No. 9575, pp.1-10). Springer Science and Business Media LLC. https://doi.org/10.1038/s41598-022-13348-1

[26] Ferres, K., Schloesser, T., & Gloor, P. A. (2022). Predicting Dog Emotions Based on Posture Analysis Using DeepLabCut. In *Future Internet* (Vol. 14 (4) No. 97, p. 1-16). MDPI AG. https://doi.org/10.3390/fi14040097

[27] Franzoni, V., Milani, A., Biondi, G., & Micheli, F. (2019). A Preliminary Work on Dog Emotion Recognition. In *IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume. WI '19: IEEE/WIC/ACM International Conference on Web Intelligence*. ACM. pp. 91-96, https://doi.org/10.1145/3358695.3361750

[28] Gehlot, A., Malik, P. K., Singh, R., Akram, S. V., & Alsuwian, T. (2022). Dairy 4.0: Intelligent Communication Ecosystem for the Cattle Animal Welfare with Blockchain and IoT Enabled Technologies. In

Applied Sciences (Vol. 12, 7316, p.1-19). MDPI AG. https://doi.org/10.3390/app12147316

[29] Guo, S., Xu, P., Miao, Q., Shao, G., Chapman, C. A., Chen, X., He, G., Fang, D., Zhang, H., Sun, Y., Shi, Z., & Li, B. (2020). Automatic Identification of Individual Primates with Deep Learning Techniques. In *iScience* (Vol. 23, No.8, 101412, p.1-9). Elsevier BV. https://doi.org/10.1016/j.isci.2020.101412

[30] Häger, C., Biernot, S., Buettner, M., Glage, S., Keubler, L. M., Held, N., Bleich, E. M., Otto, K., Müller, C. W., Decker, S., Talbot, S. R., & Bleich, A. (2017). The Sheep Grimace Scale as an indicator of post-operative distress and pain in laboratory sheep. In I. A. S. Olsson (Ed.), *PLOS ONE* (Vol. 12, Issue 4, e0175839, p.1-15). Public Library of Science (PLoS). https://doi.org/10.1371/journal.pone.0175839

[31] Hummel, H. I., Pessanha, F., Salah, A. A., van Loon, T. J. P. A. M., & Veltkamp, R. C. (2020). Automatic Pain Detection on Horse and Donkey Faces. In *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020). 2020*. IEEE. pp. 793-800, https://doi.org/10.1109/fg47880.2020.00114

[32] ICARUS, (2023). ICARUS Global Monitoring. Animals Early Warning System. https://www.icarus.mpg.de/28810/animals-warning-sensors, accessed in Oct. 2024.

[33] Iglesias, P. M., & Camerlink, I. (2022). Tail posture and motion in relation to natural behaviour in juvenile and adult pigs. In *Animals* (Vol. 16, Issue 4, 100489, p. 1-10). Elsevier BV. https://doi.org/10.1016/j.animal.2022.100489

[34] Islem Jarraya, Fatma BenSaid, Wael Ouarda, Umapada Pal and Adel M. Alimi. (2023). A New Convolutional Neural Network based on a Sparse Convolutional Layer for Animal Face Detection. In *Multimedia Tools and Applications* (Vol. 82, p. 91-124). https://doi.org/10.1007/s11042-022-12610-y

[35] João Videira, Pedro D. Gaspar, Vasco N. G. J. Soares, João M. L. P. Caldeira. (2024). A Mobile Application for Detecting and Monitoring the Development Stages of Wild Flowers and Plants. In *Informatica*. (Vol 48, No 6, pp. 43-58), https://doi.org/10.31449/inf.v48i6.5645

[36] Kret, M. E., Massen, J. J. M., & de Waal, F. B. M. (2022). My Fear Is Not, and Never Will Be, Your Fear: On Emotions and Feelings in Animals. In *Affective Science* (Vol. 3, Issue 1, pp. 182–189). Springer Science and Business Media LLC. https://doi.org/10.1007/s42761-021-00099-x

[37] Langbauer, W. R. (2000). Elephant communication. In *Zoo Biology* (Vol. 19, No. 5, pp. 425–445). Wiley. https://doi.org/10.1002/1098-2361(2000)19:5<425::AID-ZOO11>3.0.CO;2-A

[38] Lencioni, G. C., de Sousa, R. V., de Souza Sardinha, E. J., Corrêa, R. R., & Zanella, A. J. (2021). Pain assessment in horses using automatic facial expression recognition through deep learning-based modeling. In H. Nisar (Ed.), *PLOS ONE* (Vol. 16, No. 10, e0258672, p. 1-12). Public Library of Science (PLoS). https://doi.org/10.1371/journal.pone.0258672

[39] Lundblad, J., Rashid, M., Rhodin, M., & Haubro Andersen, P. (2021). Effect of transportation and social isolation on facial expressions of healthy horses. In E. Palagi (Ed.), *PLOS ONE* (Vol. 16, No. 6, e0241532, p. 1-17). Public Library of Science (PLoS). https://doi.org/10.1371/journal.pone.0241532

[40] Li, Z., Broomé, S., Andersen, P.H., & Kjellström, H. (2021). Automated Detection of Equine Facial Action Units. *ArXiv*, p. 1-5. https://arxiv.org/abs/2102.08983

[41] Maisonpierre, I. N., Sutton, M. A., Harris, P., Menzies□Gow, N., Weller, R., & Pfau, T. (2019). Accelerometer activity tracking in horses and the effect of pasture management on time budget. In *Equine Veterinary Journal* (Vol. 51, No. 6, pp. 840–845). Wiley. https://doi.org/10.1111/evj.13130

[42] Mendl, M., Neville, V., & Paul, E. S. (2022). Bridging the Gap: Human Emotions and Animal Emotions. In *Affective Science* (Vol. 3, No. 4, pp. 703–712). Springer Science and Business Media LLC. https://doi.org/10.1007/s42761-022-00125-6

[43] Marsot, M., Mei, J., Shan, X., Ye, L., Feng, P., Yan, X., Li, C., & Zhao, Y. (2020). An adaptive pig face recognition approach using Convolutional Neural Networks. In *Computers and Electronics in Agriculture* (Vol. 173, No. 105386, p. 1-10). Elsevier BV. https://doi.org/10.1016/j.compag.2020.105386

[44] Mathis, A., Mamidanna, P., Cury, K. M., Abe, T., Murthy, V. N., Mathis, M. W., & Bethge, M. (2018). DeepLabCut: markerless pose estimation of user-defined body parts with deep learning. In *Nature Neuroscience* (Vol. 21, No. 9, p. 1281–1289). Springer Science and Business Media LLC. https://doi.org/10.1038/s41593-018-0209-y

[45] McLennan, K., & Mahmoud, M. (2019). Development of an Automated Pain Facial Expression Detection System for Sheep (Ovis Aries). In *Animals* (Vol. 9, No. 4, 196, p. 1-7). MDPI AG. https://doi.org/10.3390/ani9040196

[46] Mogil, J. S., Pang, D. S. J., Silva Dutra, G. G., & Chambers, C. T. (2020). The development and use of facial grimace scales for pain measurement in animals. In *Neuroscience, Biobehavioral Reviews* (Vol. 116, pp. 480–493). Elsevier BV. https://doi.org/10.1016/j.neubiorev.2020.07.013

[47] Mota-Rojas, D., Olmos-Hernández, A., Verduzco-Mendoza, A., Hernández, E., Martínez-Burnes, J., & Whittaker, A. L. (2020). The Utility of Grimace Scales for Practical Pain Assessment in Laboratory Animals. In *Animals* (Vol. 10, Issue 10, 1838, p. 1-17). MDPI AG. https://doi.org/10.3390/ani10101838

[48] National Research Council, Critical Needs for Research in Veterinary Science. (2005). *National Academies Press*. pp. 1-239. https://doi.org/10.17226/11366

[49] Navarro, E., Mainau, E., & Manteca, X. (2020). Development of a Facial Expression Scale Using Farrowing as a Model of Pain in Sows. In *Animals* (Vol. 10, Issue 11, 2113, p. 1-11). MDPI AG. https://doi.org/10.3390/ani10112113

[50] Nath, T., Mathis, A., Chen, A. C., Patel, A., Bethge, M., & Mathis, M. W. (2019). Using DeepLabCut for 3D markerless pose estimation across species and behaviors. In *Nature Protocols* (Vol. 14, No. 7, pp. 2152–2176). Springer Science and Business Media LLC. https://doi.org/10.1038/s41596-019-0176-0

[51] Neethirajan, S. (2021). Happy Cow or Thinking Pig? WUR Wolf—Facial Coding Platform for Measuring Emotions in Farm Animals. In *AI* (Vol. 2, Issue 3, pp. 342–354). MDPI AG. https://doi.org/10.3390/ai2030021

[52] Neethirajan, S., & Kemp, B. (2021). Digital Livestock Farming. In *Sensing and Bio-Sensing Research* (Vol. 32, No.100408, pp. 1-12). Elsevier BV. https://doi.org/10.1016/j.sbsr.2021.100408

[53] Neethirajan, S., Reimert, I., & Kemp, B. (2021). Measuring Farm Animal Emotions—Sensor-Based Approaches. In *Sensors* (Vol. 21, Issue 2, 553, p. 1-22). MDPI AG. https://doi.org/10.3390/s21020553

[54] Pandey, S., Kalwa, U., Kong, T., Guo, B., Gauger, P. C., Peters, D. J., & Yoon, K.-J. (2021). Behavioral Monitoring Tool for Pig Farmers: Ear Tag Sensors, Machine Intelligence, and Technology Adoption Roadmap. In *Animals* (Vol. 11, Issue 9, 2665, pp. 1-12). MDPI AG. https://doi.org/10.3390/ani11092665

[55] Panksepp, J. (2005). Affective consciousness: Core emotional feelings in animals and humans. In *Consciousness and Cognition* (Vol. 14, No. 1, pp. 30–80). Elsevier BV. https://doi.org/10.1016/j.concog.2004.10.004

[56] Pennington, Z. T., Dong, Z., Feng, Y., Vetere, L. M., Page-Harley, L., Shuman, T., & Cai, D. J. (2019). ezTrack: An open-source video analysis pipeline for the investigation of animal behavior. In *Scientific Reports* (Vol. 9, No. 9:19979, p. 1-11). Springer Science and Business Media LLC. https://doi.org/10.1038/s41598-019-56408-9

[57] Pereira, T. D., Aldarondo, D. E., Willmore, L., Kislin, M., Wang, S. S.-H., Murthy, M., & Shaevitz, J. W. (2018). Fast animal pose estimation using deep neural networks. In *Nature Methods* (Vol. 16, Issue 1, pp. 117–125). Springer Science and Business Media LLC. https://doi.org/10.1038/s41592-018-0234-5

[58] Pessanha, F., McLennan, K., & Mahmoud, M. (2020). Towards automatic monitoring of disease progression in sheep: A hierarchical model for sheep facial expressions analysis from video. In *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020)*. IEEE. p. 387-393. https://doi.org/10.1109/fg47880.2020.00107

[59] Rashid, M., Silventoinen, A., Gleerup, K. B., & Andersen, P. H. (2020). Equine Facial Action Coding System for determination of pain-related facial responses in videos of horses. In *U. G. Munderloh (Ed.), PLOS ONE* (Vol. 15, Issue 11. e0231608, p. 1-18). Public Library of Science (PLoS). https://doi.org/10.1371/journal.pone.0231608

[60] Rashid, M., Broomé, S., Ask, K., Hernlund, E., Andersen, P.H., Kjellström, H., & Lee, Y.J. (2021). Equine Pain Behavior Classification via Self-Supervised Disentangled Pose Representation. *in proc. of 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pp. 152-162. https://doi.org/10.1109/WACV51458.2022.00023

[61] Raspa, F., Tarantola, M., Muca, E., Bergero, D., Soglia, D., Cavallini, D., Vervuert, I., Bordin, C., De Palo, P., & Valle, E. (2022). Does Feeding Management Make a Difference to Behavioural Activities and Welfare of Horses Reared for Meat Production? In *Animals* (Vol. 12, No. 14, 1740, p. 1-11). MDPI AG. https://doi.org/10.3390/ani12141740

[62] Samadiani, Huang, Cai, Luo, Chi, Xiang, & He. (2019). A Review on Automatic Facial Expression Recognition Systems Assisted by Multimodal Sensor Data. In *Sensors* (Vol. 19, No. 8, 1863, p. 1-27). MDPI AG. https://doi.org/10.3390/s19081863

[63] Sénèque, E., Lesimple, C., Morisset, S., & Hausberger, M. (2019). Could posture reflect welfare state? A study using geometric morphometrics in riding school horses. In *J. J. Loor (Ed.), PLOS ONE* (Vol. 14, Issue 2, e0211852, p. 1-20). Public Library of Science (PLoS). https://doi.org/10.1371/journal.pone.0211852

[64] Singh, S., & Benedict, S. (2020). Indian Semi-Acted Facial Expression (iSAFE) Dataset for Human Emotions Recognition. In *Communications in Computer and Information Science* (pp. 150–162). Springer Singapore. https://doi.org/10.1007/978-981-15-4828-4_13

[65] Soltis, J., Leong, K., & Savage, A. (2005). African elephant vocal communication II: rumble variation reflects the individual identity and emotional state of callers. In *Animal Behaviour* (Vol. 70, No. 3, pp. 589–599). Elsevier BV. https://doi.org/10.1016/j.anbehav.2004.11.016

[66] Soltis, J., Blowers, T. E., & Savage, A. (2011). Measuring positive and negative affect in the voiced sounds of African elephants (Loxodonta africana). In *Journal of the Acoustical Society of America* (Vol. 129, No. 2, pp. 1059-1066). Acoustical Society of America (ASA). https://doi.org/10.1121/1.3531798

[67] Sotocinal, S. G., Sorge, R. E., Zaloum, A., Tuttle, A. H., Martin, L. J., Wieskopf, J. S., Mapplebeck, J. C., Wei, P., Zhan, S., Zhang, S., McDougall, J. J., King, O. D., & Mogil, J. S. (2011). The Rat Grimace Scale: A Partially Automated Method for Quantifying Pain in the Laboratory Rat via Facial Expressions. In *Molecular Pain* (Vol. 7). SAGE Publications. https://doi.org/10.1186/1744-8069-7-55

[68] Statham, P., Hannuna, S., Jones, S., Campbell, N., Robert Colborne, G., Browne, W. J., Paul, E. S., & Mendl, M. (2020). Quantifying defence cascade responses as indicators of pig affect and welfare using computer vision methods. In *Scientific Reports* (Vol. 10, No.8933, pp. 1-13). Springer Science and Business Media LLC. https://doi.org/10.1038/s41598-020-65954-6

[69] Stolz, K., Heyder, T., Gloor, P. A., & Posegga, O. (2019). Measuring Human-Animal Interaction with Smartwatches: An Initial Experiment. In *Studies on Entrepreneurship, Structural Change and Industrial Dynamics* (pp. 165-182). Springer International Publishing. https://doi.org/10.1007/978-3-030-17238-1_10

[70] Thangavel, S., & Shokkalingam, C. S. (2021). The IoT based embedded system for the detection and discrimination of animals to avoid human–wildlife conflict. In *Journal of Ambient Intelligence and Humanized Computing* (Vol. 13, Issue 6, pp. 3065-3081). Springer Science and Business Media LLC. https://doi.org/10.1007/s12652-021-03141-9

[71] Tomkins, S. S., & McCarter, R. (1964). What and Where are the Primary Affects? Some Evidence for a Theory. In *Perceptual and Motor Skills* (Vol. 18, Issue 1, pp. 119-158). SAGE Publications. https://doi.org/10.2466/pms.1964.18.1.119

[72] Tsai, M.-F., & Huang, J.-Y. (2021). Sentiment analysis of pets using deep learning technologies in artificial intelligence of things system. In *Soft Computing* (Vol. 25, Issue 21, pp. 13741-13752). Springer Science and Business Media LLC. https://doi.org/10.1007/s00500-021-06038-z

[73] Waller, B. M., Julle-Daniere, E., & Micheletta, J. (2020). Measuring the evolution of facial 'expression' using multi-species FACS. In *Neuroscience; Biobehavioral Reviews* (Vol. 113, pp. 1-11). Elsevier BV. https://doi.org/10.1016/j.neubiorev.2020.02.031

[74] Xu, B., Wang, W., Guo, L., Chen, G., Li, Y., Cao, Z., & Wu, S. (2022). CattleFaceNet: A cattle face identification approach based on RetinaFace and ArcFace loss. In *Computers and Electronics in Agriculture* (Vol. 193, No. 106675, p. 1-10). Elsevier BV. https://doi.org/10.1016/j.compag.2021.106675

[75] Yu-Ju Chiu, Shajulin Benedict, and Michael Gerndt. (2023). E2D2: Elephant Emotion and Distraction Detection Framework using Edge-Enabled YOLOv5 Deep Learning Algorithm. in *2023 IEEE International Conference on Contemporary Computing and Communications (InC4)*, Bangalore, India, p. 1–6, https:doi.org/10.1109/InC457730.2023.10262860

[76] Zeppelzauer, M., & Stoeger, A. S. (2015). Establishing the fundamentals for an elephant early warning and monitoring system. In *BMC Research Notes* (Vol. 8, Issue 409, p. 1-15). Springer Science and Business Media LLC. https://doi.org/10.1186/s13104-015-1370-y

[77] Zhu, H., Salgırlı, Y., Can, P., Atılgan, D., & Salah, A. A. (2023). Video-based estimation of pain indicators in dogs. *proc. of 11th International Conference on Affective Computing and Intelligent Interaction (ACII)*, pp. 1-8. https://doi.org/10.1109/ACII59096.2023.10388142

Risk Assessment Method for New Energy Vehicle Supply Chain Based on Hierarchical Holographic Model and Matter Element Extension Model

Qiankun Jiang[1,2*], Haiyan Wang[1]
[1]School of Transportation and Logistics Engineering, Wuhan University of Technology
Wuhan 430063, China
[2]Department of Management, Hubei University of Technology Engineering and Technology College
Wuhan 430068, China
E-mail: 290317@whut.edu.cn, jiangqiankun163@sina.com
*Corresponding author

Keywords: new energy vehicles, hierarchical holographic model, matter element extension, risk identification, scientific evaluation

Received: August 21, 2024

New energy vehicles provide new solutions for low-carbon emissions. With the continuous expansion of the new energy vehicle industry, a more scientific supply chain management system is needed to effectively identify and evaluate risks. This study proposes a more scientific and comprehensive risk assessment method for the supply chain system of new energy vehicles based on a hierarchical holographic model and matter element extension model. The results showed that the proposed algorithm improved the classification performance of risk factors by 1.2%, 1.3%, and 1.5% compared to the clustering performance of the nearest frequency amount clustering, particle swarm optimization, and self-organizing mapping algorithms. In terms of noise processing effectiveness, the Rand index has improved by an average of 55% and 41% compared to the kernel density threshold algorithm and spectral clustering algorithm, with smaller fluctuations and significant differences ($P<0.05$). The accuracy, recall, and F-measure were 9.4%, 8.5%, and 9.6% higher than traditional spectral clustering algorithms, with smaller fluctuations and significant differences ($P<0.05$). While reducing the risk handling time by 21%, the effect has improved by 6%, and the fluctuations during the risk handling process were smaller than those of the self-exploration model. Therefore, the proposed algorithm can cope with many uncertain factors in the complex supply chain management system, ensuring the sustainability and stability of the development of the new energy vehicle industry supply chain.

Povzetek: Predlagana je metoda ocenjevanja tveganj v dobavni verigi električnih vozil, ki združuje hierarhični holografski model in model razširitve materialnih elementov.

1 Introduction

The issue of global warming caused by the increase in carbon emissions has become increasingly prominent and has received widespread attention from the international community. The importance of developing clean energy and energy transformation has deeply penetrated people's hearts [1]. New Energy Vehicles (NEVs) are an important way to achieve low-carbon emissions. The growth in the social demand for NEVs is being driven by national policies, while the Supply Chain System (SCS) for automobiles has also expanded significantly [2]. The SCS of NEVs involves business processes in all aspects of production, manufacturing, and sales. The companies involved in the process from raw materials to delivery to consumers have a significant amount of management and operational risks that need to be identified and evaluated [3]. Traditional supply chain risk identification and assessment rely on manual labor, which cannot avoid evaluation errors caused by many uncertain factors. Therefore, there is an urgent need for a new risk assessment method for the supply chain risks of NEVs. Many scholars have researched supply chain risk systems in various fields and proposed some identification and evaluation methods [4].

The first step in risk assessment is to identify the risks in SCS, and many experts have made some research progress in this direction [5]. Dhruv et al. proposed a method for exploring business process problems based on simulation data to avoid risk transfer during business operations. This method could effectively identify key risks in business processes and take targeted measures [6]. Sun et al. proposed an algorithm based on financial and supplier operational risks, which can analyze uncontrollable factors in the market, effectively capture risk incentives, and create conditions for in-depth analysis of risk causes. This method could effectively control the hidden risks of SCS in agricultural products [7]. Ge et al. proposed a supply chain risk identification model based on supply demand. This model conducted research from the end of the supply chain through reverse deduction to obtain the optimal solution for risk identification. The

identification model established by this method could effectively analyze the impact of decision preferences on risk [8]. Patibandla et al. proposed a global liquidity index evaluation model. This model could identify risk propagation for important nodes in the overall process and effectively improve the accuracy and reliability of risk identification [9]. Wu et al. proposed a risk identification model based on supplier standard selection. It combined the consideration of both price and quality factors to obtain a more reliable method for risk assessment. This method provided a basic framework for risk identification and guided supply chain risk identification [10].

After effectively identifying risks, the application of Risk Assessment Models (RAMs) to rate risks has received widespread attention. Yu W et al. proposed an NEVs RAM based on the functional-coefficient method, which can achieve supply chain risk warning and provide a quantitative method for risk assessment. This method has been applied to actual enterprise financial risk warnings, achieving high accuracy and feasibility [11]. Ghazal et al. proposed a risk matrix-based analysis and evaluation model and provided diverse and specific risk assessment methods for multi-criteria decision fuzzy problems. This method has the potential to effectively assess the degree of risk in complex environments, thereby providing a reliable decision-making basis for decision-makers [12]. Sari et al. proposed a supply chain risk assessment method based on a coordination mechanism. This method provided a reliable measurement basis for the impact of uncertain factors in the market on risk assessment. Its effectiveness in assessing the supply chain risks of NEVs was highly scientific and accurate [13]. Sardar et al. proposed a logistics RAM based on Matter Element Extension (MEE) to optimize supply chain logistics business processes and reduce transportation costs and personnel work efficiency. This model could address nonlinear influencing factors in logistics transportation processes to obtain reliable risk nodes, providing a reference for risk control in physical transportation processes [14]. Li et al. proposed a Bayesian-based RAM that can effectively address the impact of subjective and objective environmental factors to ensure the accuracy of assessment data. This model could be applied to the SCS of Otis Elevator Company to accurately classify risk levels [15].

In conclusion, a variety of risk identification and assessment techniques have been developed for use in Supply Chain Management (SCM) systems. These have contributed to the advancement of SCM, ensuring its continued healthy development [16-17]. However, the accuracy and feasibility of existing NEV SCS risk assessment methods in meeting personalized supply chain needs and considering various complex factors still need to be improved, as shown in Table 1.

This study proposes a risk assessment method for NEVs supply chain based on Hierarchical Holographic Model (HHM) and MEE model. This method helps identify important risk indicators in SCS, and enables weight calculation and priority ranking of indicators to reduce the scope of risk events. Its innovation lies in the combination of HHM and MEE models, which can identify risks in a framework and conduct systematic risk assessment, providing new ideas for NEVs SCM.

Table 1: Summary of related work.

Authors	Method/Model	Key Contributions	Strengths	Limitations	Improvement of the proposed method
Dhruv et al.	Simulation-based business process problem exploration	Avoid risk transfer phenomena	Accurate identification of key risks	May overlook non-linear factors	Consider more complex factors
Sun et al.	Algorithm based on financial and supplier operational risks	Capture risk triggers	Incorporate uncontrollable market factors	Limited adaptability to personalized needs	Provide more personalized solutions
Ge et al.	Supply-demand-based supply chain risk identification model	Analyze the impact of decision preferences on risk	Reverse derivation for optimal solution	Algorithm may be complex	Simplify the assessment process
Patibandla et al.	Overall liquidity index-based evaluation model	Improve risk identification accuracy	Analysis of critical nodes	Logistics characteristics may not be fully considered	Strengthen logistics risk management
Wu et al.	Supplier standard selection-based risk identification model	Provide a foundational framework	Integrated price and quality considerations	Generality needs improvement	Enhance model flexibility

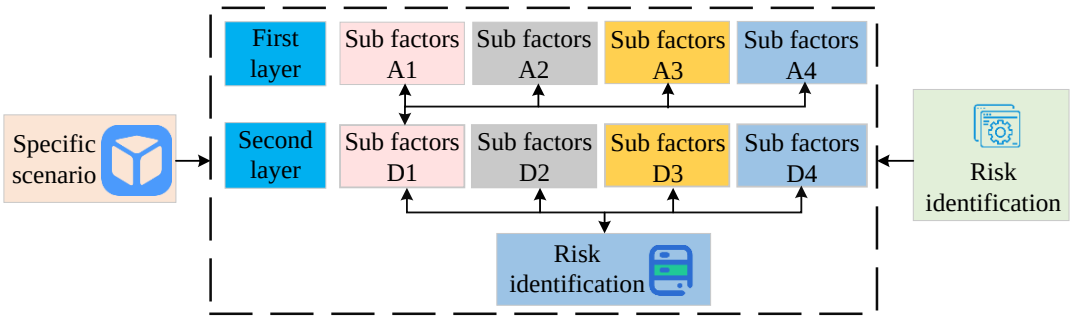


Figure 1: Schematic diagram of HHM risk identification framework.

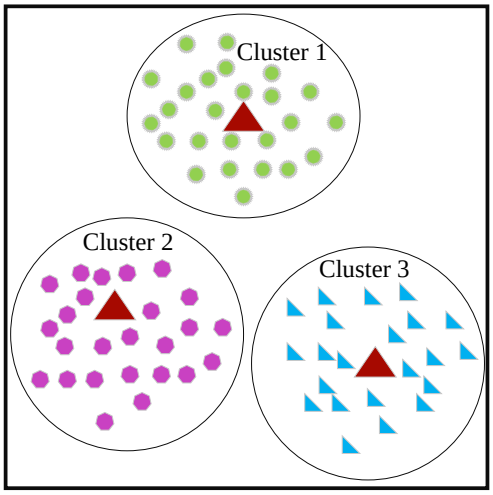


Figure 2: K-means effect diagram.

2 Methods and materials

This section constructs an HHM new energy supply chain risk identification model based on K-means Clustering (K-means), obtains important risk indicators, and further classifies them. Then, an MEE RAM based on a Long Short-Term Memory (LSTM) network is constructed, and the classified indicators are weighted and ranked according to their importance.

2.1 Risk identification model for HHM new energy supply chain based on K-Means

In the process of increasing consumer demand for NEVs, effective management of the NEVs supply chain becomes particularly important [18]. The risk identification of NEVs is the first step in supply chain risk management, which aims to detect risks and classify them for management. The process of NEVs, from raw material procurement to production and sales, is fraught with significant risks. It is therefore essential to implement a systematic and comprehensive method for the effective identification and classification of risks [19]. This study introduces a risk management model based on HHM, aiming to identify global risk factors from different perspectives. Fig.1 is a framework diagram for identifying supply chain risks.

Through the HHM framework, all risks in the process of NEVs from production to sales have been identified, and noteworthy risk factors have been identified. Due to the large number of risk factors involved, these factors need to be further summarized and categorized [20]. This study introduces the K-means algorithm to further mine the supply chain risk data identified by the HHM framework, cluster similar data, and provide important basis for the analysis of risk causes. The principle of K-means for big data is shown in Fig.2.

The first step of HHM is to classify risks from different perspectives, which can be achieved through the K-means algorithm. This algorithm aims to divide the dataset into clusters centered around K by selecting the cluster center K. Before clustering, the data are standardized to ensure that the dimensions of each risk factor data are consistent, as shown in equation (1).

$$z = \frac{x - \mu}{\sigma} \tag{1}$$

In equation (1), z represents the Z-score standardization method. x representing risk factor data. μ is the mean. σ represents standard deviation. After data preprocessing, the process of selection and clustering is continuously repeated to ultimately obtain the best data classification results. The data classification method is shown in equation (2).

$$C_i = \arg\min_j x_i - \mu_j^2 \quad (2)$$

In equation (2), x_i is the training sample of the risk dataset. u_j is a randomly selected cluster center. j is the current number of cluster centers. C_j is the evaluation attribute of the current cluster. To further obtain more representative data classification and obtain the minimum value of the $fitness\left(A[1], A[2], ..., A[n]\right)$ objective function, there is a calculation formula as shown in equation (3).

$$fitness(A[1], A[2], ..., A[n]) = \sum_{1}^{K}\sum_{i}^{N} Dist(x_i^2, C_k^2) \quad (3)$$

In equation (3), K and N are risk datasets selected from two different perspectives. $Dist\left(x_i^2, C_k^2\right)$ is the distance between x_i^2 first level risk indicators and the central point C_k^2. According to the primary indicator attribute C_k^2, the number of risk points x_i^2 under this risk attribute is calculated, and C_k^2 is optimized through the calculation results to converge the objective function to the optimal clustering center [21-22]. By using the K-means algorithm for clustering weights, the dataset is subjected to distance calculation to obtain clustering clusters, as shown in equation (4).

$$\Delta\varepsilon_k = \frac{1}{2m}(w_k \cdot dist(c_k, x))^2 \quad (4)$$

In equation (4), W_k is the weight factor calculated by the algorithm clustering. $\Delta\varepsilon_k$ is the standard deviation for calculating the distance between all data and the center point. Assuming the cluster center attribute target is C_k^3, after k^3 rounds of clustering on the dataset, the distance increment is represented as $\Delta\varepsilon_k$. Following the preliminary risk classification, the second step of the HHM algorithm is initiated. This involves further optimization of the dataset partitioning perspective and the clustering process, with the objective of combining the cross effects between various risk clustering clusters. By combining the K-means algorithm with neural networks, the algorithm learns and clusters data unsupervised, resulting in better clustering centers [24].

The neural network structure can determine the selection of K-means centers through autonomous learning, while avoiding the influence of subjectivity. Therefore, neural networks are used to improve K-means. It takes the shortest distance between the original data and the neurons as the winning distance, and iteratively optimizes and adjusts the weights between all clustering centers and various risk data. The adjustment method is shown in equation (5).

$$y_{ij}(t+1) = y_{ij}(t) + \eta(t, N^0)(x_{kj} - y_{ij}(t)) \quad (5)$$

In equation (5), x_{kj} is the initially selected cluster center point. $y_{ij}(t)$ is the weight of the risk data node at time t. t is the training time of the model. $\eta(t, N)$ is the distance function of the optimal clustering center when the training time reaches t. The distance between each risk data is calculated using the selected best clustering center, as shown in equation (6).

$$d\left(x^0, y^0\right) = \sqrt{\sum_{i^0=1}^{m^0}\left(x_{i^0}{}^0 - y_{i^0}{}^0\right)^2} \quad (6)$$

In equation (6), $x^0 = \left(x_1, x_2, x_3, ..., x_{i^0}{}^0\right)$ and $y^0 = \left(y_1, y_2, y_3, ..., y_{i^0}{}^0\right)$ are the set of cluster centers and the set of data points within the relevant clusters. Among them, i^0 is the dimension in which the current risk data point observation perspective is located. $x_{i^0}{}^0$ and $y_{i^0}{}^0$ are variables in the current dataset dimension. $d\left(a^0, b^0\right)$ is the distance between the data points within the cluster and the cluster center. Different perspectives will lead to different risk factors, and the risk factors from different perspectives are interrelated, intersecting, and overlapping. Therefore, ineffective factors are eliminated through the risk factor identification framework of the HHM.

When the initial dataset has multi-dimensional variables due to different perspectives, its calculation is shown in equation (7).

$$\sum_{X^1} = \frac{1}{k^1}(X^1 - \mu_X)^{T^1}(X^1 - \mu_X) \quad (7)$$

In equation (7), $\sum_{X^1}$ is the covariance matrix of X^1. μ_X is the mean risk point of the X^1 risk dataset. T^1 is the transpose. k^1 is the total number of risk indicators in the dataset. After the eigenvectors of the covariance matrix are rotated, the resulting variance matrix is shown in equation (8).

$$\sum_F = \frac{1}{k^{2T^2}} U(X^2 - \mu_X{}^2)^{T^2} U(X^2 - \mu_X{}^2) = \begin{pmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & \ddots & \\ & & & \sigma_m{}^2 \end{pmatrix} \quad (8)$$

In equation (8), U is the rotation matrix of the risk matrix. The coordinate of rotation matrix U is F. $\sum_F$ is the covariance matrix of the rotation matrix F. $\mu_X{}^2$ is the sample mean of the risk dataset. $\sqrt{\sigma}$ is the variance of the risk indicator. k^2 is the total number of datasets. T^2 is transposed. The improved algorithm distance is shown in equation (9).

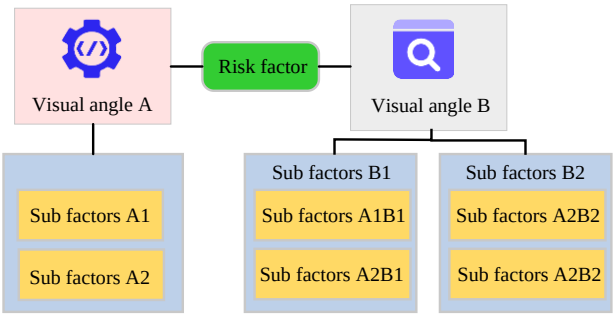


Figure 3: Risk assessment framework.

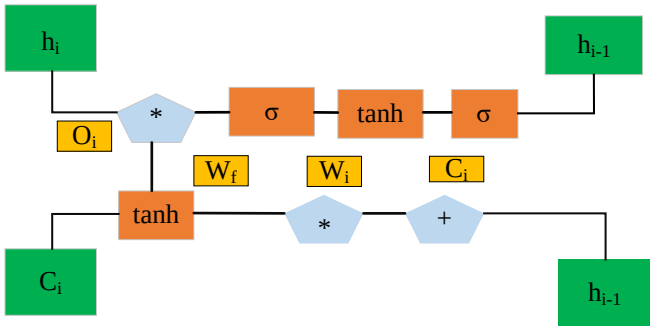


Figure 4: LSTM architecture diagram.

$$d\left(x^5, y^5\right) = \sqrt{\left(x^5 - y^5\right)^{T^5} \sum_{x^5, y^5}^{-1} \left(x^5 - y^5\right)} \quad (9)$$

In equation (9), $x^5 = \left(x_1, x_2, x_3, ..., x_h{}^5\right)$ and $y^5 = \left(y_1, y_2, y_3, ..., y_l{}^5\right)$ are datasets from different perspectives. T^3 is transposed. $\sum_{x^5, y^5}^{-1}$ is the inverse matrix of X^5.

2.2 Construction of MEE RAM combining hybrid weight method

The resolution of important risk identification issues has laid the foundation for the construction of RAMs. The RAM for new energy can effectively judge the degree of risk after identifying it, providing important basis for the formulation of risk solutions. This study proposes the LSTM algorithm, which can avoid the influence of nonlinear factors in the SCM process and has a certain degree of inclusiveness in evaluating missing risk data. Fig.3 shows the risk assessment framework.

In Fig.3, the behavior of the LSTM model is controlled by gates. Its structure mainly consists of three gate gates: forget gate, input gate, and output gate, which can effectively detect the feature sequence of risk data indicators, assign weights to risk indicators, and sort them according to their importance. The LSTM model used in the study consists of two hidden layers, each with 128 hidden units, and is trained using the Adam optimizer. In the data preprocessing stage, the raw data are standardized and the first 80% of the dataset is divided into a training

set and the last 20% as a testing set to address uncertainty in the risk assessment process. Fig.4 shows the structure of LSTM.

Based on the risk identification results of K-means, the classified risk indicators are sorted by their importance to obtain the weights of each indicator. By using gradient descent, the weights and thresholds of the loss function are repeatedly corrected to improve the accuracy of the algorithm, as shown in equation (10).

$$g_t = \frac{w_{t-1} - w_t}{y} \tag{10}$$

In equation (10), weight calculation begins at point $t=1$. w_t and $w_{t\text{-}1}$ are the weight values at times t and t-1. g_t is the gradient. The weight attenuation coefficient of risk assessment indicators is shown in equation (11).

$$\begin{cases} m_t = \varepsilon m_{t-1} + (1-\varepsilon) g_t \\ v_t = \varepsilon v_{t-1} + (1-\varepsilon) g_t^2 \end{cases} \tag{11}$$

In equation (11), m_t and v_t are the first and second momenta. ε is the attenuation coefficient. The calculation steps for weights are as follows: the first is to adaptively adjust the learning rate, and then calculate the difference between the predicted and true values. The loss function is shown in equation (12).

$$\begin{cases} MAE = |G - f(X)| \\ MSE = \sum_n G - f^2(X)) \\ LOG = -\log f(\frac{G}{X}) \end{cases} \tag{12}$$

In equation (12), MAE and MSE are the absolute and mean square values of the loss function. LOG is the logarithmic loss. G is the risk level prediction data output by the function. X is the true data of risk level. The final step in weight calculation is accuracy judgment. If the accuracy does not meet the requirements, it will be recalculated until it converges to the optimal value. To avoid getting stuck in local optima during algorithm training and reduce deep learning time, a topology structure of adding three layers of neural networks to the neural network is used. The establishment of the classical domain is shown in equation (13).

$$R_j = (N_j, C_i^*, V_{ji}) = \begin{bmatrix} N_j, C_1, (a_{j1}, b_{j1}) & \\ C_2, (a_{j2}, b_{j2}) & \\ \cdots & \cdots \\ C_n, (a_{jn}, b_{jn}) & \end{bmatrix} \tag{13}$$

In equation (13), N_j is the risk level. j is the risk indicator to be sorted. C_i^* is the characteristic value of the ranking of various supply chain risk indicators. V_{ji} is the ranking range of risk level characteristic values between indicators j and i. The asymmetric closeness of risk level indicators is shown in equation (14).

$$K_j(N) = 1 - \frac{1}{n(n+1)} \sum_{i=1}^{n} D_{ij} w_i \tag{14}$$

In equation (14), $K_j(N)$ is the closeness between the risk element to be evaluated and the existing risk level. D_{ij} is the distance of the risk indicator. w_i is the comprehensive weight value of each risk indicator. The maximum closeness obtained from the calculation is used as the final output of the MEE RAM, which is the risk assessment indicator of the model. The final risk assessment process is shown in Fig.5.

In Fig.5, the supply chain risk assessment process for NEVs includes risk identification, risk assessment, risk ranking, and final risk indicator output.

3 Results

This section introduces the dataset used for model training and presents the results of risk identification performance testing on the HHM model based on the K-means algorithm.

The results are then compared with the performance of other risk identification algorithms. Subsequently, the LSTM-based MEE RAM is trained on different datasets and its effectiveness is analyzed.

3.1 Performance testing of HHM risk identification model based on K-Means

The experimental platform adopts AMD Ryzen 55600 H with Radeon Graphics, with a main frequency of 3.30 GHz and 16 GB of memory. The dataset is collected from manufacturing, supply, and sales enterprises of NEVs. Data indicators are about the management risks and operational risk factors of the automotive supply chain. To verify the risk identification effectiveness of the K-means-based HHM and its classification performance on risk indicator datasets, three additional clustering algorithms

are used for performance analysis. They include Recent-Frequency-Monetary Clustering (RFM), Particle Swarm Optimization (PSO), and Self-Organizing Map (SOM). The clustering results of each algorithm on the risk indicator datasets of manufacturing, supply, and sales enterprises are shown in Fig.6. In Fig.6 (d), the research algorithm selects cluster centers from three datasets, with data clusters concentrated in [-0.5, 1.5], [2, 4.1], and [0.2,

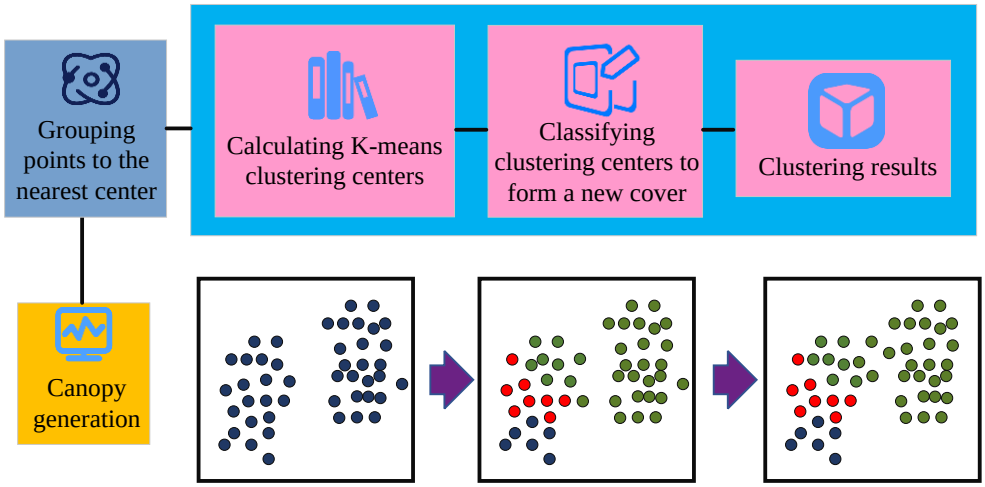


Figure 5: Schematic diagram of RAM structure.

1.8]. The clustering clusters of the comparative algorithm are significantly more dispersed, with an average distance reduction of 1.2%, 1.3%, and 1.5% from each data point to the center point. There are individual data adhesion and excessive dispersion phenomena, with smaller fluctuations and significant differences ($P<0.05$). The research algorithm can effectively cluster different risk assessment indicator datasets and has high reliability and accuracy.

To verify the noise resistance of the proposed HHM risk identification model, the noise processing capability of the K-means algorithm is tested. Dynamic Localized Clustering with Kernel Density Thresholding (DLCKDT), spectral clustering, and the proposed algorithm are tested and compared using 30% and 70% random noise. The Rand index is used as an evaluation indicator, and the results are shown in Fig.7. In Fig.7 (a), when the research algorithm is subjected to a 30% random noise distribution, the Rand index curve consistently remains above the other two clustering algorithms, exhibiting minimal fluctuations, thereby indicating high stability. The Rand index of the DLCKDT and spectral clustering algorithms is, on average, 55% and 41% lower than that of the proposed algorithm. Furthermore, the curve demonstrates a decline following an initial increase, indicating reduced stability with diminished fluctuations and notable discrepancies ($P<0.05$). In Fig.7 (b), at a higher 30% random noise distribution, the Rand indices of all three types show a decreasing trend. However, the Rand curve of the proposed algorithm still performs the best, within the range of [0.65, 0.9], with a fluctuation range 45% smaller than that of the DLCKDT algorithm. The curve of spectral clustering algorithm first increases and then decreases, gradually becoming ineffective. This indicates that the research algorithm has better noise processing capabilities and can maintain high risk identification stability in practical applications.

In NEVs SCM, risk datasets for different business processes are collected, including planning risk, production risk, sales risk, and transportation risk. To verify the accuracy of the research algorithm in risk identification, the algorithm is applied to performance testing and compared with traditional spectral clustering algorithms. The results are shown in Table 2. The research algorithm performs the best in accuracy, recall, and F-measure on different datasets, with each indicator being 9.4%, 8.5%, and 9.6% higher than traditional spectral clustering algorithms, with smaller fluctuations and significant differences ($P<0.05$). The performance test results of the two algorithms remain consistent in each dataset, with a difference of less than 3%. This indicates that the proposed algorithm has high stability, accuracy, and feasibility in practical risk assessment.

3.2 Analysis of the effectiveness of MEE RAM based on LSTM

To verify the learning and practical application effectiveness of the LSTM-based MEE RAM, the model training period is set to 200. The time and effectiveness of risk management are used as

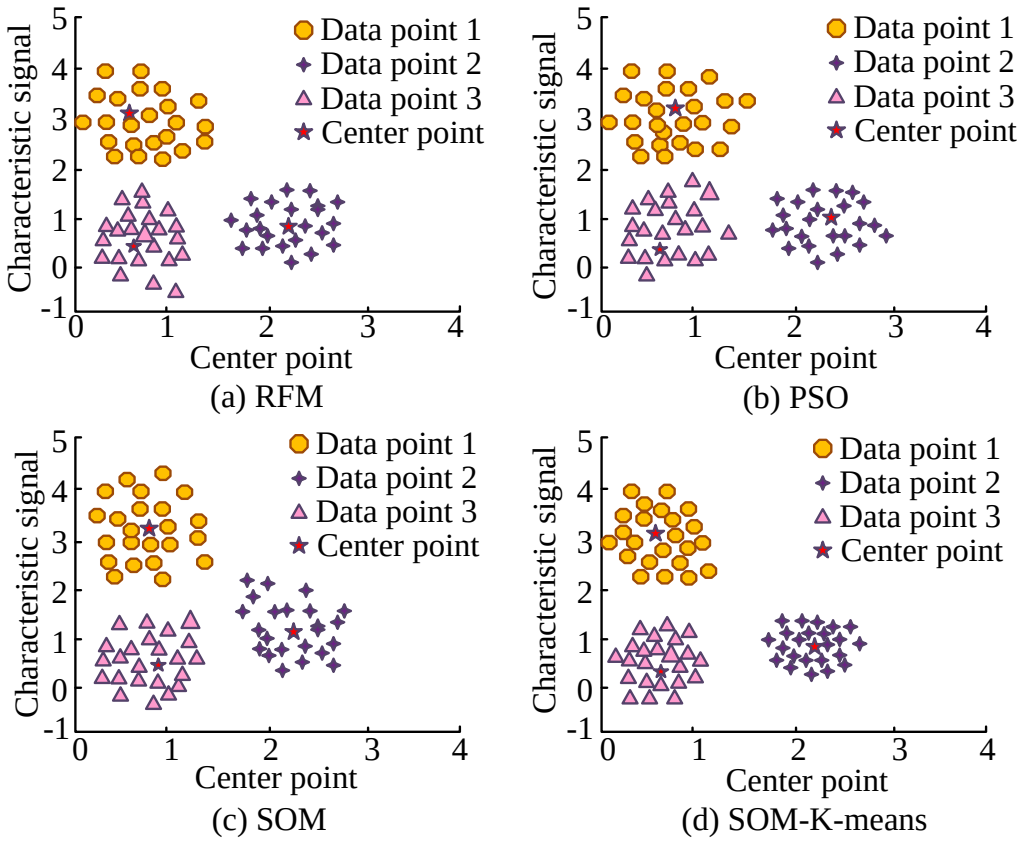
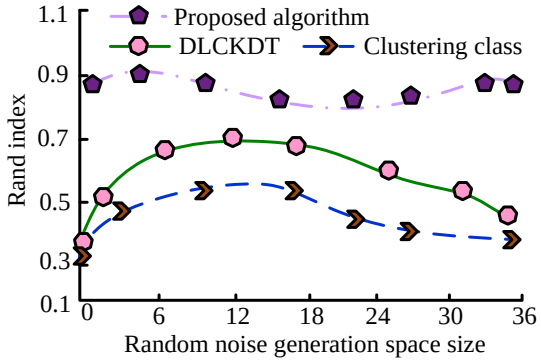
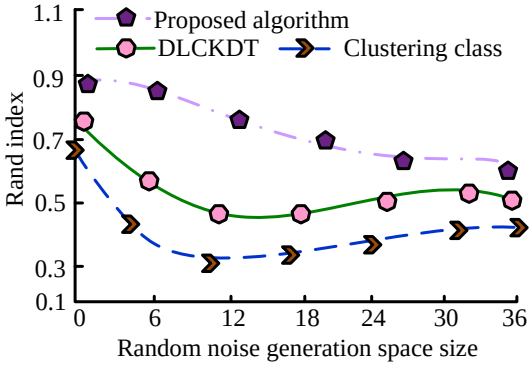


Figure 6: Comparison of the effectiveness of data categorization by algorithms.



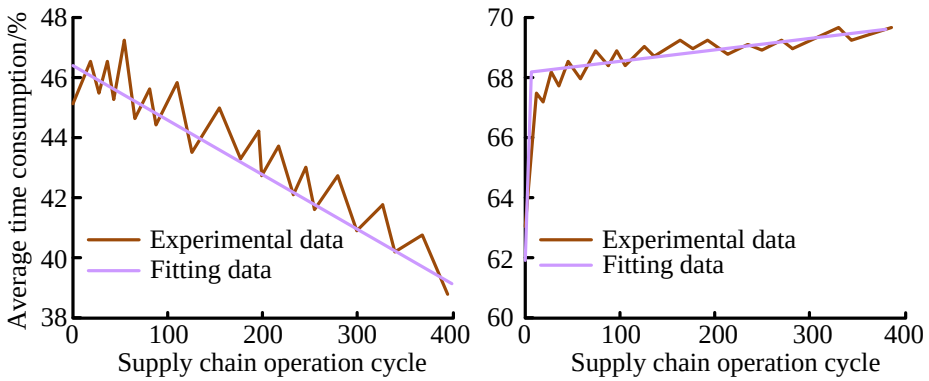
(a) 30% random noise



(b) 70% random noise

Figure 7: Comparison of noise resistance among various algorithms. Table 2: Comparison of testing performance of various algorithms.

Data set	K-means			Spectral clustering algorithm		
	Accuracy	Recall	F-measure	Accuracy	Recall	F-measure
Planning risk	0.74	0.64	0.61	0.64	0.59	0.57
Production risk	0.75	0.68	0.60	0.63	0.60	0.63
Sales risk	0.76	0.67	0.63	0.70	0.61	0.60
Transportation risk	0.81	0.63	0.67	0.73	0.58	0.59



(a) Risk management time consuming (b) Risk management effectiveness

Figure 8: Time and effect curves of the risk of the MEE model.

evaluation indicators for the model, and the results are shown in Fig.8. In Fig.8 (a), as the SCM cycle increases, the RAM shows a gradually decreasing trend in the processing time curve for risks. The management cycle decreases by an average of 23% from 0 to 200, resulting in a decrease in the average processing time of the model, with smaller fluctuations and significant differences ($P<0.05$). In Fig.8 (b), as the SCM cycle increases, the risk management effectiveness of the RAM continues to improve. When the operational management cycle reaches 20, the risk management capability improves the most, increasing by 6%. The proposed model can effectively perform deep learning on risk data, resulting in continuously improving risk management capabilities.

To further validate the research model's ability to handle supply chain risks, the data were collected from January 2022 to December 2023, covering the entire operational cycle of the NEV industry chain. This ensured the timeliness and representativeness of the data. The data come from four primary risk assessment indicators: planning, manufacturing, production, and technology. For each primary indicator, the data contain specific characteristics of multiple risk factors, and the planning indicators include production plan changes and supply plan delay features. Manufacturing indicators include production equipment failure rate and characteristics of raw material supply interruption. Production indicators include production efficiency and product quality qualification rate characteristics. Technical indicators include the cycle of technological innovation and the cost characteristics of technology introduction. Each primary indicator dataset contains 100 data points. Comparing the performance of the autonomous exploration models, as the risk data continue to increase, the processing time curves of each model are displayed in Fig.9. In Fig.9 (a), the risk treatment time curve of the research model shows a continuous downward trend, with a total reduction of 40s in treatment time, and has high stability, with a fluctuation range between [50, 75]. The autonomous exploration model spends an average of 21% more time on risk management than the research model, and the processing time fluctuates greatly, with smaller fluctuations and significant differences ($P<0.05$). Overall, there is no significant improvement. In Figures

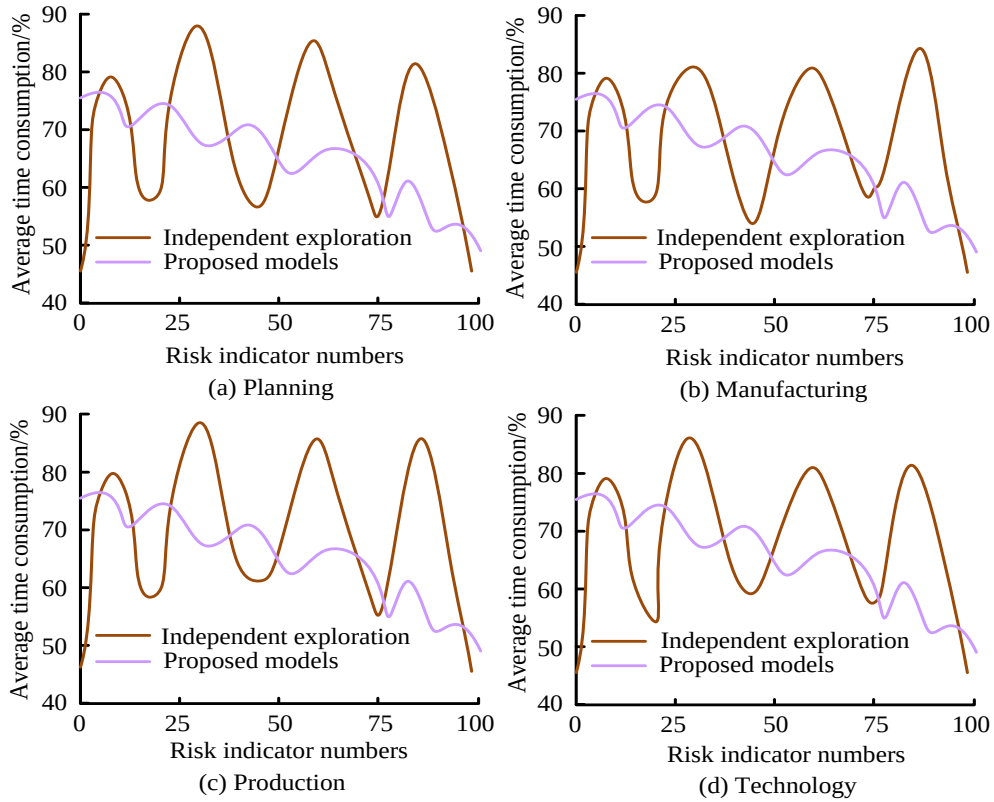


Figure 9: Comparison of risk management effects of different models.

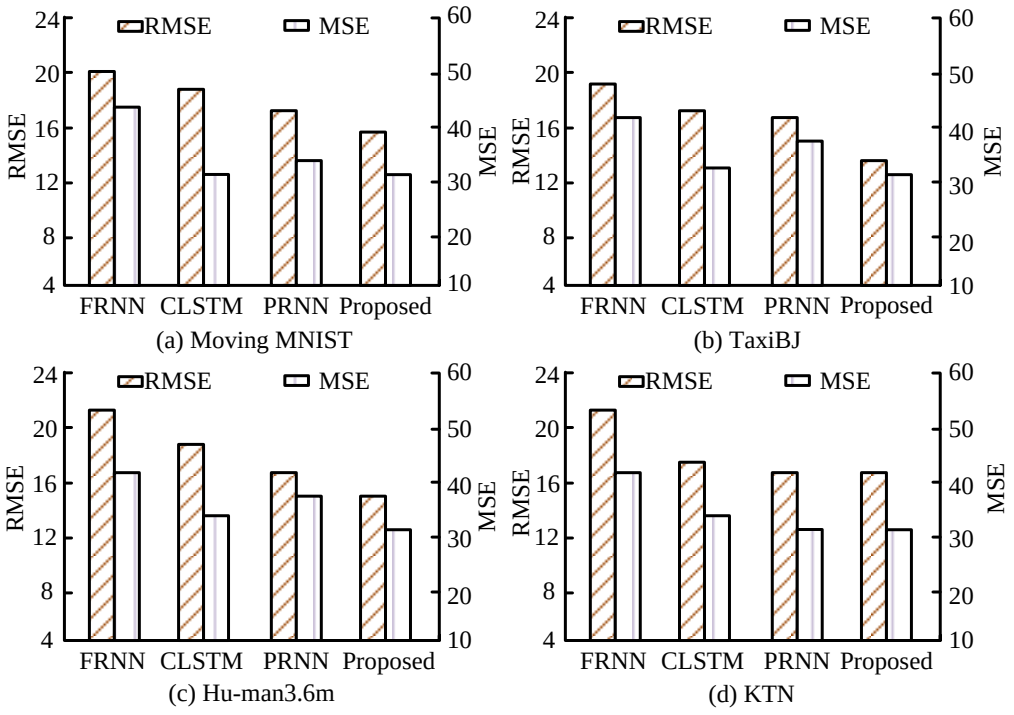
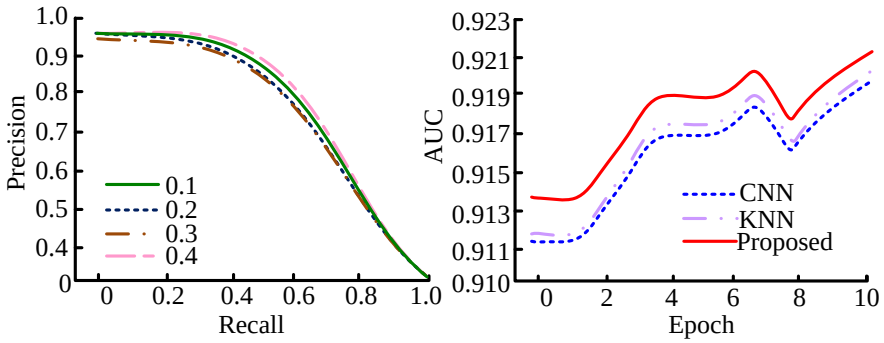


Figure 10: Comparison of detection errors among various algorithms.



(a) PR curve (b) AUC curve

Figure 11: Comparison of prediction performance of various models.

9 (b), (c), and (d), there is no significant change in the processing performance of the two models, and the average data difference is within 5% compared to Fig.9 (a). The research method can effectively enhance the processing capability of supply chain risk assessment indicators and has high stability and accuracy.

To verify the actual evaluation effect of the research model on risk indicators, Root Mean Square Error (RMSE) and Mean Square Error (MSE) are used as evaluation indicators. The research model is applied to the Moving MNIST, TaxiBJ, Hu-man 3.6m, and KTN datasets for testing, and compared and analyzed with models based on other prediction algorithms. The comparison models are Fuzzy Recurrent Neural Network (FRNN), ConvLSTM, and PredRNN algorithms, and the results are shown in Fig.10. Research algorithms have minimum error values in different datasets. Among them, in Fig.10 (a), the RMSE of the research algorithm is 16, which is 3.2%, 2.1%, and 1.5% lower than the FRNN, CLSTM, PRNN, and MIM algorithms. Its MSE is 32, which is 5.8%, 0.7%, and 1.7% lower than the FRNN, ConvLSTM, and PredRNN algorithms, with smaller fluctuations and significant differences ($P<0.05$). In Figures 10 (b), (c), and (d), there is no significant difference in the test data results of each algorithm among the three different datasets, with a difference within 5%. The proposed model has higher accuracy and stability in risk assessment.

To verify the effectiveness and generalization ability of the proposed MEE model, different sampling rates are used to validate its risk assessment performance. Precision-Recall (PR) curve is used as an evaluation indicator. The Area Under the Curve (AUC) during its training process is compared with other CNN and K-Nearest Neighbors (KNN) algorithms, and the results are shown in Fig.11. In Fig.11 (a), the research method has high PR values at different sampling rates, with the best performance observed at sampling rates of 0.1 and 0.4. In Fig.11 (b), as the number of iterations increases, the AUC values of each method show a continuous increasing trend. The average AUC value of the research algorithm is the highest, reaching 0.915, which is 9% and 3% higher than traditional CNN and KNN algorithms, with smaller fluctuations and significant differences ($P<0.05$). Therefore, when studying algorithms for weight calculation and importance ranking of risk indicators, it has high accuracy and reliability.

To verify the universality of the proposed method, two similar algorithms, Random Forest Classifier (RFC) and Naive Bayes Classifier (NBC), are compared, and accuracy, Receiver Operating Characteristic Area under the Curve (AUC-ROC), and processing time are used as evaluation metrics. The results are shown in Table 3. Table 3 shows that the proposed method has the highest accuracy, reaching 97.2%, which is significantly better than the 87.6% and 89.8% of RFC and AUC-ROC, with smaller fluctuations and significant differences ($P<0.05$). The AUC-ROC of the proposed method is 0.921, which is close to 1 and higher than the 0.882 and 0.871 of RFC and AUC-ROC, respectively, with smaller fluctuations and significant differences ($P<0.05$). The proposed method has the shortest processing time, with a reduction of 3.2 and 2.2 on the basis of RFC and AUC-ROC, respectively. The results show that the proposed method exhibits significant superiority in all indicators, is more suitable for handling complex multidimensional data, and has strong universality.

Table 3: Performance comparison of various algorithms.

Algorithm	**Accuracy**	**AUC-ROC**	**Processing Time (s)**
RFC	87.6%	0.882	18.4
AUC-ROC	89.8%	0.871	17.4
Research method	97.2%	0.921	15.2

4 Discussion and conclusion

The SCM of NEVs is crucial for the development of the NEV industry and provides important directions for the transformation and upgrading of the automotive industry. At present, various supply chain RAMs have been proposed. However, in complex and ever-changing environments, many existing methods are difficult to balance the accuracy and real-time performance of the assessment. Therefore, a NEV supply chain risk assessment method based on HHM and MEE models has been proposed, which can effectively globally identify and classify risk factors, and classify and evaluate key risk indicators.

The results indicated that the proposed risk identification model based on HHM had good performance in clustering risk data, with an improvement of 1.2%, 1.3%, and 1.5% compared to the other three clustering algorithms, with significant differences ($P<0.05$). Christie C R et al. proposed a supply chain RAM based on fuzzy comprehensive evaluation. Although the interaction of risk factors was considered, the ability to capture local features was limited when processing complex supply chain data, and the clustering accuracy was poor [23]. The proposed method improved the Rand index by an average of 55% and 41% compared to DLCKDT and spectral clustering algorithms, with smaller fluctuations and significant differences ($P<0.05$). Thesenvitz et al. proposed a supply chain risk identification model based on Analytic Hierarchy Process (AHP), which can analyze the relationship between risk factors at different levels of the supply chain. However, it was sensitive to data noise and had average noise resistance performance [24]. The accuracy of the proposed method was 9.4%, 8.5%, and 9.6% higher than traditional spectral clustering algorithms, with significant differences ($P<0.05$). The average processing time of the proposed MEE model decreased by an average of 23%, and the risk management ability increased by 6%, with significant differences ($P<0.05$). Compared with the independent exploration model, there has been a 21% reduction in time and less volatility in risk management. RMSE and MSE were significantly lower than the other three algorithms by 3.2%, 2.1%, and 1.5% on average ($P<0.05$). Tamsah et al.'s supply chain RAM based on hesitant fuzzy evaluation considers the complexity of the supply chain, but it takes a long time to process large-scale data, making it difficult to meet real-time decision-making requirements [25].

In summary, the proposed NEV supply chain risk assessment method based on HHM and MEE models outperforms existing methods in clustering accuracy, noise resistance, processing efficiency, and error rate. The proposed algorithm has high accuracy and feasibility in risk identification and assessment, and can be effectively used in automotive SCM to obtain a more comprehensive and scientific evaluation method. However, the training process of the proposed algorithm mainly utilizes existing risk factor data. In the development process of NEVs, the scientificity of SCM may also be affected by the emergence of new battery technologies or new market demands. Therefore, predicting new influencing factors and taking preventive measures in advance can be a future development direction.

5 References

[1] Kamar Zekhnini, Anass Cherrafi, Imane Bouhaddou, and Youssef Benghabrit. Jose Arturo Garza-Reyes. Supply chain management 4.0: a literature review and research framework. Benchmarking: An International Journal, 28(2):465-501, 2021. https://doi.org/10.1108/BIJ-04-2020-0156

[2] Matjaž Gams, and Tine Kolenik. Relations between electronics, artificial intelligence and information society through information society rules. Electronics, 10(4):514, 2021. https://doi.org/10.3390/electronics10040514

[3] Nicholas P. Simpson, Katharine J. Mach, Andrew Constable, Jeremy Hess, Ryan Hogarth, and Mark Howden. A framework for complex climate change risk assessment. One Earth, 4(4):489-501, 2021. https://doi.org/10.1016/j.oneear.2021.03.005

[4] Liua B, and Sunb FH. Research on the risk assessment method of PPP project based on the improved matter element model. Scientia Iranica, 27(2):614-624, 2020. https://doi.org/10.24200/SCI.2018.5295.1187

[5] Laura Kaikkonen, Tuuli Parviainen, Mika Rahikainen, Laura Uusitalo, and Annukka Lehikoinen. Bayesian networks in environmental risk assessment: A review. Integrated Environmental Assessment and Management, 17(1):62-78, 2021. https://doi.org/10.1002/ieam.4332

[6] Albert A. Koelmans, Paula E. Redondo-Hasselerharm, Nur Hazimah Mohamed Nor, Vera N. de Ruijter, Svenja M. Mintenig, and Merel Kooi. Risk assessment of microplastic particles. Nature Reviews Materials, 7(2):138-152, 2022. https://doi.org/10.1038/s41578-021-00411-y

[7] Bei Sun, Xudong Liu, Jiayuan Wang, Xuezhe Wei, Hao Yuan, and Haifeng Dai. Short-term performance degradation prediction of a commercial vehicle fuel cell system based on CNN and LSTM hybrid neural network. International Journal of Hydrogen Energy, 48(23):8613-8628, 2023. https://doi.org/10.1016/j.ijhydene.2022.12.005

[8] Qian Ge, Yu Liu, Yinghao Zhao, Yuetian Sun, Lei Zou, Yuxing Chen, and Anqun Pan. Efficient and accurate simrank-based similarity joins: experiments, analysis, and improvement. Proceedings of the VLDB Endowment, 17(4):617-629, 2023. https://doi.org/10.14778/3636218.3636219

[9] R S M Lakshmi Patibandla, and N Veeranjaneyulu. A SimRank based ensemble method for resolving

challenges of partition clustering methods. Journal of Scientific & Industrial Research, 79(4):323-327, 2022. https://doi.org/10.56042/jsir.v79i4.68681

[10] Tianhao Wu, Ji Cheng, Chaorui Zhang, Jianfeng Hou, Gengjian Chen, Zhongyi Huang, Weixi Zhang, Wei Han, and Bo Bai. ClipSim: A GPU-friendly parallel framework for single-source simrank with accuracy guarantee. Proceedings of the ACM on

[11] Weiren Yu, Julie McCann, Chengyuan Zhang, and Hakan Ferhatosmanoglu. Scaling high-quality pairwise link-based similarity retrieval on billion-edge graphs. ACM Transactions on Information Systems (TOIS), 40(4):1-45, 2022. https://doi.org/10.1145/3495209

[12] Taher M. Ghazal. Performances of k-means clustering algorithm with different distance metrics. Management of Data, 1(1):1-26, 2023. https://doi.org/10.1145/3588707
Intelligent Automation & Soft Computing, 30(2):735-742, 2021. https://doi.org/10.32604/iasc.2021.019067

[13] Indah Purnama Sari, Al-Khowarizmi Al-Khowarizmi, and Ismail Hanif Batubara. Cluster analysis using K-Means algorithm and fuzzy C-Means clustering for grou students' abilities in online learning process. Journal of Computer Science. Information Technology and Telecommunication Engineering, 2(1): 139-144. https://doi.org/10.30596/jcositte.v2i1.6504

[14] Tanvir Habib Sardar, and Zahid Ansari. An analysis of distributed document clustering using MapReduce based K-means algorithm. Journal of the Institution of Engineers (India): Series B, 101(6):641-650, 2020. https://doi.org/10.1007/s40031-020-00485-2

[15] Yongyi Li, Zhongqiang Yang, and Kaixu Han. Research on the clustering algorithm of ocean big data based on self-organizing neural network. Computational Intelligence, 36(4):1609-1620, 2020. https://doi.org/10.1111/coin.12299

[16] Mohamed Sakkari, and Mourad Zaied. A convolutional deep self-organizing map feature extraction for machine learning. Multimedia Tools and Applications, 79(27):19451-19470, 2020. https://doi.org/10.1007/s11042-020-08822-9

[17] Xinwang Liu. Simplemkkm: Simple multiple kernel k-means. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(4):5174-5186, 2022. https://doi.org/10.1109/TPAMI.2022.3198638

[18] Zengyi Huang, Haotian Zheng, Chen Li, and Chang Che. Application of machine learning-based k-means clustering for financial fraud detection. Academic Journal of Science and Technology, 10(1):33-39, 2024. https://doi.org/10.54097/74414c90

[19] Sani Saminu, Guizhi Xu, Shuai Zhang, Isselmou Ab El Kader, Hajara Abdulkarim Aliyu, Adamu Halilu Jabire, and Yusuf Kola Ahmed. Applications of artificial intelligence in automatic detection of epileptic seizures using EEG signals: A review. Artificial Intelligence and Applications, 1(1):11-25, 2023. https://doi.org/10.47852/bonviewAIA2202297

[20] Srikanta Pal, Ayush Roy, Shivakumara Palaiahnakote, and Umapada Pal. Adapting a swin transformer for license plate number and text detection in drone images. Artificial Intelligence and Applications, 1(3):145-154, 2023. https://doi.org/10.47852/bonviewAIA3202549

[21] Shen Deng, Siyu Mou, and, Huifang Liu. A comprehensive evaluation framework for China's oil import sustainability with a projection pursuit and matter-element extension model. Energy Sources, Part B: Economics, Planning, and Policy, 16(7):650-668, 2021. https://doi.org/10.1080/15567249.2021.1937402

[22] Jingwei Too, and Abdul Rahim Abdullah. A new and fast rival genetic algorithm for feature selection. The Journal of Supercomputing, 77(3):2844-2874, 2021. https://doi.org/10.1007/s11227-020-03378-9

[23] Christopher R. ChristieLuke E. K. Achenie, and Oluwafemi B. Ayeni. A model-based approach to diagnosing hypercalcemia. Industrial & Engineering Chemistry Research, 62(5):2263-2274, 2023. https://doi.org/10.1021/acs.iecr.3c00051

[24] Jodi Thesenvitz, Shelby Corley, Lana Solberg, and Chris Carvalho. Home health monitoring during the COVID pandemic: Results from a feasibility study in Alberta primary care. Healthcare Management Forum, 35(1):29-34, 2022. https://doi.org/10.1177/08404704211041969

[25] Hasmin Tamsah, and Yusriadi Yusriadi. Quality of agricultural extension on productivity of farmers: Human capital perspective. Uncertain Supply Chain Management, 10(2):625-636, 2022. https://doi.org/10.5267/j.uscm.2021.11.003

Research on Optimal Model Combination of Cross-Border E-Commerce Platform Operation Relying on Robot Hybrid Algorithm

Qiao Zhao
School of Economics and Management, Huanghuai University, Zhumadian, Henan, 463000, China.
E-mail: 20070585@huanghuai.edu.cn

Keywords: CBEC platform, optimal model, platform operation, robot hybrid algorithm, user behaviour

Received: May 29, 2024

Cross-Border E-Commerce (CBEC) has evolved significantly due to the global growth of the Internet, becoming a crucial global market. As e-commerce integrates into daily life and work, the market has transitioned from incremental growth to a more sophisticated landscape. Enhancing user conversion rates is pivotal for retail E-commerce, setting the stage for intense competition among enterprises. The swift evolution of EC has empowered users with information production and self-dissemination capabilities, reshaping traditional production and market response norms. CBEC platforms focus on user-centric operations to align with societal development. This paper explores hybrid algorithms, ultimately selecting the fuzzy analytic hierarchy process for assessing operational performance in CBEC platforms. Finally, this paper conducts empirical research, and the fuzzy comprehensive evaluation score is [82.71 79.95 78.84 79.42 83.35 82.68]. Through the mining and prediction of user consumption behavior data, we can scientifically analyze the platform operation performance, which can find high potential users and conduct accurate operation.

Povzetek: Predlagan je nov model za upravljanje čezmejnih e-trgovinskih platform, ki uporablja robotski hibridni algoritem. Model izboljšuje analizo uporabniškega vedenja ter povečuje konverzijske stopnje in operativno učinkovitost platform.

1 Introduction

Considering the fast proliferation of online users, Internet products emerge in endlessly, which has caused more and more fierce market competition. With the gradual transparency and informatization of business information, CBEC's profit space has been difficult to compare with the original, which requires CBEC to gradually establish a win-win cooperation mechanism [1-3]. Therefore, CBEC needs to continuously improve the optimal combination under different operation modes. With the gradual disappearance of the Internet traffic dividend, the user group needs to be more and more subdivided, which requires improving the user transformation stock market. Therefore, CBEC platforms must establish user thinking, which is a user centered model [4-6]. Through data driven, CBEC platforms can track user needs, which will enable refined user operations.

Pan Yong (2017) has published a paper clearly pointing out that China's CBEC has shown an oligopoly consequence, which is no longer in accordance with the needs of conventional development. Among them, the logistics mode of CBEC in China is mainly "bonded warehouse" and "direct mail", which has also been important expenditure and evidence in many regional practices. However, in practice, some regions still have some unavoidable problems, which are common problems based on China's national conditions, including high dependence on policies, lack of industry norms, lack of competitiveness, etc.

2 Related works

Extensive study has been undertaken in the field of CBEC to better understand the different aspects that influence the industry, including digital technology and customer perceptions, as well as supply chain capabilities and regulatory consequences. This section examines important studies, emphasizing their objectives, techniques, findings, and acknowledged limitations. Examining previous works highlights the strengths and flaws that the proposed study attempts to solve.

Table 1: Overview of related research at CBEC

Reference No	Objective	Methodology	Result	Limitations
[7]	Analyze the role of digital technologies and their abilities in CBEC from an RBV standpoint.	Assessment of 102 Italian enterprises in the design and furniture, fashion, and food and beverage industries.	SMEs efficiently utilize digital technology, and enterprises utilizing an e-commerce manager exhibit a stronger digital export propensity.	Restricted to enterprises in Italy and certain sectors; may not generalize to other environments.
[8]	Assess the effect of customer opinion on intention to buy in CBEC.	Structural equation modeling and intermediate impact assessment	Customer perception, confidence, and attitude have a substantial impact on intent to purchase, with risk impacting these interactions.	Concentrates mainly on customer behavior, without consideration of supply chain factors.
[9]	Determine how CBEC enterprises develop supply chain service skills to enhance the quality of relationships.	Several case study approaches using 41 semi-structured interviews, field visits, and secondary data.	Supply chain resources (data, logistics, and finance) have a vital impact on service capacity and the quality of relationships.	Data is confined to four Chinese CBEC enterprises, with the potential for differing outcomes in different areas or circumstances.
[10]	Examine the impact of the dual circulation policy on CBEC B2B export commerce during COVID-19.	System dynamics modeling and simulation of various policies and combinations.	The regulatory environment is critical for encouraging CBEC B2B exports; infrastructure, government oversight, and enterprise operation are most impacted by policy delays.	Mainly concentrates on the policy impacts in China during COVID-19; may not apply to the post-pandemic setting or other locations.
[11]	Determine key success elements for airports in CBEC logistics.	Literature review, structured interviews with industry actors, and AHP assessment.	Key factors include the capability to pre-clear e-commerce items, high airlift and land capacity, and smooth data sharing.	Particular to the air cargo industry, does not address the broader logistics concerns in CBEC.
[12]	Create an appropriate transportation path model for CBEC during COVID-19 prevention and management.	Evaluation of e-commerce logistics, environmental model, and Dijkstra algorithm for route optimization.	Compared to conventional models, this model offers shorter transportation times and improved search effectiveness.	Concentrates on transportation logistics, without considering other functional components of CBEC.
[13]	Investigate the action method and model of the CBEC	Neural network training on 24 secondary	The green supply chain model greatly enhances	Mainly investigates green supply networks in China's

	green supply chain using customer behavior.	indicators, confirmatory factor evaluation, and assessment of variance.	operational effectiveness and guides efficient profit distribution.	industrial industry, which may not apply to various CBEC scenarios.
[14]	Investigate the balance between supply chain resiliency and susceptibility in CBEC.	Empirical research on the integration of fuzzy AHP and TOPSIS algorithms.	The balance between vulnerability and resilience is crucial for optimum supply chain effectiveness.	Concentrates on the balance state without suggesting specific measures for advancement.

The examined research shed light on numerous aspects of CBEC, including digital technology adoption, customer behavior, supply chain management, legislative implications, and logistical efficiencies. Despite their contributions, many studies have limitations such as geographical focus, sector-specific assessments, and a lack of comprehensive methods to solve larger operational difficulties. The proposed study intends to build on these insights and overcome existing limits by delivering a more holistic and strong approach to improving CBEC operations, eventually establishing itself as a superior solution in the field.

2.1 Relevant theories of CBEC operation mode

2.1.1 Composition of CBEC

The industrial chain of CBEC can be divided into upstream, midstream and downstream. The CBEC platform belongs to the intermediary platform in the midstream [15-17]. Horizontally, the CBEC industry chain is composed of three parts: "operation chain, support chain and service chain" [18-20]. Each part is divided into many categories, and the whole chain tree is closely combined. The CBEC industry chain is shown in Figure 1.

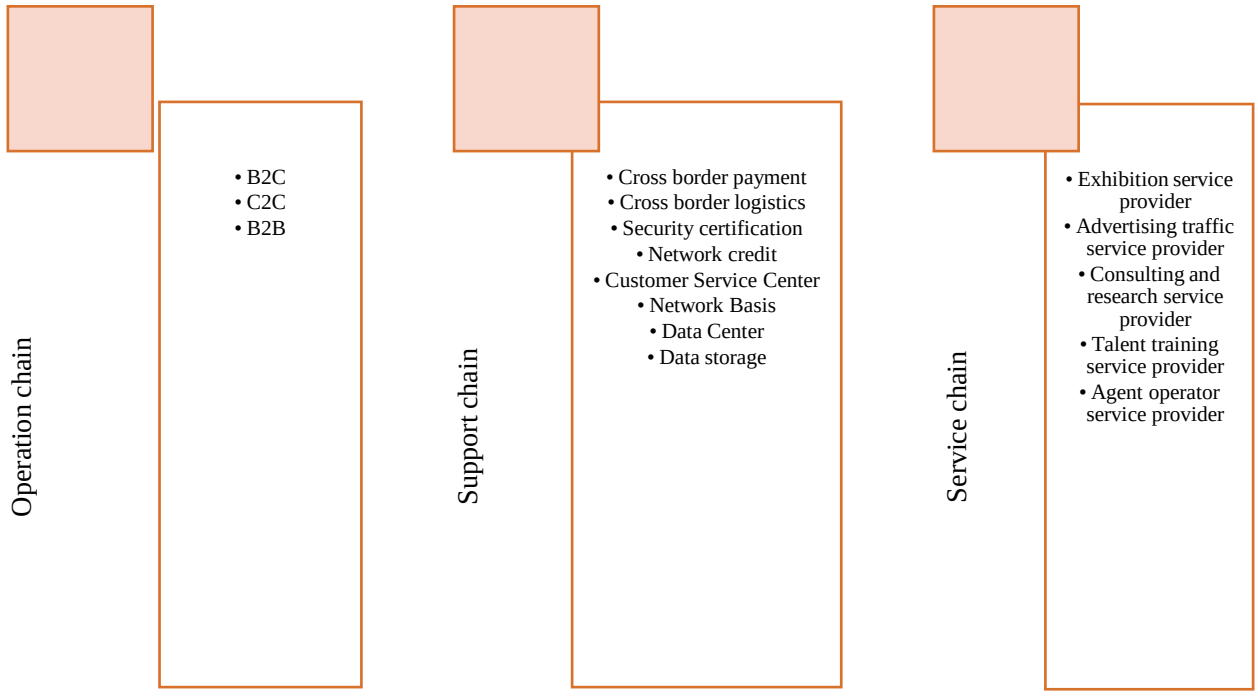


Figure 1: Cross border e-commerce industry chain

2.1.1 Elements of CBEC operation mode

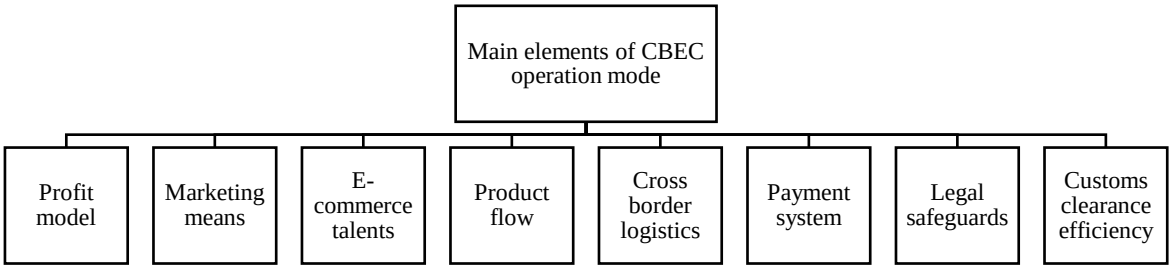


Figure 2: Elements of CBEC operation mode

The traditional operation mode is the main mode of CBEC, which is the main operation mode of EC, including operation process and operation system. Among them, the operation process is a series of business modes of input, transformation and output in CBEC's production and operation. Therefore, we can recognize the operation process of CBEC as the embodiment of labor process and value added [21-22]. However, the operation system is a means to realize CBEC's goods in the process of ownership change, which is an important way in the realization process. Because CBEC is a transnational operation mode, the requirements for the operation mode are higher than those for domestic ECs. Therefore, CBEC needs to constantly improve the level of international logistics transportation, which also needs to increase the security guarantee of payment [23-25]. At the same time, we need to build a comprehensive CBEC operation system, which will comprehensively explore the optimization strategy of CBEC operation mode. This paper constructs the elements of CBEC operation mode, as shown in Figure 2.

2.1.3 Market environment of CBEC platform

In recent years, B2C cross-border EC has a good development trend. At present, China's EC is no longer limited to traditional commodity trading, which has carried out multi-industry integration based on "Internet plus". With the development of "Internet plus", traditional enterprises have gradually reformed with the market prospect, which has initially adapted to the current EC market [26-27]. Regarding the fast expansion of online technologies, short video, live broadcast, knowledge community and other industries have successfully formed typical CBEC with Taobao, JD and Pinduoduo, which has also driven the fast rise of the actual industry. With the development of CBEC, China's industry transformation and upgrading has grown into an essential factor. According to the China CBEC market data report in 2021, the scale of China's CBEC reached 14.2 trillion yuan, which has made

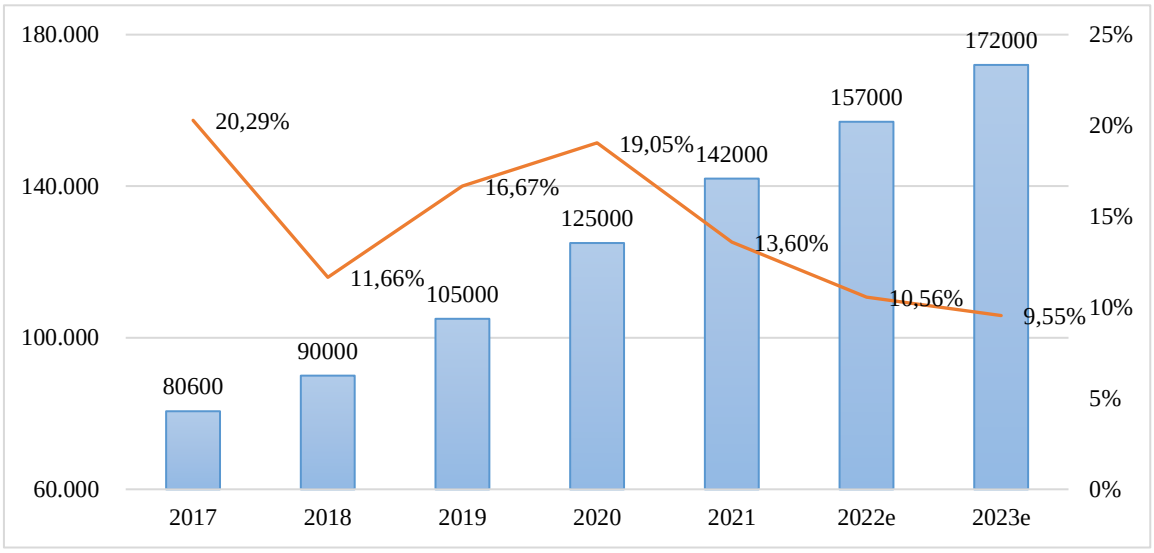


Figure 3: China's CBEC market data and forecast

important progress. In this research forecasts the data in 2022 and 2023 according to the gray prediction GM (1,1) though the Matlab, and the detailed results are shown in Figure 3.

2.2 Performance evaluation method of CBEC platform

Fuzzy analytical hierarchy process: Fuzzy Analytic Hierarchy Process (FAHP) is a new performance analysis theory formed by combining fuzzy analysis method and AHP 50. Professor Saaty's method of quantifying evaluation indicators. FAHP is an analytic hierarchy process with simple calculation and rigorous structure, which is suitable for solving structural decision-making problems. The biggest difference between the basic steps of FAHP and AHP is the improvement of reliability. By comparing the influencing factors, we can determine the importance of the two elements according to the evaluation scale. FAHP can decompose the internal analysis of the objective problem hierarchically, which will form a three-layer network structure, including the objective layer, the criterion layer and the sub criterion layer. FAHP is a way to reflect the performance of the target level through the fuzzy evaluation value of each level, which can be used as the performance evaluation of the fuzzy field.

2.2.1 FAHP model construction

Fuzzy AHP is the improvement of AHP, which can be divided into six steps.

First, determine the overall objective of performance evaluation.

Second, build a multi-level evaluation system. By determining the indicator elements, we can build a multi-level evaluation system model. The model architecture diagram is shown in Figure 4.

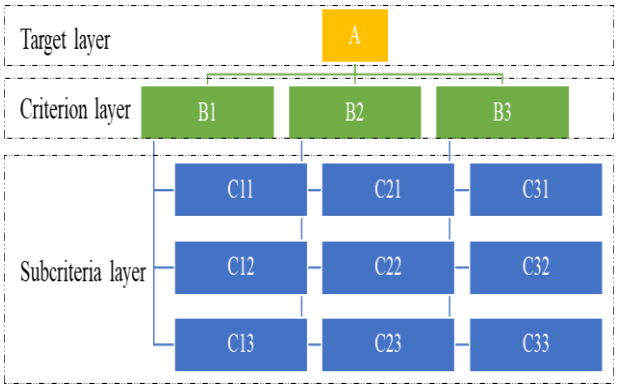


Figure 4: FAHP Model Framework

Third, form a judgment matrix. By comparing the indicator elements in pairs, we can calculate the importance of the corresponding indicator elements. According to the selected scale, we can get the corresponding judgment value. This paper analyzes the $a_1, a_2, ..., a_n$ comparison between the corresponding n elements, as shown in Table 2.

Table 2: Index comparison results

	a_1	a_2	…	a_n
a_1	a_{11}	a_{12}	…	a_{1n}
a_2	a_{21}	a_{22}	…	a_{2n}
…	…	…	…	…
a_n	a_{n1}	a_{n2}	…	a_{n3}

Therefore, we can get the fuzzy matrix of each index of element A, as shown in Formula 1.

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{n1} & a_{n2} & ... & a_{n3} \end{bmatrix} \quad (1)$$

Among them, the importance of index element i to index element j is a_{ij} , it can be concluded that the fuzzy judgment matrix of order n is $(a_{ij})_{n\times n}$, where i and j are arbitrary integers to n.

Fourth, the weight calculation of fuzzy judgment matrix. According to the matrix, we can judge the properties of its matrix, so we can choose the weight calculation method. Among them, the least square method is the most

widely used method for weight calculation. Therefore, the weight calculation formula of the fuzzy judgment matrix is shown in Formula 2.

$$w_i = \left(\sum_{j=1}^{n} a_{ij} + n/2 - 1\right) \Big/ n(n-1) \tag{2}$$

Among them, the importance of index element i to index element j is a_{ij} , w is the weight calculation. Therefore, we can calculate the weight value $W = [w_1, w_2, ...w_n]$ of the elements of this layer relative to the elements of the upper layer. At the same time, $w_{ij} = w_i - w_j + 0.5$.

If the upper element A contains several single factor B, we can get the single factor judgment matrix, as shown in Formula 3.

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{n3} \end{bmatrix} \tag{3}$$

Fifth, consistency inspection. The weight matrix W of fuzzy judgment matrix A shall meet the judgment of formula 4.

$$CI(A,W) = \frac{1}{n^2 \sum_{i=1}^{n} \sum_{j=1}^{n} \left| a_{ij} - w_{ij} \right|} \le a \tag{4}$$

If Formula 4 is satisfied, the consistency check can be passed. The smaller the value of a is, the higher the consistency requirement of the analysis on the fuzzy matrix is. According to the relevant literature, the value of a is usually 0.1.

Sixth, evaluation calculation. Evaluation calculation is a visual evaluation of performance evaluation, which is to find out the main factors affecting performance. If the criterion layer has i layer, the index layer is generally evaluated and calculated first. After obtaining the first level evaluation result C_i of an indicator, we can obtain the evaluation result C of each indicator of the inner layer. The specific evaluation method is shown in Formula 5.

$$Q = \begin{bmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_n \end{bmatrix} = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ q_{n1} & q_{n2} & \cdots & q_{n3} \end{bmatrix} \tag{5}$$

Amongthem, $Q_i = W_i B_i$.

According to the internal evaluation results, we can evaluate the final index factors, as shown in Formula 6.

$$E = WQ = W \begin{bmatrix} W_1 B_1 \\ W_2 B_2 \\ \cdots \\ W_i B_i \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix} \tag{6}$$

Among them, e_n is the final benefit value of the n-th influencing factor, which is the final basis for performance comparison of the evaluation object.

2.3 Construction of performance evaluation system and index screening

The construction of indicator evaluation system is the core part of CBEC operation performance evaluation.

Table 3: Assessment table of evaluation index importance scores

Score	Importance	sketch
1	Extremely unimportant	It will not affect the performance appraisal
2	Unimportance	Less important
3	Commonly	Average impact
4	Important	The impact is relatively large, which is used as the boundary of whether the indicators are included in the evaluation system
5	Very important	Performance appraisal is very important

In this paper, the indicator system is mainly based on the scientific, comprehensive and practical principles to choose the field research model. At the same time, this paper also uses questionnaires to consult experts in the field of CBEC research. At the same time, this paper has

formulated the score of the importance of the evaluation index, as shown in Table 3.

2.4 Screening of CBEC performance evaluation indicators

For this CBEC performance evaluation, 120 questionnaires were issued for expert confirmation, 114 were recovered, and 112 were valid.

The effective questionnaire was treated as invalid when it was sorted out.

The effective questionnaire rate was 93.33%. Through the expert confirmation questionnaire, this paper obtains the scoring statistics table, as shown in Table 4.

Table 4: Scoring statistics of experts selected for evaluation indicators

Target layer	Criterion layer	Sub standard layer	Score
Performance evaluation indicators of CBEC operation A	Basic conditions	Support CBEC policies	4.86
		Modernization level of network facilities	4.72
		Proportion of cross-border online shopping of electronic goods	4.16
		Number of online trading platforms	3.72
	Logistics Huitong	Distribution mode of overseas warehouses	4.35
		Distribution of overseas logistics outlets	4.46
		Cargo tracking capability	4.60
		Diversification of transportation modes	3.28
	Early investment	Overseas land lease investment	4.68
		Overseas channel development cost	4.49
		Overseas recruitment and training expenses	4.35
		Financing costs	3.99
	E-commerce operation	Administrative expenses	4.26
		selling expenses	4.39
		Financial expenses	4.52
		Technical improvement cost	3.14
	Sales link	Revenue growth rate	4.70
		Sales profit margin	4.58
		Return on net assets	3.80
		ROI	4.16
	After-sale service	Customer satisfaction	4.38
		Customer retention rate	4.32
		Transportation damage rate	3.87
		Market influence	4.25

According to the data in Table 4, some scores are lower than 4.00. According to the score requirements for the importance degree of the evaluation indicators in Table 3, we can think that it has not formed a significant impact on the evaluation results of CBEC operation performance. Therefore, this paper believes that relevant options should be eliminated, which can get the final filtering results, as shown in Figure 5.

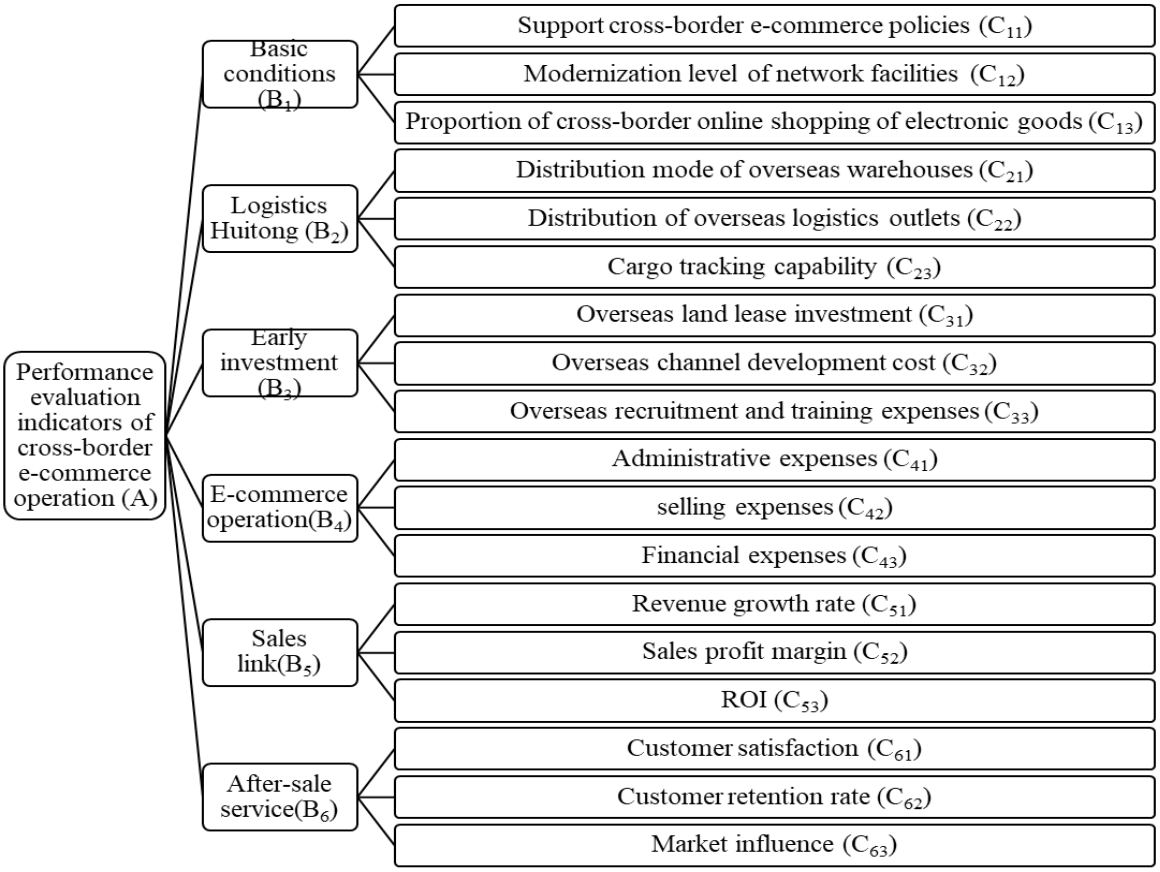


Figure 5: Screening results of CBEC performance evaluation indicators

2.5 Empirical analysis of CBEC platform performance

Data sources: The data collection of this study is divided into two parts. The first part is the construction and weight determination of each evaluation index, and the second part is the field research on CBEC.

First, through the construction of the CBEC operation performance evaluation system, this paper combines the actual research needs to design the index weight questionnaire. At the same time, this paper uses the Delphi method to invite experts to score the index weight. Through the comparison of results, the judgment matrix table is obtained in this paper, as shown below.

$$A=\begin{bmatrix} 1 & 2 & 1/2 & 1/2 & 1/3 & 1/2 \\ 1/2 & 1 & 1/2 & 1/2 & 1/2 & 1 \\ 2 & 2 & 1 & 1/2 & 1/2 & 2 \\ 2 & 2 & 2 & 1 & 1 & 2 \\ 2 & 2 & 2 & 1 & 1 & 3 \\ 2 & 1 & 1/2 & 1/2 & 1/3 & 1 \end{bmatrix} \quad (7)$$

Criterion layer index: Using MATLAB software, this paper calculates the eigenvector of matrix index. Through Formula 2, we can obtain the corresponding weights of the six indicators of this layer. At the same time, according to Formula 4, we can calculate the CI value of the consistency check of the matrix. The specific results are shown in Table 5.

Table 5: Criterion layer index weight result

Criterion layer	Feature vector	Weight value	CI
Basic conditions (B_1)	0.66	10.1%	0.037
Logistics Huitong (B_2)	0.63	9.6%	
Early investment (B_3)	1.12	17.1%	
E-commerce operation (B_4)	1.59	24.2%	
Sales link (B_5)	1.82	27.7%	
After-sale service (B_6)	0.74	11.3%	

When the CI value is less than 0.1, we can judge that the matrix can pass the consistency test, which can judge that the result is acceptable. Therefore, we can get the weight result, as shown in the matrix results below.

$$w = [0.101 \quad 0.096 \quad 0.171 \quad 0.242 \quad 0.277 \quad 0.113] \tag{8}$$

Through the above method, this paper can calculate the weight of each indicator in the whole CBEC operation evaluation indicator system w_i, as shown in the matrix results below.

$$\begin{aligned} w_1 &= [0.542 \quad 0.317 \quad 0.141] \\ w_2 &= [0.365 \quad 0.243 \quad 0.392] \\ w_3 &= [0.581 \quad 0.262 \quad 0.156] \\ w_4 &= [0.515 \quad 0.252 \quad 0.233] \\ w_5 &= [0.503 \quad 0.325 \quad 0.173] \\ w_6 &= [0.371 \quad 0.449 \quad 0.180] \end{aligned} \tag{9}$$

So, we ca get the corresponding weight set w, as shown in the matrix results below.

$$w = \begin{bmatrix} 0.542 & 0.317 & 0.141 \\ 0.365 & 0.243 & 0.392 \\ 0.581 & 0.262 & 0.156 \\ 0.515 & 0.252 & 0.233 \\ 0.503 & 0.325 & 0.173 \\ 0.371 & 0.449 & 0.180 \end{bmatrix} \tag{10}$$

Score of comprehensive performance evaluation: According to the fuzzy comprehensive evaluation of the sub criteria layer, the fuzzy judgment matrix Q of the above six indicators can be obtained in this paper, which can calculate the evaluation value of the single factor of the criteria layer, as shown in the matrix results below.

$$Q_1 = \begin{bmatrix} 0.341 & 0.185 & 0.236 & 0.207 & 0.031 \\ 0.283 & 0.325 & 0.223 & 0.119 & 0.050 \\ 0.113 & 0.125 & 0.173 & 0.441 & 0.147 \end{bmatrix} \tag{11}$$

$$Q_2 = \begin{bmatrix} 0.066 & 0.254 & 0.549 & 0.081 & 0.050 \\ 0.118 & 0.110 & 0.203 & 0.457 & 0.112 \\ 0.052 & 0.129 & 0.166 & 0.519 & 0.135 \end{bmatrix} \tag{12}$$

$$Q_3 = \begin{bmatrix} 0.076 & 0.227 & 0.548 & 0.093 & 0.056 \\ 0.052 & 0.172 & 0.684 & 0.077 & 0.015 \\ 0.080 & 0.138 & 0.121 & 0.471 & 0.190 \end{bmatrix} \tag{13}$$

$$Q_4 = \begin{bmatrix} 0.025 & 0.114 & 0.391 & 0.347 & 0.123 \\ 0.047 & 0.114 & 0.575 & 0.175 & 0.088 \\ 0.033 & 0.148 & 0.291 & 0.470 & 0.058 \end{bmatrix} \tag{14}$$

$$Q_5 = \begin{bmatrix} 0.196 & 0.403 & 0.305 & 0.046 & 0.050 \\ 0.234 & 0.329 & 0.310 & 0.099 & 0.029 \\ 0.028 & 0.115 & 0.470 & 0.308 & 0.078 \end{bmatrix} \tag{15}$$

$$Q_6 = \begin{bmatrix} 0.170 & 0.110 & 0.356 & 0.304 & 0.060 \\ 0.141 & 0.440 & 0.361 & 0.053 & 0.006 \\ 0.158 & 0.453 & 0.336 & 0.004 & 0.050 \end{bmatrix} \tag{16}$$

Therefore, we can calculate the fuzzy evaluation value of the single factor basic conditions of the criterion layer, as shown in the matrix below.

$$E = WQ = W\begin{bmatrix} Q_1 \\ Q_2 \\ \cdots \\ Q_n \end{bmatrix} = \begin{bmatrix} 0.235 & 0.209 & 0.210 & 0.286 & 0.061 \\ 0.075 & 0.201 & 0.418 & 0.258 & 0.048 \\ 0.055 & 0.150 & 0.498 & 0.218 & 0.079 \\ 0.038 & 0.234 & 0.396 & 0.294 & 0.037 \\ 0.146 & 0.296 & 0.345 & 0.173 & 0.040 \\ 0.114 & 0.296 & 0.364 & 0.198 & 0.028 \end{bmatrix} \quad (17)$$

According to the questionnaire, this paper develops the score of the comment set, as shown in T. Among them, T={Excellent, good, average, poor}. At the same time, we assign T, T=[100 90 80 70 60].

$$M = ET = \begin{bmatrix} E_1 \\ E_2 \\ \cdots \\ E_6 \end{bmatrix} T = \begin{bmatrix} 0.235 & 0.209 & 0.210 & 0.286 & 0.061 \\ 0.075 & 0.201 & 0.418 & 0.258 & 0.048 \\ 0.055 & 0.150 & 0.498 & 0.218 & 0.079 \\ 0.038 & 0.234 & 0.396 & 0.294 & 0.037 \\ 0.146 & 0.296 & 0.345 & 0.173 & 0.040 \\ 0.114 & 0.296 & 0.364 & 0.198 & 0.028 \end{bmatrix} \times \begin{bmatrix} 100 & 90 & 80 & 70 & 60 \end{bmatrix} = \begin{bmatrix} 82.71 \\ 79.95 \\ 78.84 \\ 79.42 \\ 83.35 \\ 82.68 \end{bmatrix} \quad (18)$$

He distribution of fuzzy comprehensive evaluation scores is relatively centralized, which indicates that all indicators are at the edge of a good state, and the development level of each stage is relatively balanced. Based on the empirical results and specific comprehensive evaluation values, this paper draws the overall performance results of the evaluation system, as shown in Figure 6.

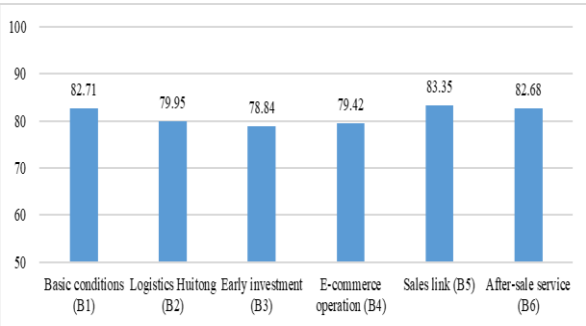


Figure 6: Overall performance results of the evaluation system

2.6 Optimization of CBEC operation mode

Expand product flow: The development of CBEC has a high demand on the product supply chain, which requires the platform to cover multiple high-quality goods. At the same time, e-commerce platforms should have various basic information about products, which will be more convenient for consumers to search. By listing the product categories and comparing the prices, the platform can provide consumers with choices, which can also standardize the launch and promotion of products. The domestic manufacturers of imported substitutes have a certain stimulating effect, which does not constitute the main factor but assists in enhancing national manufacturing structures through supply side reform. Therefore, expanding the product Circulation will be an advantageous factor in guiding and benefiting the enlargement of global free trade. At the same time, the platform should be strictly audited when merchants enter, which requires improving the basic information of commodities, including information overview, sales volume, popularity and collections. At the same time, the platform side should give more consideration to how to improve the customer price, the number of orders placed by platform users and the frequency of purchase, which become the key factors that need to be paid attention to in platform operation.

Improve platform user loyalty: In the CBEC mode, imported overseas goods reduce the cost of intermediaries to a certain extent, which is lower than the price of retail goods imported through traditional channels. Therefore, many people have become CBEC customers, which can be purchased through import platforms. Therefore, the price of imported goods is an important factor affecting the operation of CBEC import platforms, which will have far-reaching effects for owners of platforms. While doing so, the decline in the price of a single commodity will reduce the transaction amount of the platform operation, which requires the platform to consider how to improve the customer unit price, order quantity and purchase frequency. However, with the rapid development of CBEC import platform operation, competition will become increasingly fierce. Therefore, the commodity advantages of CBEC import will gradually disappear in the future, which requires accurate grasp of consumer demand. By improving consumers' loyalty to the platform, the platform can lock in loyal users. Therefore, the platform operator should strengthen the rights and interests of application platform members, which can improve the loyalty of platform users.

Improve and optimize the logistics system: The development of CBEC has had a great impact on cross-border logistics. The lagging development of logistics will greatly limit the development of CBEC, which requires us to constantly improve the cross-border logistics system. First of all, the Chinese government should support and introduce policy support to optimize logistics, which can attract more capital investment.

Through communication with foreign governments, we can jointly formulate bilateral strategies that encourage the growth of international supply chain management, which can make it easier for capital forces to build infrastructure. Second, cross-border logistics enterprises should follow the development of art and machinery, which requires the construction of cross-border logistics information based on Internet technology. Through computer technology, cross-border logistics enterprises can strengthen the development of logistics system, which can continuously transmit information in the operation process. By building an information-based logistics system, CBEC can reflect the process of receipt, transportation, warehousing, settlement, etc. in real time, which will directly reflect the operation capability of the platform. Third, CBEC develops overseas warehousing business, which can not only expand business, but also reduce transportation costs. Through the rational use of overseas warehouses, CBEC can effectively shorten the delivery time, which can not only improve customer satisfaction, but also deal with customer returns and exchange.

Strengthen the cultivation of CBEC talents: Cross border e-commerce is a new industry. Therefore, the lack of talents has emerged as a crucial method for restrict the development of CBEC. We can cultivate CBEC talents in the following ways. First, the government should strengthen the CBEC talent training program. By designating CBEC training institutions, relevant units can carry out large-scale CBEC training, which can improve talent training. Second, all kinds of training institutions should increase their investment in training CBEC talents, which can be carried out through a variety of training or activities, including knowledge, skills, business, service competitions, etc. Third, CBEC enterprises should increase publicity, which can better obtain the recognition of talents participating in CBEC. a lot of universities and colleges in China have set up e-commerce talent training courses, and these talents have mastered basic e-commerce theoretical knowledge after completing their professional studies. Targeted training of professional agricultural e-commerce talents can shorten the time of on-the-job training of enterprises, which will reduce the trial and error cost of personnel training. Fourth, relevant practitioners should strengthen the cultivation of knowledge and ability, which can continuously strengthen personal quality. The premise of talent return is to improve the follow-up security, and it can only become a reality after cutting off all the life concerns of the outflow talents.

Solve the problem of tax refund: Improving the export tax rebate policy will directly affect the operation and development of CBEC enterprises. By combining preferential tax policies with CBEC operations, CBEC enterprises can effectively reduce costs, which can also promote industrial transformation and upgrading. First, the General Administration of Customs of China should give full play to its regulatory advantages over bonded areas. Through communication and cooperation with CBEC enterprises, China can allow CBEC enterprises to import commodities in bulk into bonded warehouses for storage. Second, customs clearance is carried out after sales on the CBEC platform, which reduces the logistics cost of cross-border goods. By shortening the logistics time of goods, we can enable consumers to receive goods more quickly. Third, establish a green channel for cross-border direct purchase, which can provide consumers with a high-quality online shopping environment. Through the green channel, we can make tax collection and supervision faster.

Establish and improve the credit system: CBEC is a virtual shopping mode based on the Internet, which is a consumption situation based on the credit system. Therefore, CBEC's credit rating is a model based on consumers' trust in the platform, which is an important key standard for consumers to choose. Therefore, CBEC has high requirements for proprietary goods, mainly to maintain consumers' trust in the platform. Therefore, the platform will conduct credit rating on merchants, which is a mode to reduce the number of customers entering the platform. Through credit evaluation, CBEC can strengthen the construction of credit system. At the same time, CBEC will regularly maintain the development of enterprises according to the credit level of the merchants, which will regularly release blacklists, enterprise certification, payment information, etc. For the operation of CBEC import platform, government biggest influence comes from policy. Through the improvement and accumulation of experience in the pilot practice, it can be concluded that the regulatory policy is more consistent with the applicable scenario of CBEC imported goods. CBEC shall jointly establish a public information service platform to release CBEC's identity information, commodity information and commodity logistics information., Similarly, we will greatly stimulate market confidence and promote the follow-up action of the capital market. At the same time, CBEC can conduct more scientific information investigation and management system by establishing a third-party credit system. Consumers can check the credit of various businesses on CBEC, which will become an important guarantee for consumption.

Improve third-party payment: CBEC trading is a kind of commodity trading behavior based on the Internet. Therefore, online payment is an indispensable part of CBEC transactions, which is an important part of commodity exchange. Online payment is an Internet finance, which needs to ensure the security of online payment. This can be done through the following steps. First, financial institutions vigorously support third-party payment, which can make it safer for Bianjie2 to carry out cross-border payment business. Through various financial means, CBEC can enhance electronic payment for cross-border business.

Statistical analysis

The study that evaluated tailored support networks and treatments for teenage mental health in the context of the COVID-19 pandemic's educational effects included Analysis of Variance (ANOVA) techniques, which is indicative of a more general shift in research approaches. This is demonstrated by the equation (19) that governs the Research on E-Commerce Platform Operations that Leverage an Optimal Model Hybridization of Robots, where creative solutions are being investigated to adjust to the changing educational environment following the global health crisis.

$$\begin{cases} N: \mu_1 = \mu_2 = \cdots . = \mu_o \\ N_1: \mu_1 \neq \mu_2 \neq \cdots . \neq \mu_o \end{cases} \quad (19)$$

The ANOVA is used to divide the variance of all data into two groups: within-group variance and between-group variance.

$$SST = SSB + SSW \quad (20)$$

Calculating SSB involves:

$$SSB = \frac{1}{O-1} \sum_{m=1}^{O} c_m (t_m - \bar{t})^2 \quad (21)$$

Here, v_z define the number of samples of cluster z_{th}represents the cluster's mean, and $\bar{y}$ represents the cluster's average.

$$SSW = \frac{1}{(o-1)y} \sum_{m=1}^{o} \left(\sum_{a=1}^{y} \left(t_{m,a} - t_m \right)^2 \right) \quad (22)$$

Equation (23) describes how the F-statistic is created to test the hypothesis, where $y_{z,s}$denotes the s_{th} sample of the z_{th} group.

$$K = \frac{SSB}{SSW} \quad (23)$$

The two-way analysis of variance (ANOVA) was used for statistical analysis within the context of the research on the Best Models to Use Together for an E-Commerce Platform on a Global Scale a Robot Hybrid Algorithm, with the level of significance set at $P = 0.04$. Users just need to look at the mean and standard deviation (SD) values to see how effective the recommended algorithm is in forecasting the behaviour of teenagers.

3 Discussion

The study uses a robotic technology in cross-border e-commerce platforms reveals the varying opinions from international and local authors. Although 70% of respondents reported success incorporating robotic technology, 30% voiced misgivings, believing that the procedures in place are already effective without it. This highlights the need for considering diverse perspectives when assessing the collision of technology on e-commerce. International authors highlight the challenges of adjusting and the need for ongoing technological adaptability, while local authors focus on legal frameworks, data privacy, security, and potential worker displacement. A comprehensive strategy is essential for sustainable and ethical use of robotic technology, considering both technical advancements and social ramifications. The study provides valuable insights into robotic technology and the best mix of models for running an international online store using a Robot Hybrid Algorithm. However, the study's limitations, such as the need for further exploration into specific challenges and ethical considerations, warrant careful consideration in future research and policy development.

4 Conclusion

As the web evolves, we have entered a new era; the market in all directions is gradually saturated. Users have become the resources that enterprises are competing for. The importance of user growth is growing. The operation mode of CBEC serves a critical part in CBEC's growth as a company. In light of past purchasing patterns of some users of a famous domestic e-commerce platform, a set of performance algorithm for the optimal model of CBEC platform operation with robot hybrid algorithm is built. This research has developed a new e-commerce evaluation index system for new agricultural operators, and completed e-commerce performance evaluation using the index system. Finally, this paper conducts empirical research, and the score of fuzzy comprehensive evaluation is [82.71 79.95 78.84 79.42 83.35 82.68]. Through the mining and prediction of user consumption behavior data, we can scientifically analyze the platform operation performance, which can find high potential users and conduct accurate operation. The results of our study indicate that successful robotic technology integration in international online marketplaces is viewed favorably. however, the varied viewpoints and limitations highlight the need for a comprehensive and nuanced approach that takes into account both ethical and technical challenges in order to promote sustainable and ethical advancement in this ever-changing landscape.

Data availability

All data are included within the article.

Conflicts of interest

The authors declare no conflicts of interest.

Funding statement

(1) Soft science research program of Henan Province in 2019, research on rural e-commerce poverty alleviation in Henan Province, 192400410215.
(2) Research project of Humanities and social sciences of Henan Provincial Department of education in 2020, research on Influencing Factors of e-commerce development of agricultural products in Henan Province, 2020-ZDJH-224.
(3) Zhumadian philosophy and social science planning project, research on the path of rural e-commerce Promoting Rural Revitalization in the post poverty era, 21L007.
Thank these projects for supporting this article!

References

[1] Wang B. 2022. Research on the reform of CBEC talent training in higher vocational education under the+X certificate system [J*]. Journal of Nanjing Open University*, (03): 56-62 https://doi.org/10.23977/avte.2023.050212
[2] Ouyang Y, 2022.Exploration on the integration of ideological and political concepts into CBEC English teaching in higher vocational education [J]. *Journal of Hubei Open Vocational College*, 35 (17): 160-162https://doi.org/10.24294/ijmss.v6i2.2413
[3] Ge D, 2022. Research on Demand Analysis and Training Policy of Cross border E-commerce Talents in the Context of Mass Entrepreneurship and Innovation [J]. *Jiangsu Business Review*, (09): 14-16. 10.4236/oalib.1109725
[4] Gao Si, 2022. The current situation, problems and opportunities faced by CBEC enterprises in the new era [J]. *Marketing of time-honored brands*, (15): 104-106 10.4018/IJEEI.2019010103
[5] Peng Y.P, 2022. Analysis on the development and operation mode of CBEC platform in Southeast Asia -- taking SHOPEE as an example [J]. *Mall Modernization,* (11): 34-36. 10.1145/3226116.3226138
[6] Chen Y., 2022. Research on the Training Mode of Business English Professionals in the Background of Cross border E-commerce [J]. *Journal of Hubei Open Vocational College*, 35 (10): 191-192 https://doi.org/10.47297/wspiedwsp2516-250001.20210510
[7] Luo B.J., 2022. Research on the Sustainable Reform of Cross border E-commerce Courses in the Context of "1+X" Certificate [J]. *Science and Technology Economic Market, (*05): 142-144. https://doi.org/10.1051/shsconf/202315301019
[8] Jiang T., 2022. Research on Suzhou CBEC operation teaching mode in the context of RCEP [J]. *China Management Informatization,* 25 (09): 203-206 https://doi.org/10.61360/bonicetr242016230502
[9] Xu S., 2022. Research on the monitoring process of CBEC import products based on multi sectoral cooperation [J]. *Standard Science,* (04): 65-69 10.1371/journal.pone.0304393
[10] Zhang H., 2022. Construction and practice of CBEC professional talent training mode in higher vocational colleges under the+X certificate system [J]. *Vocational and Technical Education*,43 (11): 17-21 10.23977/avte.2023.051113
[11] Huang R., 2022. Research on the training path of CBEC application-oriented undergraduate talents in international trade [J]. *Taiwan Strait Technology and Industry,* 35 (02): 36-38 10.23977/jhrd.2024.060208
[12] Zhou T., 2022. Countermeasures for Export Cross border E-Commerce under the Background of Amazon Store Closing Tide [J*]. Enterprise Management*, (01): 120-123 https://doi.org/10.2991/assehr.k.210407.188
[13] Wei H., 2021. Problems and Countermeasures in the Development of China's Cross border E-commerce Import [J]. *International Trade,* (11): 44-50+69 10.2991/assehr.k.211209.442
[14] Xu D., 2021. Research on the integration of CBEC and domestic sales of small and medium-sized foreign trade enterprises in Quanzhou -- under the background of the prevention and control of the new crown epidemic [J]. *North Economic and Trade*, (11): 24-27 https://doi.org/10.47297/wspciwsp2516-252706.20200411
[15] Hua G., 2021. A brief analysis of the development opportunities and strategies of small and medium-sized CBEC enterprises in Yiwu in the post epidemic era [J]. *Management and Technology of Small and Medium sized Enterprises* (Mid term), (11): 168-170 https://doi.org/10.54691/bcpbm.v37i.3542
[16] Yang S., 2021. Research on the curriculum reform of CBEC application-oriented talents training for international trade majors based on the employment market demand of Guangdong Hong Kong Macao Greater Bay Area [J]. *Research on Industrial Innovation,* (19): 163-165 https://doi.org/10.38007/proceedings.0000958
[17] Chen J., 2021. Research on the Construction of Cross border E-commerce Specialty Groups and Curriculum System in Higher Vocational Colleges under the Background of "Double High Construction" [J]. *The Age of Wealth*, (09): 115-118

https://doi.org/10.2991/iserss-19.2019.220
[18] Xiao Y.Z., 2021. Empirical Study on the Influencing Factors of the Explicit Service Quality and Efficiency of Cross border E-commerce Logistics [J]. *Business Economics Research*, (16): 108-111 https://doi.org/10.3233/atde231333
[19] Chen J., 2021. Training of new foreign trade talents in vocational colleges under the background of CBEC [J]. *Hebei Vocational Education*, 5 (04): 33-37 https://doi.org/10.1109/icsgea53208.2021.00081
[20] Jiang Y., 2021 Opportunities, Challenges and Countermeasures for the Development of Sino Russian Cross Border E-commerce under the Background of the "Belt and Road" [J]. *Eurasian Economy,* (04): 102-124+126 https://doi.org/10.25236/icidel.2017.046
[21] Zhu Y., 2021. The status quo, model and optimization of CBEC -- take Wenzhou Jiabo Crafts Co., Ltd. as an example [J]. *North Economic and Trade,* (08): 27-30 https://doi.org/10.1109/icemme49371.2019.00133
[22] Qiao L., 2021. Research on Problems and Countermeasures of Hainan Agricultural Products Cross border E-commerce Development [J]. *Marketing Circle*, (30): 13-14 https://doi.org/10.7753/ijsea1202.1036
[23] Cai H., 2021. Analysis of factors affecting the operation of China's CBEC import platform based on PEST theory [J]. *Mall Modernization,* (13): 37-39 https://doi.org/10.1061/9780784480915.187
[24] [Gong Y.Q., 2021. Research on portrait and talent demand of CBEC enterprises in Beijing [J]. *Journal of Beijing Vocational College of Labor and Social Security*, 15 (02): 31-39 https://doi.org/10.11648/j.jhrm.20210904.15
[25] Ding Q.Q., 2021. Research on innovation of CBEC platform operation mode [J]. *China Economic and Trade Guide* (Central), (06): 99-100 https://doi.org/10.1109/iciii.2013.6702937
[26] Xiong J.H., 2021. Research on the Construction Strategy of Independent Stations for Cross border E-commerce Enterprises [J]. *Journal of Jiaozuo University*,35 (02): 84-87 https://doi.org/10.1787/888933148101
[27] Li Q., 2021 Exploring the branding operation path of independent CBEC stations based on DTC model [J]. *China Business Review,* (07): 31-34 https://doi.org/10.1109/pesgm41954.2020.9281384

Reinforcement Learning Algorithms for Adaptive Load Balancing in Publish/Subscribe Systems: PPO, UCB, and Epsilon-Greedy Approaches

Rana Zuhair Al Shaikh*, Muna M. Jawad Al-Nayar, Ahmed M. Hasan
University of Technology, Iraq
E-mail: cse.22.11@grad.uotechnology.edu.iq , Muna.m.jawad@uotechnology.edu.iq , 60163@uotechnology.edu.iq
*Corresponding author

Keywords: load balancing, reinforcement learning, pub/sup system

Received: August 12, 2024

This research addresses load balancing challenges in publish/subscribe (Pub/Sub) systems by comprehensively exploring reinforcement learning (RL) techniques. Algorithms such as epsilon-greedy, Upper Confidence Bound (UCB), round-robin, and least connections were evaluated to establish baseline performance metrics. Building on this foundation, we develop enhanced versions of epsilon-greedy and UCB algorithms tailored to the Pub/Sub context. Additionally, we introduce a custom approach utilizing Proximal Policy Optimization (PPO) to learn adaptive load-balancing policies. Our work provides a thorough comparative analysis of diverse RL methods, offering insights into their strengths and weaknesses in optimizing Pub/Sub system performance. Experimental results demonstrate the potential of RL, particularly our developed algorithms, to improve performance significantly. These enhanced algorithms showed marked improvements in makespan, achieving completion times up to 30% faster than traditional methods. Moreover, they exhibited notable gains in throughput, particularly in the Burst Load scenario, where EUCB and PPO showcased a 10-15% increase in throughput compared to baseline algorithms. This research also highlighted the enhanced algorithms' superior ability to maintain high message success rates, exceeding 90% in most scenarios, and their contribution to more stable and predictable latency, leading to improved QoS. Notably, the PPO-based approach exhibits superior performance during burst traffic and failure scenarios, highlighting its resilience and adaptability in dynamic environments.

Povzetek: Razvit je nov pristop na osnovi globokega učenja za dinamično uravnavanje obremenitve v sistemih Pub/Sub. Modeli PPO, UCB in epsilon-greedy izboljšujejo učinkovitost, skrajšujejo čas obdelave in povečujejo prepustnost sporočil v dinamičnih okoljih.

1 Introduction

Load balancing enhances application performance and resource utilization by distributing incoming traffic across multiple servers [1] [2]. This is especially crucial in high-traffic environments since it ensures system responsiveness and reduces overload. [3]. In publish/subscribe (Pub/Sub) systems, efficient load balancing significantly affects messaging service reliability [4].

Load balancing strategies can be classified into static and dynamic [5] [6]. Static techniques employ established rules, frequently based on hashing algorithms [7], while dynamic approaches adjust to system variables such as server response delays in real time. Recent developments in dynamic algorithms provide greater efficiency and determinism for balanced load distribution [8].

Even though static algorithms are wildly deployed and robust for their swift response to direct the incoming flow to its distention, they still have some harmful features. The Round-Robin (RR) and Least Connection (LC), as examples used in this work as static algorithms for compression, are blind algorithms. In the case of RR, cyclic distribution can be problematic when subscriber loads or capabilities change dynamically; RR will continue to send it an equal share of messages, potentially leading to delays and performance degradation [9]. Moreover, RR doesn't consider each subscriber's capacity or processing power. This can result in some subscribers being underutilized while others are overwhelmed, leading to inefficient resource allocation. While LC's focus on the number of active connections can make it sensitive to short-term fluctuations in traffic[10]. A subscriber might temporarily have fewer connections due to a recent burst of messages, but it might still be heavily loaded regarding CPU or memory usage. LC might mistakenly send more messages to this subscriber, exacerbating its load imbalance. Also, LC assumes all subscribers have equal capabilities. In reality, subscribers might have different hardware configurations, software versions, or network connectivity, leading to varying processing speeds. LC's simplistic approach can lead to

suboptimal performance in such heterogeneous environments.

The shortcomings of static load balancing methods, particularly in scenarios with fluctuating traffic patterns and heterogeneous subscriber capabilities, motivate the investigation of Reinforcement Learning (RL) as a potential solution to overcome these limitations. The RL has recently emerged as a practical approach for dynamic load balancing across many domains. Its adaptability with fluctuating network conditions makes it well-suited for optimizing communication load balancing [11]. RL approaches are actively investigated in distributed systems to enhance parallel particle tracing [12] and enhance cloud resource allocation, hence improving system performance [13] [14].

While load balancing has been extensively studied in various computing domains, its application within pub/sub systems remains relatively unexplored, as exemplified by the limited research in this area. Existing works primarily focus on enhancing scalability and performance through techniques like vertical clustering [15] [16] [17], flooding-based message dissemination [18], and SDN-controlled multicast groups [19] [20]. These approaches, however, often lack the adaptability and efficiency required for large-scale, dynamic IoT environments. Additional research has investigated dynamic load-balancing techniques within networks, offering valuable insights into modern approaches in this field. Some studies, such as [21] [22], leverage reinforcement learning to improve load balancing and network performance. Others propose hybrid algorithms and optimization techniques, as exemplified by [23] [24]. Table 1 concisely summarizes these studies, highlighting their main contributions, the metrics employed, their key achievements, and any identified limitations.

Many researchers aim to enhance the performance of networks and task scheduling by mixing static and dynamic load balance, as in [25][26]. Others use optimization algorithms such as Particle Swarm Optimization or the Cuckoo algorithm in [27] [28] [29] [30].

While previous research has primarily focused on load balancing across distributed brokers in Pub/Sub systems, our work addresses the equally important challenge of optimizing load balancing within a single broker, particularly in scenarios where a distributed architecture might be impractical or introduce unnecessary complexity.

The present work aims to develop and evaluate an RL-based algorithm for load balancing in pub/sub systems. We seek to enhance existing algorithms like epsilon-greedy and UCB and introduce a custom PPO-based approach. Our objective is to demonstrate the effectiveness of these algorithms in improving system performance metrics such as makespan, throughput, Quality of service (QoS), performance, and system latency, particularly under dynamic conditions.

The remainder of this paper is organized as follows. Section 2 provides an overview of publish/subscribe systems, traditional load balancing methods, and the potential of RL in this domain. Section 3 details our methodology, including the system model, RL framework, algorithm descriptions, and experimental design. In Section 4, we present and analyze the results of our experiments, comparing the performance of different RL algorithms and highlighting the benefits of our PPO-based approach. Finally, Section 5 concludes the paper with a summary of our findings, their implications, and directions for future research.

Table 1: The summary table of related work

No.	Main Contribute	Metrics used	Main achievements	Limitation
[15]	Proposed a distributed MQTT broker system for large-scale location-based IoT applications. The system introduces a topic structure suitable for handling location-dependent data and distributed brokers and gateways to reduce broker load and support heterogeneous brokers.	Number of requests and received messages by brokers.	The proposed method outperforms existing broker implementations, especially when the number of subscribers is significant or frequent subscription changes occur.	The system's reliance on pre-configured gateway knowledge about brokers and their assigned areas might limit its adaptability to changes in the network topology or broker availability.
[16]	Investigated the sub-linear scalability of MQTT clusters, where adding more brokers doesn't lead to a linear increase in performance. Proposed a multi-session best-matching strategy to reduce inter-broker traffic and improve scalability.	Routing and forwarding overheads, latency, CPU usage, memory consumption, and network traffic.	Reduced scaling penalty from 40% to 10%, demonstrating improved performance and resource utilization in MQTT clusters.	the increased complexity on both the client and broker side, along with the potential overhead of multiple TCP/IP connections
[17]	Proposes a fog-based pub/sub system using dynamic broadcast groups to manage	Latency, Redundant Messages	Achieves low latency comparable to global flooding while	The group formation process may not lead to a globally optimal

	the trade-off between latency and excess data dissemination.		significantly reducing excess data compared to flooding, approaching the efficiency of cloud relay	topology. Additionally, the choice of flooding for intra-group communication might lead to excess data if broadcast groups become too large.
[20]	Presents a complete solution for creating a flexible and efficient distributed system of MQTT brokers, focusing on broker discovery, overlay creation, message routing, and topic-based optimization	Average end-to-end delay, Traffic overhead, CPU and RAM usage, Convergence and repair time	Achieves lower end-to-end delay compared to flooding, especially with topic-based overlay. Reduces traffic overhead significantly in most scenarios. Maintains similar resource usage to the benchmark under normal conditions, with increased CPU usage under stress.	The topic-based overlay approach can lead to increased signaling overhead due to the maintenance of multiple overlay networks. The system's performance under extreme stress conditions requires further optimization to manage CPU usage effectively.
[23]	Introduced SWARM, an adaptive load-balancing protocol for distributed streaming systems processing big spatial data. SWARM continuously monitors workloads, reacting to changes in data and query distributions.	Throughput, response time, resource utilization	Achieved higher throughput and lower response time than static partitioning, improving cluster utilization and handling larger volumes of spatial data and queries.	Tuple-at-a-time systems may not be suitable for micro-batched systems with higher latency requirements.
[21]	Explored deep reinforcement learning for intelligent load balancing, focusing on QoS parameters correlated with QoE. Proposed centralized and distributed solutions using actor-critic and multi-agent architectures.	QoS parameters (flow delivery delay, packet dropping, throughput) and QoE (for video).	Showed improved QoE compared to traditional methods (ECMP) and matched performance of QoE-based reward methods using only network-level QoS metrics.	Primarily based on simulations, the algorithm's complexity could pose challenges for real-world deployment.
[18]	Proposed a multi-objective optimization scheduling model using the Artificial Bee Colony algorithm (ABC) with a Q-learning algorithm called the MOABCQ method.	Makespan, cost, and resource utilization.	It outperforms other algorithms in terms of reducing makepan, cost, and degree of imbalance and increasing throughput, average, and resource utilization.	The algorithm's performance can vary depending on the dataset, and its complexity might be a limitation for large-scale environments.
[19]	Proposed an automatic load-balancing architecture based on reinforcement learning (ALBRL) in SDN. It adapts the improved Deep Deterministic Policy Gradient (DDPG) algorithm to find a near-optimal path between network hosts and generates an inter-link-weight matrix.	Network throughput, link-load-balancing factor, link utilization.	Faster training speed than existing reinforcement-learning algorithms and significantly improves network throughput.	Therefore, its reliance on a single network topology for evaluation indicates a poor ability to handle dynamic networks.
[24]	Proposed a Differential Grey Wolf (DGW) load balancing with stochastic Bellman deep reinforced resource optimization (DGW-SBDR) in fog environments. It uses a DGW Optimization algorithm	Load balancing efficiency, makespan, latency, and energy consumption.	Compared to benchmark methods, improved load balancing efficiency, makespan, latency, and energy consumption in fog environments.	Primarily based on simulations, the algorithm's complexity could pose challenges for real-world deployment.

	for optimal resource management and an SBDR Learning-based Resource Allocation Model for optimal resource allocation.			
[22]	Proposed an RL-based load balancer (MERL-LB) for financial cloud services to reduce idle servers without disconnecting users. It uses a scalable neural network policy and evolutionary multi-objective training to balance load imbalance and server idle time.	Load imbalance and server idle time.	Reduced idleness by over 130% compared to traditional methods while slightly improving load balancing. Offers diverse Pareto-optimal policies for user flexibility.	It can be computationally expensive. The algorithm's complexity, primarily based on simulations, could pose challenges for real-world deployment.

2 Background

The publish/subscribe system is a messaging pattern system that facilitates flexible and scalable communication in distributed applications [24]. Unlike traditional request-response models, pub/sub introduces a layer of indirection, where publishers send messages to designated topics or channels without knowing who might receive them. Subscribers express interest in specific topics and receive only the messages relevant to those topics. Decoupling publishers and subscribers enable flexibility and scalability, while topic-based filtering only ensures efficient communication [24].

However, pub/sub systems present challenges in designing and implementing effective load-balancing mechanisms. While simple, traditional methods such as round-robin (RR) and least connections (LC) have limitations. RR distributes messages cyclically without considering subscriber capacities or loads, potentially leading to suboptimal resource utilization. LC directs messages to the subscriber with the fewest active connections but may not be ideal when subscriber capabilities or message processing times vary significantly [25]. These methods generally lack adaptability to changing traffic patterns and system conditions, may not efficiently utilize resources, and may not consider the varying nature of message content.[10]

These limitations underscore the need for more intelligent and adaptive load-balancing techniques. With its ability to learn from interactions and dynamically adjust decisions based on real-time feedback, RL offers a promising avenue for overcoming these challenges [10]. In the following section, we discuss how RL can be leveraged to improve load balancing in pub/sub systems.

The Publisher is responsible for generating and sending messages (requests) and categorizing them into relevant topics. Subscribers express interest in specific topics and receive messages only for those topics. The Broker (or Messaging Server) acts as an intermediary, receiving messages from publishers, filtering them according to their topic, and delivering them to the appropriate subscribers [24].

Reinforcement Learning (RL) is a machine learning paradigm where an agent learns optimal decision-making by interacting with an environment and receiving feedback as rewards or penalties [26]. Unlike supervised or unsupervised learning, RL does not rely on pre-labeled data or inherent data patterns. In load balancing in a pub/sub system, the RL agent would act as the message broker, the environment would be the dynamic state of the pub/sub system, and actions would involve selecting the appropriate subscriber for each incoming message. Rewards for the agent could be based on minimizing message response time and ensuring balanced utilization across subscribers.

The present work focuses on three RL algorithms for load balancing:

- Epsilon-greedy: This algorithm balances exploration (trying random actions to gather information) and exploitation (choosing the action with the highest estimated reward). A parameter ε controls the balance between these two modes [27].
- Upper Confidence Bound (UCB) favors actions that have been less explored or have previously shown potential for high rewards. It uses an optimistic estimate of the potential reward for each action to guide its decision [11].
- Proximal Policy Optimization (PPO): this policy gradient method aims to improve the current policy by taking small steps in the direction that maximizes the expected reward. It is known for its stability and sample efficiency [28].

By leveraging the learning capabilities of these RL algorithms, the broker can dynamically adapt its load-balancing decisions based on the current system state and the feedback received, potentially leading to more efficient and resilient load balancing than the traditional methods.

Having established the foundation of the Pub/Sub systems, traditional load balancing limitations, and the principles of RL, we now delve into the specific methodology employed in this research. The following section describes our system model, RL framework, algorithm enhancements, evaluation metrics, and experimental design.

3 The methodology

The Pub/Sub system is deployed on the Amazon Web Services (AWS) cloud, leveraging Elastic Compute Cloud (EC2) instances for its core components. A single t3. medium EC2 instance (2 vCPUs, 4GB RAM) hosts the custom Python message broker, which incorporates a load balancer capable of implementing the tested algorithms and manages internal queues for message distribution. Three EC2 instances are dedicated to the subscribers, each paired with a Nginx web server to handle incoming requests. The publisher component, however, runs locally on a separate machine, generating diverse traffic patterns analogous to using the JMeter tool to thoroughly evaluate the load balancer's performance.

Figure 1 illustrates the architecture of the Pub/Sub system, designed to emulate a real-world web application. Publishers send messages to the custom Python message broker, which employs a load balancer to intelligently route each message to the most suitable queue based on the chosen load-balancing algorithm. Each subscriber is hosted on a dedicated EC2 instance. It utilizes the Pika library and threading to efficiently consume messages from its assigned queue, similar to how Nginx workers handle concurrent requests. Upon receiving a message, the subscriber unpacks it into a web request format and forwards it to the co-located Nginx web server, which simulates the application logic and generates the appropriate response.

3.1 Reinforcement learning framework

Our load-balancing strategy is based on a reinforcement learning framework, where the broker acts as the agent, learning to make optimal load-balancing decisions. The following components characterize the RL framework:

- **States:** A vector representing the current state of each subscriber. The current load on each subscriber (e.g., active connections, CPU utilization, response time), queue length, and system-wide averages.
- **Actions:** The broker's decisions, such as which subscriber to assign a new message to.
- **Rewards:** Feedback signals that indicate the effectiveness of the broker's actions. The reward function is designed to incentivize both fast response times, queue length, and efficient resource utilization, calculated as shown in Equation (1):

Reward *= 1.0 + (1.0 / response_time) - (cpu_percent * 0.02)- (queue_length * 0.01)* ……Eq. (1)

This ensures the algorithm prioritizes both fast responses and efficient resource utilization. It starts with a base value of 1.0. This provides a positive reward even for somewhat slower response times. The term (1.0 / response_time) is added. It means shorter response times result in a more significant fraction, increasing the overall reward, and the longer response times lead to a smaller fraction, decreasing the reward. The (cpu_percent * 0.02) portion is subtracted from the reward, which means at 100% CPU usage, the reward is reduced by 2. Finally,

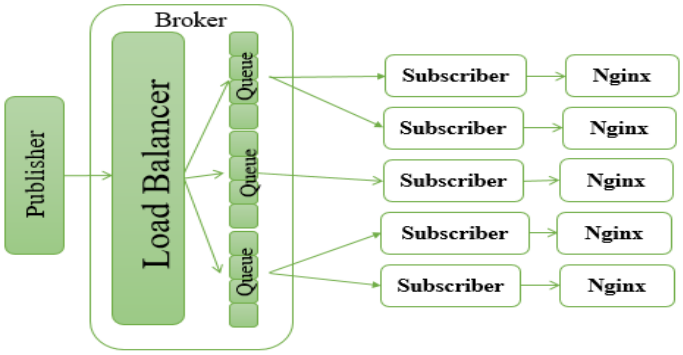


Figure 1: Proposed system design

(*Queue_length* * 0.01) penalizes the agent for selecting subscribers with longer queues, encouraging it to distribute the load more evenly.

Additionally, the adaptive exploration strategy is introduced. The adjusting of the exploration rate (ε) through the implementing Equation (2):

exploration rate *= 0.01+ sqrt (2 *log(total_counts) / (n_a + 1))* ------- *Eq. (2)*

The initial value of the exploration rate is 0.01 to prevent it to be zero at the start of the system. Where (total_counts) represents the total number of iterations, and (*n_a*) represents the number of times the specific action (*a*) has been taken. The natural logarithm aligns perfectly with the desired behavior of the exploration bonus. It emphasizes exploration early in learning and gradually reduces exploration over time.

Policy: The broker's strategy is to select actions based on the current state. RL aims to learn an optimal policy that maximizes the cumulative reward over time. Reinforcement Learning Algorithms

Three RL algorithms were evaluated in the present work for load balancing in Pub/Sub systems. These algorithms are as follows:

- **Epsilon-Greedy (EG)**

  Our enhanced epsilon-greedy algorithm Incorporates several modifications to improve its adaptability to dynamic Pub/Sub environments. The reward function dynamically considers both server

responsiveness and CPU load, as shown in Eq. (1). This ensures the algorithm prioritizes fast responses and efficient resource utilization. Additionally, we introduce an adaptive exploration strategy, adjusting the exploration rate (ε) using Equation (2).

- **Upper Confidence Bound (UCB) Algorithm**

The UCB algorithm shares a similar structure with epsilon-greedy but differs in its action selection strategy. Instead of relying on random exploration, UCB selects actions based on an upper confidence bound that considers the estimated Q-value and the uncertainty associated with that estimate [26]. This approach encourages the exploration of less-visited actions while exploiting actions with high expected rewards, leading to more informed and potentially superior decision-making. Figure 2 presents the general learning process for the epsilon-greedy and UCB algorithms within the proposed load-balancing framework. Both algorithms initialize parameters, compute the system state, and determine whether to explore or exploit. However, they differ in their action selection strategies. Epsilon-greedy explores with probability ε and exploits with probability 1-ε, while UCB uses a confidence interval-based formula to balance exploration and exploitation. Regardless of the algorithm, the chosen action is executed, a reward signal is received, and the Q-table is updated, enabling the agent to learn over time.

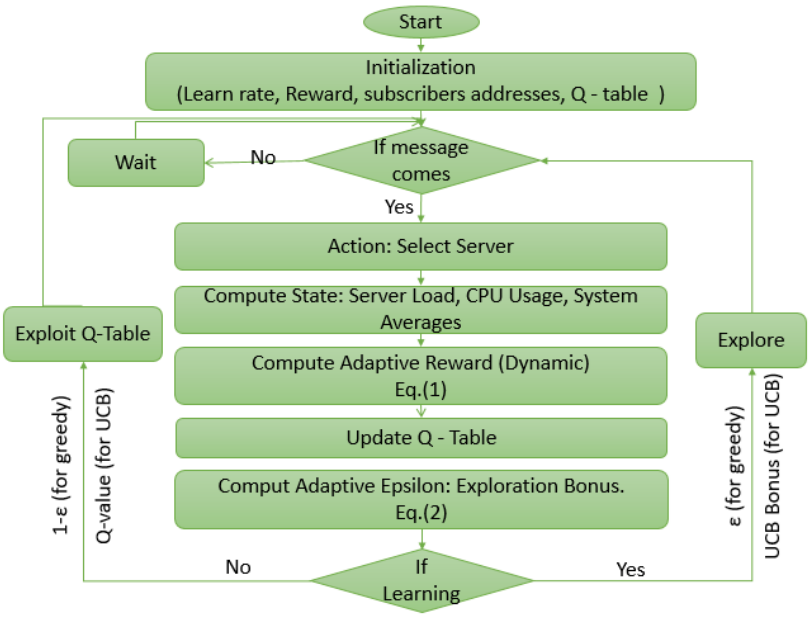


Figure 2: Flowchart of enhanced epsilon greedy and UCB algorithms for pub/sub system

- **Proximal policy optimization (PPO)**

Proximal Policy Optimization (PPO) is a policy gradient reinforcement learning algorithm renowned for its stability and efficiency. Unlike value-based methods like epsilon-greedy and UCB, PPO directly learns a policy that maps states to actions, connections, CPU utilization, response time, and queue length) for each subscriber and system-wide averages. To balance simplicity with adequate capacity for learning, the network utilizes two hidden layers with ReLU activation functions with 128 neurons each. Finally, an output layer produces a probability distribution over the available actions, effectively guiding the selection of a specific subscriber for each incoming message.

The reward function is crucial in guiding the PPO agent's learning process. The same dynamic reward function in Eq (1) is used.

Figure 3 illustrates the architecture of the Proximal Policy Optimization (PPO) agent employed for load balancing in the Pub/Sub system. The agent's neural network receives a state representation encompassing load metrics (active connections, CPU utilization, response time) for each subscriber, queue length, and system-wide averages as input. This state information is processed through two hidden layers with ReLU activation functions, culminating in an output layer that produces two key components: a policy, which is a probability distribution over possible actions (subscriber selections), and a value function, which estimates the expected cumulative reward from the current state.

The selected action, according to the policy's probabilities, is then executed within the Pub/Sub environment, specifically targeting one of the subscriber instances. The environment responds by

providing a reward signal, calculated using Equation (1), and a new state reflecting the updated system conditions. This reward and state information is fed back to the PPO agent. The clipped surrogate objective function utilizes them to update the policy and value function networks. This iterative process of interaction, reward collection, and network updates allows the PPO agent to learn and refine its

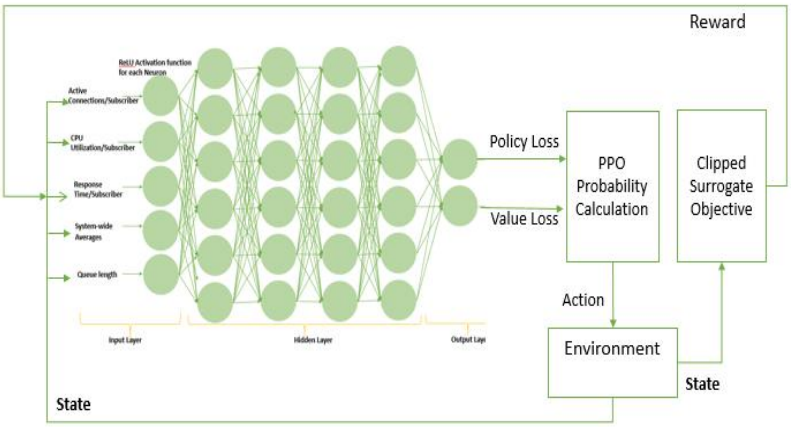


Figure 3: PPO Architecture for Load Balancing in Pub/Sub Systems

load-balancing strategy over time, adapting to the dynamic nature of the Pub/Sub system. The value function helps the agent estimate the long-term consequences of its actions, guiding it towards better decisions.

JMeter was employed to simulate different load scenarios and evaluate the system's performance under various conditions. The following four scenarios were designed:

- **Scenario 1: Normal load**. This scenario simulated a moderate traffic pattern using a Thread Group with 50 threads (representing 50 concurrent users) and a loop count of 20. A total of 1000 messages were sent to the message broker.
- **Scenario 2: Burst load**. This scenario aimed to stress the system with a sudden surge in traffic. It was implemented using a Thread Group with 100 threads and a loop count of 20, with target throughput 6000 message per minute.
- **Scenario 3: Server failure**. This scenario tested the system's resilience to subscriber failures. A normal load of 50 threads and 20 loops (1000 messages) was used, with one subscriber intentionally failing during the test.
- **Scenario 4: Heterogeneous instances**. This scenario evaluated the system's performance with subscribers having varying resource capabilities. A normal load was simulated, but one of the three subscriber EC2 instances was configured with reduced resources (1 vCPU and 2GB RAM). At the same time, the remaining two instances retained their original configuration (2 vCPU and 4GB RAM).

4 Result and discussion

This section presents the results of our experimental evaluation of various load balancing algorithms in a simulated Pub/Sub system deployed on AWS.

The performance of baseline algorithms (RR, LC, EG and UCB) are alkalized and compared with the enhanced algorithms (Enhanced Epsilon Greedy (EEG), Enhanced UCB (EUCB), and PPO) across four scenarios: normal load, burst load, server failure, and heterogeneous instances. Each experimental scenario was run 10 times, and the results are presented as mean values with 95% confidence intervals. The evaluation metrics include makespan, message throughput, latency, successful massage rate, Quality of Service, and efficiency.

4.1 Makespan comparison

The makespan, representing the total time to process all messages, is a critical indicator of system behavior. As depicted in Figure 4, the enhanced algorithms consistently outperform the baseline algorithms across all scenarios. This advantage stems from their ability to dynamically adapt to changing conditions. Unlike RR and LC, which rely on fixed rules, the enhanced algorithms leverage real-time feedback to make informed decisions. For instance, in the 'Failed Scenario,' the improved algorithms, especially PPO, demonstrate significantly lower makespans, indicating their superior ability to adapt and recover from disruptions.

4.2 Message throughput

Figure 5 presents a comparative analysis of throughput achieved by various load-balancing algorithms across the four distinct scenarios. Across all scenarios, the enhanced algorithms (EUCB and PPO) consistently outperform the other algorithms specially (RR, LC, and EG), demonstrating their superior ability to maintain high throughput even under challenging conditions. This is particularly evident in the Burst Load scenario, where EUCB and PPO exhibit significantly higher throughput than the other algorithms. The results highlight the effectiveness of the enhanced algorithms in maximizing

the system's capacity to process messages and maintain a high rate of successful message delivery.

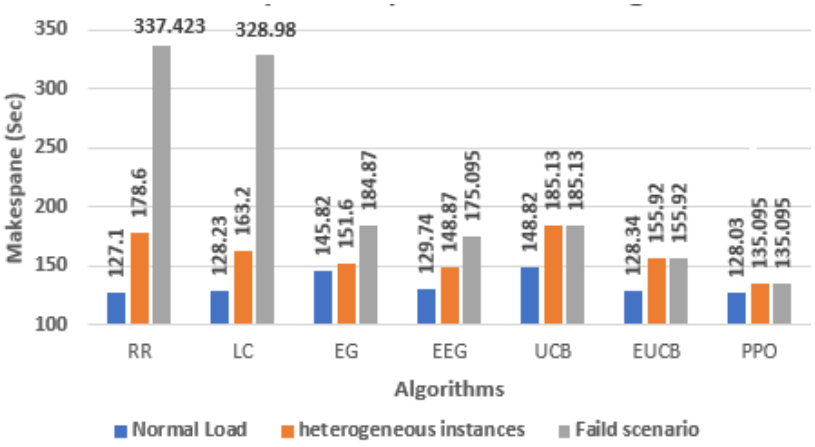


Figure 4: Makespan comparison across all algorithms

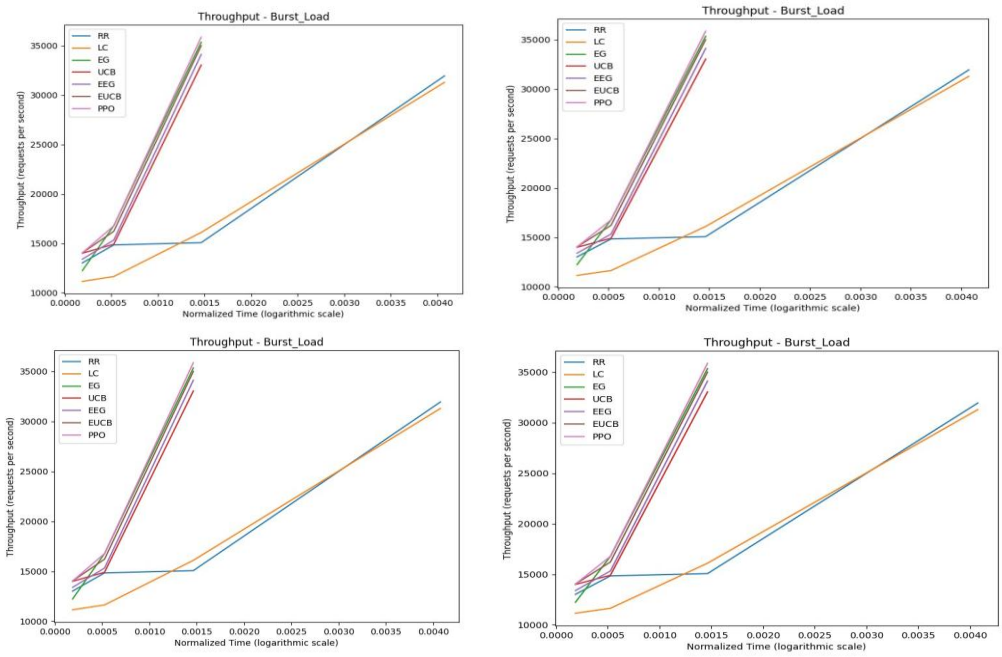


Figure 5: System message throughput across all algorithms

4.3 The latency

Figure 6 illustrates a comparative analysis of latency across the four scenarios. A key observation is the variability in latency for the baseline algorithms (RR, LC, EG, and UCB), particularly in the Normal Load and Burst Load scenarios. This indicates an inconsistency in response times and potential delays for specific messages. In contrast, the enhanced algorithms (EUCB and PPO) exhibit more stable and predictable latency across all scenarios, with tighter interquartile ranges and fewer outliers. This suggests these algorithms can deliver more consistent and reliable performance, even under challenging conditions. However, it's important to note that the enhanced algorithms generally show slightly higher median latency than the baseline algorithms, indicating a potential trade-off between performance consistency and raw speed.

4.4 Successful message rate

Table 2 clearly shows the percentage of successful messages achieved by each load-balancing algorithm across different scenarios. Notably, the enhanced UCB and PPO algorithms consistently demonstrate higher success rates than the other algorithms in all scenarios. This highlights their effectiveness in ensuring reliable message delivery and minimizing request failures, especially in challenging conditions like burst loads or

server failures. The PPO algorithm, in particular, exhibits the highest success rates across most scenarios, further emphasizing its potential for robust load balancing in Pub/Sub systems.

4.5 Quality of service (QoS):

Figure 7 illustrates the relationship between latency and throughput, two critical QoS metrics, for various load-balancing algorithms under different scenarios. The baseline algorithms exhibit more significant variability in balancing latency and throughput. In contrast, the enhanced algorithms, especially PPO, consistently achieve higher throughput with more stable latency. Distinct clusters for each scenario underscore the impact of varying load conditions on algorithm behavior. For instance, the Burst Load scenario generally results in higher latency and throughput than the Normal Load scenario, reflecting the increased system stress.

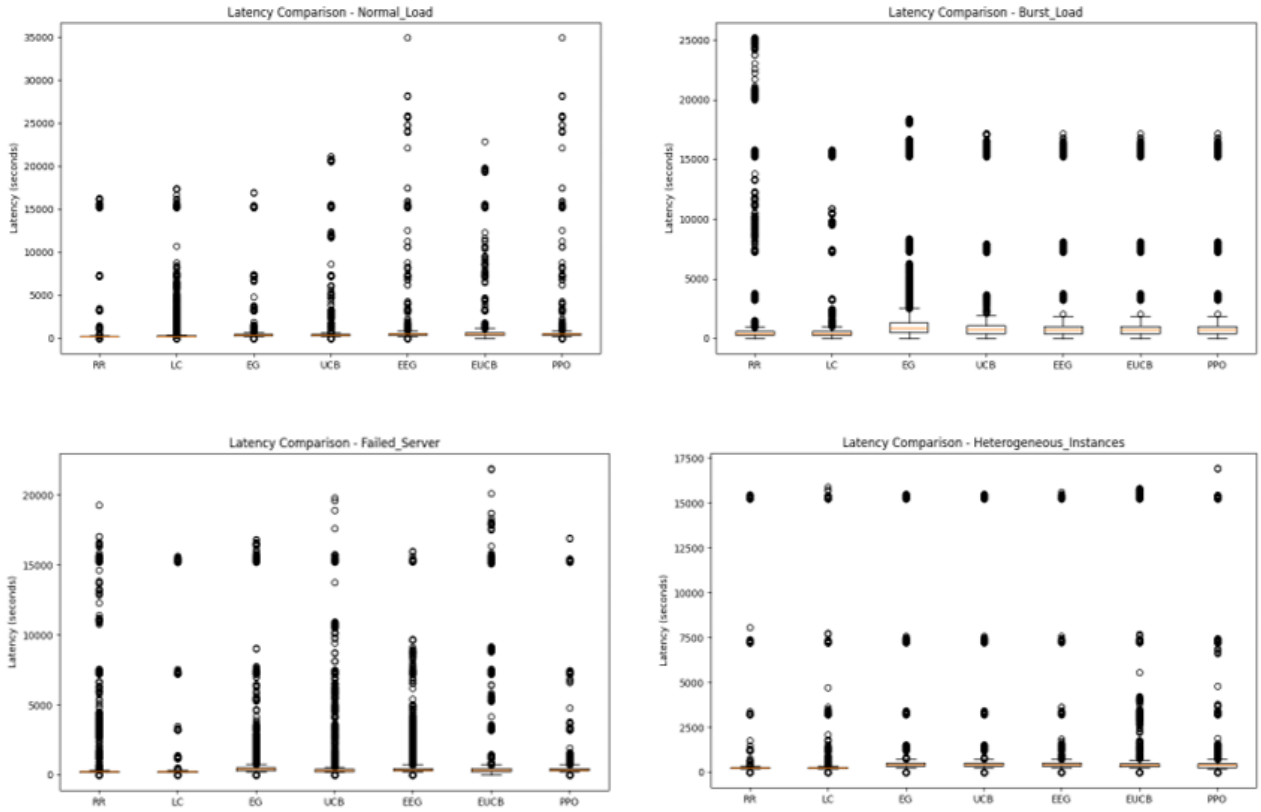


Figure 6: System Latency across all algorithms.

Table 2: The Percentage of successful requests across all scenarios.

ios / Algorithms (%)	*RR*	*LC*	*EG*	*UCB*	*EEG*	*EUCB*	*PPO*
Normal Load	89.5	92.0	91.1	92.2	91.6	91.9	97.1
Burst Load	86.9	86.2	93.0	87.6	90.3	92.5	94.7
Failed Server	84.4	88.5	92.1	91.3	83.9	91.8	93.6
Heterogeneous Instances	90.4	90.9	91.0	91.0	91.8	92.0	93.1

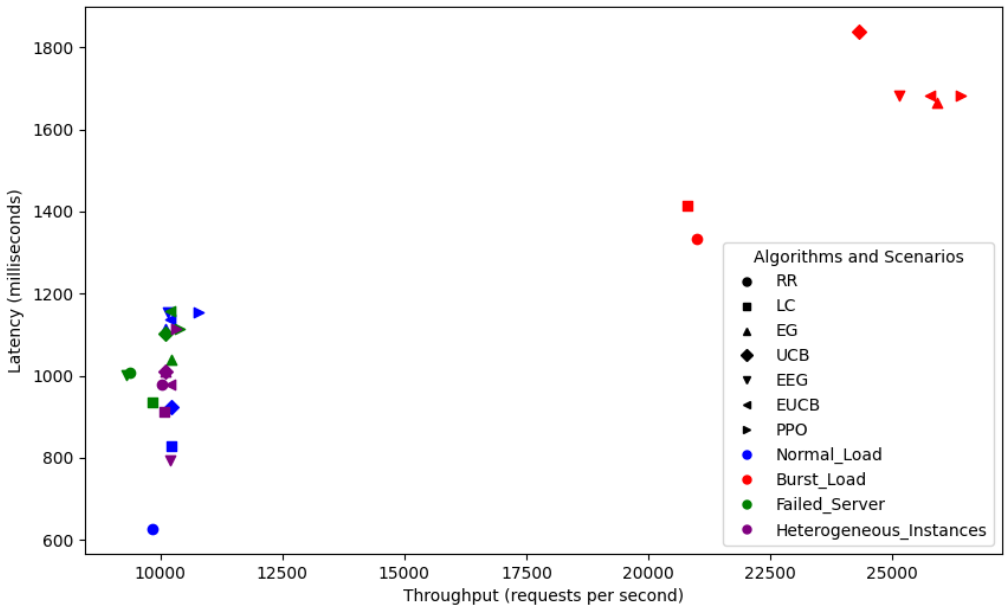


Figure 7: The Quality of Services across all scenarios.

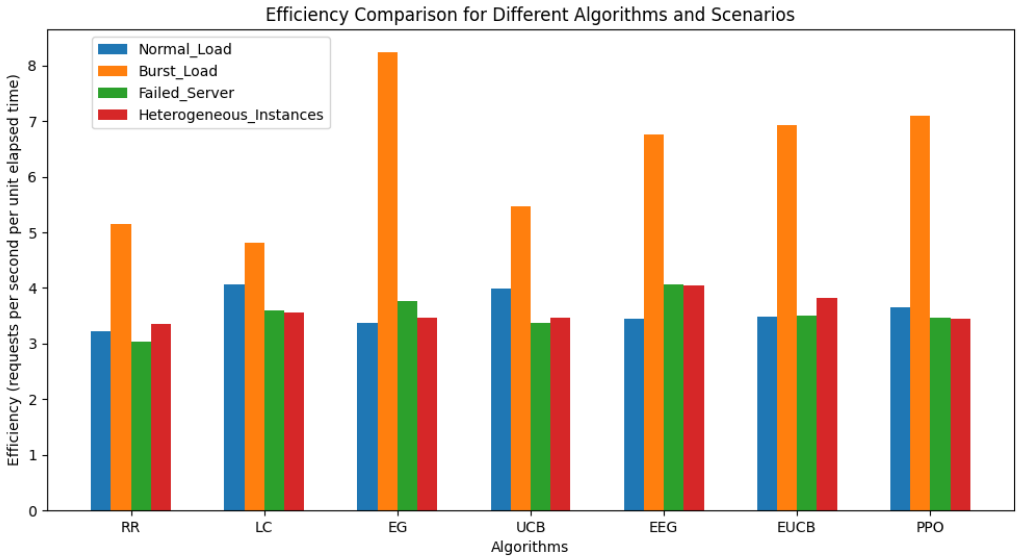


Figure 8: The Effeciency analysis of the proposed Pub/Sub System.

4.6 The efficiency of the Pub/Sub system

Figure 8 presents the efficiency of various load-balancing algorithms across four distinct scenarios. Enhanced algorithms (EUCB and PPO) consistently outperform the other algorithms, demonstrating their superior ability to maintain high throughput, especially during Burst Load. These results highlight the effectiveness of the enhanced algorithms in maximizing the system's capacity to process messages and ensure high delivery rates.

The enhanced algorithms, particularly PPO, utilize reinforcement learning to make dynamic load-balancing decisions based on real-time system feedback. This adaptability enables them to effectively handle fluctuations in traffic patterns and subscriber loads, outperforming static algorithms. Moreover, these algorithms actively route messages to available and healthy subscribers, resulting in lower failure rates and a more resilient system. Including CPU usage in the reward function of the enhanced algorithms further contributes to balanced resource allocation and improved system performance by detecting and mitigating potential subscriber bottlenecks.

While recent research is focused on distributed brokers, our single-broker optimization approach using RL demonstrates the potential for enhancing Pub/Sub system performance, complementing existing work, and opening avenues for broader system improvements.

5 Conclusions

This research explored the application of reinforcement learning (RL) for load balancing in publish/subscribe systems. We evaluated traditional algorithms (Round Robin, Least Connections) and developed enhanced versions of epsilon-greedy and UCB alongside a custom PPO-based approach. Our experimental results demonstrate that RL significantly outperforms traditional methods, particularly the PPO and EUCB algorithms. These enhanced algorithms showed marked improvements in makespan, achieving completion times up to 30% faster than conventional methods. Moreover, they exhibited notable gains in throughput, particularly in the Burst Load scenario, where EUCB and PPO showcased a 10-15% increase in throughput compared to baseline algorithms. This research also highlighted the enhanced algorithms' superior ability to maintain high message success rates, exceeding 90% in most scenarios, and their contribution to more stable and predictable latency, leading to improved QoS. Overall, this research underscores the potential of RL for adaptive and efficient load balancing in Pub/Sub systems, paving the way for more resilient and responsive distributed applications.

6 Future work

This research can be expanded upon in several promising ways. One area of focus is exploring alternative reward function formulations and systematically varying the weights assigned to different factors. Additionally, the investigation of more comprehensive state representations could enhance the algorithms' learning capabilities. Another potential direction is developing hybrid algorithms that combine the strengths of different RL methods or integrate RL with traditional load-balancing techniques. Furthermore, evaluating the proposed algorithms in more diverse and realistic scenarios would provide a more comprehensive understanding of their performance characteristics. Finally, deploying and evaluating the RL-based load-balancing system in a real-world production environment would provide valuable insights into its practical feasibility and effectiveness.

References

[1] A. Javahar, R. Ananth, K. K. Arun Ritthik, and R. Dharun, “Efficient load balancing for Micro Services based applications,” in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, Jan. 2023, pp. 1–5. https://doi.org/10.1109/iccci56745.2023.10128431

[2] G. Barlas, “Load balancing,” in *Multicore and GPU Programming*, Elsevier, 2023, pp. 887–941. doi: https://doi.org/10.1016/B978-0-12-814120-5.00022-6.

[3] D. I. Sukhoplyuev and A. N. Nazarov, “Analysis of Application-Level Load Balancing Algorithms,” in *2023 Systems of Signals Generating and Processing in the Field of on-Board Communications*, IEEE, Mar. 2023, pp. 1–4. doi: 10.1109/IEEECONF56737.2023.10092019.

[4] M. G. Spina, G. M. Marotta, S. Gualtieri, and F. De Rango, “Topic Load Balancing in a multi IoT Gateways Scenario under Publish/Subscribe Paradigm,” in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2022, pp. 521–522. doi: https://doi.org/10.1109/CCNC49033.2022.9700606.

[5] D. Man, W. Yang, and G. Tian, “Polymorphic Load Balancing Algorithm Based on Packet Classification,” in *Proceedings of the 2nd International Conference on Telecommunications and Communication Engineering*, New York, NY, USA: ACM, Nov. 2018, pp. 258–261. doi: https://doi.org/10.1145/3291842.3291911.

[6] S. Gilbert, U. Meir, A. Paz, and G. Schwartzman, “On the Complexity of Load Balancing in Dynamic Networks,” in *Proceedings of the 33rd ACM Symposium on Parallelism in Algorithms and Architectures*, New York, NY, USA: ACM, Jul. 2021, pp. 254–264. doi: https://doi.org/10.1145/3409964.3461808.

[7] S. K. Mishra, B. Sahoo, and P. P. Parida, “Load balancing in cloud computing: A big picture,” Feb. 01, 2020, *King Saud bin Abdulaziz University*. doi: https://doi.org/10.1016/j.jksuci.2018.01.003.

[8] Panjwani, K., Pathan, S., Yadav, N., Lokhande, S. and Thakare, B., “Load Balancing, Optimal Routing and Scheduling in Hyper-Local.,” *International Journal of Computer Applications*, p. 975, Dec. 2015. https://doi.org/10.5120/ijca2015907393

[9] Erl, Ricardo Puttini Thomas, and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture (The Pearson Service Technology Series from Thomas Erl) 1st Edition*, 1st ed. Pearson, 2013.

[10] A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh, “Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey,” *J Ambient Intell Humaniz Comput*, vol. 11, no. 11, pp. 4785–4814, Nov. 2020, doi: https://doi.org/10.1007/s12652-020-01747-z.

[11] D. Wu, Li Jimmy, Ferini Amal, Xu Yi Tian, Jenkin Michael, Jang Seowoo, Liu Xue, and Dudek Gregory, “Reinforcement learning for communication load balancing: approaches and challenges,” *Front Comput Sci*, vol. 5, May 2023, doi: https://doi.org/10.3389/fcomp.2023.1156064.

[12] J. Xu, H. Guo, H.-W. Shen, M. Raj, S. W. Wurster, and T. Peterka, “Reinforcement Learning for Load-Balanced Parallel Particle Tracing,” *IEEE Trans Vis Comput Graph*, vol. 29, no. 6, pp. 3052–3066, Jun. 2023, doi: https://doi.org/10.1109/TVCG.2022.3148745.

[13] J. Wang, "A reinforcement learning-based network load balancing mechanism," in *Fifth International Conference on Computer Information Science and Artificial Intelligence (CISAI 2022)*, Y. Zhong, Ed., SPIE, Mar. 2023, p. 162. doi: https://doi.org/10.1117/12.2667915.

[14] M. Shahakar, S. Mahajan, and L. Patil, "Load Balancing in Distributed Cloud Computing: A Reinforcement Learning Algorithms in Heterogeneous Environment," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 2, pp. 65–74, Mar. 2023, doi: https://doi.org/10.17762/ijritcc.v11i2.6130.

[15] R. Kawaguchi and M. Bandai, "A Distributed MQTT Broker System for Location-based IoT Applications," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, Jan. 2019, pp. 1–4. doi: https://doi.org/10.1109/ICCE.2019.8662069.

[16] A. Detti, L. Funari, and N. Blefari-Melazzi, "Sub-Linear Scalability of MQTT Clusters in Topic-Based Publish-Subscribe Applications," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1954–1968, Sep. 2020, doi: https://doi.org/10.1109/TNSM.2020.3003535.

[17] J. Hasenburg, F. Stanek, F. Tschorsch, and D. Bermbach, "Managing Latency and Excess Data Dissemination in Fog-Based Publish/Subscribe Systems," in *2020 IEEE International Conference on Fog Computing (ICFC)*, IEEE, Apr. 2020, pp. 9–16. doi: 10.1109/ICFC49376.2020.00010.

[18] B. Kruekaew and W. Kimpan, "Multi-Objective Task Scheduling Optimization for Load Balancing in Cloud Computing Environment Using Hybrid Artificial Bee Colony Algorithm with Reinforcement Learning," *IEEE Access*, vol. 10, pp. 17803–17818, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3149955.

[19] J. Chen, W. Yong, O. Jiangtao, F. Chengyuan, L. Xiaoye, L. Cenhuishan, and H. Xuefeng "ALBRL: Automatic Load-Balancing Architecture Based on Reinforcement Learning in Software-Defined Networking," *Wirel Commun Mob Comput*, vol. 2022, pp. 1–17, May 2022, doi: https://doi.org/10.1155/2022/3866143.

[20] E. Longo and A. E. C. Redondi, "Design and implementation of an advanced MQTT broker for distributed pub/sub scenarios," *Computer Networks*, vol. 224, p. 109601, Apr. 2023, doi: https://doi.org/10.1016/j.comnet.2023.109601.

[21] O. Houidi, Z. Djamal, P. Victor, A. Quang, P. Tran, H. Nicolas, L. Jeremie, M. Paolo, "Constrained Deep Reinforcement Learning for Smart Load Balancing," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2022, pp. 207–215. doi: https://doi.org/10.1109/CCNC49033.2022.9700657.

[22] P. Yang, L. Zhang, H. Liu, and G. Li, "Reducing idleness in financial cloud services via multi-objective evolutionary reinforcement learning based load balancer," *Science China Information Sciences*, vol. 67, no. 2, p. 120102, Feb. 2024, doi: https://doi.org/10.1007/s11432-023-3895-3.

[23] A. Daghistani, W. G. Aref, A. Ghafoor, and A. R. Mahmood, "SWARM: Adaptive Load Balancing in Distributed Streaming Systems for Big Spatial Data," *ACM Transactions on Spatial Algorithms and Systems*, vol. 7, no. 3, pp. 1–43, Sep. 2021, doi: https://doi.org/10.1145/3460013.

[24] S. V. Nethaji and M. Chidambaram, "Differential Grey Wolf Load-Balanced Stochastic Bellman Deep Reinforced Resource Allocation in Fog Environment," *Applied Computational Intelligence and Soft Computing*, vol. 2022, pp. 1–13, Aug. 2022, doi: https://doi.org/10.1155/2022/3183701.

[25] N. M. M. Muna Mohammed Jawad, "RHLB: Improved Routing Load Balancing Algorithm Based on Hybrid Policy," *Journal of University of Babylon for Engineering Sciences*, , vol. 27, no. 1, Feb. 2019. Doi: https://doi.org/10.29196/jubes.v27i1.2005

[26] H. A. J. Saja Dheyaa Khudhur, "DLSTM-MSF: Distributed LSTM Models for Multimedia Streaming Workload Forecasting Based on Kafka Environment," *Iraqi Journal of Computers, Communications, Control, and Systems Engineering*, vol. 24, no. 1, pp. 103–118, Mar. 2024. Doi: https://doi.org/10.33103/uot.ijccce.24.1.7

[27] E. K. H. Eman K Ibraheem, "Load Balancing Performance Optimization for LI-Fi/Wi-Fi HLR Access Points Using Particle Swarm Optimization and DL Algorithm," *International Journal of Intelligent Engineering & Systems*, vol. 15, no. 6, Nov. 2022. Doi: https://doi.org/10.22266/ijies2022.1231.34

[28] A. Mudheher, K. Ghalib, Safanah Mudheher, "Enhanced Performance of Consensus Wireless Sensor Controlled System via Particle Swarm Optimization Algorithm," *Journal of Engineering*, vol. 23, no. 9, Sep. 2017. Doi: https://doi.org/10.31026/j.eng.2017.09.05

[29] Yossra Ali, Nuha Ibrahim, sajjad jaber, "Task Scheduling in Cloud Computing Based on The Cuckoo Search Algorithm," *Iraqi Journal of Computer, Communication, Control and System Engineering*, vol. 22, no. 1, pp. 86–96, Mar. 2022, doihttps:/doi.org/10.33103/uot.ijccce.22.1.9.

[30] Hanan Al-asady. Ekhlas K. Hamza, "Indoor Localization System Using Wireless Sensor Network," *Iraqi Journal of Computers, Communications, Control, and Systems Engineering*, vol. 18, no. 1, 2018. Doi: https://doi.org/10.33103/uot.ijccce.18.1.3

Edge Detection Using Sobel Algorithm and YCbCr Colour Space Optimized on FPGA

Yang An*, Qianqian Yuan, Han Zhang
School of Science, Jiaozuo Normal College, Jiaozuo 454002, China
E-mail: jzszay@126.com, yuan-qianqian@vip.163.com, kxmytzxh@163.com
*Corresponding author

Keywords: edge detection, FPGA, YcbCr, sobel algorithm

Received: August 26, 2024

Edge detection plays a crucial role in image processing and computer vision, and is widely used in tasks such as object recognition and image segmentation. Traditional edge detection algorithms perform well in many applications, but there are still some shortcomings in terms of real-time performance and processing efficiency. To address this issue, a highly efficient image edge detection model combining Sobel algorithm and field programmable gate array technology was proposed. YCbCr color space conversion was performed on the image, then Sobel operator was utilized to calculate the image gradient, and adaptive thresholding method was applied to determine the edges. Finally, the model was implemented and optimized on a field programmable gate array. The experimental results showed that when the dataset size was 1000, the information retention rate of the proposed image preprocessing model was 0.89, and the structural information loss was 0.05. When the data volume was 100, the accuracy of the proposed image edge detection model was 0.90, and the root mean square error value was 0.16. The research results indicate that the proposed image edge detection model based on field programmable gate arrays has significant advantages in edge detection performance and processing efficiency. The model has high accuracy and speed in image edge recognition, which can provide certain guidance for research in the field of image edge detection.

Povzetek: Razvito je optimizirano zaznavanje robov slik s Sobelovim algoritmom v YCbCr barvnem prostoru na FPGA. Metoda izboljšujekvaliteto obdelave, kar omogoča hitrejšo in učinkovitejšo analizo slik.

1 Introduction

Image edge detection takes a critical part in the areas of computer vision and image processing, and is broadly applied in tasks such as pattern recognition [1]. The edge detection's main goal is to identify areas in an image with discontinuous grayscale or significant gradient changes, which typically correspond to important structural information in the image. Traditional edge detection algorithms perform well in many applications, but there are still some shortcomings in terms of real-time performance and processing efficiency. As a result of the accelerated advancement of artificial intelligence and computer vision technology, there has been a notable rise in the demand for image processing solutions in the field of image detection, especially in scenarios that require efficient and real-time processing, such as autonomous driving, intelligent monitoring, and medical image analysis. Traditional edge detection methods are inadequate [2]. In recent years, with the advancement of hardware technology, field programmable gate arrays (FPGAs) have gradually become an important direction in image processing research due to their high parallel processing capability and low power consumption characteristics. The advantage of FPGA lies in its flexible hardware programming ability and high parallel processing capability, which enables it to meet the needs of different application scenarios while maintaining high performance. Therefore, innovative research has proposed an efficient image edge recognition model that combines edge detection algorithms and FPGA technology. By performing YCbCr color space conversion on the image, the effect of edge detection is enhanced. Then, the Sobel operator is applied to calculate the image gradient, and the edge is determined through adaptive thresholding. Finally, the model is implemented and optimized on FPGA to improve processing efficiency. The research content contains four parts. Part 1 is a review of other scholars' relevant research topics. Part 2 is a simple introduction of the main methods utilized in this paper. Part 3 is the model findings acquired by using the methods to the research and analyzing the findings. Part 4 is a summary of the study and prospects for future research.

2 Related works

Image edge detection is a technique that is employed extensively in a multitude of tasks, including object recognition, image segmentation, and pattern recognition. To further optimize the performance of the large law threshold method, Yang et al. proposed a threshold deviation adjustment strategy based on the analysis of the relationship between pixel grayscale values and cumulative pixel changes. The experimental findings denoted that this strategy could better segment test images and obtain competitive misclassification errors [3]. Zheng et al. found that traditional particle swarm optimization (PSO) algorithm has a slow convergence speed in image

segmentation and is prone to getting stuck in local optima. Therefore, the research team proposed an improved particle swarm algorithm that combines the large law threshold method. The experiment finding indicated that the execution time of this algorithm was, on average, 30% faster than that of other algorithms, and its accuracy was superior to that of other algorithms [4]. Vite-Chávez et al. pointed out that significant challenges were encountered nal methods [5]. Chen et al. proposed an adaptive fractional order genetic classification method by combining PSO algorithm to improve the performance of the large law threshold method in image segmentation. The experimental outcomes indicated that the test results of this method in terms of regional contrast and peak signal-to-noise ratio (SNR) indicators, both qualitatively and quantitatively, were superior to the algorithm before improvement [6].

Gtifa et al. proposed a novel hardware architecture to improve the accuracy of brain tumor segmentation in 3D MRI images and optimize the diagnosis and treatment tion faced by convolutional neural networks when applied to edge devices. FPGAs demonstrated significant advantages in optimizing convolution operations due to their high flexibility and low power consumption. The research results indicated that FPGA is a promising energy-saving platform, providing important guidance for future artificial intelligence hardware research [8]. Narang et al. proposed an innovative hardware simulator to accelerate the design cycle of microelectromechanical system (MEMS) vibration gyroscopes. This simulator was easy to reconfigure and fully integrated on a FPGA board. The research results indicated that the simulator successfully simulated the Coriolis effect and various typical MEMS gyroscope error sources, and preliminary experiments demonstrated its effective performance in noise and nonlinear models [9].

in the classification, recognition, and detection of fruits and vegetables. Therefore, the research team proposed an image recognition method that enhanced binary segmentation by combining the idea of interest classification and the large law threshold method. The experimental outcomes denoted that regardless of the presence of additional noise, the recognition accuracy of this method was always superior to traditio

process of brain tumors. This architecture integrated intelligent algorithms, especially PSO and Darwin PSO techniques, and was implemented on the Xilinx Virtex6 FPGA platform. The outcomes indicated that this hardware architecture outperformed in segmenting brain tumors, with efficient and robust performance, providing clinical doctors with powerful diagnostic tools and potentially improving the speed and accuracy of diagnosis and treatment [7]. Hong et al. developed a convolutional neural network model design method using FPGAs as accelerators to overcome the challenges of large models, high computational complexity, and huge power consump In summary, in the last few years, many scholars have begun to explore image recognition and contour extraction, and have successively proposed various recognition methods. However, this field still faces challenges such as complex backgrounds and uneven lighting, which limits the effectiveness of traditional methods such as simple threshold segmentation. To address these challenges, a highly efficient image edge recognition model combining Sobel algorithm and FPGA technology has been proposed. It is expected to provide an efficient image edge recognition solution suitable for real-time image processing applications, showcase the potential application of FPGA in image processing for providing reference for research and application in related fields, and further explore the combination of FPGA and traditional image processing algorithms to promote the development of image processing technology.

Table 1: Related works

Authors	Method	Application	Key findings	Performance comparison	References
Yang P et al.	Threshold deviation adjustment strategy	Image segmentation	Improved segmentation results and reduced misclassification rate	Superior to Otsu's method	[3]
Zheng J et al.	Improved Particle Swarm Algorithm	Image segmentation	Enhanced convergence speed and accuracy; 30% faster runtime	Faster and more accurate than traditional PSO	[4]
Vite-Chávez O et al.	Interest classification + Otsu's method	Fruit and vegetable recognition	Recognition accuracy superior to traditional methods	Robust to noise	[5]
Chen L et al.	Adaptive fractional-order genetic classification	Image segmentation	Superior results in contrast and peak SNR	Better than pre-improved algorithms	[6]
Gtifa W et al.	Hardware architecture + PSO	Brain tumor segmentation	Enhanced accuracy for clinical diagnosis support	Efficient and robust	[7]
Hong H et al.	FPGA-accelerated convolutional neural network	Edge device application	Reduced power consumption and improved computational efficiency	Superior to traditional deep learning models	[8]
Narang S et al.	Hardware simulator	MEMS gyroscope design	Effectively simulated Coriolis effects and error sources	Good performance in noise and nonlinear models	[9]

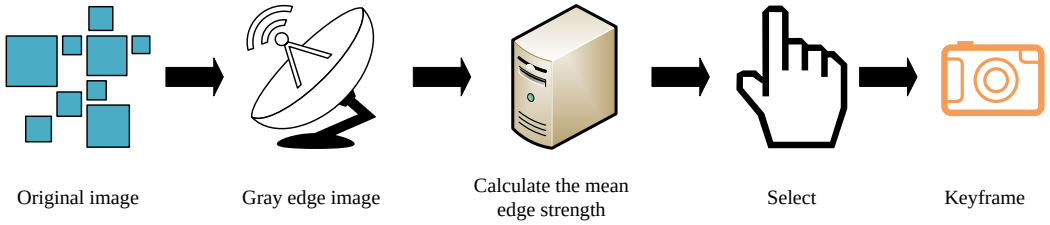


Figure 1: Keyframe image extraction process.

3 Methods

The first section addresses the issue of a large amount of noise in the dataset by using optical flow (OF) to process the image data, and then converting the RGB image into YCbCr image. In the second section, the Sobel algorithm is improved to address the issues with traditional algorithms and controlled using FPGA technology.

3.1 Image preprocessing method based on YCbCr

Different from the situation where the scale distribution of detection objects is relatively uniform in actual environments and conventional applications, it is necessary to preprocess the video data to improve the training performance of subsequent models. The study used OF for preprocessing video data [10-11]. To ensure that the images in the input algorithm model contain more information, it is necessary to select the keyframe with the highest information content from the video clip as the input of the model. The extraction flow is denoted in Figure 1.

In Figure 1, firstly, the edge grayscale image is extracted from the initial image, and then its average edge intensity (AEI) is calculated. The expression for the AEI is shown in equation (1) [12-13].

$$D_i = \frac{\sum_{x=1}^{W}\sum_{y=1}^{H} edge_i(x,y)}{W \times H} \tag{1}$$

In equation (1), D_i denotes the AEI of the i th frame image. H and W denote the height and width of the grayscale edge image. $edge_i(x,y)$ denotes the grayscale edge image The higher the AEI of an image, the more information it contains and the higher its clarity.

The image with the highest AEI is selected from each segment and it is considered as the key image frame, with its position shown in equation (2).

$$Index = \arg\max(D_i) \tag{2}$$

In equation (2), denotes the max edge intensity of the image. In some cases, both the camera and objects in the scene are in motion, and OF calculations can be used to estimate the joint motion of the camera and objects. The OF method requires the assumption of constant brightness in advance, that is, the grayscale values of pixels remain stable and unchanged during motion. The formula for brightness consistency is indicated in equation (3).

$$I(x,y,t) = I(x+dx, y+dy, t+dt) \tag{3}$$

In equation (3), $I(x,y,t)$ denotes the grayscale value of a pixel point with x on the x-axis and y on the y-axis at time t. y represents the variation of pixel points. By expanding equation (3) with a first-order Taylor formula, the basic OF constraint equation is obtained, as shown in equation (4).

$$I_x u + I_y v + I_t = 0 \tag{4}$$

In equation (4), I_x, I_y, and I_t represent the partial derivatives of $I(x,y,t)$ to x, y, and t, respectively. For image data, dense OF needs to be obtained, which requires calculating the motion velocity vector of each pixel in the image, rather than only calculating a selected portion of the pixels [14-15]. Therefore, total variation regularization with L1 norm minimization (TV-L1) is used to extract the OF of video frames in both directions, with the objective function denoted in equation (5).

$$\min_{u,v} E(u,v) = \iint [|T(x,y) - I(x+u, y+u)| + \lambda(|\nabla u| + |\nabla v|)]dxdy \tag{5}$$

In equation (5), $I(x,y)$ represents the current video frame, $T(x,y)$ represents the reference video frame, and these two video frames are continuous. λ represents the weight parameter. u represents the horizontal offset of a pixel, while v represents the vertical offset of a pixel. $|\nabla u|$ and $|\nabla v|$ respectively represent the length of the two-dimensional gradient. By solving equation (5) through TV-L1, the simplified objective function is obtained as shown in equation (6).

$$\min_{u,v} E(u,v) = \int \left[|\lambda| \rho(v) + \frac{1}{2\theta}(u-v)^2 + |\nabla u| \right] dx \tag{6}$$

In equation (6), θ represents a constant. The image processed by OF method is still an RGB image. To extract more features, the RGB image is converted to a YCbCr image. The conversion from RGB to YCbCr is actually based on the conversion of three basic colors in the color space of brightness and chromaticity.

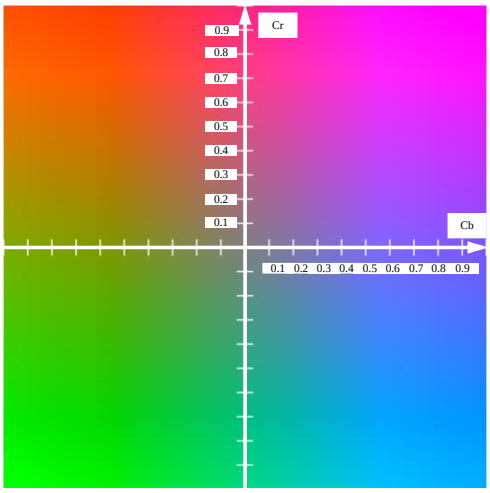


Figure 2: YCbCr color space.

image, while the chromaticity component denotes the color information. This separation makes it more flexible in handling brightness and chromaticity [16-17]. Secondly, the human eye is more sensitive to brightness information than chromaticity information, and different sampling rates can be used to handle the degree and chromaticity components when compressing images. Usually, the luminance component retains a higher resolution, while the chrominance component undergoes a higher degree of compression. The brightness component Y represents the brightness of the image, that is, the grayscale information. The brightness component usually occupies most of the information encoded in the image. The blue CDC Cb represents the color difference information of blue. The blue CDC denotes the difference between the blue color and brightness of a pixel. The red CDC Cr denotes the color difference information of red, and the red CDC represents the difference between the pixel's red color and brightness. The expression for converting the brightness component Y from the RGB color space is shown in equation (7).

$$Y = 0.299R + 0.587G + 0.114B \tag{7}$$

In equation (7), R refers to the value of the red CDC in RGB, G indicates the value of the green CDC in RGB, and B expresses the value of the blue CDC in RGB. The expressions for the blue CDC Cb and the red CDC Cr are shown in equation (8).

$$\begin{cases} Cb = -0.1687R - 0.3313G + 0.5B + 128 \\ Cr = 0.5R - 0.4187G - 0.0813B + 128 \end{cases} \tag{8}$$

YCbCr represents a pixel with three components, namely brightness component Y, blue color difference component (CDC) Cb, and red CDC Cr. There are two advantages to image processing using the YCbCr format. Firstly, the YCbCr format divides image colors into luminance and chrominance components. The brightness component represents the brightness information of the

In equation (8), B represents the value of the blue CDC in RGB. The color space of YCbCr is shown in Figure 2.

One of the main advantages of YCbCr is that it optimizes the perceptual characteristics of the human eye, allowing for more effective compression while maintaining image quality, fully utilizing the human eye's sensitivity to brightness changes and relatively low sensitivity to color changes.

3.2 Establishment of Image edge recognition model based on FPGA

After analyzing the original image data, the feature information in the data can be recognized. The research adopted Sobel algorithm combined with FPGA. Sobel operator is a classic edge detection method used in the fields of image processing and computer vision. This method recognizes edges in an image by calculating the gradient of image grayscale values [18-19]. The core feature of this method is directional detection ability, which can capture edge information in the X and Y directions through two convolution kernels, horizontal and vertical. Meanwhile, the Sobel operator can be extended to larger convolution kernels and more detection directions can be added to improve the accuracy of edge detection. In addition, the Sobel operator has a certain built-in smoothing effect, which gives it good noise suppression ability. Compared to simple differential operators, Sobel operator can effectively reduce small noise in images during edge extraction, ensuring its stability in low SNR images. Especially on hardware platforms such as FPGA, efficient parallel operations can be achieved, thereby improving processing speed. In terms of implementation, the Sobel operator algorithm has a simple principle and mainly uses addition and subtraction operations. It has low hardware and programming requirements and is easy to integrate into various image processing systems. Ultimately, the Sobel operator can generate clear edge responses in edge detection, resulting in distinct edge contours that are suitable for tasks such as image enhancement and feature extraction. The Sobel operator mainly uses convolution operations to calculate the gradient value of each pixel point, thereby detecting the edges of the image. The Sobel operator is based on a pair of 3×3 convolution kernels, which are used to calculate gradients in both directions. By convolving these two convolution kernels separately with the image, the gradient of the image in both directions can be calculated, as expressed in equation (9).

$$\begin{cases} G_x = \sum_{i=-1}^{1}\sum_{j=-1}^{1} K_x(i,j)\cdot I(x+i,y+i) \\ G_y = \sum_{i=-1}^{1}\sum_{j=-1}^{1} K_y(i,j)\cdot I(x+i,y+i) \end{cases} \quad (9)$$

In equation (9), K_x and K_y represent the convolution kernels in the horizontal and vertical directions, respectively. $I(x+i,y+i)$ represents the grayscale value of the image at the corresponding position. After calculating the gradient of each pixel in both directions, the gradient amplitude and direction of that point can be further calculated [20]. The gradient amplitude is indicative of the strength of the edge, while the gradient direction is representative of the edge's orientation. The expression is shown in equation (10).

$$\begin{cases} G = \sqrt{G_x^2 + G_y^2} \\ \theta = \arctan\left(\dfrac{G_y}{G_x}\right) \end{cases} \quad (10)$$

In equation (10), G represents the gradient amplitude and θ represents the gradient direction. However, an approximate value without a square is usually used instead to improve efficiency, so its expression can be rewritten as shown in equation (11).

$$|G| = |G_X| + |G_Y| \quad (11)$$

In equation (11), G_X and G_Y indicate the gradient amplitudes in the X and Y directions, respectively. An appropriate threshold is set based on the actual situation and accuracy requirements of image edge detection. When the gradient exceeds the threshold, it indicates that the pixel point is an edge point. Otherwise, the point is not an edge point. The judgment expression is shown in equation (12).

$$E = \begin{cases} 1 & \mathrm{G} \geq \mathrm{T} \\ 0 & else \end{cases} \quad (12)$$

In equation (12), E represents a Boolean quantity, T represents a threshold, and G represents the gradient amplitude. Although the Sobel operator has many advantages, its shortcomings are also quite obvious, as it is very sensitive to noise when detecting image edges.

The noise in the image can introduce high-frequency components, leading to an abnormal increase in gradient values and interfering with edge detection results. In this case, the edges detected using the Sobel operator may not be accurate and may even produce many false edges. The Sobel operator uses a fixed 3×3 convolution kernel, although this kernel size calculation is simple, it may not be flexible enough when processing images of different scales [21-22]. For images with rich details, a 3×3 kernel may not be sufficient to capture all the details, while for simple images, this kernel may introduce unnecessary computational complexity.

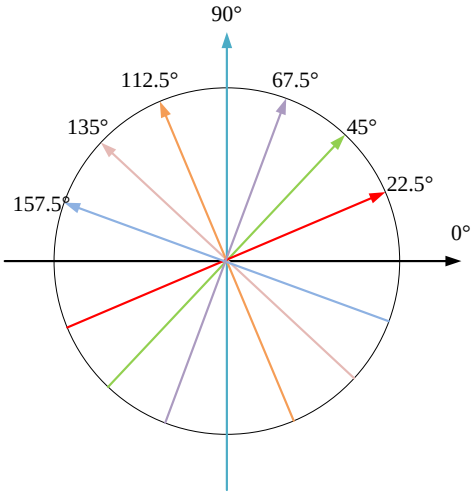


Figure 3: Direction detected by improved Sobel operator.

Therefore, it was improved by changing the size to 5×5 and eight directions based on the traditional 3×3 template, as shown in Figure 3.

The noise in the image can introduce high-frequency components, leading to an abnormal increase in gradient values and interfering with edge detection results. In this case, the edges detected using the Sobel operator may not be accurate and may even produce many false edges. The Sobel operator uses a fixed 3×3 convolution kernel, although this kernel size calculation is simple, it may not be flexible enough when processing images of different scales [21-22]. For images with rich details, a 3×3 kernel may not be sufficient to capture all the details, while for simple images, this kernel may introduce unnecessary computational complexity. Therefore, it was improved by changing the size to 5×5 and eight directions based on the traditional 3×3 template, as shown in Figure 3.

In Figure 3, in the improved Sobel operator, the eight angles are 0°, 22.5°, 45°, 67.5°, 90°, 112.5°, 135°, and 157.5°, respectively. By convolving the original image data with eight directional templates, the edge information of the image can be more complete, and each pixel can obtain eight different values. The improved Sobel module flowchart is shown in Figure 4. From Figure 4, it can be seen that firstly, a 5×5 filtering template is generated through two dual terminal RAM two-stage registers. Secondly, the derivatives in each direction are calculated separately. Then, the square root of the partial derivatives is calculated, and in contrast with the threshold, the value greater than the threshold is 1, and the opposite is 0. Finally, the row field signal and the enable signal are synchronously delayed. The study uses FPGA to control Sobel modules. FPGA is an integrated circuit device that can be programmed by users to achieve specific logic functions and digital circuits. FPGA has programmability and flexibility, and can be reconfigured and reprogrammed according to user needs. FPGA is composed of a large number of programmable logic units, programmable interconnect resources, and other supporting circuits. Programmable logic units allow users to define logical functions, while programmable interconnect resources are responsible for connecting

signal paths between logic units. Its structure is shown in Figure 5.

In Figure 5, configurable logic block (CLB) is the most basic programmable logic unit in FPGA, utilized to implement logic functions. CLB has programmable logic functions and connection resources, enabling it to implement various digital circuits. The arithmetic units in FPGA usually include adders, multipliers, and accumulators, which are used to implement tasks such as digital signal processing and algorithm operations. Block

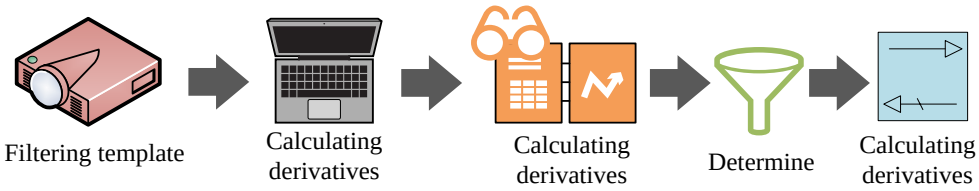


Figure 4: Improved Sobel module process.

RAM (BRAM) is a block storage unit used in FPGA to store data, with high-speed read and write characteristics and low power consumption. BRAM is typically used to store data, intermediate results, and algorithm parameters. Phase-locked loop (PLL) is a module in FPGA used to generate stable clock signals. It can generate multiple internal clock signals based on external clock signals and has the function of a PLL to ensure the stability and accuracy of clock signals. Input output block (IOB) refers to input/output resources, which are modules used in FPGA to connect external input/output signals and communicate with external devices. Network interconnection resources in FPGA are responsible for connecting various logic blocks, storage units, and input/output resources to form a complete digital circuit. The final model structure is shown in Figure 6.

In Figure 6, first is to generate a 5×5 matrix. Next is to calculate the mean of the matrix, and then calculate the gradients of the image in multiple directions, to enhance the edge detection effect. Then, the amplitude of the gradients in each direction is obtained by taking the square sum and square root of the gradients.

Subsequently, the adaptive threshold method is used to compare the gradient amplitude and determine whether it is an edge.

The final model is mainly divided into four modules. The first module is the filtering template generation module, which uses FPGA's dual terminal RAM to generate 5×5 Sobel templates for edge detection in different directions. The use of dual terminal RAM reduces access latency and provides sufficient band width to support parallel processing, making data flow smoother. Next is the gradient calculation module, which calculates gradients in the horizontal, vertical, and eight directions respectively. The gradient calculation in each direction is implemented through dedicated adders and multipliers, utilizing the parallel computing characteristics of FPGA to reduce processing time. In the sum of squares module, the gradient values in each direction are subjected to a sum of squares operation, followed by square root calculation to obtain the gradient amplitude of each pixel point. This module adopts the FPGA pipeline processing architecture, where each operation is executed within an independent clock cycle, ensuring the continuity of the data stream and improving computational efficiency. Finally, there is the threshold judgment module. After the gradient amplitude calculation is completed, the threshold judgment module performs adaptive threshold comparison on the amplitude to determine whether it is an edge. The Otsu method was used as the adaptive threshold method in the study. Firstly, the histogram of the image was calculated and the intra-class and inter-class variances were initialized. Then, by gradually traversing the gray levels, the optimal segmentation point is found, where the inter-class variance is maximized. Finally, the selected threshold is applied to edge detection.

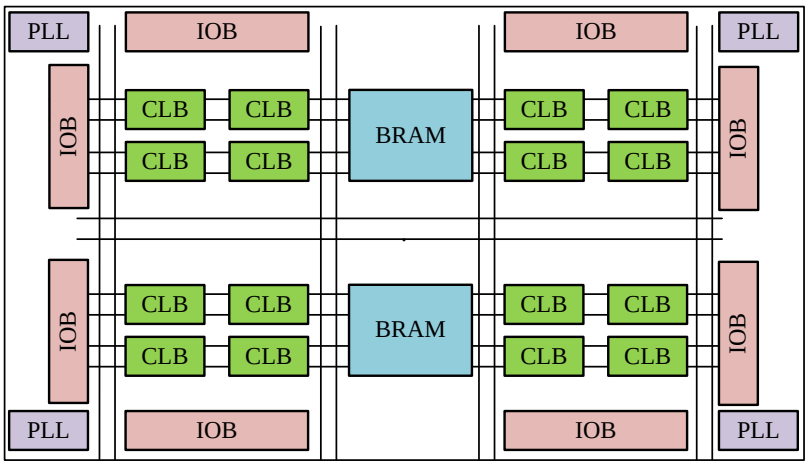


Figure 5: FPGA structure analysis.

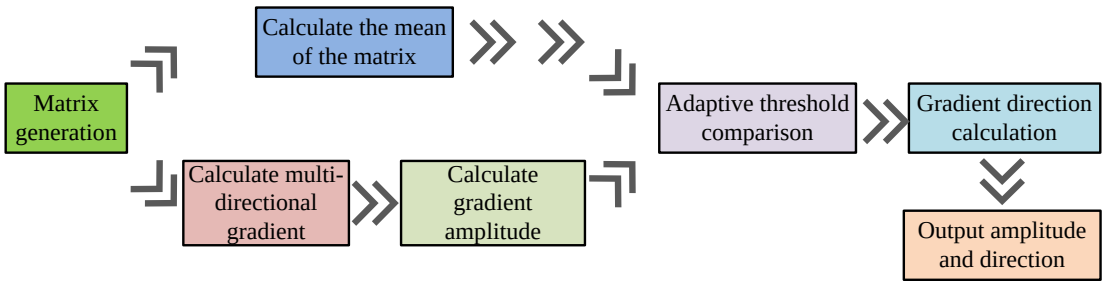


Figure 6: Flow of improved Sobel operator on FPGA.

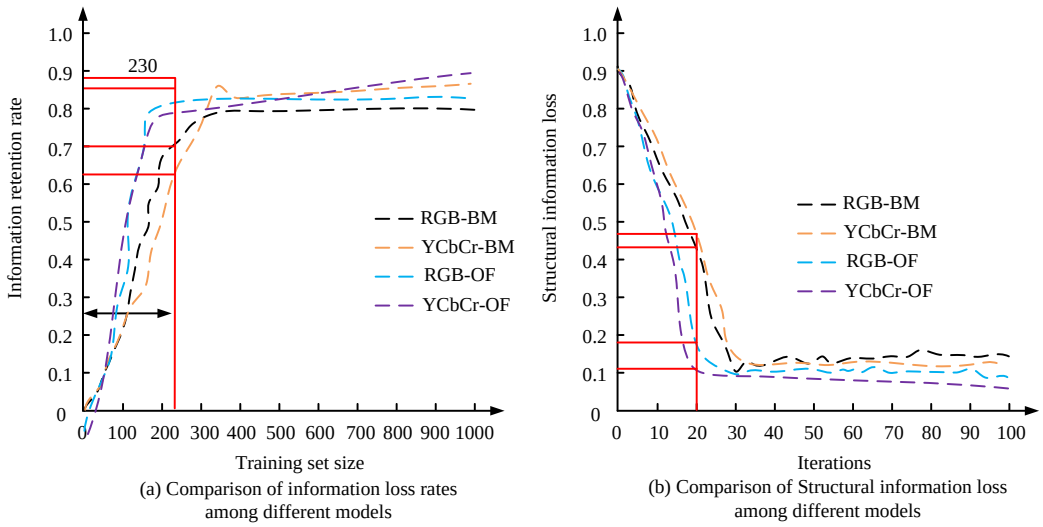


Figure 7: Comparison of information retention rate and structural information loss among various models.

4 Results

The first section of the study analyzes the performance of the raised data preprocessing method, and the second section analyzes and simulates the performance of the image edge detection model.

4.1 Image preprocessing method based on YCbCr

The server CPU used in the study was Inter (R) Core (TM) i5-10210U, with 16GB of RAM, NVIDIA Geforce GTX2080Ti GPU, and 8GB of video memory. The operating system was Windows 10. The dataset was the publicly available Kaggle dataset, named Kaggle Surveillance Video Dataset, which contains 6000 images extracted from surveillance videos at different time periods. It was mainly used for object detection and behavior recognition tasks. In terms of image properties, the dataset included color images or grayscale images in PNG format. The resolutions were 640x480 (VGA), 1280x720 (720p), and 1920x1080 (1080p). The diversity of image content was reflected in the pedestrians, vehicles of different types and colors, and various background scenes that may appear in the monitoring scene. The monitoring images also included different lighting conditions, covering both daytime and nighttime scenes, ensuring the diversity and complexity of the dataset. A dataset consisting of 6000 images was divided into a training set and a validation set in a 5:1 ratio. The introduction of Block Matching (BM) method was compared and analyzed with the method proposed in the study, and the results are shown in Figure 7.

Figure 7 (a) showcases the comparison of information retention rates of various models under different dataset sizes, and Figure 7 (b) showcases the comparison of structural information loss of various models under different iteration times. In Figure 7 (a), with the increase of the dataset, the information retention rate of the images processed by the four models also increased. When the dataset size was around 230, the performance of RGB-OF model and YCbCr-OF model basically reached the best. When the dataset size was 1000, the information retention rates of RGB-BM model, YCbCr-BM model, RGB-OF model, and YCbCr-OF model were 0.81, 0.83, 0.86, and 0.89, respectively. In Figure 7 (b), with the increase of iteration times, the loss of structural information in the images processed by the four models decreased. When the iteration times were around 20, the performance of RGB-OF model and YCbCr-OF model basically reached the best. When the amount of iterations was 100, the structural information loss of RGB-BM model, YCbCr-BM model, RGB-OF model, and YCbCr-OF model was 0.15, 0.13, 0.09, and 0.05, respectively. The experiment outcomes

illustrated that the proposed YCbCr-OF-based image preprocessing model had a high information retention rate and low structural information loss. The dataset was divided into dataset A and dataset B according to size, and the processing time of each model was compared. The findings are illustrated in Figure 8.

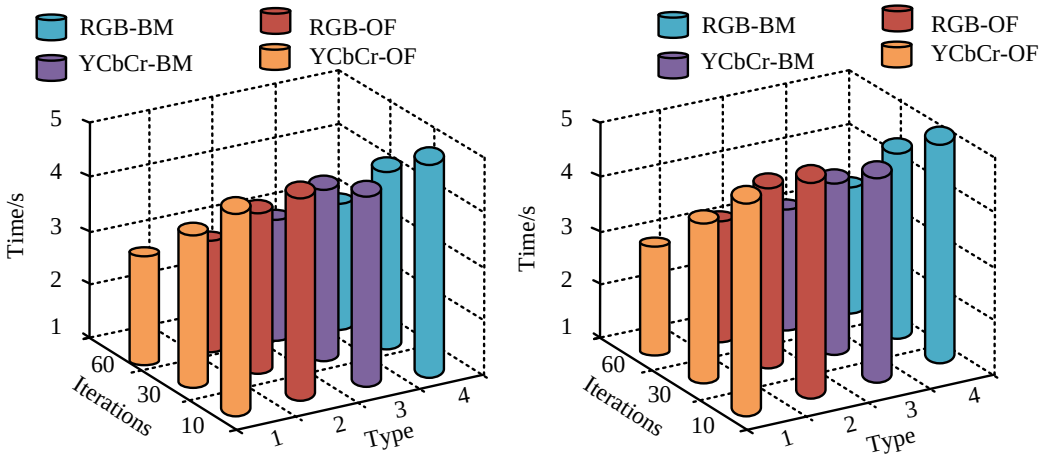
Figures 8 (a) and (b) show the recognition time of different algorithms in dataset A and dataset B, respectively. According to Figure 8 (a), the effectiveness of the model did not reach its optimal level when the number of iterations was low, resulting in longer recognition time. When the number of iterations was 60, the processing times for YCbCr-OF model, RGB-OF model, YCbCr-BM model, and RGB-BM model were 2.3, 2.6, 2.7, and 2.9 seconds, respectively. In Figure 8 (b), each algorithm model took slightly more time on dataset B than on dataset A. When the number of iterations was 60, the scheduling times for YCbCr-OF model, RGB-OF model, YCbCr-BM model, and RGB-BM model were 2.6s, 2.8s, 3.0s, and 3.1s, respectively. The findings illustrated that the developed algorithm model performed well in two different datasets, and the YCbCr-OF model took less processing time than other algorithm models. The comprehensive performance of the four models was analyzed, and the outcomes are indicated in Table 2.

According to Table 2, in dataset A, the loss function value (Loss), intersection over union (IoU), F1 value, and Micro F1 of the YCbCr-OF algorithm model were 0.189, 0.883, 0.612, and 0.957, respectively. In dataset B, the Loss, IoU, F1 value, and Micro F1 of the YCbCr-OF algorithm model were 0.177, 0.899, 0.618, and 0.939, respectively. The YCbCr-OF algorithm model proposed in the four methods has excellent performance in various aspects.

4.2 Analysis of image edge recognition model Based on FPGA

In the Roberts operator, the learning rate was set to 0.001, the batch size was 32, the number of iterations was 1000, the initial adaptive threshold was set to 20-40, and the step size was 5. In terms of FPGA configuration, the clock speed was 100 MHz, the data width was 16 bit fixed-point, the on-chip memory used 50% BRAM, and the power consumption was controlled within 10 W. To verify the performance advantages of FPGA, it was compared with CPU and GPU, and the results are shown in Table 3.

According to Table 3, the processing time of FPGA was 15 milliseconds, which is significantly faster than GPU's 28 milliseconds and CPU's 45 milliseconds. FPGA utilized its high parallel computing architecture to efficiently perform convolution operations and gradient calculations, thereby reducing computational latency and meeting real-time edge detection requirements. In terms of power consumption, the average power consumption of



(a) Comparison of time in dataset A

(b) Comparison of time in dataset B

Figure 8: Processing time of different models in different datasets.

Table 2: Comparison of comprehensive performance of models.

Index	Dateset	RGB-BM	YCbCr-BM	RGB-OF	YCbCr-OF
Loss	A	0.322	0.279	0.252	0.189
	B	0.308	0.267	0.238	0.177
IoU	A	0.751	0.793	0.82	0.883
	B	0.764	0.809	0.834	0.899
F1	A	0.472	0.515	0.542	0.612
	B	0.513	0.528	0.56	0.618
Micro F1	A	0.823	0.868	0.893	0.957
	B	0.837	0.879	0.907	0.939

Table 3: Performance Comparison of FPGA, GPU, and CPU.

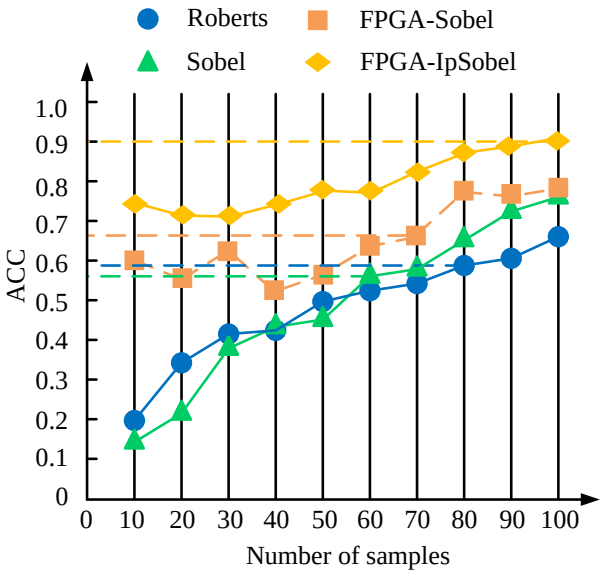
Implementation model	Hardware model	Average processing time (ms)	Average power consumption (W)
FPGA	Xilinx Zynq UltraScale+ MPSoC	15	4
GPU	NVIDIA GeForce RTX 2080	28	75
CPU	Intel Core i7-9700K	45	65

FPGA was only 4W, significantly lower than GPU and CPU. This indicates that the low-power characteristics of FPGA make it more suitable for deployment in power sensitive applications such as embedded systems and IoT devices.

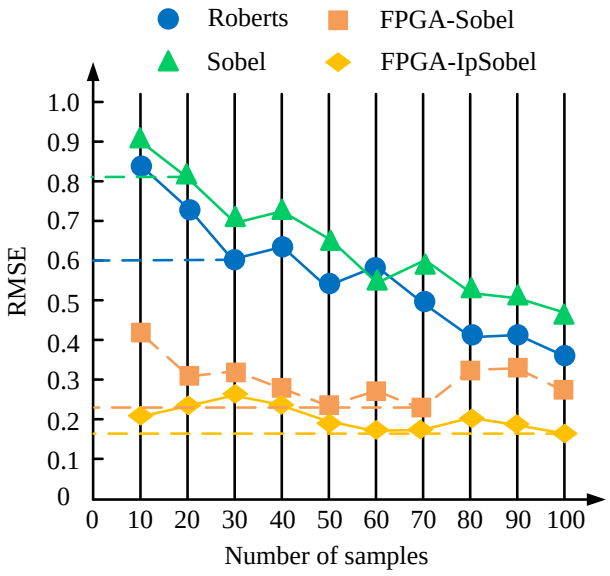
After verifying the effectiveness of the data preprocessing method, a performance analysis was conducted on the FPGA-based image edge detection model, and the Roberts operator model was introduced for comparison. The findings are indicated in Figure 9.

Figure 9 (a) represents the comparison of model accuracy (ACC) in case of different sample sizes and Figure 9 (b) represents the comparison of root mean square error (RMSE) in case of different sample sizes. From Figure 9(a), the ACC of each model increased as the sample size increased. The ACC of Roberts model, Sobel model, FPGA-Sobel model, FPGA-IpSobel model was 0.67, 0.77, 0.79, and 0.90 respectively for a data size of 100. From Figure 9(b), the RMSE values of the models were decreasing as the sample size increased. The RMSE values of Roberts' model, Sobel's model, FPGA-Sobel's model, and FPGA-IpSobel's model were 0.45, 0.37, 0.28, and 0.16, respectively, when the data size was 100. The experimental results show that the proposed FPGA-IpSobel model has a more excellent performance. Classic images in the image field were selected for analysis, and the outcomes are indicated in Figure 10.

Figure 10 (a) shows the image without edge recognition, and Figures 10 (b), (c), and (d) show the image processed by the FPGA-IpSobel model, FPGA-Sobel model, and Sobel model, respectively. From Figure 10, among the three models, the FPGA-IpSobel model was more satisfactory in image processing, retaining a large amount of details and having clearer edges.

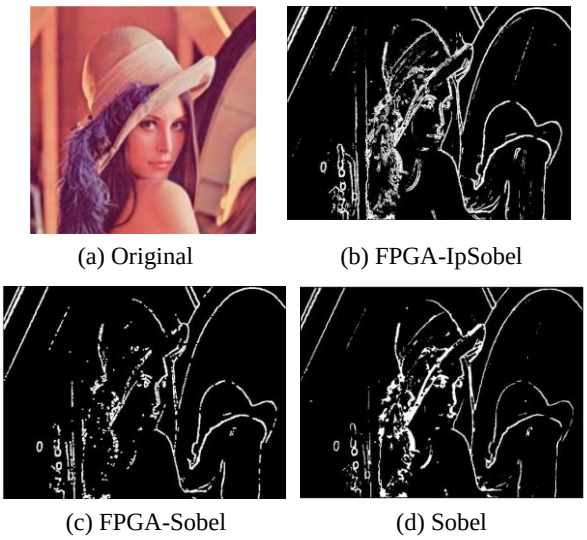


(a) Comparison of ACC among various models



(b) Comparison of RMSE among various models

Figure 9: Comparison of ACC and RMSE values for various models.



(a) Original (b) FPGA-IpSobel

(c) FPGA-Sobel (d) Sobel

Figure 10: Performance analysis of edge recognition model.

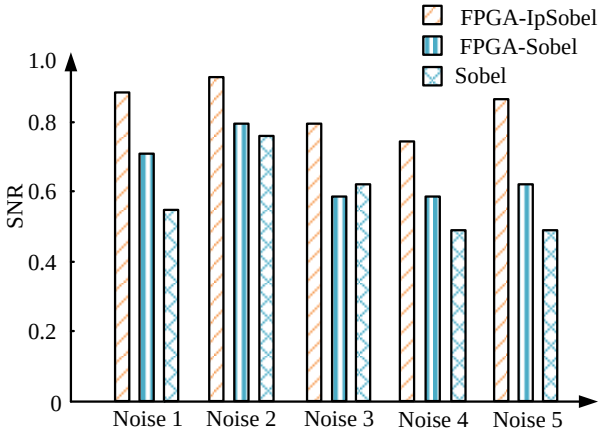


Figure 11: Comparison of SNR ratios for different noise images processed by various models.

Table 4: Actual performance analysis of various models.

Model	P	R	IoU	F1	mAP	Loss
Roberts	0.83	0.78	0.86	0.82	0.83	0.097
Sobel	0.87	0.81	0.92	0.87	0.84	0.082
FPGA-Sobel	0.90	0.86	0.96	0.91	0.88	0.076
FPGA-IpSobel	0.92	0.93	0.98	0.97	0.92	0.064

However, the FPGA-Sobel model and Sobel model had significantly poorer performance in image processing, with varying degrees of noise. The performance of the model was analyzed by selecting different types of noise, and the results are shown in Figure 11. Figure 11 shows the comparison of SNRs of different models for processing noisy images. From Figure 11, the proposed FPGA IpSobe model exhibited excellent performance in five different noisy images. Among the noisy images, the performance of each model was the best for image type 2 noise. The comprehensive effectiveness of each model was evaluated, and the findings are illustrated in Table 4.

According to Table 4, when comparing the performance of various algorithms, the difference between the Roberts method and the Sobel method was not significant, while the FPGA-IpSobel method performed well compared to the other three methods. The P-value, R-value, IoU value, F1 value, mAP, and Loss value corresponding to the FPGA-IpSobel method were 0.92, 0.93, 0.98, 0.97, 0.92, and 0.064, respectively. The experiment findings illustrated that the designed FPGA-IpSobel method exhibited excellent effectiveness.

5 Discussion

In the study, the proposed FPGA-IpSobel model demonstrated superior performance, with significant advantages in ACC and RMSE compared to other models. The experimental results showed that the FPGA-IpSobel model performed well in multiple performance indicators, such as an ACC of 0.90 under different sample sizes, which was significantly higher than the Roberts model and

the traditional Sobel model. This ACC difference was mainly due to the improved Sobel algorithm, which used a 5×5 convolution kernel and eight directional edge detection to enhance the ability to capture edge information. Meanwhile, the parallel processing capability of FPGA enabled multiple edge detection operations to be performed simultaneously, greatly improving processing speed. On the other hand, in terms of processing time, the RMSE of the FPGA-IpSobel model at a data volume of 100 was 0.16, significantly lower than that of the Roberts model and Sobel model. This efficiency improvement is mainly due to the hardware acceleration of FPGA. The hardware architecture of FPGA can efficiently configure computing resources, optimize data flow, and achieve fast real-time processing. In contrast, traditional models rely on CPUs or GPUs, which are limited by processing power and resource allocation, and can easily cause delays. In addition, the adaptive threshold processing method used in the FPGA model effectively filtered out edge information, reduces unnecessary calculations, and further improved processing efficiency. The difference between accuracy and efficiency was also reflected in the flexibility of model design. FPGA allows for the reconfiguration of logic units according to specific application requirements, providing broad space for algorithm optimization. However, traditional algorithms are often fixed and difficult to optimize specifically. In addition, models implemented on FPGA can achieve algorithm level optimization through specific hardware resources, fully utilizing the parallel computing characteristics of FPGA to improve overall efficiency.

6 Conclusion

A high-efficiency image edge recognition model combining Sobel algorithm and FPGA technology was proposed to address the real-time and processing efficiency issues of traditional edge detection algorithms. The model first performed YCbCr color space conversion on the image, then used Sobel operator to calculate the image gradient, and used adaptive thresholding to determine the edges. Finally, the model was implemented and optimized on FPGA. The experiment findings indicated that when the dataset size was 1000, the information retention rates of RGB-BM model, YCbCr-BM model, RGB-OF model, and YCbCr-OF model were 0.81, 0.83, 0.86, and 0.89, respectively, and the structural information loss was 0.15, 0.13, 0.09, and 0.05, respectively. When the data volume was 100, the ACC of Roberts model, Sobel model, FPGA-Sobel model, and FPGA-IpSobel model were 0.67, 0.77, 0.79, and 0.90, respectively, with RMSE values of 0.45, 0.37, 0.28, and 0.16, respectively. Among the three models, the FPGA-IpSobel model was more satisfactory in image processing, retaining a large amount of details and having clear edges, while the FPGA-Sobel model and Sobel model had significantly poorer performance in image processing, with varying degrees of noise. The research results indicated that the proposed FPGA-based image edge detection model improved the ACC and speed of image edge detection. However, there are also some shortcomings in the research, as the performance of this model is poor in scenarios such as high-frequency textures, complex lighting, or overlapping multiple objects. For example, in complex textured scenes such as forests, grasslands, and architectural complexes, due to the multitude of texture details, the adaptive thresholding method of the model may misidentify many small irrelevant textures as edges, leading to an increase in false edges and affecting the overall recognition accuracy. Future work can be improved in the following aspects. Firstly, a more robust edge detection algorithm is introduced and fused with Sobel algorithm to enhance the model's detection accuracy for texture backgrounds. In addition, based on the adaptive thresholding method, a scene-based threshold self-learning algorithm can be introduced to dynamically adjust edge detection parameters according to different scene features, thereby reducing false edges.

References

[1] Ádria Barros de Oliveira, and Fernanda Lima Kastensmidt. Evaluating fault-tolerant techniques on COTS RISC-V NOEL-V processor in Zynq UltraScale+ FPGA under proton testing. IEEE Transactions on Nuclear Science, 70(8):1708-1715, 2023. https://doi.org/10.1109/TNS.2023.3281396

[2] Wafa Gtifa, and Anis Sakly. Integrating Xilinx FPGA and intelligent techniques for improved precision in 3D brain tumor segmentation in medical imaging. Journal of Real-Time Image Processing, 20(6):115.1-115.15, 2023. https://doi.org/10.1007/s11554-023-01372-x

[3] Pei Yang, Wei Song, Xiaobing Zhao, Rui Zheng, and Letu Qingge. An improved Otsu threshold segmentation algorithm. International Journal of Computational Science and Engineering, 22(1):146-153, 2020. https://doi.org/10.1504/ijcse.2020.107266

[4] Zheng J, Gao Y, Zhang H, Lei Y, Zhang J. OTSU multi-threshold image segmentation based on improved particle swarm algorithm. Applied Sciences, 12(22):11514-11515, 2022. https://doi.org/10.1109/ICICSP48821.2019.8958573

[5] O. Vite-Chavez, J. Flores-Troncoso, Reynel Olivera-Reyna, and Jorge Ulises Munoz. Improvement procedure for image segmentation of fruits and vegetables based on the otsu method. Image Analysis and Stereology, 42(3):185-196, 2023. https://doi.org/10.5566/ias.2939

[6] Liping Chen, Jinhui Gao, António M. Lopes, Zhiqiang Zhang, Zhaobi Chu, and Ranchao Wu. Adaptive fractional-order genetic-particle swarm optimization Otsu algorithm for image segmentation. Applied Intelligence, 53(22):26949-26966, 2023. https://doi.org/10.1007/s10489-023-04969-8

[7] Wafa Gtifa, and Anis Sakly. Integrating Xilinx FPGA and intelligent techniques for improved precision in 3D brain tumor segmentation in medical imaging. Journal of Real-Time Image Processing,

20(6):115.1-115.15, 2023. https://doi.org/10.1007/s11554-023-01372-x

[8] Hyeonseok Hong, Dahun Choi, Namjoon Kim, Haein Lee, Beomjin Kang, Huibeom Kang, and Hyun Kim. Survey of convolutional neural network accelerators on field-programmable gate array platforms: architectures and optimization techniques. Journal of Real-Time Image Processing, 21(3):156-167, 2024. https://doi.org/10.1007/s11554-024-01442-8

[9] Sanjoli Narang, and Siddharth Tallur. Field-programmable gate array (FPGA) based programmable digital emulator of vibratory microelectromechanical systems (MEMS) gyroscopes. The Review of Scientific Instruments, 93(3):353-359, 2022. https://doi.org/10.1063/5.0065642

[10] Raúl Lora-Rivera, Óscar Oballe-Peinado, and Fernando Vidal-Verdú. Texture detection with feature extraction on embedded FPGA. IEEE Sensors Journal, 23(11):12093-12104, 2023. https://doi.org/10.1109/JSEN.2023.3268794

[11] Mara Pistellato, Filippo Bergamasco, Gianluca Bigaglia, Andrea Gasparetto, Andrea Albarelli, Marco Boschetti, and Roberto Passerone. Quantization-aware NN layers with high-throughput FPGA implementation for edge AI. Sensors, 23(10):141-149, 2023. https://doi.org/10.3390/s23104667

[12] Srinivasan Kalaiarasu, and Sudhakar Natarajan. Conducted electromagnetic interference mitigation on two-stage cascaded boost (TSCB) DC-DC converter using FPGA based DCPWM technique for EV Applications. Journal of Electrical Engineering & Technology, 18(3):2003-2013, 2022. https://doi.org/10.1007/s42835-022-01264-3

[13] Yuchen Yang, Zhongtao Shen, Xing Zhu, and Ziqi Wang. FPGA-based electronic system for the control and readout of superconducting quantum processors. The Review of Scientific Instruments, 93(7):74701.1-74701.14, 2022. https://doi.org/10.1063/5.0085467

[14] Christian Pilato, Zhenman Fang, Yuko Hara-Azumi, and Jim Hwang. Introduction to the special section on high-level synthesis for FPGA: next-generation technologies and applications. ACM Transactions on Design Automation of Electronic Systems, 27(4):29-31, 2022. https://doi.org/10.1145/3519279

[15] Yongli Gao, and Zijie Zhou. Automatic recognition and repair system of mural image cracks based on cloud edge computing and digitization. Mobile Information Systems, 22(31):1534596.1-1534596.12, 2022. https://doi.org/10.1155/2022/1534596

[16] K. P. Krishna Kumar, and Varghese Paul. Complementary spatial transformer network for real-time 3D object recognition a tiny deep learning model in target space. Journal of Real-Time Image Processing, 20(5):88.1-88.12, 2023. https://doi.org/10.1007/s11554-023-01340-5

[17] Yuzhuo Li, Jiang Lei, Xinrong Li, and Wenqian Feng. Non-contact clothing anthropometry based on two-dimensional image contour detection and feature point recognition. Industria Textila, 74(1):67-73, 2023. https://doi.org/10.35530/IT.074.01.202279

[18] Florian A. Mann, Phillip Galonska, Niklas Herrmann, and Sebastian Kruss. Quantum defects as versatile anchors for carbon nanotube functionalization. Nature Protocols, 17(3):727-747, 2022. https://doi.org/10.1038/s41596-021-00663-6

[19] Yanmin Guo, Yu Wang, Kai Meng, and Zongna Zhu. Otsu multi-threshold image segmentation based on adaptive double-mutation differential evolution. Biomimetics, 8(5):418-421, 2023. https://doi.org/10.3390/biomimetics8050418

[20] Bo Xu, Songting Zou, Libing Bai, Kai Chen, and Jia Zhao. A general discrete memristor emulator based on Taylor expansion for the reconfigurable FPGA implementation and its application. Nonlinear Dynamics, 112(2):1395-1414, 2024. https://doi.org/10.1007/s11071-023-09092-4

[21] Padmaprabha Preethi, and Hosahalli Ramappa Mamatha. Region-based convolutional neural network for segmenting text in epigraphical images. Artificial Intelligence and Applications, 1(2):119-127, 2023. https://doi.org/10.47852/bonviewAIA2202293

[22] Oussama Azzouzi, Mohamed Anane, Mouloud Koudil, Mohamed Issad, and Yassine Himeur. Novel area-efficient and flexible architectures for optimal Ate pairing on FPGA. Journal of supercomputing, 80(2):2633-2659, 2024. https://doi.org/10.1007/s11227-023-05578-5

Consumer Behavior Analysis and Enterprise Marketing Strategy Optimization Based on Decision Tree Model and Association Rule Algorithm

Hui Wang
School of Economics and Management, Liuzhou Institute of Technology, Liuzhou 545006, Guangxi, China
E-mail: wanghui_edu@hotmail.com

Keywords: big data, consumer behavior, enterprise, marketing strategy

Recieved: September 25, 2024

With the rapid advancement of big data technology, enterprises are encountering increasingly complex market environments, making consumer behavior patterns harder to predict. This study leverages big data analysis to explore the relationship between consumer behavior and corporate marketing strategies. Using a combination of decision tree models and association rule algorithms, we analyze the purchasing behaviors of 1,000 consumers in Shenyang City. The results indicate that personalized marketing and dynamic pricing strategies significantly enhance sales growth and customer loyalty. Specifically, dynamic pricing strategies resulted in a 16.7% increase in sales growth, while personalized promotions led to a 10.5% increase in customer retention. The decision tree model achieved an accuracy of 89.5%, with key performance metrics including precision, recall, and F1-score being evaluated for model performance. Furthermore, the association rule algorithm identified frequent purchase patterns with a support degree of 0.25 and a confidence degree of 67%. These findings highlight the importance of accurate consumer behavior analysis in optimizing marketing strategies, improving market competitiveness, and increasing customer loyalty. The study demonstrates that big data-driven approaches can effectively guide enterprises in making data-informed, real-time marketing decisions.

Povzetek: Prispevek analizira več klasičnih modelov strojnega učenja in značilk (npr. Count Vectorizer, TF-IDF) za zaznavanje sovražnega govora, pri čemer se najboljši rezultati doseženi z algoritmom naključnih gozdov..

1 Introduction

In the modern marketplace, characterized by rapid e-commerce development and the pervasive application of big data technology, enterprises face increasingly intense competition. Consumer behavior patterns and purchasing preferences have grown more complex and diverse, rendering traditional marketing strategies insufficient to meet individualized needs. Big data analysis allows enterprises to accurately capture consumer behavioral traits, enabling the development of more adaptive and effective marketing strategies. In China's dynamic consumer market, data derived from consumers' online activities, purchasing decisions, and brand interactions offers a rich resource for businesses. By leveraging this data, companies can gain deeper insights into their target markets and execute precise, personalized marketing through product recommendations, pricing strategies, and promotional campaigns. This study employs big data analysis to examine consumer behavior patterns and investigate methods to enhance sales revenue and market competitiveness through personalized marketing and dynamic pricing strategies.

Suleymanov examined the intricate relationship between consumer behavior and agricultural markets, highlighting behavioral differences across various market contexts and proposing strategies based on consumer preferences in the agricultural sector [1]. Duarte et al. introduced the "Ethical Consumer Behavior Scale," emphasizing the influence of corporate social responsibility on consumer behavior [2]. Niewczas-Dobrowolska et al. explored the impact of COVID-19 on consumer behavior, noting significant changes in purchasing preferences and decision-making processes that compelled businesses to revise their market strategies [3]. Rozenkowska systematically reviewed the application of planned behavior theory in consumer behavior research, underscoring its utility in understanding purchasing decisions [4]. Uliana investigated the behavioral traits of online consumers in Brazil, finding that price sensitivity and social media interactions significantly shaped purchasing choices [5]. Zhang et al. analyzed consumer behavior within the sharing economy, revealing how strategic consumer actions influenced market performance and transaction efficiency [6]. Yang et al. studied the role of value co-creation in fostering consumer citizenship behaviors, proposing that enterprises can bolster brand loyalty and engagement through collaborative value creation [7].

With increasing consumer demand for diversity and personalization, traditional marketing strategies fail to satisfy various consumer groups, leading to customer attrition and reduced competitiveness. The e-commerce and digital marketing era further complicate matters, as consumers' behavioral trajectories and purchase preferences are increasingly difficult to predict. Extracting meaningful insights from vast consumer data to formulate accurate marketing strategies has become a critical challenge for businesses. The volatile market environment, characterized

by fluctuating prices and the necessity for real-time adjustments to promotional strategies, further complicates dynamic pricing and marketing decisions. This study seeks to analyze consumer behavior patterns through big data technology to assist enterprises in making informed and flexible decisions in personalized marketing and dynamic pricing, thereby enhancing market share and customer loyalty.

With the rapid development of the information society, the relationship between electronic technology, artificial intelligence and the information society has become increasingly close, which has a profound impact on the market strategy and consumer behavior analysis of modern enterprises. In The Relationship between Electronics, Artificial Intelligence, and the Information Society Through the Rules of the Information Society, Matja Gams and Tien Kolenic [8] emphasize that the rules and technical frameworks of the information society provide the foundation for the application of artificial intelligence, while enhancing the decision-making ability of enterprises in complex market environments. They pointed out that by combining electronic technology and artificial intelligence, consumer behavior data can be mined and analyzed more efficiently, helping companies achieve personalized marketing and dynamic pricing strategies. This is highly consistent with the goal of this study to analyze large-scale consumer data through decision tree models and association rule algorithms to optimize the market competitiveness of firms. Citing relevant research results further supports the importance of big data technology in marketing and provides theoretical basis and technical guidance for this study.

To achieve these objectives, this study employs a decision tree model and association rule algorithm as technical tools. The decision tree model allows enterprises to construct effective classification models based on consumer behavior characteristics, identify key factors influencing purchase decisions, and segment the market. Meanwhile, the association rule algorithm uncovers correlations between product purchases, revealing consumers' preferred shopping combinations and informing strategies such as product bundling and targeted promotions. By processing and analyzing large-scale data, these technologies enable businesses to dynamically refine marketing strategies and optimize pricing, thereby enhancing overall competitiveness and profitability. This study provides robust scientific decision-making support for enterprises navigating complex market environments and underscores the theoretical and practical importance of applying big data analysis to marketing, as shown in Table 1

Table 1 Summary of current relevant studies

Study	Methodology	Data	Results	Key Findings	Identified Gaps
Suleymanov [1]	Behavioral analysis in agricultural markets	Consumer preferences in agricultural settings	Identified market-specific consumer patterns	Market behavior varies significantly across regions and needs tailored marketing strategies	Limited focus on urban consumer behaviors and non-agricultural sectors
Duarte et al. [2]	Ethical Consumer Behavior Scale development	Ethical consumer surveys	Scale validated to measure ethical consumer traits	CSR significantly impacts consumer behavior	Does not explore transactional or behavioral data
Niewczas-Dobrowolska et al. [3]	Impact of COVID-19 on consumer behavior	Pandemic-era consumer data	Shifts in preferences for essential goods	COVID-19 significantly altered consumer priorities and purchase decision processes	Context-dependent, not generalizable post-pandemic
Rozenkowska [4]	Theory of Planned Behavior in consumer studies	Decision-making datasets	Demonstrated planned behavior theory validity	The theory effectively explains decision-making processes	Lacks application to real-time or dynamic decision-making scenarios
Uliana [5]	Analysis of online consumer behavior	Data from Brazilian e-commerce platforms	Social media and price sensitivity as major factors	Online interaction heavily influences purchasing choices	Limited to regional online consumer behavior without cross-channel integration
Zhang et al. [6]	Sharing	Transactional data	Strategic	Strategic	Narrow

	economy consumer behavior analysis	from sharing platforms	behavior impacts market efficiency	consumer decisions can improve market performance	application scope focused on sharing platforms
Yang et al. [7]	Value co-creation and consumer citizenship	Consumer engagement and brand loyalty data	Value co-creation strengthens brand relationships	Co-created value positively affects loyalty and consumer-brand participation	Lacks quantitative data on purchase patterns
This Study	Decision tree model and association rule algorithm	Multisource data: purchase records, online behavior, social media	Sales growth: dynamic pricing (16.7%), personalized promotions (12.4%)	Personalized strategies, dynamic pricing, and membership programs enhance sales and loyalty	Addresses dynamic adaptation but can integrate advanced machine learning methods for improved generalization

The limitations of existing research, including a lack of real-time adaptability, limited cross-channel analysis, and insufficient quantitative evaluation of purchasing patterns, emphasize the need for a robust, data-driven methodology. By integrating decision tree models and association rule algorithms, this study addresses these gaps effectively. The decision tree model provides clear interpretability and the ability to handle nonlinear relationships, making it suitable for analyzing complex consumer behaviors and segmenting markets. Meanwhile, association rule algorithms efficiently uncover purchase correlations, enabling the identification of actionable insights for personalized marketing strategies. This combined approach is critical in leveraging multisource data—such as purchase records, online behaviors, and social interactions—to formulate precise and dynamic strategies. Its adaptability to fluctuating market demands and diverse consumer preferences ensures relevance in modern, highly competitive environments. Furthermore, the application of these methods bridges the gap between theoretical frameworks and practical implementation, contributing significantly to the advancement of big data-driven marketing strategies.

2 Materials and methods

2.1 Data collection and teleprocessing

2.1.1 Description of data sources

The data sources for this study include the following three aspects.

(1) Consumer purchase records: The data were collected from 1000 consumers in Shenyang from January to March 2024, covering online and offline purchasing behaviors, mainly related to food, daily necessities and electronic products. A total of 7869 items of purchase data were collected, including details on product categories, purchase frequency, payment methods and shopping channels. As shown in Figure 1.

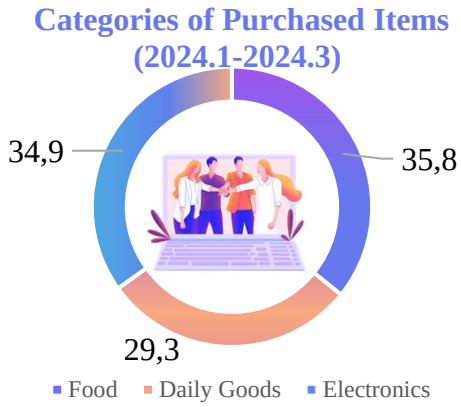


Figure 1: Categories of purchased items

(2) Online behavior data: collect browsing history, click behavior, search keywords and other information of users through the user logs of Jingdong platform. The total amount of data is 85436 pieces. After re-processing, this part of data will be used to analyze consumer behavior patterns.

(3) Social media interaction data: Collected from the API of Weibo and wechat, including users' comments, likes and sharing behaviors on brands, 37892 pieces of relevant interaction data were collected. Multi-source data provides a reliable data basis for consumer behavior feature extraction and marketing strategy design.

2.1.2 Data cleaning and reprocessing steps

In this study, data cleaning and processing are essential to ensure data quality. For the 7869 purchase records analyzed, approximately 1.6% of the data contained missing values, such as unfilled product categories or payment methods. Missing values were addressed using mean imputation for numerical variables and deletion for records with extensive missing information. Redundant data, resulting from repeated consumer purchase behaviors, accounted for about 3.2% of the dataset. These duplicates were identified and removed by cross-checking unique identifiers, including user IDs and order numbers. Outlier detection and processing were also conducted, with items exhibiting abnormally high purchase

frequencies or exceptionally low transaction amounts being identified and excluded through predefined upper and lower thresholds. Finally, the dataset was standardized and normalized to harmonize features such as purchase amounts and transaction frequencies, ensuring uniform scaling across all variables for model training. These meticulous steps significantly enhanced the dataset's integrity, providing a robust foundation for subsequent consumer behavior analysis and ensuring reliable insights [9].

For model training and validation, the data preprocessing pipeline involves several crucial steps. Initially, raw consumer behavior data, including purchase records, browsing logs, and social interactions, were cleaned and standardized. Outliers were removed using interquartile range (IQR) methods, and missing values were handled with mean imputation for numerical features. Feature engineering was performed by transforming categorical data into one-hot encoded variables and normalizing continuous features using Min-Max scaling. Dimensionality reduction was applied to high-dimensional data using Principal Component Analysis (PCA), which helped reduce feature space while maintaining 95% of the variance. For model training, a decision tree was chosen due to its interpretability, and hyperparameters were optimized using grid search with cross-validation. The association rule algorithm used the Apriori method, with a minimum support threshold of 0.05 and confidence of 0.6. Model validation was carried out using a hold-out test set, with accuracy, precision, recall, and F1-score as evaluation metrics. These methods ensure that the analysis is both reproducible and transparent, supporting the accuracy and robustness of the resulting marketing strategies.

During the data cleaning process, specific steps were taken to handle missing and redundant data across multiple datasets. Missing values in the purchase records dataset, accounting for 1.6% of the data, were imputed using the mean for numerical attributes (e.g., purchase amount) and mode for categorical attributes (e.g., product category). For the browsing logs dataset, missing entries were excluded if they constituted less than 5% of the total records, as they were deemed non-critical to the analysis. Redundant data, identified as duplicate entries with the same user ID, timestamp, and product information, was filtered out using a combination of hashing and unique identifier matching, which removed 3.2% of the records. For the social interaction data, overlapping interactions (e.g., multiple likes or comments on the same post) were consolidated into a single entry to avoid inflating activity levels. All datasets were standardized to ensure uniform formatting and normalized to align numerical features such as transaction values, ensuring consistency across data sources. These measures ensured that the cleaned dataset-maintained integrity and was free from biases introduced by missing or redundant entries.

2.1.3 Consumer behavior feature extraction and data integration

After data cleaning is completed, the characteristics of consumer behavior are extracted and data integration is carried out. Five main characteristics are extracted from the purchasing data of consumers. As shown in Table 2.

Table 2: Consumer behavior feature categories

Feature Category	Description
Purchase Frequency	Average monthly purchases per consumer
Purchase Amount	Average spending per consumer (RMB)
Product Preference	Preference for specific product categories
Payment Method Preference	Percentage of consumers choosing mobile payment

(1) Purchase frequency: By analyzing the average monthly purchases of consumers to determine their consumption activity, it is found that the average monthly purchases of consumers in Shenyang are 2.7 times.

(2) Purchase amount: Calculate the average purchase amount of each consumer, and the average is 356.78 yuan.

(3) Product preference: Based on product categories, consumers' preferences for food, daily necessities and electronic products are extracted. The preference for food products accounts for the highest proportion, reaching 35.8% [10].

(4) Payment preference: By analyzing the payment methods chosen by consumers, it is found that more than 60% of consumers choose mobile payment.

(5) Purchase channels: The proportion of online and offline purchase behaviors is classified as behavioral preferences. The feature data is integrated with consumer online behavior and social interaction data to more comprehensively characterize consumer behavior and form a complete data set for market segmentation and marketing strategy design.

2.2 Model construction

2.2.1 Model selection

In this study, in order to accurately analyze consumer behavior and optimize the marketing strategy of enterprises, the combination of decision tree model and association rule algorithm is chosen. Decision tree model can recursively segment the data, reveal the key characteristics of consumer behavior and its decision path, and is suitable for dealing with nonlinear relations [11]. Decision trees perform well in classification and regression tasks, and their easy interpretation helps enterprises understand the logic of consumers' purchasing behavior. The loss function of the decision tree model is set to minimize the sum of squares of error, and the objective function of the model is shown in Equation (1).

$$L(\theta) = \sum_{i=1}^{n} (y_i - f(x_i, \theta))^2 \quad (1)$$

y_i is the true value, $f(x_i, \theta)$ is the predicted value of the model, and θ is the model parameter.

Association rules algorithms uncover potential associations between goods by looking for frequent item sets in the data. This algorithm is suitable for mining purchase combination patterns among consumer goods. According to Apriori, consumers who buy groceries have a 67.3 percent probability of buying food [12]. This correlation helps companies make product portfolio recommendations. The confidence formula of association rules is shown in Equation (2).

$$Confidence(A \Rightarrow B) = \frac{Support(A \cap B)}{Support(A)} \quad (2)$$

To ensure the robustness and generalizability of the model, the dataset was split into training and testing sets with a 7:3 ratio. Model accuracy was evaluated using cross-validation to validate the reliability and effectiveness of the selected approach. The decision to use the decision tree model and association rule algorithm was guided by the study's goal of analyzing consumer behavior through big data to develop actionable marketing strategies. These models offer several advantages in specific application scenarios:

(1) Ease of interpretation: Decision tree models provide a high level of interpretability compared to complex black-box models such as neural networks [13]. In practical business applications, it is crucial not only to predict outcomes but also to understand the decision-making process behind consumer behavior. Decision trees clearly highlight key factors influencing decisions, such as price or product type. Neural networks, while capable of handling high-dimensional data, are less practical for marketing strategy design due to their complexity and limited interpretability.

(2) Handling nonlinear relationships: Consumer behavior often involves complex nonlinear patterns. Decision tree models excel at capturing these interactions, providing a better fit for data with such characteristics. By contrast, linear regression models are limited to linear relationships and fail to address the intricacies of consumer behavior.

(3) Efficient extraction of commodity correlations: The association rule algorithm effectively identifies correlations between commodities from large datasets, supporting accurate product bundling and promotion strategies by uncovering frequent purchase combinations. Unlike clustering algorithms, which focus on grouping similar consumer profiles, association rules are particularly suited for analyzing discrete data and detecting relationships between purchasing behaviors and products [14].

Together, the decision tree model's interpretability and the association rule algorithm's ability to uncover product correlations provide a comprehensive and practical framework for developing effective marketing strategies.

The decision to use decision tree models and association rule algorithms over more modern techniques like ensemble methods (e.g., Random Forests) or gradient boosting methods was driven primarily by the need for model interpretability and computational efficiency. While ensemble methods typically outperform individual decision trees in terms of prediction accuracy, they do so at the cost of model complexity and reduced interpretability. For consumer behavior analysis, where understanding and explaining the decision-making process is crucial, the interpretability of a decision tree becomes a valuable asset. Additionally, the data used in this study, which includes consumer purchase records, browsing logs, and social interactions, exhibits complex, yet often relatively straightforward, decision-making patterns that can be effectively captured by a decision tree model. The simplicity of decision trees allows for transparent insights into how features such as product categories and customer demographics influence purchasing decisions. Thus, the choice of the decision tree model was based on a trade-off between predictive power and the need for an understandable model that can directly inform marketing strategies. The association rule algorithm was chosen to uncover hidden patterns in customer purchasing behavior, offering valuable insights into product co-purchase behaviors, which are key for designing personalized marketing campaigns.

The decision tree model and association rule algorithms used for consumer behavior analysis offer clear advantages over recent advancements like ensemble learning, deep neural networks, or clustering algorithms, particularly in terms of interpretability and computational efficiency. Decision trees, unlike deep neural networks, provide a transparent and easily interpretable structure, which is crucial for enterprises seeking to understand consumer decision-making processes. While ensemble methods like random forests can improve accuracy, they lack the intuitive decision paths that decision trees provide, making them less practical for marketing strategy design. Deep learning models, although powerful, require large datasets and computational resources that may not be readily available in typical market scenarios. Furthermore, clustering algorithms are primarily used to group similar consumers but do not capture transactional relationships between products as effectively as the association rule algorithm. The decision to use these models is thus driven by their ability to directly address the specific needs of businesses, offering both high predictive accuracy and actionable insights for dynamic pricing and personalized promotions, without the complexity and resource requirements of newer techniques.

2.2.2 Design of consumer behavior analysis model based on big data

In this study, the consumer behavior analysis model based on big data adopts the combination of decision tree model and association rule algorithm to comprehensively analyze consumers' purchasing behaviors and preferences [15]. The consumer's behavior characteristic data is taken as input variable, and the decision tree model is combined to make classification prediction of consumer's purchasing behavior.

The feature set is X = {x1, x2, ... xn}, the target variable is the consumer's purchase decision Y, and the prediction function of the model is shown in Equation (3).

$$Y = f(X, \theta) \quad (3)$$

θ is the parameter of the model. The decision tree constructs a series of decision nodes by recursively dividing the feature space. The selection of each node is based on the information gain or Gini index. The entropy of the current node is H(X), and the information gain calculation formula is shown in Equation (4).

$$IG(T, X) = H(T) - \sum_{i=1}^{n} \frac{|T_i|}{|T|} H(T_i) \quad (4)$$

H(T) represents the entropy of the initial data set, and $H(T_i)$is the entropy of the partitioned subset. By maximizing information gain, the optimal features are selected for node segmentation. The decision path generated by the model will clarify how the behavioral characteristics of consumers affect their purchase decisions. On this basis, association rules algorithms are used to discover potential patterns in consumer buying behavior. The Apriori algorithm is used to analyze product purchase records, generate frequent item set F, and then establish the association relationship between products based on the support and confidence of the association rules [16]. The calculation formula of support degree is shown in Equation (5).

$$Support(A \Rightarrow B) = \frac{Support(A \cap B)}{N} \quad (5)$$

In order to improve the robustness of the model, the data set is divided into training sets and test sets, and the cross-validation method is used for evaluation to ensure the generalization ability of the model.

By integrating the decision tree model and association rule algorithm, this consumer behavior analysis model focuses on extracting essential behavioral characteristics from big data and identifying underlying patterns in purchasing behaviors. The decision tree model iteratively segments consumer behavior attributes, such as purchase frequency, spending amount, and product preferences, to elucidate how these factors influence purchasing decisions. This model effectively handles nonlinear relationships while providing a transparent decision-making process through an intuitive tree structure, enabling enterprises to comprehend consumer behavior more deeply [17]. The association rule algorithm identifies correlated purchasing patterns across products, revealing consumer preferences by analyzing frequently co-purchased items. For example, the analysis highlights that consumer buying daily necessities often purchase food. The model integrates data from various sources, including purchase records, online interactions, and social media activity, leveraging these algorithms to deliver actionable marketing strategies and enhance personalized product recommendations.

2.2.3 Data processing layer and feature selection configuration

The data processing layer and feature selection configuration are critical components of this model. The data processing layer integrates and transforms multi-source data, such as consumer purchase records, online browsing behavior, and social media interactions. Data is first standardized and normalized to ensure consistency across features, thereby mitigating biases during model training. Categorical variables, such as payment methods and product categories, are converted into numerical formats suitable for machine learning algorithms [18]. Feature selection employs recursive feature elimination (RFE) and importance score-based algorithms to identify the most influential features for predicting consumer behavior. Key features include purchase frequency, product preferences, and payment method choices. These selected features are then used for model training and behavioral pattern recognition, improving computational efficiency, enhancing model accuracy, and enabling enterprises to design more precise and effective marketing strategies.

2.2.4 Implementation and optimization of decision tree and association rule algorithm

In this study, decision tree and association rule algorithms help enterprises optimize their marketing strategies by analyzing consumer behavior data. According to the decision tree model, the classification model is trained by using the purchasing data of 1000 consumers in Shenyang.

As shown in Table 3, the decision tree selects the optimal segmentation point according to the information gain or Gini index, which is characterized by "Purchase Amount". By calculating the information gain, it is found that for the feature of "purchase amount", the segmentation point with the lowest Gini index is 350yuan, and the model forecasts 1000consumers [19]. Classification accuracy is 89.5%. According to the characteristics "purchase frequency" and "product preference", the model optimizes the segmentation points and improves the classification accuracy.

In the association rule algorithm, the Apriori algorithm is used to analyze the correlation of commodity purchases. In the commodity purchase mix, it is found that the support degree of "food" and "daily necessities" is 0.25, and the confidence degree is 0.67. Through calculation, the rule is formed as "consumers who buy food have a 67% probability of buying daily necessities". Optimize rule filtering to ensure the validity and practicality of rules by adjusting support and confidence thresholds.

If the Support degree of the combination of " Food ⇒ DailyGoods " is 0.25and the total number of consumers is 1000, the support degree of this rule is calculated as follows, as shown in Equation (6).

$$Support(Food \Rightarrow DailyGoods) = \frac{250}{1000} = 0.25 \quad (6)$$

The confidence is calculated, as shown in Equation (7).

$$Confidence(Food \Rightarrow DailyGoods) = \frac{Support(Food \cap DailyGoods)}{Support(Food)} = \frac{250}{375} = 0.67 \quad (7)$$

Table 3: Sample consumer behavior data

Consumer ID	Purchase Frequency	Purchase Amount (RMB)	Product Preference	Payment Method	Channel Preference
001	3.2	357.89	Food	Mobile Payment	Online
002	1.8	421.75	Electronics	Credit Card	Offline
003	2.5	279.32	Daily Goods	Mobile Payment	Online
004	4.1	689.47	Electronics	Mobile Payment	Offline

Through the above calculation, association rules help to identify the product mix with high correlation, and provide the basis for personalized recommendation of marketing strategy.

The thresholds for the association rule metrics, namely support, confidence, and lift, were determined based on both computational considerations and practical business relevance. The support threshold was set to 0.01 to ensure that only the most frequent itemsets, which are relevant to a significant portion of the consumer base, were considered. A higher support threshold may result in too few associations, while a lower threshold might lead to the inclusion of rules that are not practically useful. Confidence was set at 0.7, indicating that the rule must have a relatively high likelihood of occurring in the data, which strikes a balance between specificity and generality. Finally, the lift threshold was set at 1.2 to focus on rules that provide significant value over random chance, ensuring that identified patterns are meaningful and actionable. These thresholds were chosen to optimize both computational efficiency and the practical applicability of the rules in formulating targeted marketing strategies. While these thresholds help narrow down the number of associations to a manageable and meaningful set, they may also exclude less obvious but potentially valuable rules, which is a limitation inherent in setting arbitrary thresholds.

2.3 Training and verification

2.3.1 Model training

In this study, model training is the key to the successful implementation of decision tree and association rule algorithms. The training data set of the model comes from the purchase records of 1000 consumers in Shenyang City from January to March 2024, with a total of 7869 purchasing behavior data. The data set is divided into training sets according to the proportion of 70% for training the model and 30% for subsequent verification. In the process of decision tree model training, information gain is used as the main segmentation standard to determine the optimal features of each node. Firstly, the model performs recursive segmentation on consumer behavior characteristics (such as purchase frequency, purchase amount) to form multiple decision paths, each path corresponds to different behavior decisions of consumers. In the training process, the depth parameters of the decision tree model are constantly adjusted by cross-validation method to prevent the model from overwriting. In the training of association rule algorithm, Apriori algorithm is adopted, which uses frequent item set to find consumers' potential product combination preference. Food and daily necessities are purchased jointly more frequently, and after training, this combination pattern is effectively extracted and incorporated into the model. In the entire training process, the training speed of the model is proportional to the amount of data, so we choose to improve the training efficiency through parallel computation to ensure that the model is still efficient when dealing with large-scale data [20].

To ensure the robustness of the model and provide a reliable performance evaluation, a k-fold cross-validation approach was employed, where the data was randomly divided into five subsets (k=5). Each subset was used as a test set once, while the remaining four subsets served as the training set. This process was repeated five times, ensuring that each data point was used for both training and testing, thus reducing model overfitting and improving generalizability. For performance evaluation, several metrics were used beyond simple classification accuracy. The F1-score, which balances precision and recall, was calculated to assess the model's ability to correctly identify both positive and negative instances. Additionally, the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) was computed to evaluate the model's performance across different classification thresholds, providing a more comprehensive understanding of its predictive capability. These metrics were chosen to provide a more complete and nuanced evaluation of the model's effectiveness in real-world marketing scenarios, where both false positives and false negatives can have significant business implications.

2.3.2 Model verification

Model verification is essential to assess the accuracy and reliability of training outcomes. A 30% test set, consisting of 2361 purchase records randomly selected from 1000 consumers in Shenyang, was used to validate the decision tree and association rule models. Key metrics, including classification accuracy, precision, and recall, were calculated for the decision tree model, which achieved a classification accuracy of 89.5%, demonstrating its high effectiveness in differentiating consumer behavior types. A confusion matrix was generated to evaluate the model's performance across various classes. For the association rule algorithm, support and confidence values were calculated using the test set. The association rule linking food and daily necessities exhibited a confidence of 67.8%, closely matching training phase results, thereby confirming the model's robustness. Cross-validation techniques further enhanced the reliability of these results [21]. Overall, model verification ensures strong performance on both training and unseen data, validating the predictive power and consistency of the analysis.

2.3.3 Model optimization

Optimizing the model was crucial to improving its generalization and stability. For the decision tree model, this involved adjusting tree depth and applying pruning techniques. Results from the validation set indicated that while increased depth captured more consumer behavior details, it also heightened the risk of overfitting. Techniques such as re-pruning and post-pruning helped maintain accuracy while eliminating unnecessary branching. Hyperparameter tuning, including adjustments to the minimum number of sample splits and leaf nodes, further refined the model. For the association rule algorithm, the support and confidence thresholds were critical optimization targets. Initially, a high support threshold restricted the identification of potentially useful commodity associations [22]. Reducing the threshold allowed the discovery of more valuable purchase combinations. Confidence values were also adjusted to align with real-world consumption patterns, ensuring the rules were actionable. These optimizations enhanced the overall model accuracy by approximately 3.2%, providing a stronger foundation for developing enterprise marketing strategies.

2.4 Enterprise marketing strategy design

2.4.1 Market segmentation and target market selection based on consumer behavior

In this study, through the analysis of the purchasing behavior of 1000 consumers in Shenyang, market segmentation and target market selection become an important basis for the design of enterprise marketing strategy. Based on consumers' purchase frequency, consumption amount, product preference and other characteristics, market segmentation can be carried out in terms of purchasing power, product type preference and shopping channel preference. Purchasing power divides consumers into three categories of high consumption, medium consumption and low consumption, accounting for about 20%, 55% and 25% respectively. This provides a basis for enterprises to identify potential high-value consumer groups. In terms of commodity preference, consumers can be subdivided into three categories: preference for food, daily necessities and electronic products, and the proportion of consumers who prefer food is the highest, reaching 35.8% [23]. The use of online and offline channels also shows the shopping habits of different groups, with about 60 percent of consumers preferring to buy online, while the remaining 40 percent prefer offline physical stores. Through segmentation, companies are able to identify different target markets. High consumer groups and consumers who prefer electronic products may be more suitable for the promotion of high-end products and membership services, while medium consumer groups become the main target of promotion and preferential activities. By analyzing consumer behavior through big data, market segmentation helps companies accurately identify their target markets and also provides clear direction for their subsequent marketing activities.

Consumer segmentation was conducted using clear operational definitions based on behavioral attributes. Five key attributes were used for classification: purchase frequency, purchase amount, product category preference, payment method preference, and shopping channel preference. High-frequency consumers were defined as those with an average of four or more purchases per month, while low-frequency consumers had fewer than two purchases. Consumers were categorized as high spenders if their average monthly expenditure exceeded 500 RMB, medium spenders for amounts between 200-500 RMB, and low spenders for less than 200 RMB. Product preferences were derived from the proportion of purchases in specific categories, with a dominant category (e.g., food or electronics) accounting for at least 50% of the purchases. Payment method preferences were determined by the percentage use of mobile payments versus other methods, with more than 60% mobile usage classified as a preference. Channel preference was identified as online or offline based on the dominant shopping method exceeding 70%. These operational definitions ensure transparency in classification, enabling a systematic and reproducible approach to consumer segmentation.

2.4.2 Personalized marketing strategy design and dynamic pricing

Personalized marketing strategies focus on tailoring content to consumer behavior patterns and preferences, enhancing their shopping experience and purchase likelihood. Using the consumer behavior analysis model, this study identifies preferences among Shenyang consumers and aligns personalized strategies with market segmentation. Consumers inclined towards food and daily necessities typically make frequent, smaller purchases, making them suitable targets for promotions centered on daily needs. Based on historical consumption data, companies offer personalized discounts and coupons timed around specific periods, such as holidays or month-ends, to foster engagement and loyalty. High-spending groups and electronics-oriented consumers are incentivized with membership programs and value-added services, offering premium product recommendations and exclusive deals [24]. Dynamic pricing complements personalized marketing by leveraging real-time big data analysis of market demand and inventory levels. Prices are increased moderately during high demand and lowered when inventory is excessive to stimulate purchases. This strategy enhances profit margins and equips companies to adapt to market fluctuations, fostering customer satisfaction and translating into tangible sales growth.

2.4.3 Data-driven marketing channel optimization and customer experience improvement

Optimizing marketing channels and enhancing customer experience are pivotal for modern enterprises. Analyzing behavioral data from 1000 Shenyang consumers reveals distinct preferences, with 60% favoring online shopping and 40% preferring offline stores. This information provides a foundation for refining marketing channels. Online channels benefit from big data analytics to enhance user interface design, recommendation systems, and logistics processes. By monitoring browsing histories and buying patterns, e-commerce platforms deliver precise product recommendations, faster search responses, and personalized displays. Offline channel optimization focuses on analyzing in-store interactions, leading to improved layouts, self-checkout facilities, and better-trained staff. Cross-channel integration bridges these experiences, allowing customers to order online for in-store pickup or explore in-store products before completing online purchases [25]. Enterprises use customer feedback data to address issues promptly, refining service processes. These efforts boost operational efficiency while offering consumers a seamless and personalized shopping experience, strengthening customer loyalty and satisfaction.

3 Results and discussion

3.1 Results

3.1.1 Consumer behavior pattern recognition results

In this study, the recognition of consumer behavior pattern is an important basis for enterprises to formulate marketing strategies. Through the analysis of the purchase records, online behavior and social interaction data of 1000 consumers in Shenyang, the behavior pattern of consumers was extracted from multiple dimensions, including purchase frequency, product preference, channel choice and payment method preference. In this process, the decision tree model is used to classify and predict various features, and the association rule algorithm is used to analyze the potential

combination relationship of commodity purchases. Through data processing and model training, the behavioral characteristics of different consumer groups are identified. High-spending groups are more inclined to buy electronic products, while consumers who frequently buy food prefer to use mobile payments. Behavioral patterns help identify market segmentation opportunities and provide data support for how companies can better target different consumer groups in marketing.

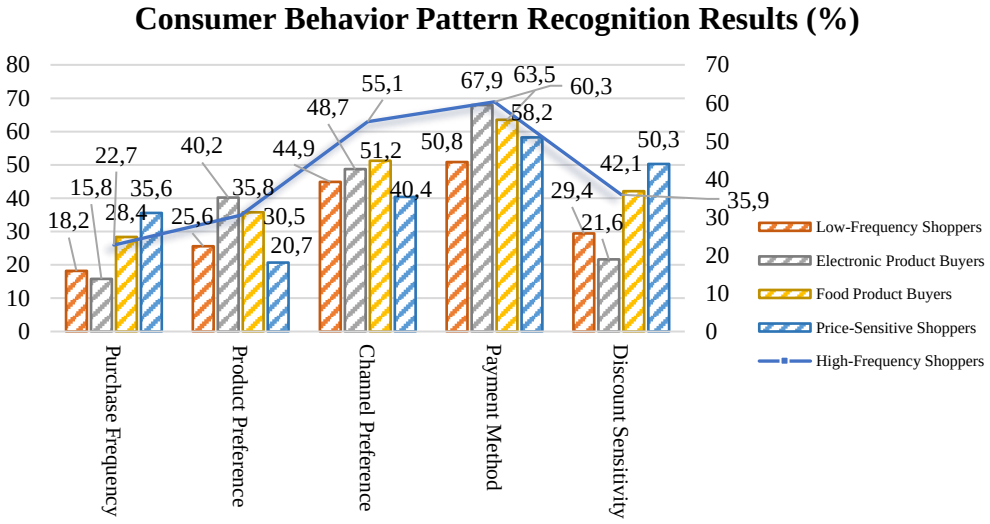


Figure 2: Consumer behavior pattern recognition results

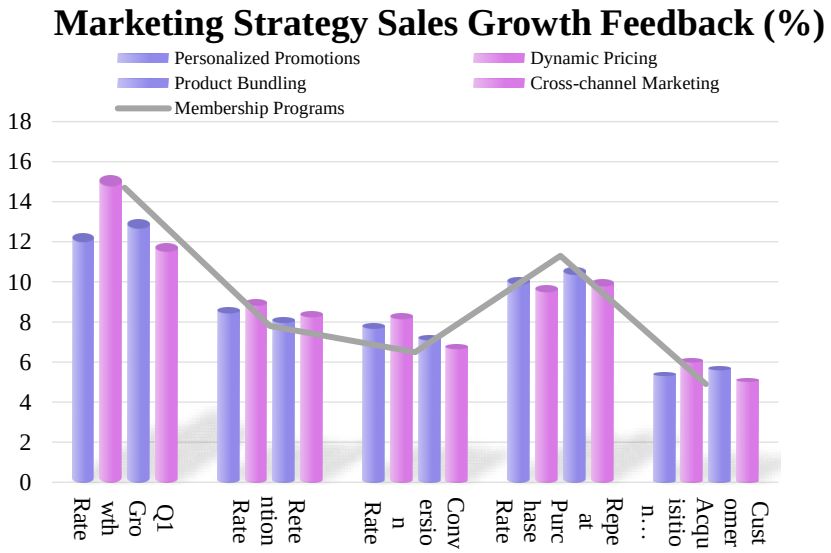


Figure 3: Marketing strategy sales growth feedback

As shown in Figure 2, consumer behavior patterns can be classified into five categories: high-frequency shoppers, low-frequency shoppers, electronic product shoppers, food shoppers and price-sensitive shoppers. High-frequency shoppers accounted for 22.7%, this group is mainly concentrated in the purchase of food and daily consumer goods, prefer online channels 55.1% and mobile payment 60.3%, they are less sensitive to discounts, only 35.9%. In contrast, low-frequency shoppers, who account for 18.2%, are also 29.4% less discount sensitive and 44.9% more inclined to buy goods through offline channels. In terms of product preference, electronic product buyers accounted for 15.8%, they showed a higher propensity to buy online 48.7%, and preferred mobile payment 67.9%, indicating that this group has a higher acceptance of emerging payment means.

Food buyers accounted for 28.4%, which is a more common category of consumer groups, their use of online channels and mobile payments were 51.2% and 63.5%, respectively, and their discount sensitivity was relatively high 42.1%. Price sensitive shoppers accounted for 35.6%, and their reliance on discounts was the highest, reaching 50.3%, with a lower preference for product categories. The behavioral characteristics of such consumers indicate that they pay more attention to price and promotions when making consumption decisions.

Different groups show significant differences in purchase frequency, product preference, channel choice and other aspects, which provides a basis for enterprises in market segmentation and target marketing, and helps enterprises to design more targeted market strategies, so as to improve marketing effects. In order to provide a more comprehensive evaluation of the model's performance, quantitative metrics such as confusion matrix, precision-recall curve, and ROC curve were included. The confusion matrix was used to assess the number of true positives, false positives, true negatives, and false negatives, which provides insights into the model's ability to classify correctly and its error types. Additionally, precision-recall curves were plotted to examine the trade-off between precision and recall across different thresholds, which is especially useful for imbalanced datasets where one class is much more prevalent than the other. The ROC curve, along with its area under the curve (AUC) score, was also presented to evaluate the model's ability to distinguish between positive and negative classes. The addition of these metrics provides a more nuanced understanding of the model's performance, beyond the descriptive statistics that were initially emphasized, and allows for a deeper interpretation of its strengths and weaknesses across different evaluation criteria.

3.1.2 3.1.2Market feedback and effect evaluation of marketing strategies

In this study, enterprises develop personalized marketing strategies based on consumer behavior analysis, and evaluate the effectiveness of the strategies through market feedback.

As shown in Figure 3, the feedback indicators mainly concerned include sales growth rate, customer buyback rate, customer satisfaction, market share Through different dimensions of market data, companies can understand the effectiveness of their marketing strategies in different consumer groups. Whether personalized promotions for high-frequency shoppers have increased customer buyback rates, or whether dynamic pricing strategies have effectively increased sales revenue. In order to evaluate the actual effect of the marketing strategy, the company collected relevant feedback data from January to March 2024 in a sample group of 1000 consumers in Shenyang, and conducted analysis based on the feedback.

As shown in Table 4, Different marketing strategies exhibit varying levels of effectiveness in driving sales growth and customer satisfaction. Dynamic pricing emerged as the most impactful, achieving a 15.3% increase in sales growth, along with strong customer retention and conversion rates at 9.1% and 8.4%, respectively. This demonstrates dynamic pricing's ability to not only boost enterprise sales but also attract new customers and significantly improve conversion rates. Personalized promotions recorded a slightly lower sales growth rate of 12.4%, yet excelled in fostering customer loyalty, as evidenced by a 10.2% customer buyback rate. Membership programs outperformed others in the buyback rate, reaching 11.3%, showcasing their effectiveness in encouraging repeat purchases through exclusive services and benefits.

Table 4: Marketing strategy customer satisfaction feedback

Strategy Type	Satisfaction Rate	Service Response Rate	Ease of Use Rate	Product Quality Perception	Recommendation Likelihood
Personalized Promotions	85.3	82.1	78.9	80.4	75.6
Dynamic Pricing	83.7	80.2	76.4	79.1	74.8
Membership Programs	87.2	83.5	80.2	82.3	76.9
Product Bundling	84.5	81.7	77.5	80.8	74.3
Cross-channel Marketing	82.9	79.8	75.6	78.4	73.5

Regarding customer satisfaction, membership programs delivered the highest satisfaction rate at 87.2%, reflecting the value customers place on personalized benefits and exclusive offerings. Personalized promotions followed with an 85.3% satisfaction rate, though their recommendation likelihood was slightly lower at 75.6%. Dynamic pricing also maintained a high satisfaction level at 83.7%, but occasional negative perceptions of price fluctuations affected its recommendation scores. Cross-channel marketing and product bundling strategies demonstrated stable performance, with satisfaction and product quality perception hovering around 80%, indicating their reliability as complementary approaches. The varied feedback highlights the unique strengths of each strategy, enabling enterprises to refine and optimize their marketing efforts to better target specific consumer groups in future campaigns.

3.1.3 Analysis of data-driven sales growth and market share improvement

In this study, big data-driven marketing strategies help companies achieve sales growth in the short term and increase market share in the long term. Combining the consumer behavior data of 1000 consumers in Shenyang, the enterprise accurately reaches different consumer groups through personalized marketing strategies, dynamic pricing and cross-channel marketing optimization, thereby improving the overall market competitiveness. In this

process, data-driven decision making enables companies to adjust their strategies in real time and respond quickly to market changes.

Table 5 shows companies' data-driven sales growth and market share gains for the period from January to March 2024, both presented as percentages. It shows the change of sales growth and market share of enterprises from different dimensions, which provides a basis for the evaluation of subsequent marketing strategies.

\

Table 5: Sales growth analysis by strategy (%)

Strategy Type	Q1 Sales Increase	Customer Conversion	Repeat Purchase	New Customer Rate	Overall Revenue Growth
Personalized Promotions	14.8	12.3	10.5	7.9	11.2
Dynamic Pricing	16.7	13.1	9.8	8.5	12.4
Cross-channel Marketing	12.9	11.2	9.3	7.2	10.6
Membership Programs	15.3	10.9	11.7	7.5	11.7
Product Bundling	13.5	11.5	9.1	6.8	10.9

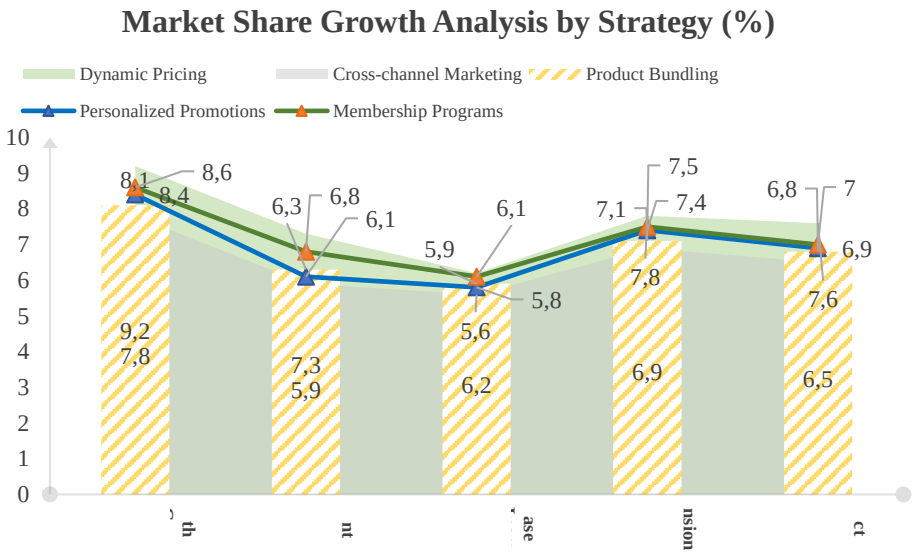


Figure 4: Market share growth analysis by strategy

As shown in Figure 4, Different marketing strategies exhibit distinct effects on enterprise sales growth. Dynamic pricing showed the most remarkable performance, achieving a 16.7% sales growth rate, a 13.1% customer conversion rate, and a 12.4% increase in overall revenue. By leveraging real-time market demand analysis and price adjustments, this strategy effectively captures high-demand opportunities, driving overall sales growth. Personalized promotions demonstrated strong results with a 14.8% sales growth rate and a 10.5% buyback rate, highlighting their ability to boost customer loyalty and repeat purchases. Membership programs achieved an 11.7% revenue increase and an equally strong buyback rate of 11.7%, showcasing their potential to foster long-term customer relationships through exclusive benefits and rewards. Although product bundling and cross-channel marketing strategies achieved slightly lower total sales growth rates, their customer conversion and new customer acquisition rates were notable at 11.5% and 9.1%, respectively.

Dynamic pricing also led in market share gains, with a 9.2% increase and a competitor replacement rate of 7.3%, reinforcing its role in capturing competitive advantage. Personalized promotions increased market share by 8.4% and significantly enhanced brand loyalty by 5.8%, demonstrating their effectiveness in cultivating long-term customer commitment. Membership programs followed closely with an 8.6% market share growth and a 6.8% competitor replacement rate, emphasizing their ability to erode competitors' market positions gradually. Cross-channel marketing and product bundling strategies showed moderate

effects on market share and brand loyalty, indicating their continued relevance for specific consumer groups. Data-driven marketing strategies not only deliver notable sales growth but also expand market share, highlighting the critical role of big data analysis in precision marketing and supporting strategic decision-making for enterprises.

4 Discussion

4.1 Result analysis and research findings

Personalized marketing and dynamic pricing strategies have had a positive impact on sales growth and customer buyback rates. The data show that the sales growth rate of dynamic pricing strategy reached 16.7%, while the buyback rate of personalized promotion was as high as 10.5%. This shows that businesses can use big data to analyze consumer behavior in real time, flexibly adjust prices or promotions, and maximize sales opportunities. Secondly, the customer buyback rate of the membership program reached 11.7%, which proves that by providing exclusive benefits and services to members, customers can effectively increase long-term loyalty. Market share analysis shows that dynamic pricing strategies are outstanding in terms of sales growth and also take the lead in market share gains, with a growth rate of 9.2%. Personalized promotions and membership programs also play a significant role in increasing brand loyalty and competitor replacement rates. Through the analysis of the results, the conclusion is drawn: enterprises can develop more targeted marketing strategies through accurate consumer behavior analysis, improve market competitiveness and long-term customer relationship maintenance effect.

The results from the decision tree and association rule models differ significantly from those found in studies using more advanced algorithms, such as deep learning or ensemble methods. For example, studies like those of Zhang et al. and Yang et al. have utilized deep learning techniques to predict consumer behavior, which generally yield high accuracy rates but lack interpretability. In contrast, decision tree models provide a clearer view of how specific features such as purchase frequency and product preference directly impact consumer decisions. The dynamic pricing strategies, which resulted in a 16.7% increase in sales growth, align with findings from other research that suggests price sensitivity is a crucial factor in consumer behavior, as seen in studies using regression analysis. However, these studies typically lack the actionable insights provided by the association rules, which effectively link products in consumer baskets. The observed differences may stem from the dataset used in this study, which is focused on a specific region (Shenyang) and incorporates both online and offline behaviors, offering a more holistic view compared to datasets used in other studies. Furthermore, the simplicity and lower computational demands of decision trees make them more applicable in real-world business environments, where interpretability and fast decision-making are key.

Leveraging a combination of decision tree models and association rule algorithms, this study offers a unique, data-driven approach to optimizing marketing strategies in complex, competitive environments. Unlike studies that rely solely on advanced machine learning models, this analysis uses decision trees to provide interpretable insights into consumer behavior paths, specifically through features such as purchase frequency and spending patterns. Association rule algorithms further enhance this approach by uncovering high-confidence purchase patterns, such as a 67% likelihood of purchasing daily necessities alongside food products. These insights support precise, actionable strategies for personalized marketing and dynamic pricing, demonstrated by a 16.7% increase in sales growth through price adjustments and a 10.5% boost in customer buyback rates from targeted promotions. By integrating online and offline data sources, this analysis bridges a critical gap in big data marketing research, where real-time adaptability and transparent decision-making are vital. These results underscore the study's contribution to the practical application of data analytics in achieving substantial improvements in customer loyalty and market share.

4.2 Applicability and limitations of the model and algorithm

Through the recursive division of information gain, the decision tree model can efficiently identify the characteristics of consumer behavior, and show the decision path in a clear and easy to explain form. This provides companies with intuitive tools to understand the behavior logic of different consumer groups, especially in market segments. Decision tree model also has some limitations, which are easy to overfit. When dealing with complex data, excessive depth of the decision tree can cause the model to be sensitive to noise, which affects the generalization ability. To this end, pruning techniques are used in this study for optimization, but the complexity and accuracy of the model still need to be balanced. The association rule algorithm performs well in mining the purchase association between goods, and by mining frequent item sets, enterprises can discover the potential combination pattern of goods. Association rule algorithm is not effective in dealing with sparse data, especially in the face of large-scale high-dimensional data, which may lead to a sharp increase in computational complexity. Future studies consider introducing other algorithms, such as random forests or support vector machines, to improve the model's stability and data processing efficiency.

The proposed model, while effective for the dataset used in this study, faces potential challenges in dynamic or cross-cultural markets where consumer behaviors vary significantly. Dynamic markets, characterized by frequent changes in consumer preferences, require real-time adaptability, which may be limited by the static nature of the decision tree model. Incorporating dynamic learning algorithms, such as reinforcement learning, could address this limitation by allowing continuous updates to the model as new data becomes available. Cross-cultural applications also present challenges, as consumer behaviors influenced by cultural norms, socioeconomic factors, and regional preferences may differ drastically from those in the dataset. For example, mobile payment preferences or product category dominance may shift in markets with differing levels of technology adoption or purchasing power. Adapting the model for such markets would require the inclusion of culturally relevant features and localized data. These factors highlight the importance of tailoring the model to the unique characteristics of the target market, ensuring its generalizability while acknowledging the need for customization.

4.3 Enlightenment and improvement suggestions for enterprise marketing strategy

Personalized marketing strategies have proven to be highly effective in enhancing customer satisfaction and loyalty. Companies should leverage big data analytics to address individual consumer needs by analyzing historical purchase records and browsing behaviors. Tailored product recommendations for distinct customer groups can significantly improve sales conversion rates. The effectiveness of dynamic pricing underscores the importance of flexible price adjustments, particularly during periods of demand fluctuations. Real-time market demand monitoring and adaptive pricing strategies based on inventory and competition are essential for maximizing revenue. Membership programs, which have excelled in boosting customer buyback rates and market share, should be further optimized. Adding incentives such as exclusive offers and bonus points can enhance long-term customer retention. While these strategies have achieved considerable short-term sales growth, enterprises should prioritize long-term improvements in brand loyalty and customer experience. Building robust customer relationships and continuously optimizing marketing strategies using big data analytics will enable businesses to sustain growth and maintain competitiveness in challenging market environments.

5 Conclusion

Personalized marketing strategies have proven to be highly effective in enhancing customer satisfaction and loyalty. Companies should leverage big data analytics to address individual consumer needs by analyzing historical purchase records and browsing behaviors. Tailored product recommendations for distinct customer groups can significantly improve sales conversion rates. The effectiveness of dynamic pricing underscores the importance of flexible price adjustments, particularly during periods of demand fluctuations. Real-time market demand monitoring and adaptive pricing strategies based on inventory and competition are essential for maximizing revenue. Membership programs, which have excelled in boosting customer buyback rates and market share, should be further optimized. Adding incentives such as exclusive offers and bonus points can enhance long-term customer retention. While these strategies have achieved considerable short-term sales growth, enterprises should prioritize long-term improvements in brand loyalty and customer experience. Building robust customer relationships and continuously optimizing marketing strategies using big data analytics will enable businesses to sustain growth and maintain competitiveness in challenging market environments.

References

[1] Suleymanov F. Consumer behavior and agricultural consumer market. Scientific Papers-Series Management Economic Engineering in Agriculture and Rural Development,21(3): 753-758, 2021.

[2] Duarte P, Silva SCE, Mangei I, Dias JC. Exploring ethical consumer behavior: a comprehensive study using the ethically minded consumer behavior-scale (EMCB) among adult consumers. International Review on Public and Nonprofit Marketing, 2024. http://doi.org/10.1007/s12208-024-00404-x

[3] Niewczas-Dobrowolska M, Górka-Chowaniec A, Sikora T. Changes of consumer behavior caused by the COVID-19 pandemic. International Journal for Quality Research, 18(1): 129-152, 2024. https://doi.org/10.24874/IJQR18.01-09.

[4] Rozenkowska K. Theory of planned behavior in consumer behavior research: A systematic literature review. International Journal of Consumer Studies, 47(6): 2670-2700, 2023. https://doi.org/10.1111/ijcs.12970.

[5] Uliana MP, Kraus CB, dos Santos T. Consumer behavior: The Brazilian online consumer profile. Caderno Profissional de Marketing Unimep, 11(1): 129-145, 2023.

[6] Zhang JZ, Choi TM, Cai YJ. Consumer-to-consumer product trading with strategic consumer behaviors in the sharing economy. IEEE Transactions on Engineering Management, 70(5): 1708-1723, 2023. https://doi.org/10.1109/TEM.2021.3065099.

[7] Yang JL, Ren JF, Zhao MH, Chen HY, Wang HH. The impact of value co-creation on consumer citizenship behavior: Based on consumer perspective. Frontiers in Psychology, 131110011, 2023. https://doi.org/10.3389/fpsyg.2022.1110011.

[8] Gams M, Kolenik T. Relations between Electronics, Artificial Intelligence and Information Society through Information Society Rules. Electronics, 10:514, 2021. https://doi.org/10.3390/electronics10040514

[9] Tassell C, Aurisicchio M. Refill at home for fast-moving consumer goods: Uncovering compliant and divergent consumer behaviour. Sustainable Production and Consumption, 39: 63-78, 2023. https://doi.org/10.1016/j.spc.2023.04.018.

[10] Snyder H, Witell L, Gustafsson A, McColl-Kennedy JR. Consumer lying behavior in service encounters. Journal of Business Research, 141: 755-769, 2022. https://doi.org/ 10.1016/j.jbusres.2021.11.075.

[11] Wlodarczyk K. Trends of evolution in consumer behavior in the contemporary world. Problems and Perspectives in Management, 19(1): 39-50, 2021. https://doi.org/10.7172/1644-9584.91.3.

[12] Tau D, Kunz MC, Onwezen MC. Changing consumer behaviour in virtual reality: A systematic literature review. Computers in Human Behavior Reports, 3: 100093, 2021. https://doi.org/10.1016/j.chbr.2021.100093.

[13] Singla M, Sharma AM. Consumer behaviour towards healthy nutrition. Cardiometry, 23: 561-576, 2022. https://doi.org/10.18137/cardiometry.2022.23.561576.

[14] Utkarsh, Singh H. How perceived corporate social responsibility affects consumer citizenship behavior? Investigating the mediating roles of perceived employee behavior and consumer company identification. Marketing Intelligence & Planning, 41(7): 1037-1053, 2023. https://doi.org/10.1108/MIP-06-2023-0269.

[15] Dangelico RM, Schiaroli V, Fraccascia L. Is Covid-19 changing sustainable consumer behavior? A survey of Italian consumers. Sustainable Development, 30(6): 1477-1496, 2022. https://doi.org/10.1002/sd.2322.

[16] Omelchyk O, Ivanashko O, Sipko L, Virna Z, Saienko V, Tolchieva H. Economic behavior of consumers during instability. AD ALTA: Journal of Interdisciplinary Research, 12(2): 89-95, 2022.

[17] Mielinger E, Weinrich R. A review on consumer sorting behaviour: Spotlight on food and fast-moving consumer goods plastic packaging. Environmental Development, 47: 100890, 2023. https://doi.org/10.1016/j.envdev.2023.100890.

[18] Garg P, Kumar A, Mittal RK. What drives consumers' sustainable mobility behaviour? An empirical investigation of Delhi consumers. Visions for Sustainability, 19: 289-319, 2023. https://doi.org/10.13135/2384-8677/7064.

[19] Smakova V, Piligrimiene Z. Religion in consumer behavior research: A systematic literature review. Eurasian Business and Economics Perspectives, 20: 179-191, 2021. https://doi.org/10.1007/978-3-030-85304-4_11.

[20] Özturan P, Grinstein A. Can the marketing department benefit from socially responsible marketing activities? The role of legitimacy and customers' interest in social responsibility. European Journal of Marketing, 56(2): 400-441, 2022. https://doi.org/10.1108/EJM-09-2020-0670.

[21] Özsomer A, Simonin B, Mandler T. Marketing agility in subsidiaries: Market orientation and marketing program standardization as the "twin engines" of performance. Journal of International Marketing, 31(2): 6-24, 2023. https://doi.org/10.1177/1069031X221130740.

[22] Keller KO, Guyt JY, Grewal R. Soda taxes and marketing conduct. Journal of Marketing Research, 61(3): 393-410, 2024. https://doi.org/10.1177/00222437231195551.

[23] Bhattacharya A, Sardashti H, Faramarzi A. Marketing and bankruptcy risk: the role of marketing capabilities. Journal of Strategic Marketing, 31(8): 1454-1468, 2023. https://doi.org/10.1080/0965254X.2022.2117398.

[24] Patel PC, Feng C, Guedes MJ. Marketing capability and new venture survival: The role of marketing myopia. Industrial Marketing Management, 93: 307-326, 2021. https://doi.org/10.1016/j.indmarman.2021.01.020.

[25] Skålén P, Cova B, Gummerus J, Sihvonen A. Marketing-as-practice: A framework and research agenda for value-creating marketing activity. Mark Theory. 23(2): 185-206, 2023. https://doi.org/10.1177/14705931221123949.

A Paillier Homomorphic Encryption-Based Lightweight Privacy Protection Model for Mobile Crowd Sensing Networks

Shijie Feng[1*], Yanyan Qin[2,] Zhixiang Zeng[1], Bing Wen[1], Weijie Zhong[1], Ning Wang[2], Wei Guo[2], Yu'nan Zhang[3]
[1]Hainan Power Grid Co., Ltd., Haikou 570203, China
[2]Information and Telecommunication Branch of Hainan Power Grid, Haikou 570203, China
[3]CSG Electric Power Research Institute Co., Ltd., Guangdong Provincial Key La-boratory of Power System Network Security, Guangzhou 510663, China
Email: fengshijie198811@163.com, qinyy@hn.csg.cn, zengzx2@hn.csg.cn, wb@hn.csg.cn, zhongwj@hn.csg.cn, wangn3@hn.csg.cn, guow@hn.csg.cn, zhangyn2@csg.cn
*Corresponding author

Keywords: MCSN, homomorphic encryption, paillier, DNN, network security, privacy preservation

Received: July 16, 2024

The objective of this study is to enhance the privacy protection capability of mobile crowd perception networks and improve the detection accuracy of security threat data. To this end, a three-level collaborative distributed architecture is designed, which combines the concept of zero trust and proposes a lightweight security threat detection model based on the Paillier homomorphic encryption, deep neural networks, and box graph methods. Firstly, by optimizing the mobile crowd sensing networks framework and introducing three different network structures, a collaborative distributed system of terminal edge cloud was constructed. Secondly, the Paillier homomorphic encryption algorithm was designed to protect data privacy. The experimental results showed that the designed model achieved a detection accuracy of 98.84%, a mean square error of 0.03, and an average detection time of 0.15 seconds for A-class threats. In terms of processing efficiency, this model significantly improved data transmission efficiency, had lower computational overhead, and was suitable for various types of security threat detection. Therefore, the security threat detection model proposed in this study provides effective privacy protection technology for mobile crowd-sensing networks, significantly improving network security.

Povzetek: Razvit je nov model zaščite zasebnosti za mobilna senzorska omrežja, ki združuje Paillierjevo homomorfno šifriranje in globoke nevronske mreže.

1 Introduction

With the popularization of smart devices and the advancement of IoT technology, mobile crowd sensing networks (MCSN) have been widely used in the fields of environmental monitoring, public safety, and intelligent transportation [1]. The current MCSN collects data through mobile terminal devices and processes and analyzes it through a cloud platform, which greatly improves the efficiency of data collection and processing [2]. However, with the continuous growth of data size, data privacy preservation (PP) becomes an important problem to be solved. Traditional PP methods, such as data anonymization and encrypted transmission, have been difficult to meet the increasingly complex security requirements [3-4]. In this context, homomorphic encryption (HE) techniques have gradually attracted the attention of researchers due to their ability to directly compute data in the encrypted state. Among them, Paillier homomorphic encryption (PHE) algorithm is widely used in the field of PP for its excellent additive homomorphic property. However, it is difficult for a single encryption method to cope with complex and changing security threats. In order to better protect data privacy and improve the accuracy of threat detection at the same time, researchers have proposed comprehensive schemes combining multiple techniques. Zheng et al. proposed an HE-based grid matching scheme. The scheme first encrypted the grid used for task assignment so that the task matching process took place in an encrypted environment. Second, the location information of the applicant and the publisher kept secret from each other, thus protecting location privacy. Finally, the applicant fed back the results of the tasks in the grid, and the publisher received these results to complete the whole crowd sensing process. Research results demonstrated that this scheme outperformed other similar schemes in terms of performance and security [5]. With the rapid proliferation of mobile applications, mobile crowd sensing became an increasingly important topic, where the anonymity of the participants was crucial for network security. Ganjavi and Sharafat proposed an efficient edge-assisted mobile crowd sensing scheme that protected the privacy and anonymity of participants while

guarding against adversaries and verifying the authenticity of aggregation results. In this scheme, the joining and leaving problems were transparent and the computational cost and communication overhead were fixed and independent of the crowd size. The results of the study indicated that the scheme was able to identify and block malicious adversaries while providing anonymity to ordinary participants [6]. With the rapid increase in the amount of data generated by industrial devices in the Internet of Things (IoT), Jia et al. designed a blockchain-supported federated learning application model for industrial IoT and proposed a data protection aggregation scheme. The study introduced multiple data clustering methods based on differential privacy and HE to achieve multiple protections in data and model sharing. The final experimental results demonstrated that the proposed scheme performed well on various metrics [7]. Currently, encryption-based PP collaborative filtering is widely used for generating recommendation tasks. However, the existing solutions are slow and not scalable. To solve this problem, Jumonji et al. proposed the privacy-preserving collaborative filtering protocol based on BGV fully homomorphic encryption (BGV-CF). The results indicated that BGV-CF significantly simplified the recommendation process and improves the recommendation speed by reducing the interaction and communication traffic between users and recommendation servers [8].

In summary, although existing research has made some progress in data processing and PP, there are still some shortcomings. First, a single PP technique is difficult to cope with complex and changing security threats, and the existing methods are inefficient in processing large-scale data and have a large computational overhead in the encryption and decryption process. Second, the existing threat detection models still need to be improved in terms of real-time and accuracy. Especially in the face of large-scale mobile crowd sensing data, the existing scheme has a bottleneck in detection performance. To address the above shortcomings, the research proposes a lightweight security threat detection model (STDM) combining PHE, deep neural network (DNN), and box plot method (BPM). There are two innovations in the research. First, the PHE algorithm is used, which is able to maintain high encryption and decryption efficiency while protecting data privacy. Second, through the terminal-edge-cloud (TEC) three-tier collaborative architecture, it aims to improve the real-time and accuracy of threat detection. It is hoped that this research will provide new techniques and methods for MCSN PP. The summary of related work is shown in Table 1.

Table 1: Summary of related work

Researcher	Methodologies	Key performance metric	Limitation
Zheng et al. [5]	HE-based grid matching scheme; encrypted task assignment; location PP	Superior performance and security	Potential computational overhead due to encryption
Ganjavi et al. [6]	Efficient edge-assisted MCSN; privacy and anonymity of participants	Ability to identify and block malicious adversaries; fixed computational cost and overhead	Scalability with varying crowd sizes not addressed
Jia et al. [7]	Blockchain-supported federated learning for industrial IoT; differential privacy & HE	Performs well on various metrics, multiple protections in data and model sharing	Potential complexity in implementation
Jumonji et al. [8]	BGV-CF	Simplified recommendation process; improved speed by reducing interaction/communication	Scalability issues

2 Methods and materials

To improve the PP in MCSN, the research designs the MCSN framework in conjunction with the zero-trust concept (ZTC) that considers the secure access of mobile users. To address the threat data security detection in MCSN framework, the research further builds STDM jointly with lightweight HE algorithms Paillier, DNN, and BPM.

2.1 Design of MCSN framework based on zero trust concept

Crowd sensing network (CSN) is a network that utilizes a large number of users to collect data and share data through various devices, such as smartphones and wearable devices [9]. CSN focuses on collecting data through voluntary or organized user participation, which can be either static or dynamic. However, with the development of various intelligent technologies, the data

collection method is gradually changing from static collection to dynamic collection, which consequently also causes the problem of data explosion. In the field of network privacy and security protection, MCSN, as a subset of CSN, has been widely used in more practical scenarios because of its efficient data dynamic collection capability [10-11]. The network framework of MCSN is shown in Figure 1.

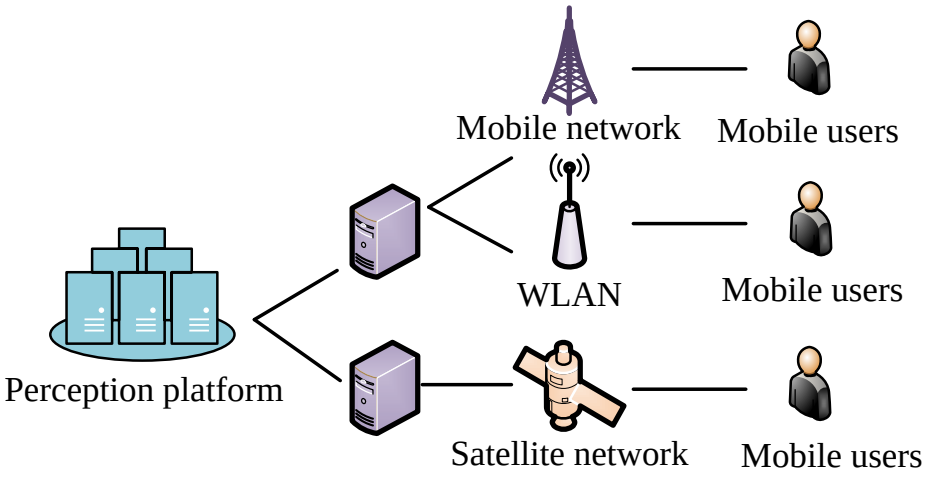


Figure 1: Network structure diagram of MCSN

The MCSN illustrated in Figure 1 utilizes mobile terminals as a source of data acquisition to construct a perception network. Task allocation and data aggregation are realized through cooperation between different communication networks. In the MCSN architecture, there are two main parts: the perception cloud platform with cloud server clusters and mobile users. The sensing cloud platform is responsible for the processing and analysis of the collected data, while the mobile users are tasked with the collection of data such as geographic information, speed, and pressure through the sensors of their devices. These devices then connect to the sensing cloud platform through various forms of wireless connectivity, including Wi-Fi, 4G, and 5G, and ultimately upload the sensing data. The access of a large number of mobile users fuels the development of MCSNs, but also introduces new security risks. On the one hand, users may fraudulently obtain rewards through Sybil attacks or duplicate submission of reports, which reduces the quality of reports and affects the effectiveness of the platform. On the other hand, users who are data consumers may engage in overstepping access or data corruption when accessing resources, threatening the security of platform resources [12]. In addition, users may use vulnerable devices to access the network, further exacerbating security risks. The common types of security threats in MCSN are shown in Table 2.

In Table 2, the types of security threats are mainly six categories: system attack, illegal intrusion, false identity, Sybil, malware, and various types of network Trojans, which are numbered as A, B, C, D, E, and F. In order to detect these security threats more effectively, the study introduces the ZTC to build the brand new MCSN. The structure of the security model using the ZTC is shown in Figure 2.

Table 2: Security threat types in MCSN

Types of security threats	Explaination	Threat type number
System attack	Malicious users can access system resources through remote control and eavesdropping	A
Trespassing	The user accesses an unauthorized resource	B
False identity	The user accesses an unauthorized resource	C
Sybil	Users declare multiple illegal identities in the sense cloud platform	D
Malware	Scripts or programs that control software processes exist on the access device	E
Various network trojans	The access device contains various network Trojans	F

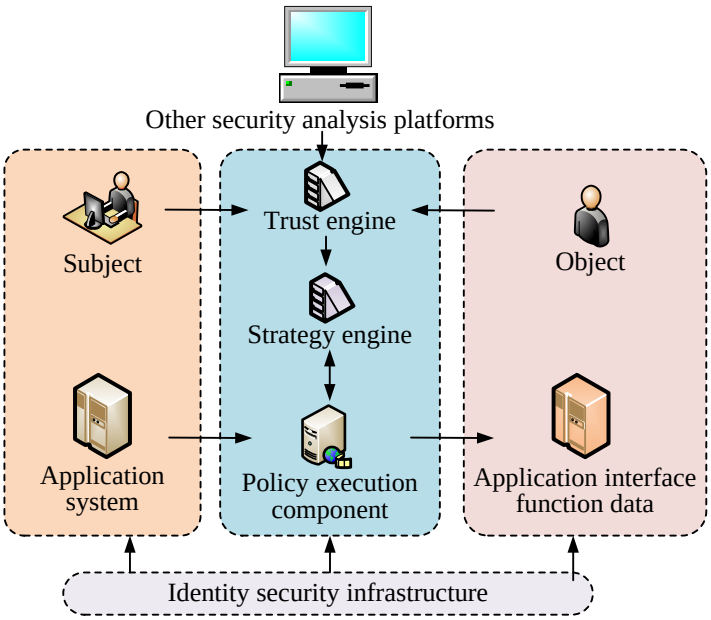


Figure 2: Frame diagram of zero trust concept

In Figure 2, the zero-trust architecture consists of four main components, namely the identity security infrastructure, the policy enforcement component, the policy engine, and the trust engine. The identity security infrastructure manages the identity and privileges of entities, including identity digitization, privilege auditing, and verifying the validity of authentication information. For users, it provides authentication techniques based on multiple factors, and for devices, only devices with installed identity credentials can access system resources, and those without will be denied [13-14]. The policy enforcement component decides the release or denial of user access requests based on the real-time authorization policy of the policy engine. The policy engine develops access control policies to assess the legitimacy of resource requests. The trust engine evaluates the user's trust level, based on behavioral logs and identity information, and improves the trustworthiness of trust metrics using big data and artificial intelligence techniques. The MCSN incorporating ZTC is notated as ZT-MCSN and its framework diagram is shown in Figure 3.

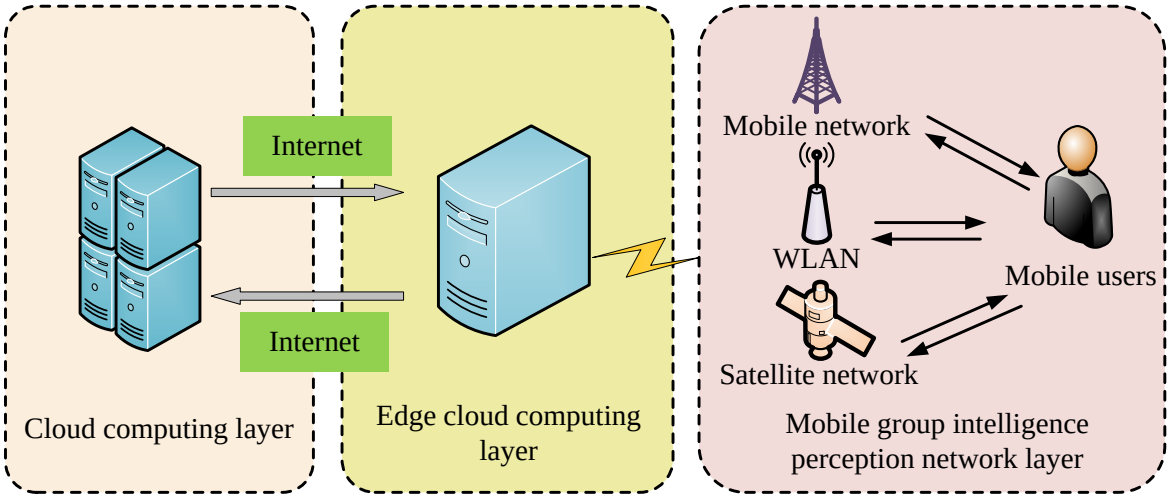


Figure 3: ZT-MCSN frame structure diagram

The ZT-MCSN network architecture in Figure 3 is divided into the MCSN network layer, edge cloud computing layer, and cloud computing layer from bottom to top. The MCSN network layer includes a large number of mobile users and a variety of communication networks, which are responsible for performing sensing tasks, local security model training and inference. In addition, the MCSN network layer has a variety of sensing nodes, including smart terminals and various types of mobile devices, and the mobile users collect data

through built-in sensors and upload data through communication technologies such as Wi-Fi and 5G. The edge cloud computing layer is located at the edge of the perceptual network and provides perceptual task processing and zero-trust security services by utilizing the computing and storage capabilities of edge servers. This layer is mainly responsible for the management of sensing tasks and secure access control of mobile users, ensuring network security through authentication and dynamic access control. The cloud computing layer consists of distributed server clusters that handle high-complexity services such as perceptual application management and resource scheduling to optimize perceptual activities and enhance user services.

2.2 Security threat detection model construction based on improved PHE

In the ZT-MCSN network, the distributed architecture of "TEC" is generally adopted. This architecture can distribute the training and inference tasks of STDM to each mobile device. By executing model training and reasoning locally, it effectively reduces the data transmission in the network and improves the data PP. The three-level collaborative distributed architecture is shown in Figure 4. The specific components of the "TEC" three-level collaborative distributed architecture are given in Figure 4. Although this architecture can ensure data privacy to a certain extent, distributed machine learning itself cannot completely ensure data privacy, and the insufficient generalization of the model may also lead to reverse attacks, which may leak device data [15]. In ZT-MCSN, device data privacy leakage mainly occurs in two links. One is during the transmission of model parameters; the attacker may obtain the parameters through eavesdropping and utilize them for reverse attacks. The second is that in the process of model parameter aggregation, there may be servers accessing device data through reverse analysis of the aggregated model. For this reason, the research combines PHE algorithm, DNN, and BPM in ZT-MCSN to design a new distributed training technique to enhance the protection capability of STDM for device data. The final constructed STDM is denoted as STDM with improved PHE (Paillier-deep neural network-box plot method, Paillier-DNN-BPM), and the structure diagram of its distributed training framework is shown in Figure 5.

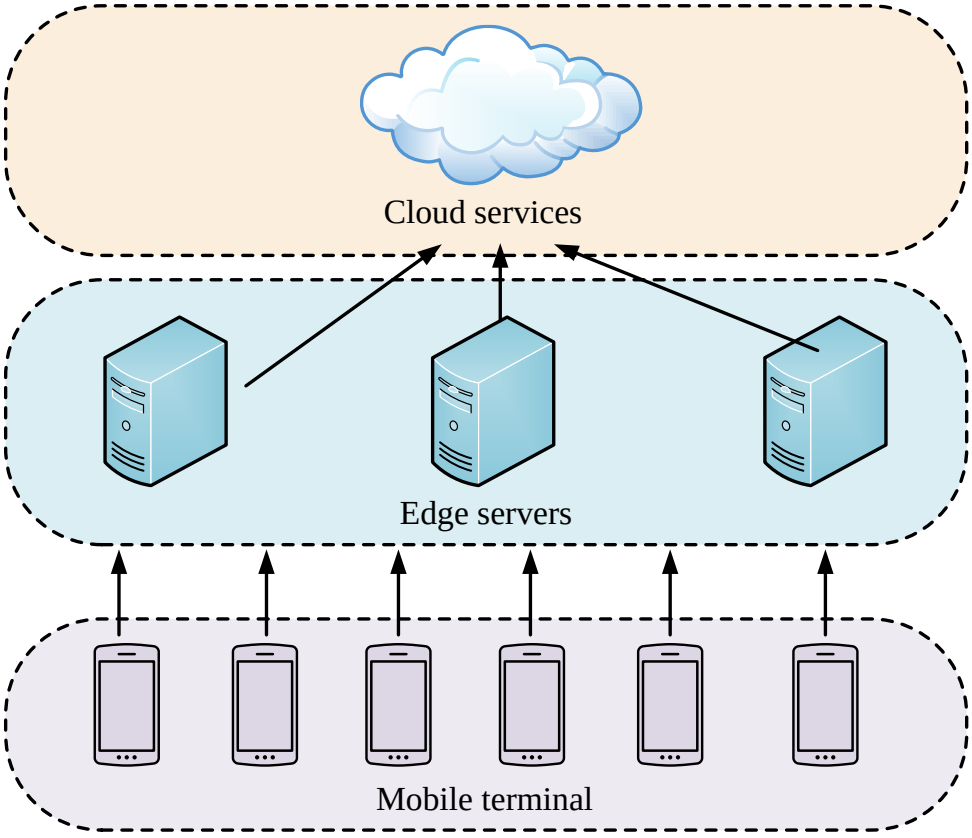


Figure 4: Three-level collaborative distributed architecture diagram

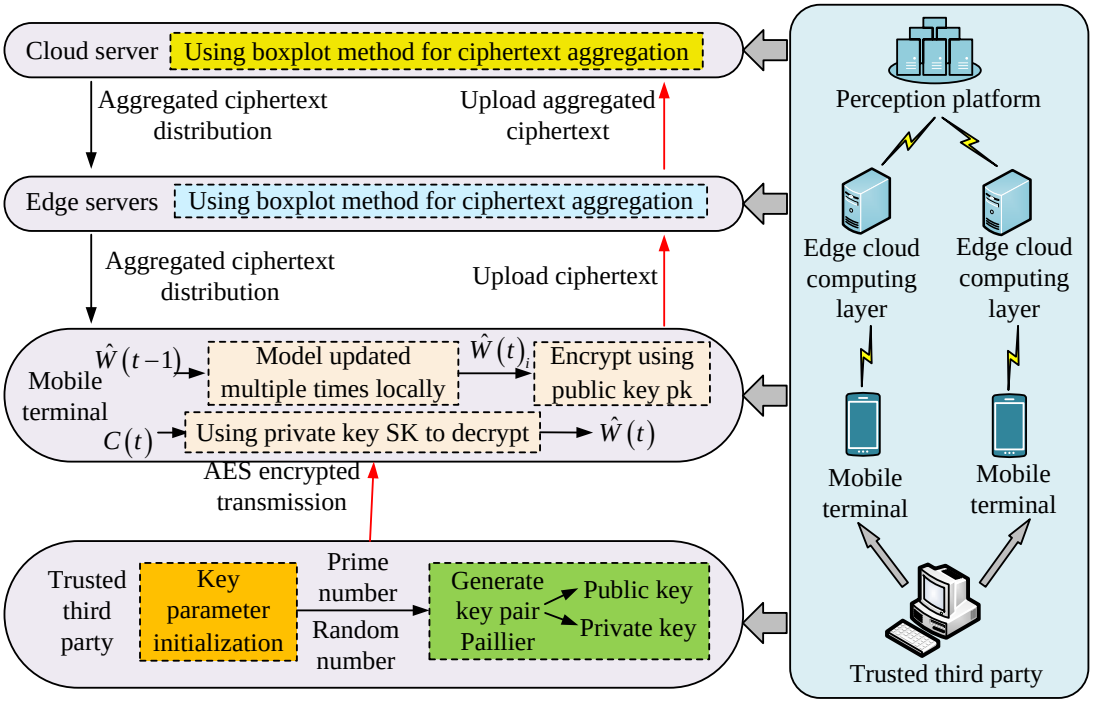


Figure 5: Paillier-DNN-BPM structure diagram

In Figure 5, the distributed training architecture of STDM Paillier-DNN-BPM, which combines PHE algorithm, DNN, and BPM, mainly consists of four parts: trusted third party, mobile terminal, edge server, and cloud server. The mobile terminal acts as a working node to decrypt the model parameters distributed by the server using the private key of the Paillier algorithm, and utilizes the local data for model training and parameter updating. The updated model parameters are encrypted by the public key of Paillier algorithm and uploaded to the edge server. The edge server, as a local parameter server in the distributed model training architecture, is responsible for filtering and aggregating the locally updated ciphertexts submitted by the mobile terminals, and uploading the local aggregation results to the cloud server for further computation. As the global parameter server in the distributed model training architecture, the cloud server is mainly responsible for initializing the model parameters and filtering and aggregating the local aggregated ciphertexts submitted by the edge servers to generate the global model parameter ciphertexts. The generated parameter ciphertexts are distributed to mobile terminals through the scheduling edge servers. In addition, to ensure that the encryption keys are only shared among mobile devices, the model architecture introduces a trusted third party. The trusted third party securely shares the key pairs of the Paillier algorithm among mobile devices via the advanced encryption standard (AES) algorithm. The Paillier algorithm is a packet cipher based HE algorithm. The algorithm is additively homomorphic, which means that encrypted data can be added without first being decrypted, and the result of the operation remains encrypted. In Paillier's algorithm, it is assumed that p and q are two different large prime numbers. Based on these two different large prime numbers, the formulae for the modulus n and the parameter λ can be obtained as shown in Equation (1) [16-17].

$$\begin{cases} n = p \cdot q \\ \lambda = lcm(p-1, q-1) \end{cases} \tag{1}$$

In Equation (1), $lcm(\cdot)$ denotes the least common multiple of $p-1$ and $q-1$. Setting a certain random number as g, $g \in Z_{n^2}^*$, the formula for the parameter u is obtained as shown in Equation (2).

$$u = \left(L\left(g^{\lambda} mod n^2\right)\right)^{-1} \tag{2}$$

In Equation (2), $L(\cdot)$ is a function used to calculate the intermediate value in the decryption process. n^2 denotes the modulus square, which is used to define the modulus space of the encryption operation. mod denotes modulo operation. In the Paillier encryption algorithm, the modulus operation is used to keep the value within a

specific range, preventing the value from being too large, while ensuring the correctness and consistency of the calculation results. The expressions for the public and private keys of Paillier algorithm are shown in Equation (3).

$$\begin{cases} p_k = (n, g) \\ s_k = (\lambda, u) \end{cases} \quad (3)$$

In Equation (3), p_k and s_k denote the public key and private key respectively. Setting x and y as two different plaintexts, combining Equation (1) ~Equation (3) can get the encryption process of Paillier's algorithm as shown in Equation (4).

$$\begin{cases} x' = E(x) = g^x r^n \bmod n^2 \\ y' = E(y) = g^y r^n \bmod n^2 \end{cases} \quad (4)$$

In Equation (4), x' and y' denote the plaintext x and y encrypted ciphertexts, respectively. $E(x)$ and $E(y)$ denote the encryption function respectively. r is some random number and $r < n$. Further the decryption process of the ciphertext is obtained as shown in Equation (5).

$$\begin{cases} x = D(x') = L\left(x'^{\lambda} \bmod n^2\right) * u \bmod n \\ y = D(y') = L\left(y'^{\lambda} \bmod n^2\right) * u \bmod n \\ L(a) = a - 1/n \end{cases} \quad (5)$$

In Equation (5), $D(x')$ and $D(y')$ denote the decryption function, respectively. $L(a)$ denotes a function in the decryption process. a denotes the variable of that function.

In Paillier's algorithm, its additive homogeneity is manifested as a multiplication computation on the ciphertexts of plaintexts x and y. The result obtained from the computation is decrypted using a key and the decrypted plaintext is obtained. The former encrypted and decrypted content is the same as the result of the addition operation performed directly on the plaintext. The expression for additive homogeneity is shown in Equation (6).

$$E(x) \times E(y) = E(x + y) \quad (6)$$

In Equation (6), $E(x+y)$ denotes the addition operation directly on the plaintext. Paillier has addition homogeneity in addition to number multiplication homomorphism. Number multiplication homomorphism means that the z-power computation is performed on the ciphertext of x, and the result of the computation is the same as that of the number multiplication z computation on the plaintext x after decryption using the key. The expression for the number multiplication homomorphism is shown in Equation (7).

$$E(x \times z) = E(x)^z \quad (7)$$

In Equation (7), z denotes the number of times a certain power square is calculated and is a constant. Based on the generated key pairs, the study utilizes trusted third-party AES encryption algorithms to achieve secure sharing of data across devices.

In DNN, it is assumed that l denotes the neuron of layer l in the DNN, $2 \le l \le 4$. In this way, the weights and biases of the neurons of layer l can be obtained as $W^{(l)}$ and $BS^{(l)}$, respectively. Let the output of the previous layer be $OP^{(l-1)}$ to get the output of layer l as shown in Equation (8) [18].

$$OP^{(l)} = f\left(W^{(l)} OP^{(l-1)} + BS^{(l)}\right) \quad (8)$$

In Equation (8), $f(\cdot)$ denotes the activation function of the neuron, and the study chooses Relu as the activation function as a way to save the computation time of the network and prevent the gradient from disappearing. In order to simplify the formula, the study expresses the weight values and bias values of all neuron layers in the DNN in the form of vectors, which is denoted as $\hat{W} = (W; BS)$. If the input layer data is $IN = (in_1, in_2, \cdots, in_m)$, its output layer data can be denoted as $OP = f\left(\hat{W}, IN\right)$. The mean-square error (MSE) calculation formula in the regression model is used to determine whether the to-be-detected data of the

DNN is threatening data. The calculation formula of MSE is shown in Equation (9).

$$MSE = \frac{\sum_{s=1}^{no}\left(o\hat{p}_s - op_s\right)^2}{no} \quad (9)$$

In Equation (9), s and no denote the number and total number of training samples, respectively. $o\hat{p}_s$ and op_s denote the true and detected values of the s th training sample, respectively. The updating of parameters is accomplished using gradient descent method as shown in Equation (10) and Equation (11).

$$\Delta\hat{W}(t)_i = \eta\nabla_{\hat{W}}\left\{\frac{\left[O\hat{P}_i - f\left(\hat{W}(t-1), IN_i\right)\right]^2}{no}\right\} \quad (10)$$

In Equation (10), $\hat{W}(t)_i$ denotes the updated model parameters of the mobile terminal i locally. $\hat{W}(t-1)$ denotes the global model parameters before updating. $\Delta\hat{W}(t)_i$ denotes the adjusted value of the update. η denotes the learning step parameter. $O\hat{P}_i$ denotes the real output data of mobile terminal i. IN_i denotes the input data of mobile terminal i. The specific expansion of $\hat{W}(t)_i$ is shown in Equation (11).

$$\hat{W}(t)_i = \hat{W}(t-1) - \Delta\hat{W}(t)_i \quad (11)$$

For $\hat{W}(t)_i$, the mobile terminal i will enter the information of p_k in the Paillier algorithm and compute the ciphertext $c(t)_i$ waiting to be transmitted. The transmission process of $c(t)_i$ is shown in Equation (12).

$$c(t)_i = g^{\hat{W}(t)_i} r^n \left(mod n^2\right) \quad (12)$$

According to Equation (8) to Equation (12), DNN is chosen as the detection model in the study, which is utilized to complete the task of security threat detection for mobile devices. The mobile terminals participating in the DNN model training will train and update the initial parameter set obtained in the local data before encrypting the model parameters for transmission using the p_k public key in Paillier's algorithm. The encrypted transmitted parameters will enter into the edge-end server, and in this part the parameter ciphertexts are then selected and aggregated using the BPM, so as to obtain the global parameter ciphertexts. The global model parameter ciphertext obtained by the mobile terminal will be decrypted again by the private key s_k in the Paillier algorithm.

3 Results

In order to demonstrate the superior benchmark performance and practical applicability of the proposed Paillier-DNN-BPM model, this study introduces AES, HE, and secure hash algorithm (SHA) as comparison algorithms and employs the following criteria for the comparison test: detection precision, MSE, key sensitivity, and data encryption relevance.

3.1 Algorithm benchmark performance testing

Since the final designed Paillier-DNN-BPM model is composed of three parts, Paillier, DNN and BPM, the study starts with an ablation test of the Paillier-DNN-BPM model as a way of proving the performance of each part of the model. The results of the ablation test are shown in Table 3.

In Table 3, the various benchmark performances of Paillier+DNN+BPM, i.e., Paillier-DNN-BPM, have the best performance in the seven sets of ablation tests. The detection precision, recall, and F1 value of Paillier-DNN-BPM are as high as 0.982, 0.989, and 0.988, respectively. The value are much higher than those of the single BPM of 0.831 precision, 0.842 recall, and 0.836 F1 value. The performance of all models decreases after introducing noise and adversarial attacks. However, the Paillier DNN-BPM model still maintains high accuracy, recall, and F1 score. In adversarial attack scenarios, its F1 value is 0.931, indicating the robustness of the model in the face of noise and attacks. It can be concluded that the various components used in the study in the Paillier-DNN-BPM model all have important roles. The sensitivity of the four algorithms HE, AES, SHA, and Paillier-DNN-BPM is further tested and the results are shown in Figure 6. Figure 6(a) and Figure 6(b) show the sensitivity values of HE, AES, SHA, and Paillier-DNN-BPM in the training set and test set, respectively. In Figure 6(a), the fluctuation ranges of the sensitivity values of HE, AES, SHA, and Paillier-DNN-BPM in the training set are -0.19-0.46, -0.21-0.28, -0.13-0.25, and -0.05-0.15, respectively. Compared to HE, AES, and SHA, the sensitivity values of Paillier-DNN-BPM fluctuation range is minimized. Similarly, it can be found that Paillier-DNN-BPM has the smallest fluctuation range of sensitivity values in the test set of Figure 6(b), which is only -0.15~0.09. Thus, it can

be concluded that Paillier-DNN-BPM has the best sensitivity and is able to detect the existence of threat data in time. The MSE values of the four algorithms are shown in Figure 7.

Table 3: Ablation test results of Paillier-DNN-BPM model

Model	Precision	Recall	F1 value	F1 value after introducing Gaussian noise	F1 value after introducing adversarial attacks
Paillier	0.862	0.875	0.871	0.842	0.815
DNN	0.885	0.892	0.890	0.861	0.832
Box diagram method	0.831	0.842	0.836	0.806	0.781
Paillier+Box diagram method	0.905	0.912	0.910	0.876	0.852
DNN+Box diagram method	0.921	0.926	0.922	0.889	0.865
Paillier+DNN	0.943	0.956	0.951	0.917	0.893
Paillier+DNN+Box diagram method (Paillier-DNN-BPM)	0.982	0.989	0.988	0.954	0.931

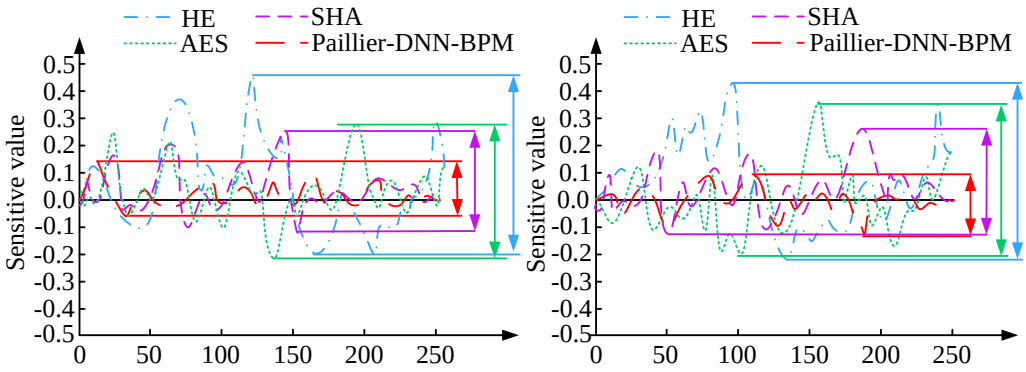


Figure 6: Sensitivity of different algorithms

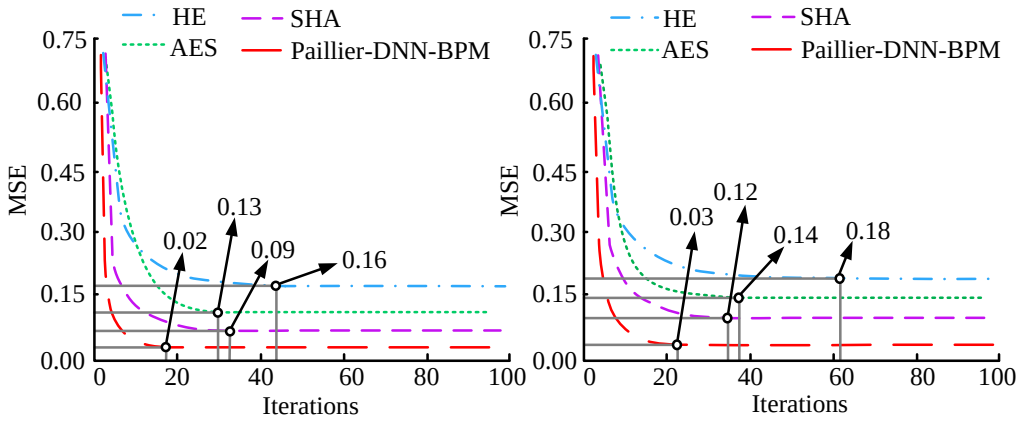


Figure 7: MSE of different algorithms

In Figure 7, the MSE values of the four algorithms in the training and test sets are given. In Figure 7(a), the MSE values of HE, AES, SHA, and Paillier-DNN-BPM are 0.16, 0.13, 0.09, and 0.02, respectively, when they reach the stability in the training set. In Figure 7(b), Paillier-DNN-BPM reaches the stability in the test set

first, and at this time, the MSE value is also the smallest, which is only 0.03. Taken together, the Paillier-DNN-BPM has better error performance during both training and testing.

3.2 Effect of practical application of the model

Four algorithms, HE, AES, SHA, and Paillier-DNN-BPM, are applied to the MCSN to build the corresponding four types of STDMs, respectively. In order to test the effectiveness of the four models in practical applications, the study chooses the intelligent transportation system of a first-tier city as the object. The MCSN is applied to this intelligent transportation system to test the detection precision of the four types of STDM for the six types of threat data in the intelligent transportation MCSN, as shown in Table 4.

In Table 4, when MCSN is applied to the intelligent transportation system, at this time, the detection rates of STDMs built using the four algorithms of HE, AES, SHA, and Paillier-DNN-BPM are all above 80%. Among them, the detection precision of Paillier-DNN-BPM model for all six types of threats is higher, up to 98.84%. While HE has generally lower detection precision for the six categories of threats, as low as 81.25%. The average detection time of the four models for the six categories of threats is tested and shown in Figure 8. In Figure 8, the average detection time of Paillier-DNN-BPM model is lower than that of HE, AES, and SHA models for all six classes of threats. Taking class, A threat as an example, the average detection time of HE, AES, SHA, and Paillier-DNN-BPM for this class of threat is 0.62, 0.56, 0.19, and 0.15, respectively, which shows that the detection time of Paillier-DNN-BPM is shorter and its detection efficiency is higher in practical applications. Comparing the encryption relevance and decryption relevance of the four types of models for data, as shown in Table 5.

Table 4: Detection precision of different models for six types of threats

Threat type	HE	AES	SHA	Paillier-DNN-BPM
A	81.25%	89.24%	92.36%	96.52%
B	84.06%	85.74%	90.58%	98.10%
C	85.97%	87.89%	89.17%	98.84%
D	82.23%	86.30%	91.25%	96.78%
E	85.79%	88.15%	90.21%	96.29%
F	83.41%	87.96%	89.73%	97.06%

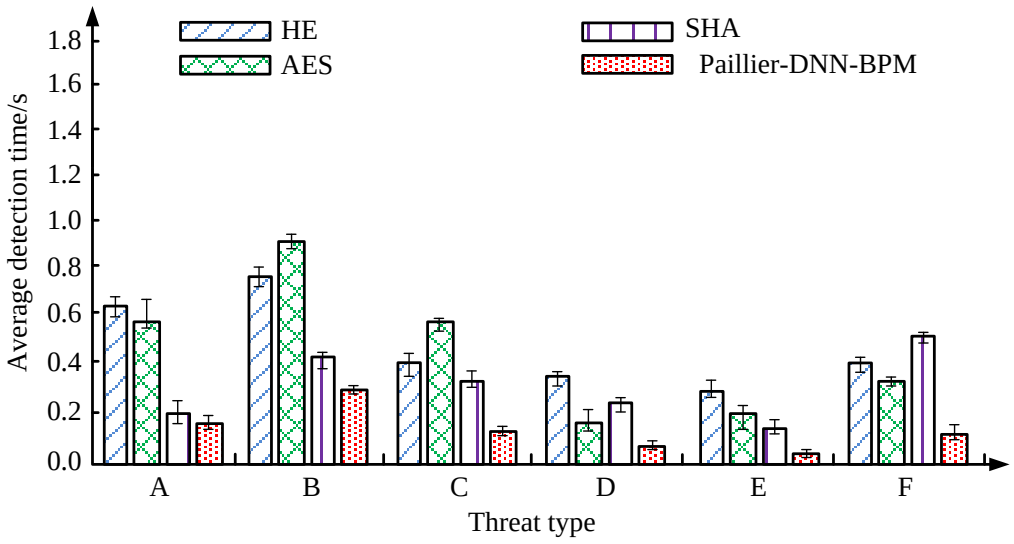


Figure 8: Average detection time of different models for six types of threats

Table 5: Correlation of data encryption and decryption of different models

Threat type	Cryptographic correlation				Decryption correlation			
	HE	AES	SHA	Paillier-DNN-BPM	HE	AES	SHA	Paillier-DNN-BPM
A	0.853	0.876	0.921	0.975	0.862	0.855	0.914	0.971
B	0.846	0.872	0.918	0.973	0.858	0.886	0.902	0.975
C	0.860	0.869	0.911	0.981	0.869	0.873	0.919	0.979
D	0.859	0.852	0.925	0.969	0.832	0.859	0.913	0.965
E	0.855	0.861	0.908	0.986	0.821	0.864	0.901	0.982
F	0.842	0.878	0.913	0.992	0.835	0.859	0.921	0.987

Combining all the correlation values in Table 5, it can be observed that the maximum correlation differences of HE, AES, SHA, and Paillier-DNN-BPM are 0.026, 0.021, 0.016, and 0.005, respectively, which shows that Paillier-DNN-BPM has the smallest loss during encryption and decryption, and the final detected threat data is more accurate. To investigate the universality of the proposed model, the study applies it to healthcare and smart city environments. The performance indicators obtained are shown in Figure 9.

In Figure 9, the proposed model still maintains high accuracy, recall rate, and F1 value in both healthcare and smart city environments, further verifying the generality and practical application potential of the model.

4 Discussion

In order to improve the PP capability of MCSN and the accuracy of security threat detection, a Paillier DNN BPM model was designed, and its performance was verified in the study. The PP joint learning method based on multi-bond HE proposed by Ma J et al. in reference [19] mainly focused on the application of multi-bond HE in joint learning. Although the Ma J method performed well in protecting data privacy, it lacked real-time threat detection and adaptability in complex network environments. To comprehensively evaluate the superiority of the proposed model, its performance in detection accuracy, computational efficiency, and scalability was compared with other common methods, including HE, AES, and SHA. The experimental results showed that the proposed model achieved detection accuracy, recall rate, and F1 score of 0.982, 0.989, and 0.988, respectively, which were significantly better than single encryption algorithms or traditional detection models. Especially in the application of intelligent transportation systems, the detection accuracy of the proposed model was as high as 98.84%, while the detection accuracy of HE, AES, and SHA were 94.32%, 91.76%, and 88.45%, respectively. In terms of computational efficiency, the proposed model demonstrated higher efficiency in encryption and decryption operations by combining PHE and DNN technologies. Compared with the HE

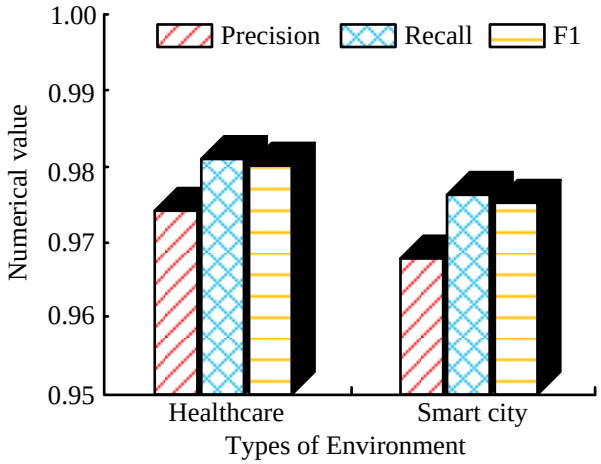


Figure 9: Performance of Paillier DNN-BPM model in different environments

model, the proposed model could significantly reduce computation time in large-scale data processing and maintain lower latency at different network scales. In terms of scalability, the proposed model adopted a distributed architecture of TEC three-level collaboration, which enabled the model to better adapt to complex network environments when processing large-scale data, demonstrating higher practicality and flexibility.

Although FHE can theoretically achieve homomorphic computation of any function, its computational complexity is extremely high, making it difficult to meet real-time requirements in practical applications. In contrast, Paillier encryption is a partially HE technique that supports only additive homomorphisms, which makes its computational complexity much lower than FHE, thus showing higher computational efficiency in practical applications. Federated learning models have privacy advantages, but are susceptible to network latency and synchronization issues due to the need for model synchronization and updates among multiple participants. A comparison of the HE-based PP deep learning method proposed by Falcetta A et al. in the literature [20] with other methods indicates that, although the method had high accuracy in PP of deep learning models, its complex structure may result in lower computational efficiency in large-scale MCSNs. The proposed model reduced the dependence on network synchronization on the basis of data privacy protection by adopting the TEC architecture, while improving the flexibility and adaptability of the overall system through distributed computing. The proposed model combined DNN for threat detection, leveraging the advantages of DNN in handling complex pattern recognition tasks to improve the real-time and accuracy of threat detection. In contrast, FHE models were difficult to achieve the same effect in real-time applications due to their high complexity, while federated learning models were limited by data dispersion and network synchronization issues, resulting in poor real-time performance. The key to the superiority of the proposed model over other alternative methods in multiple performance metrics lied in its architecture selection. The TEC three-level collaborative structure provided high flexibility and scalability for the model, enabling it to maintain efficient performance at different network sizes and complexities. Through the TEC architecture, the proposed model could improve system reliability while reducing network latency. The Paillier encryption algorithm's principal advantage lies in its low computational complexity, which enables the system to maintain efficient encryption and decryption processes at various stages of data transmission and processing. This results in efficient PP.

In summary, the study proposes an efficient and accurate lightweight STDM by combining PHE, DNN and BPM: Paillier-DNN-BPM. This not only provides new ideas and technical means for future PP of MCSN, but also positively impacts on improving the overall security of the network.

5 Conclusion

The results demonstrated that the Paillier-DNN-BPM model had better ablation test results and showed the best performance in detection precision, recall and F1 value, which was significantly higher than a single encryption algorithm or a traditional detection model. In addition, the Paillier-DNN-BPM model also had better performance in sensitivity and error detection, with smaller sensitivity fluctuation ranges and error values. Finally, the performance of the model was tested in a real operating environment, and compared with the HE, AES, and SHA models, Paillier-DNN-BPM demonstrated high detection accuracy and low system response time in intelligent transportation system application scenarios. In summary, the Paillier-DNN-BPM model not only performs well in ablation tests, but also achieves excellent detection results in practical applications. Further optimization of the computational and communication overhead of the model may be achieved through the implementation of follow-up studies. Additionally, the threat detection effect of different combinations of Paillier-DNN-BPM models in other complex network environments can be evaluated, thereby enhancing the generalizability and practicality of the model.

The equation symbols and their explanations are shown in Table 6.

Table 6: Equation symbols and their explanations

Equation Symbol	Explanation
n	Modulus
p, q, u	Large prime numbers
λ	Parameter
$lcm(\cdot)$	Least common multiple
$L(\cdot)$	Function used to calculate the intermediate value in the decryption process
g, r	Random number

n^2	Modulus square
p_k, s_k	Public key, private key
x, y	Plaintext
x', y'	Encrypted ciphertext
$E(x)$, $E(y)$	Encryption function
$D(x')$, $D(y')$	Decryption function
a	Variable of that function
$E(x+y)$	Addition operation directly on the plaintext
z	Number of times a certain power square is calculated and is a constant
l	Neuron of layer l in the DNN
$f(\cdot)$	Activation function of the neuron
$OP^{(l-1)}$	Output of the previous laye
$W^{(l)}$	Weights of the neurons of layer l
$BS^{(l)}$	Biases of the neurons of layer l
i	Mobile terminal
$\hat{W}(t)_i$	Updated model parameters of the mobile terminal i locally.
$\Delta\hat{W}(t)_i$	Adjusted value of the update
η	Learning step parameter.
$\hat{OP}_i$	Real output data of mobile terminal i
IN_i	Input data of mobile terminal i

References

[1] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. Fitzek, and N. Aaraj, "Survey on fully homomorphic encryption, theory, and applications," Proceedings of the IEEE, vol. 110, no. 10, pp. 1572-1609, 2022. https://doi.org/10.1109/JPROC.2022.3205665

[2] S. Saminu, G. Xu, S. Zhang, I. A. E. Kader, H. A. Aliyu, A. H. Jabire, Y. K. Ahmed, and M. J. Adamu, "Applications of artificial intelligence in automatic detection of epileptic seizures using EEG Signals: A review," Artificial Intelligence and Applications, vol. 1, no. 1, pp. 11-25, 2023. https://doi.org/10.47852/bonviewAIA2202297

[3] M. Dai, Z. Su, Q. Xu, Y. Wang, and N. Lu, "A trust-driven contract incentive scheme for mobile crowd-sensing networks," IEEE Transactions on Vehicular Technology, vol. 71, no. 2, pp. 1794-1806, 2021. https://doi.org/10.1109/TVT.2021.3117696

[4] D. Asprone, S. Di Martino, P. Festa, and L. L. L. Starace, "Vehicular crowd-sensing: a parametric routing algorithm to increase spatio-temporal road network coverage," International Journal of Geographical Information Science, vol. 35, no. 9, pp. 1876-1904, 2021. https://doi.org/10.1080/13658816.2021.1893737

[5] X. Zheng, Q. Yuan, B. Wang, and L. Zhang, "A homomorphic encryption-based location privacy preservation scheme for crowdsensing tasks allocation," Wireless Personal Communications, vol. 126, no. 1, pp. 719-740, 2022. https://doi.org/10.1007/s11277-022-09767-y

[6] R. Ganjavi, and A. R. Sharafat, "Edge-assisted public key homomorphic encryption for preserving privacy in mobile crowdsensing," IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 1107-1117, 2022. https://doi.org/10.1109/TSC.2022.3172136

[7] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," IEEE Transactions on Industrial Informatics, vol. 18, no. 6, pp. 4049-4058, 2021. https://doi.org/10.1109/TII.2021.3085960

[8] S. Jumonji, K. Sakai, M. T. Sun, and W. S. Ku, "Privacy-preserving collaborative filtering using fully homomorphic encryption," IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 3, pp. 2961-2974, 2021. https://doi.org/10.1109/TKDE.2021.3115776

[9] Y. Ren, T. Wang, S. Zhang, and J. Zhang, "An intelligent big data collection technology based on micro mobile data centers for crowdsensing vehicular sensor network," Personal and Ubiquitous Computing, vol. 27, no. 3, pp. 563-579, 2023. https://doi.org/10.1007/s00779-020-01440-0

[10] T. N. Nguyen, and S. Zeadally, "Mobile crowd-sensing applications: Data redundancies, challenges, and solutions," ACM Transactions on Internet Technology (TOIT), vol. 22, no. 2, pp. 1-15, 2021. https://doi.org/10.1145/3431502

[11] X. Li, G. Feng, Y. Liu, S. Qin, and Z. Zhang, "Joint sensing, communication, and computation in mobile crowdsensing enabled edge networks," IEEE Transactions on Wireless Communications, vol. 22, no. 4, pp. 2818-2832, 2022. https://doi.org/10.1109/TWC.2022.3214535

[12] C. Xu, and W. Song, "An adaptive data uploading scheme for mobile crowdsensing via deep reinforcement learning with graph neural network," IEEE Internet of Things Journal, vol. 9, no. 18, pp. 18064-18078, 2022. https://doi.org/10.1109/JIOT.2022.3163456

[13] Y. Ren, H. Jiang, X. Feng, Y. Zhao, R. Liu, and H. Yu, "ACP-based modeling of the parallel vehicular crowd sensing system: Framework, components and an application example," IEEE Transactions on Intelligent Vehicles, vol. 8, no. 2, pp. 1536-1548, 2022. https://doi.org/10.1109/TIV.2022.3221927

[14] K. Munjal, and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," Complex & Intelligent Systems, vol. 9, no. 4, pp. 3759-3786, 2023. https://doi.org/10.1007/s40747-022-00756-z

[15] X. Yang, S. Zheng, T. Zhou, Y. Liu, and X. Che, "Optimized relinearization algorithm of the multikey homomorphic encryption scheme," Tsinghua Science and Technology, vol. 27, no. 3, pp. 642-652, 2021. https://doi.org/10.26599/TST.2021.9010047

[16] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things," IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14542-14550, 2021. https://doi.org/10.1109/JIOT.2021.3066427

[17] Z. Cheng, F. Ye, X. Cao, and M. Y. Chow, "A homomorphic encryption-based private collaborative distributed energy management system," IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5233-5243, 2021. https://doi.org/10.1109/TSG.2021.3091624

[18] M. D. Boomija, and S. V. K. Raja, "Securing medical data by role-based user policy with partially homomorphic encryption in AWS cloud," Soft Computing, vol. 27, no. 1, pp. 559-568, 2023. https://doi.org/10.1007/s00500-022-06950-y

[19] J. Ma, S. A. Naas, S. Sigg, and X. Lyu, "Privacy-preserving federated learning based on multi-key homomorphic encryption," International Journal of Intelligent Systems, vol. 37, no. 9, pp. 5880-5901, 2022. https://doi.org/10.1002/int.22818

[20] A. Falcetta, and M. Roveri, "Privacy-preserving deep learning with homomorphic encryption: An introduction," IEEE Computational Intelligence Magazine, vol. 17, no. 3, pp. 14-25, 2022. https://doi.org/10.1109/MCI.2022.3180883

Tourism Promotion Mechanism Based on Virtual Reality Technology for Real-life Interactive Experience

Xinxin Nie[1], Jing Pu[2*]
[1]College of Literature and Media, Chengdu Jincheng College, Chengdu 611731, China
[2]School of Arts and Media, Sichuan Agricultural University, Ya'an 625014, China
E-mail: niexinxin@cdjcc.edu.cn, pujing325@163.com
[*]Corresponding author

Keywords: virtual reality technology, tourism recommendations, image retrieval, residual network, panoramic splicing

Received: May 28, 2024

The development of the national economy has promoted the development of the tourism industry, and outdoor tourism has gradually become the main leisure and entertainment method for people during holidays. However, the current tourism promotion mechanism only considers tourist preferences, resulting in tourists receiving recommendations. The unique features of the tourist attractions in the destination area are extremely similar to those of previous tourist areas. Therefore, the research is based on the Visual Geometry 19 model, using skip connections and soft threshold functions to improve the Visual Geometry 19 network. A residual network is designed for feature extraction, and panoramic stitching technology is used to construct virtual scenes of tourist attractions. The findings indicated that the residual network designed in the study demonstrated convergence after 50 iterations of training and testing on the tourism map dataset, with an accuracy of scene reconstruction reaching 85%. The designed tourism location image reconstruction could be completed in about 90 seconds, effectively improving the speed of the virtual reconstruction of tourism scenes. The designed tourism attraction promotion mechanism based on virtual reality technology effectively solves the problem of single tourism promotion and improves the experience of national outbound tourism.

Povzetek: Razvit je sistem za promocijo turizma, ki uporablja virtualno resničnost in slikovno analizo za interaktivno izkušnjo destinacij, kar izboljšuje priporočila turističnih krajev in prepečuje estetsko utrujenost obiskovalcev.

1 Introduction

The continuous growth of the global economy has led to an increase in people's disposable income, and the frequency of people traveling has gradually increased [1]. With the growth of the middle class, especially in the Asian region, the demand for tourism consumption has significantly increased [2]. Many countries and regional governments recognize the importance of tourism in stimulating economic growth. Consequently, they have implemented a range of policies designed to facilitate the expansion of the tourism sector. These include measures to streamline visa procedures, invest in tourism infrastructure, and promote cultural tourism [3-4] In addition, technological advancements and networking in transportation such as aviation, railways, and highways have made tourism more convenient and efficient [5]. The rise of low-cost airlines has also greatly reduced travel costs, making long-distance travel affordable for everyone [6]. The development of the Internet, mobile payment, social media, and online travel services has greatly facilitated the travel planning and booking process. Passengers can easily compare different tourism products and services and make online reservations [7-8]. However, due to the wide variety of tourist destinations, it is difficult for tourists to choose their favorite attractions. The current common tourist destination recommendation algorithms are mostly based on the introduction of scenic spots or tourist preferences. This recommendation method can easily cause aesthetic fatigue among tourists, leading to a poor travel experience. Therefore, to improve the tourism recommendation service experience of tourists, this study proposes to use a residual network (ResNet) structure to retrieve and extract features from relevant images of tourist attractions. The combination of virtual reality (VR) technology with a simulated virtual scene of a scenic location enables tourists to gain a firsthand understanding of the characteristics of the location, thus assisting them in making an informed choice regarding their preferred destination.

This study innovatively combines VR and image processing technology to build simulated scenes of scenic spots, allowing tourists to directly experience some of the features of the scenic spots, thereby helping them choose their desired attractions. The primary contribution is to

address the aesthetic fatigue that tourists often experience as a result of being consistently recommended similar attractions during their travels. This is achieved by enhancing their travel experience, promoting the advancement of the tourism industry, and stimulating the growth of related VR devices.

2 Related works

Tourism is one of people's daily entertainment activities. Nitu et al. proposed a travel recommendation system to provide customized travel destinations that meet the specific needs and preferences of users. The system identified travel tweets by analyzing Twitter data and user social networks, combined with machine learning classifiers, and considered time-sensitive recent weights. This model was superior to existing models, with an overall accuracy of 75.23% [9]. Gao et al. proposed the DeepTrip model to improve the understanding of human mobility in travel recommendation systems. This model used a travel encoder and a trip decoder, combined with an adversarial network, to better model the transition distribution of POI in human motion patterns. DeepTrip was effective both theoretically and empirically, outperforming the advanced baselines [10]. Liu et al. proposed a multi-task deep learning-based Hydra recommendation system to improve the user experience of transportation recommendations, implementing multi-modal transportation planning and considering contextual environments. By deploying on Baidu Maps, the system has effectively improved user click through rates [11]. Huang et al. proposed a multi-task deep travel route planning framework to improve tourism route planning and meet the diverse needs of tourists, integrating rich auxiliary information such as interest point attributes and user preferences. This framework demonstrated flexibility and superiority in route recommendation [12]. Wang et al. proposed an Internet of Things (IoT) system based on 5G and AI to address the challenges faced by the IoT in smart tourism. The system employed 5G technology to facilitate efficient data transmission and artificial intelligence (AI) to enable intelligent data processing, thereby enabling the development of smart tourism applications. The case study showed that the proposed method performed well in POI recommendation, verifying its effectiveness and excellent performance [13].

VR technology is widely used in various fields and has a promising future market. Lv et al. proposed an intrusion detection model for industrial control networks based on Class and Sample Weighted C-Support Vector Machine (CSWC-SVM) to protect industrial security and simulate VR environments. Simulation experiments showed that the CSWC-SVM algorithm exhibited high recognition accuracy and low false alarm rate under different kernel functions, and its accuracy remained above 90% under different sample sizes [14]. To explore the potential of 360° VR videos and real VR settings in teaching, Pirker and Dengel conducted a systematic evaluation of VR and proposed research on its application in education. 360° VR videos were beneficial for multiple disciplines and could enhance the learning experience [15]. Image retrieval technology (IRT) helped to build VR scenes. Dubey et al. conducted a comprehensive survey of relevant IRTs to explore content-based IRTs based on deep learning. A classification method was proposed that includes supervision, network, descriptor types, and retrieval types. Deep learning has shown outstanding performance in automatically learning image features, which contributed to the further development of IRT [16]. Fernandez-Beltran et al. proposed a probabilistic latent semantic hashing model to address the limitations of existing unsupervised hashing methods in processing complex semantic content in remote sensing images. It effectively learned hash codes through three steps: data grouping, topic calculation, and hash code generation. This method was significantly superior to the best unsupervised hashing methods [17]. Liu et al. proposed a similarity Siamese convolutional neural networks (CNNs) model based on unsupervised transfer learning to overcome the problems of sparse labeled samples and cumbersome CNNs in remote sensing image retrieval. This model was superior to existing CNN-based methods [18].

In summary, in the current global economic environment and situation, local tourism has become the main leisure and entertainment method for people during their holidays. Common attraction recommendation algorithms often use specially captured attraction images to recommend tourist areas to visitors. The utilization of this recommendation method has the potential to result in aesthetic fatigue among tourists. Conventional tourist attraction recommendations do not facilitate a comprehensive understanding of the distinctive attributes of the scenic spots, limiting tourists to a general perception of the types of scenery present in these locations. VR technology can build simulation scenes for scenic spots, allowing tourists to experience the unique features of the attractions firsthand. Therefore, this study proposes to use IRT to assist in building VR scenes for tourist attractions (VRSFTA) and recommend them to tourists.

Table 1: Summary of relevant work survey results

Author	Contribute
Nitu et al.	Improved the accuracy of customized recommendations
Gao et al.	Analyzed the flow characteristics of tourist tourism

Liu et al.	Improved the user experience of the recommendation system
Huang et al.	Improved the flexibility of recommending travel routes
Wang et al.	Proposed a new type of tourism recommendation method
Lv et al.	Strengthened the protection technology of virtual networks
Pirker and Dengel	Proposed evaluation methods for the role of VR systems in other fields
Dubey et al.	A deep learning-based image feature retrieval technique has been proposed
Fernandez-Beltran et al.	A novel image semantic content processing technology has been proposed
Liu et al.	Proposed an image feature retrieval technique

3 Methods and materials

3.1 Image feature extraction based on ResNet

The construction of VRSFTA requires a large amount of scenic feature data. The Visual Geometry Group (VGG) 19 model is one of the architectures of CNN models, which has high localization ability [19-20]. When constructing VRSFTA, it is necessary to locate the high correlation features of scenic spots in the VR scene based on photos from different angles. However, the VGG19 model is prone to network degradation or gradient disappearance when extracting features from scenic spot images [21]. Therefore, this study improves the VGG19 model and designs a ResNet. The ResNet structure is shown in Figure 1. ResNet adopts batch normalization (BN) and Dropout mechanisms. BN is a widely used technique in deep neural networks that can improve the stability and speed of model training [22-23]. When performing BN processing on data in a network model, it is necessary to subtract the batch mean and divide it by the batch standard deviation to standardize each small batch of data, making the input distribution of each layer of the network more stable. At the same time, the study introduces a soft threshold function in the network to process the interference noise in image feature extraction. The soft threshold function is shown in equation (1).

$$\begin{cases} soft(x,T)=\begin{cases} x+T, & x\le T \\ 0, & |x|\le T \\ x-T, & x\ge T \end{cases} \\ \dfrac{\partial y}{\partial x}=\begin{cases} 1, & x\le -T \\ 0, & |x|\le -T \\ 1, & x\ge T \end{cases} \end{cases} \tag{1}$$

In equation (1), x represents the input variable. T represents the noise processing threshold. y represents the output result of the soft threshold function. BN helps alleviate the problem of internal covariate shift in deep network training, which is the problem of the input distribution of the network layer constantly changing with the training process. During the one-way transmission of each batch of data, the BN operation is usually placed after the fully connected or convolutional layer and before the activation function. This approach ensures that the hidden activation inputs of the network are normalized, thereby reducing differences between different training batches [24-25]. In BN, the training batch mean needs to be calculated first, as shown in equation (2).

$$\mu_B \leftarrow \frac{1}{m}\sum_{i=1}^{m} x_i \tag{2}$$

In equation (2), μ_B represents the mean of a small batch of input sets. m represents the size of the small batch input set. x_i represents the input set elements. After calculating the mean of each small batch, the variance of each small batch can be calculated according to equation (3).

$$\sigma_B^2 \leftarrow \frac{1}{m}\sum_{i=1}^{m}(x_i-\mu_B)^2 \tag{3}$$

In equation (3), σ_B^2 represents the variance of a small batch of inputs. According to equation (4), the small batch data is normalized.

$$\hat{x}_i \leftarrow \frac{x_i - \mu_B}{\sqrt{\sigma_B^2 + \varepsilon}} \tag{4}$$

In equation (4), $\hat{x}_i$ represents the normalized input data. ε is to prevent positive numbers with zero denominators in normalization calculations. After normalizing the input data, the final adjustment can be made to the input data using equation (5).

$$y_i \leftarrow \gamma \hat{x}_i + \beta \tag{5}$$

In equation (5), y_i represents the input data after completing BN. γ and β represent transformation reconstruction parameters, where γ is the scale transformation reconstruction factor, and β is the translation reconstruction factor. Dropout is a commonly used regularization technique in deep learning, mainly used to prevent overfitting in neural networks during operation [26]. During the training process, during each forward propagation, Dropout randomly selects a batch of neurons and sets their output to zero. In each iteration, the structure of the network is different. Activation functions in neural networks can increase the expressive power of the model and affect the learning speed of the network. Different activation functions have different effects on the network [27-28]. Common activation functions include rectified linear unit (ReLU), parametric rectified linear unit (PReLU), and exponential linear unit (ELU). The definition of the PReLU function is shown in equation (6).

$$f(x_i) = \begin{cases} x_i, & x_i > 0 \\ a_i x_i, & x_i \le 0 \end{cases} \tag{6}$$

In equation (6), x_i represents the input of the activation function. a_i represents the negative half axis slope parameter. When parameter a_i in equation (6) is 0, the PReLU function is the ReLU function. If parameter a_i is a normal number $\leqslant 0.1$, the PReLU function is the Leaky ReLU function. The definition of the ELU function is given by equation (7).

$$f(x_i) = \begin{cases} x_i, & x_i > 0 \\ a\left(e^{x_i} - 1\right), & x_i \le 0 \end{cases} \tag{7}$$

In equation (7), a represents the parameter. The above functions can effectively avoid the problem of gradient vanishing in the learning process of neural networks. ResNet is composed of stacked residual blocks, and the common residual block structure is shown in Figure 2 [29-30].

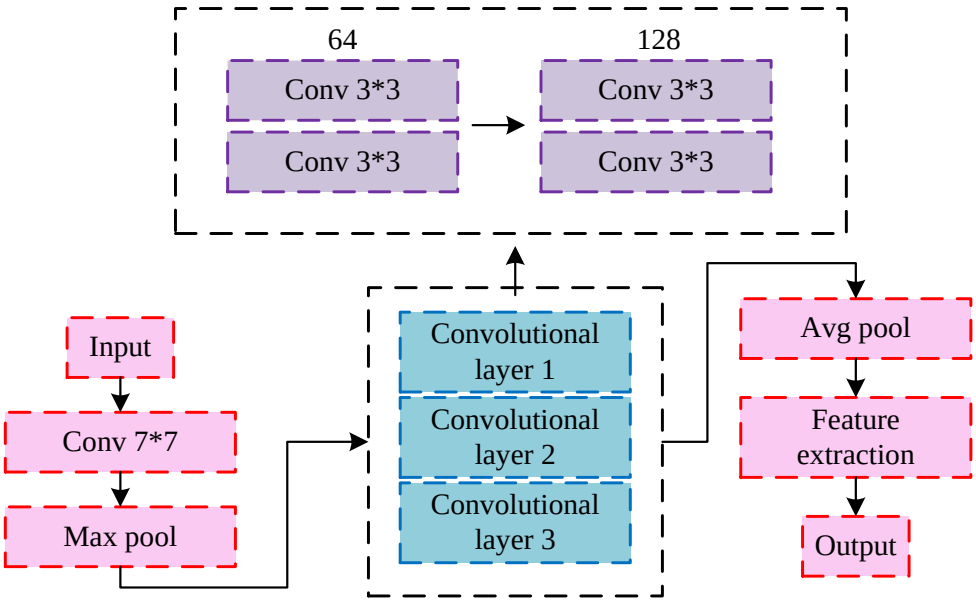


Figure 1: ResNet structure based on improved VGG19

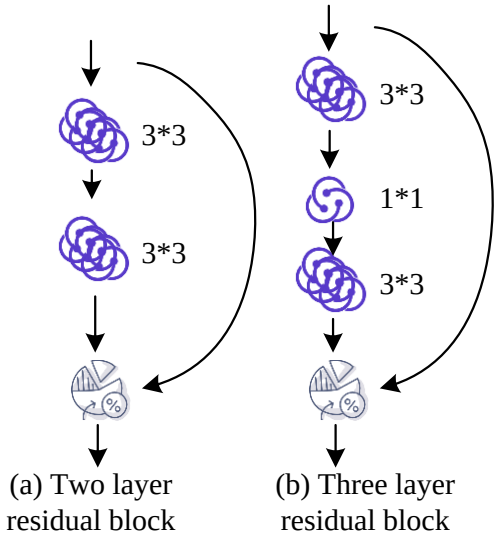


Figure 2: Residual block structure

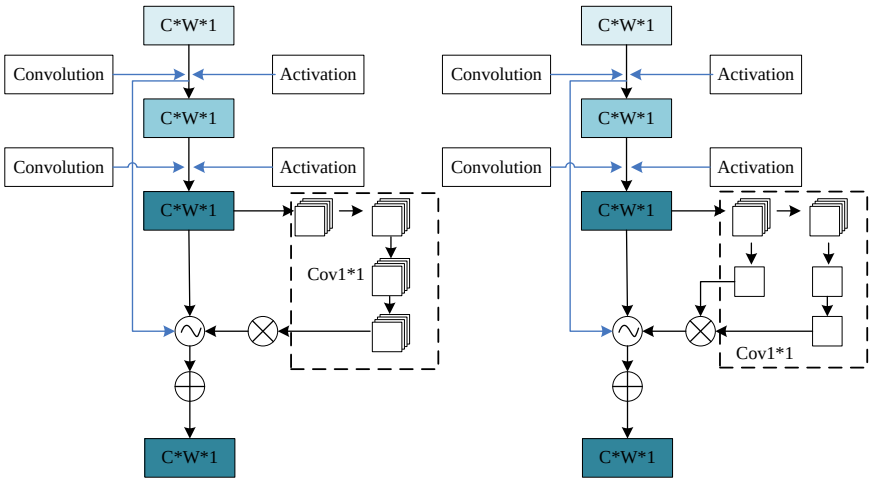
The two-layer residual block structure contains two 3*3 convolutional structures. The three-layer residual structure consists of two 1*1 and one 3*3 convolutional structures. The expression for the residual structure is given by equation (8).

$$x_{l+1} = x_1 + F\left(x_l, W_l\right) \tag{8}$$

In equation (8), x_l represents shallow units. $F\left(x_l, W_l\right)$ represents the residual function. The feature expression of deep units in ResNet is given by equation (9).

$$x_L = x_l + \sum_{i=1}^{L-1} F\left(x_i, W_i\right) \tag{9}$$

In equation (9), x_L represents a deep unit. In the design of residual modules, a division into channel-specific threshold modules and inter-channel shared threshold modules can be implemented, depending on the complexity of the network and the requirements of the task at hand. In different threshold modules for each channel, each channel has an independent threshold, which means that each channel can adjust its threshold according to its own characteristics to adapt to different feature responses. In the inter-channel shared threshold module, all channels share the same threshold, which means that regardless of the characteristics of the input data, all channels will use the same threshold for processing. The two structures are shown in Figure 3.



(a) Different thresholds per channel (b) Inter channel threshold sharing

Figure 3: Different threshold modules by channel share threshold modules between channels

3.2 Tourism scene reconstruction based on PIS technology

ResNet can effectively reduce the impact of unimportant features on tourism scene reconstruction in scenic spot captured images. Panoramic image stitching (PIS) technology is the technique of stitching images from different angles in the same region, discarding overlapping parts, and synthesizing panoramic images of the region [31-32]. Therefore, this study first uses ResNet to extract features from tourist attraction images, removing non important features from the captured images, and then uses PIS technology to synthesize panoramic images of tourist attractions. In PIS technology, most images used for stitching are imaged using fish eye images, as shown in Figure 4.

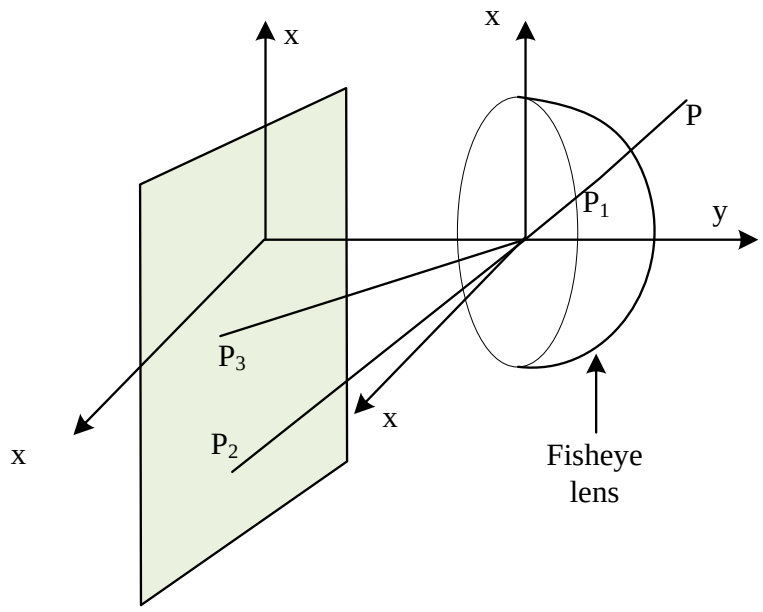


Figure 4: Imaging principle of fisheye images

Any point situated outside the lens is associated with the camera's position. Subsequent to traversing the fish eye lens, the camera's light path undergoes a shift, and the position of the imaging point on the imaging plane also undergoes a corresponding change. The imaging models for fish eye images include four types: isometric projection models (IPM), stereo angle projection models (SAPM), orthogonal projection models (OPM), and stereo projection models (SPM). The expression for the IPM is given by equation (10).

$$l = f\theta \tag{10}$$

In equation (10), l represents the imaging distance. θ represents the angle between the incident light and the longitudinal axis of the optical axis. f represents the camera focal length. The SAPM expression is given by equation (11).

$$l = 2f\sin\left(\frac{\theta}{2}\right) \tag{11}$$

The viewing range of IPM and SAPM is both 360°. The imaging distance in IPM is positively correlated with the angle between the light rays. Compared to IPM, when the imaging distance is the same, the light angle of SAPM will be larger. The viewing range of OPM is only 180°, and the distortion of its imaging pattern is more obvious, as expressed in equation (12).

$$l = f\sin\theta \tag{12}$$

The perspective range of SPM is greater than that of OPM, but lower than that of IPM and SAPM, as expressed in equation (13).

$$l = 2f\tan\left(\frac{\theta}{2}\right) \tag{13}$$

The four imaging models of fish eye images can be uniformly expressed, as shown in equations (14) [33-34].

$$l = \theta\left(1 + k_1\theta^2 + k_2\theta^4 + k_3\theta^6 + k_4\theta^8\right) \quad (14)$$

In equation (14), k_i represents the imaging parameters of the image. Fish eye images may experience radial distortion, tangential distortion, or thin prism distortion during shooting due to their large viewing angle range and planar imaging. Radial distortion refers to the basic absence of distortion at the center point of an image, typically exhibiting barrel shaped distortion that is stretched outwards or pillow shaped distortion that is compressed towards the center [35]. The correction of radial distortion is given by equation (15).

$$\begin{cases} x_c = x\left(1 + m_1r^2 + m_2r^4 + \cdots\right) \\ y_c = y\left(1 + m_1r^2 + m_2r^4 + \cdots\right) \end{cases} \quad (15)$$

In equation (15), (x_c, y_c) represents the corrected radial distortion point. (x, y) represents the radial distortion point before correction. m_n represents the distortion coefficient of the fish eye image. The tangential distortion correction model is equation (16) due to the mechanical error caused by the equipment.

$$\begin{cases} x_c = 2p_1xy + P_2\left(r^2 + 2x^2\right) \\ y_c = 2p_2xy + P_1\left(r^2 + 2y^2\right) \end{cases} \quad (16)$$

In equation (16), p_n represents the tangential distortion coefficient in the camera hardware facilities. Thin prism distortion is similar to tangential distortion and is also caused by mechanical errors in hardware facilities, but can be basically ignored in imaging. The panoramic projection models of tourist attractions are divided into planar panoramic, cylindrical panoramic, and spherical panoramic. A planar panoramic image uses feature point matching and image registration techniques to project and stitch photos onto the same plane, suitable for scenes with limited viewing angles. The cylindrical panoramic view uses a fixed fulcrum and is captured by horizontal rotation of the camera, projecting the image onto the cylindrical surface to achieve a 360° horizontal viewing angle. However, the vertical viewing angle is less than 180°, making it suitable for scenes with wider viewing angles. A spherical panoramic image provides a panoramic view by projecting the image onto a spherical surface. Both horizontal and vertical viewing angles can reach 360° and 180°, making it suitable for virtual scene roaming that requires all-round observation. This splicing technique is more complex, but the effect is more outstanding. These three methods each adapt to different application requirements, and through different projection and stitching techniques, can achieve a limited to comprehensive perspective expansion. This study uses fish eye images for VRSFTA reconstruction, and uses ResNet to extract and filter features from fish eye images. The specific PIS steps are shown in Figure 5. When constructing VRSFTA, it is necessary to first bring a fish eye imaging device to the scenic spot for photo collection. After completing the collection, the fish eye image is corrected to conform to human vision, and the image is transformed into linear storage. After preprocessing the image, ResNets can be used for feature extraction, which requires constructing the image scale space. When constructing the scale space, a Gaussian pyramid structure is used, with the original image placed at the bottom of the pyramid. After Gaussian blur processing, the original image is placed on the upper layer of the original image, and so on. The image scale space is shown in equation (16).

$$L(x, y, \sigma) = \mathrm{G}(x, y, \sigma) * I(x, y) \quad (17)$$

In equation (16), $L(x, y, \sigma)$ represents the two-dimensional image scale space. σ represents the scale space parameter. $\mathrm{G}(x, y, \sigma)$ represents a two-dimensional Gaussian function. $I(x, y)$ represents the converted grayscale image.

After preprocessing the image, ResNet can be used for feature extraction. After completing feature extraction, it is necessary to observe whether there is overlap between the images. If there is no overlapping area, the images with other overlapping areas are replaced. After there are overlapping areas in the image, image registration can be performed. The erroneous matching points in the image are removed, and the image with the proposed erroneous matching points is projected onto a sphere, which is then reflected as a planar image. Finally, all images can be fused. After completing the reconstruction of the virtual scene, collision detection is also required to ensure the authenticity of the scene. This study uses the bounding box method (BBM) for collision detection, and the process is shown in Figure 6.

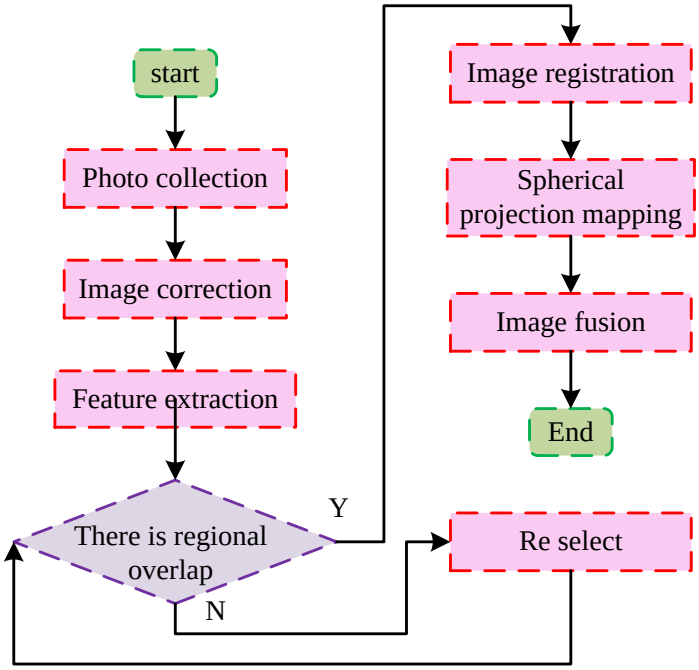


Figure 5: VR scene reconstruction process of tourist attractions

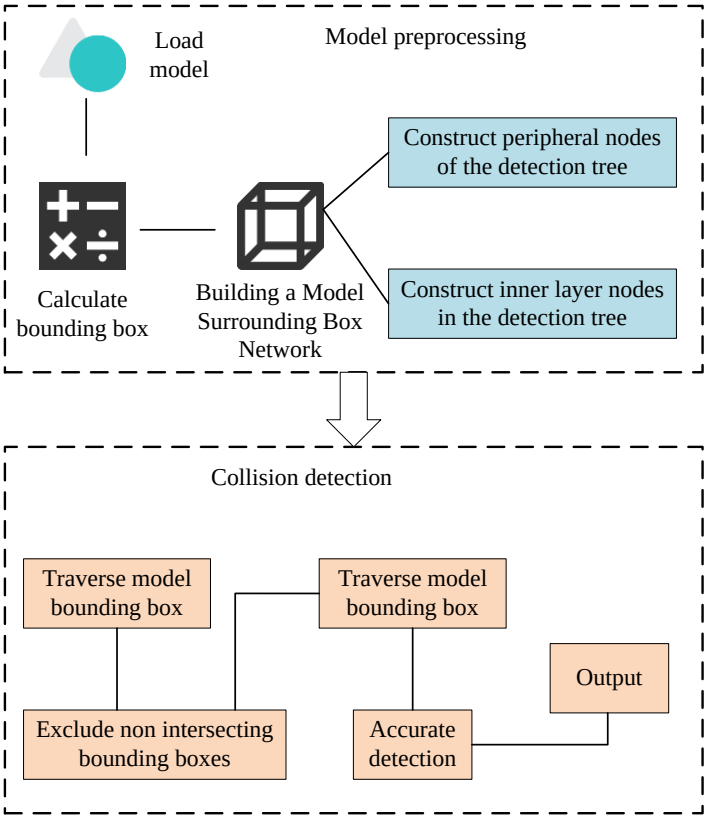


Figure 6: Process of model collision detection method based on BBM

When using BBM for collision detection, it is necessary to first initialize the detection scene, determine the set of objects that need collision detection, and then calculate the bounding boxes of all objects to be detected. The bounding boxes of all objects are compared to be detected, and if the bounding boxes do not intersect, it is considered that no collision has occurred. If the bounding boxes intersect, it is considered a collision and the virtual

scene needs to be rearranged based on the detection results.

4 Results

4.1 Experimental parameters and environmental settings

The experiments are all conducted in the Python framework, with the device operating system being Windows 10 Pro 64bit and the device processor being Intel (R) Core (TM) i5-10300H CPU@ 2.50GHz. The operating memory of the device is 32.0GB, and the GPU of the device is NVIDIA GeForce GTX 1660Ti. The algorithm training and testing process adopts SGD optimizer with cross entropy loss function, and the initial learning rate is 0.01. After every 20 iterations, the learning rate decreases by 0.1, the batch size is 128, and the maximum number of iterations is 200. Table 2 shows the specific configuration of the environment.

Table 2: Experimental environment setting

Hardware configuration		Software configuration	
CPU	Intel(R) Core (TM) i5-10300H	Operating system	Windows 10 Pro 64-bit
GPU	NVIDIA GeForce GTX 1660Ti	Deep learning framework	PyTorch 1.7.1
RAM	32 GB DDR4	Python version	Python 3.8
Storage	1 TB SSD	CUDA Version	CUDA 11.2
/	/	CuDNN version	CuDNN 8.1

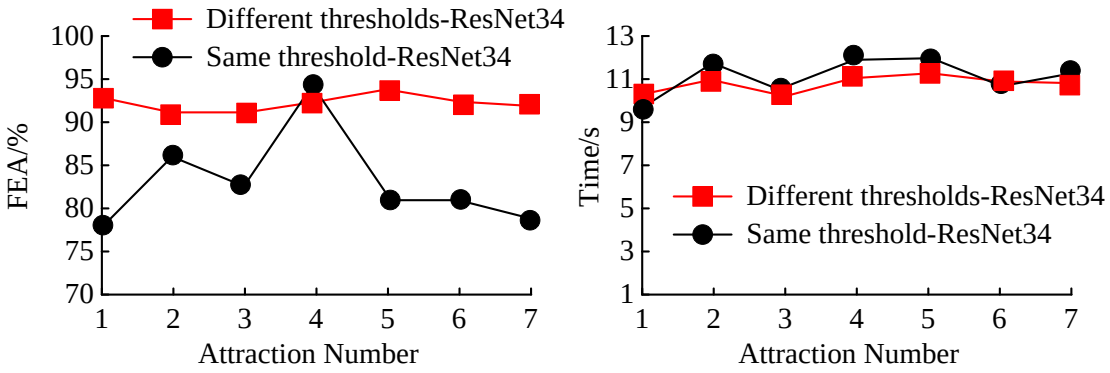
The dataset used for simulation training and testing of ResNets is the CIFAR-10 dataset. The CIFAR-10 dataset contains 60,000 32×32-pixel color images, divided into 10 categories with 6,000 images per category. These categories include airplanes, cars, birds, cats, deer, dogs, frogs, horses, boats, and trucks. These data come form a publicly available dataset for image feature extraction and processing, which can be directly used for feature processing of image data. The dataset is divided into 50,000 training images and 10,000 test images. This dataset is commonly used for image recognition and classification tasks in computer vision research. The study divides the training dataset into 5 batches, each containing 10,000 images. The hardware facilities for building VR scenes are the same as those for image feature extraction experiments. The VR system development engine is the Unity engine, and the system's new energy optimization adopts LOD technology. In the virtual scene, the architectural structure of the scenic area is modeled using 3D models, and the landscape and climate are integrated using 2D images. In the modeling of building structures, 3D models mainly focus on the structural contours, and structural details are implemented using textures.

4.2 Verification of image feature extraction effect based on ResNet

The constructed ResNet34 is based on the VGG16 network. To compare the extraction effects of different threshold-ResNet34 (DT-RN) modules and same threshold-ResNet34 (ST-RN) on important features of tourist attraction images, the feature extraction effects using DT-RN and ST-RN structures are compared. The results are shown in Figure 7.

Figure 7 (a) shows the comparison of feature extraction accuracy (FEA) between two residual structures. When using the DT-RN structure, the FEA of the network for scenic spot images is stable between 90%-95%. When using the ST-RN module, ResNet has a wide range of FEA fluctuations for scenic spots. After analysis, when using ST-RN, the feature extraction performance of complex images is poor, making it difficult to distinguish between important and non important features of the image. Figure 7 (b) compares the feature extraction efficiency (FEE) of two residual structures. The FEE of the two feature extraction methods is basically the same. This study compares the training efficiency and recall of ResNet34, VGG16, and ResNet18 networks on the TMD, as shown in Figure 8. Figure 8 (a) shows the comparison of training efficiency among three models. As the number of training iterations increases, the training time of all three networks begins to increase. The training time variation of ResNet34 is the smallest, followed by VGNN16. As for the time required to complete 100 iterations, ResNet34 is 2.6 seconds, VGG16 is 17.2s, ResNet18 is 16.8s. The training efficiency of ResNet34 network is the highest, with only 2.6s required for 100 iterations of training. Figure 8 (b) shows a comparison of the training recall rates of the model. As iterations increase, the recall rates of all three models are increasing. The recall rates of ResNet18 and ResNet34 can both increase to around 90%. For the highest recall rate, ResNet18 is 90.8%, ResNet34 is 95.2%, wile the VGG16 is only 88.7%. The recall rates of all three

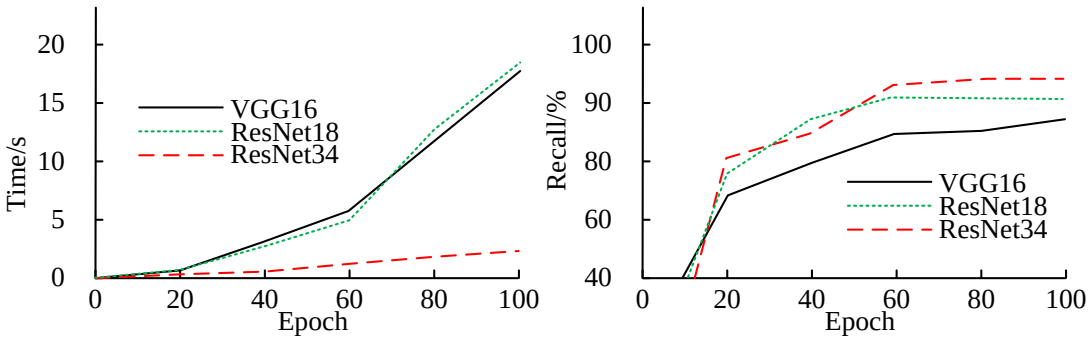
models can reach a high level, while the ResNet34 network has the best recall level. The testing time and recall results of ResNet18, ResNet34, and VGG16 on the TMD are displayed in Figure 9.



(a) Comparison of FEA for different residual structures

(b) Comparison of FEE for different residual structures

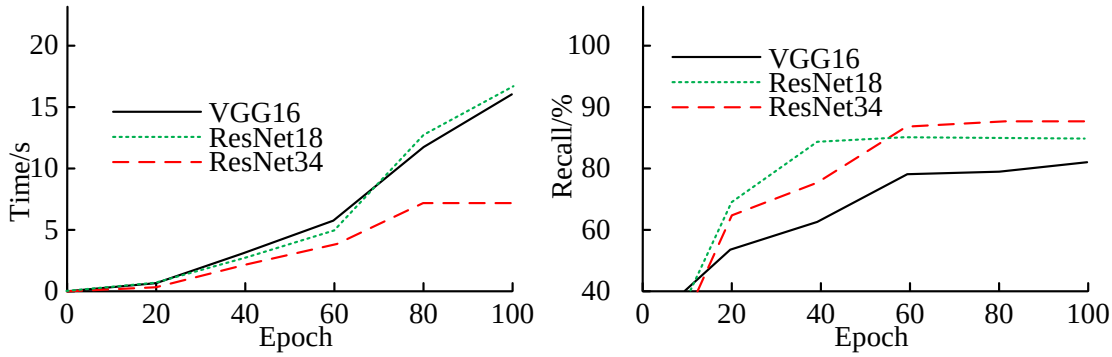
Figure 7: Comparison of feature extraction effects of different structures



(a) Training efficiency comparison

(b) Comparison of recall rates

Figure 8: Analysis of neural network training time and recall rate



(a) Training efficiency comparison

(b) Comparison of recall rates

Figure 9: Analysis of neural network testing time and recall rate

Figure 9 (a) shows a comparison of the testing time for each neural network. As the number of network detection iterations increases, the time required for each network to complete testing also increases significantly. ResNet34 has the least increase in time consumption, and completing 100 iterations of testing for this network takes about 7s. The time consumption of VGG16 is much higher than ResNet34 but slightly lower than ResNet18, and it takes about 15.5s for the network to complete 100 iterations. ResNet18 takes the most time to complete testing, but it is very close to VGG16, taking about 16s to complete 100 tests. Figure 9 (b) shows the changes in

recall rates of three networks during testing. The recall rates of ResNet18 and ResNet34 tend to stabilize at the 40th and 60th iterations, with stable recall rates approaching 85% and 89%, respectively. The recall rate of VGG16 dies not show a stable trend and continues to rise in the 100th iteration. At this time, the recall rate of VGG16 testing is only about 80%. The fusion of residual modules can effectively accelerate the training and testing efficiency of the network, and improve the recall rate of the network to the output results. To further verify the effectiveness of ResNet34 network in extracting features of tourist attractions, this study compares the loss values and accuracy of VGG16 and ResNet34. The training and testing loss values of VGG16 and ResNet34 on the TMD are exhibited in Figure 10. In Figure 10 (a), the change in loss values of the VGG16 network during training on this dataset is similar to the training results on the CIFAR-10 dataset. On the TMD, the change in loss values is more pronounced, with greater fluctuations. The test results of VGG16 on two datasets are completely different. When tested on the TMD, the model does not show a convergence trend and shows a certain upward trend as the iterations increase. In Figure 10 (b), the ResNet34 model converges well during training, completing convergence directly in the 50th iteration, and the network loss value after convergence tends to 0. The testing performance of this network on the TMD is poor, but overall, it shows a significant downward trend. After the 30th iteration, the loss value during network testing begins to fluctuate around 1.5. Compared to the VGG16 network, ResNet34 has better convergence performance on complex TMDs. Figure 11 shows the accuracy changes of VGG16 and ResNet34 on the TMD.

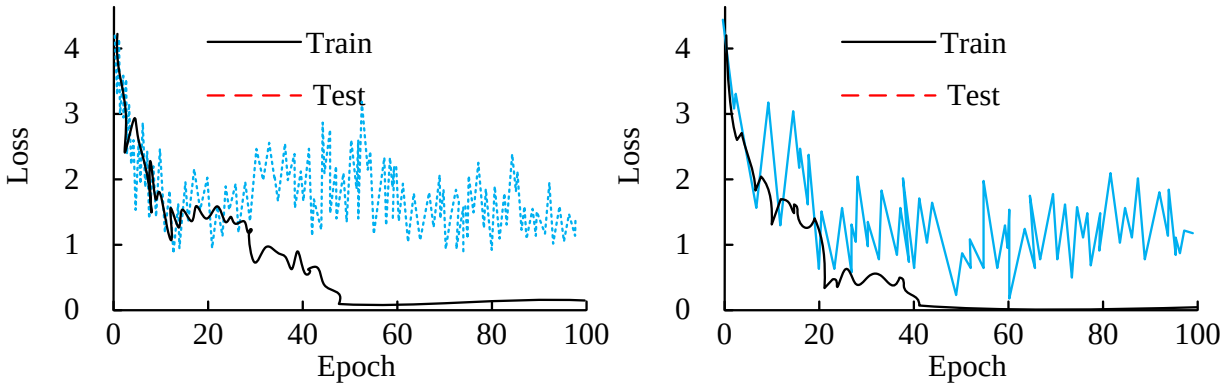


Figure 10: VGG 16 and ResNet34 changes in loss values in the TMD

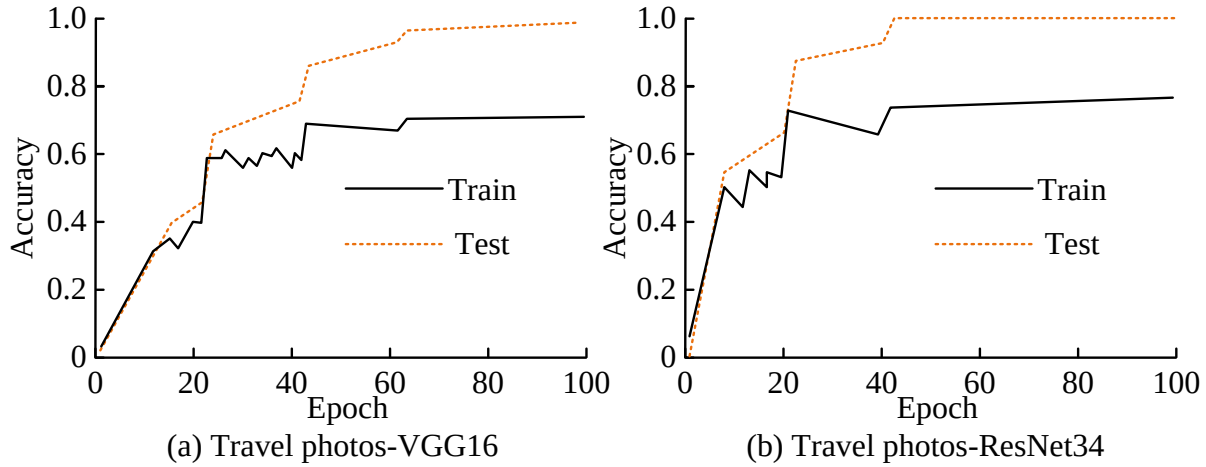


Figure 11: Changes in the accuracy of VGG16 and ResNet34 on the TMD

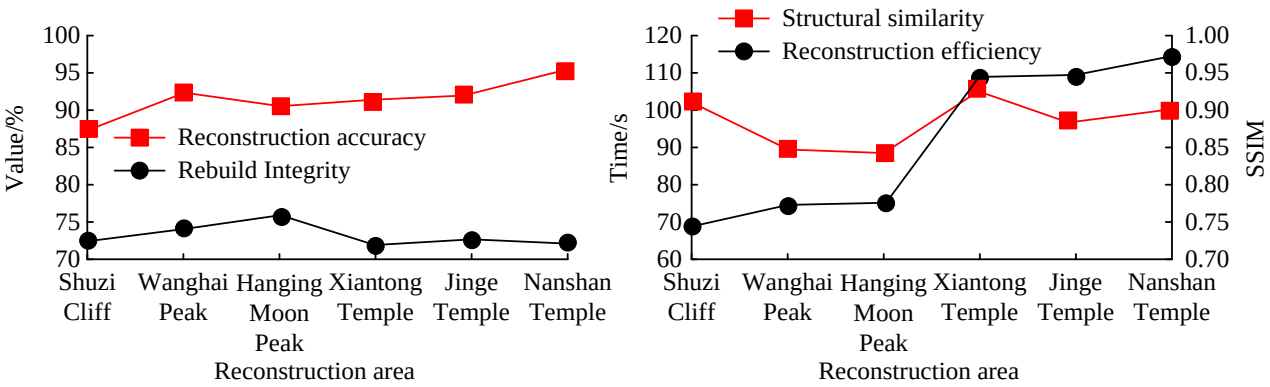
In Figure 11 (a), when VGG16 is trained on the TMD, the accuracy of the network increases with the increase of iterations. At the 70th iteration, the training accuracy of the network tends to 100%. Before reaching 70 iterations, the training accuracy of the network shows a phased increase. In the first 20 iterations, the accuracy of the network increases the fastest, from 0 to about 45%, and then increases by about 10% in each stage. The testing accuracy of this network on the TMD is at a relatively low level. After 70 iterations, its testing accuracy is only about 70%, far lower than the training accuracy. In Figure 11 (b), during training, compared to VGG16, at the 50th iteration, ResNet34's accuracy approaches 100%. When the iteration is less than 50, the accuracy of the ResNet34 network has also shown a phased increase. ResNet34 reaches its highest accuracy during the 30th iteration of

training, and then its accuracy decreases to around 60% before the 50th iteration after the 30th iteration, and then increases to around 75% after the 50th iteration.

4.3 Verification of tourism promotion effect based on VR

When analyzing the promotion effect of tourist attractions based on VR tourism promotion mechanism, this study first determines the reconstruction effect of VRSFTA. This study takes the Mount Wutai tourist attractions as an example to analyze the reconstruction accuracy, reconstruction efficiency, reconstruction integrity and structural similarity of different areas of the scenic spots. The results are shown in Figure 12.

Figure 12 (a) shows the comparison of reconstruction accuracy and reconstruction integrity of virtual scenes in different regions of Mount Wutai. The reconstruction accuracy of the constructed virtual scenes of scenic spots in various regions is maintained at over 85%, and the reconstruction completeness of all positions is also maintained at around 70%. Figure 12 (b) shows the comparison between the reconstruction efficiency of virtual scenes and the structural similarity of the reconstructed scenes. The reconstruction of the internal structure of the Mount Wutai building takes the highest time, about 110s. The reconstruction of other locations takes about 90s. The structural similarity of all scenes in the scenic spot can reach 0.7 or above. The interior reconstruction effect of the scenic building is shown in Figure 13. Figures 13 (a) and (b) show the virtual reconstruction effect of the left and front structures inside the building. In Figure 13, this scenic spot is a temple type attraction. The reconstruction effect of the left side chapel structure is good, and the reconstruction scene can better display the main structure of the temple's side chapel, such as the two door pillars and structures similar to door curtains. The main goal of the reconstruction of the front structure is to worship Buddha statues and their protectors in temples. The details of the Buddha statues in the reconstruction scene are relatively comprehensive, but the reconstruction effect of the protectors is slightly poor. After analysis, the reason is that during the extraction of image features, the Buddha statue protector statue was mistakenly identified as non-important features such as tourist flow in the scenic area, resulting in feature loss in the reconstruction of the front structure. The visualization results of VR reconstruction of tourist attractions are shown in Figure 14.



(a) Analysis of Reconstruction Accuracy and Reconstruction Integrity

(b) Reconstruction efficiency and structural similarity analysis

Figure 12: Analysis of the reconstruction effect of the VRSFTAs

Figure 13: Visualization results of VR reconstruction scenes within scenic spots

Figure 14: Visualization results of VR reconstruction of tourist attractions

This study investigates the comprehensive evaluation of tourists on VR attraction promotion, and the results are shown in Table 3.

Table 3: Scenic spot promotion effect evaluation

Tourist ID	Recommended methods	Count the number of people	Satisfaction rating	Surprise rating	Experience effect
1	This paper	50	89***	92***	Good
	Traditional method	50	72	72	Generality
2	This paper	50	87***	96***	Excellent
	Traditional method	50	70	71	Generality
3	This paper	50	88***	95***	Excellent
	Traditional method	50	71	69	Generality
4	This paper	50	87***	94***	Excellent
	Traditional method	50	70	68	Generality
5	This paper	50	89***	92***	Good
	Traditional method	50	69	72	Generality
6	This paper	50	92***	91***	Good
	Traditional method	50	71	72	Generality

Note: *: P<0.05%; **: P<0.01%; ***: P<0.001%.

In Table 2, the volunteers are relatively satisfied with the comprehensive rating of the promotion mechanism for the tourist attraction, all of which remain above 85 points. Among them, participant 6 rates the promotion mechanism above 90 points. All participants in the test show a high level of surprise towards the recommended attractions through the promotion mechanism, with scores consistently above 92. Participants 2, 3 and 4 rate the experience of VR scenes in scenic spots as excellent, while participants 1, 5 and 6 rate the spots as good.

5 Discussion

A new method for tourism promotion has been proposed, which utilizes VR technology and ResNet for image feature extraction and scenic spot recommendation. Compared with the advanced methods outlined in related works, several key differences and advantages have emerged. Nitu et al. [9] enhanced the precision of personalized recommendations through the examination of Twitter data and the application of machine learning

classifiers. However, the proposed method exceeds this by offering an immersive virtual reality experience. This not only helps with decision-making but also enhances the overall appeal of the destination through more attractive and realistic previews. Compared with the method proposed by Gao et al. [10], the proposed method focuses on visual and experiential aspects, providing virtual tours of potential destinations for tourists and helping them make more informed and personalized travel choices.

The experimental results show that the proposed ResNet34 model has a fast convergence speed and high accuracy in scene reconstruction, which is superior to other models such as VGG16 and ResNet18. This outstanding performance can be attributed to the skip connections in ResNet, which helps alleviate the problem of gradient vanishing and enable deeper network architectures. VR reconstruction technology also demonstrates a high degree of detail and structural similarity, providing almost realistic experiences for tourist attractions.

Integrating VR technology into tourism promotion mechanisms has a profound impact on the industry. Firstly, it has the potential to change the way tourists interact with and perceive tourist destinations, providing more immersive and informative decision-making tools. Secondly, achieving product differentiation through virtual experiences can enhance the competitiveness of tourism enterprises. Finally, it can reduce the impact on the environment and achieve more sustainable tourism practices by reducing the need for on-site visits during the decision-making stage.

Although the proposed method has performed well in personalized travel recommendations for tourists, there are still several areas that need improvement in the future. The representation of long-range structures in VR scenes still needs improvement and currently lacks details. Advanced image processing techniques and deeper neural networks can be explored to solve this problem. In addition, the integration of real-time data, such as weather conditions and crowd levels, can provide more value to tourists. Finally, developing more interactive and user-customizable VR experiences can further enhance user engagement and satisfaction.

6 Conclusion

To optimize the current tourism recommendation mechanism and change the current situation where recommendations are only based on tourists' past preferences or recent browsing content, this study used VR to design a scenic spot recommendation mechanism based on tourists' own experience. This technology used ResNet to extract features from scenic spot images, and then utilized panoramic stitching technology to construct VR scenes of relevant scenic spots. This allowed tourists to experience certain attractions in advance, thereby attracting them to the actual location of the attraction. The results verified that the designed ResNet34 could converge after 50 iterations of training on both the TMD and the CIFAR-10 dataset, and the loss values after convergence tended to 0. When tested on CIFAR-10, the converged loss value of ResNet34 was about 0.4, and the lowest loss value on the TMD was about 0.1. All tourists gave a comprehensive rating of 85 or above for the promotion mechanism, with a surprise rating of 90 or above for the promotion. The VR reconstruction technology designed in this project could clearly display the texture, structure, and other details of the target building structure when reconstructing virtual scenes of scenic spots. However, this technology has a poor reconstruction effect on distant structures when reconstructing panoramic views of scenic spots, and cannot show more details to tourists. In the future, it is possible to add a distance dimension to virtual scenes, so that tourists can intuitively experience all the characteristics of the scenic spot when experiencing them in the virtual scene.

References

[1] X. Zheng, B. Han, and Z. Ni, “Tourism route recommendation based on a multi-objective evolutionary algorithm using two-stage decomposition and pareto layering,” IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 2, pp. 486-500, 2023. https://doi.org/10.1109/JAS.2023.123219

[2] W. Tu, K. Mai, Y. Zhang, Y. Xu, J. Huang, M. Deng, L. Chen, and Q. Li, "Real-time route recommendations for e-taxies leveraging GPS trajectories," IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3133-3142, 2021. https://doi.org/10.1109/TII.2020.2990206

[3] Y. Wu, K. Li, G. Zhao, and X. Qian, "Personalized long- and short-term preference learning for next POI recommendation," IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 4, pp. 1944-1957, 2022. https://doi.org/10.1109/TKDE.2020.3002531.

[4] Y. Liu, F. Wu, C. Lyu, X. Liu, and Z. Liu, "Behavior2vector: Embedding users’ personalized travel behavior to vector," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 8346-8355, 2022. https://doi.org/10.1109/TITS.2021.3078229

[5] Y. Liu, H. Wu, K. Rezaee, M. R. Khosravi, O. I. Khalaf, A. A. Khan, D. Ramesh, and L. Qi, "Interaction-enhanced and time-aware graph convolutional network for successive point-of-interest recommendation in traveling enterprises," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 635-643, 2023. https://doi.org/10.1109/TII.2022.3200067

[6] Y. Li, F. Xiong, Z. Wang, Z. Chen, C. Xu, Y. Yin, and L. Zhou, "Spatial-temporal deep intention destination networks for online travel planning," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 3, pp. 2688-2700, 2022. https://doi.org/10.1109/TITS.2021.3091534

[7] H. Mezni, D. Benslimane, and L. Bellatreche, "Context-aware service recommendation based on knowledge graph embedding," IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 11, pp. 5225-5238, 2022. https://doi.org/10.1109/TKDE.2021.3059506

[8] Y. Yin, N. Zhang, Z. Chen, M. Li, Y. Li, H. Gao, and L. He, "Exploiting user preferences for multiscenarios in query-less search," IEEE Transactions on Computational Social Systems, vol. 9, no. 6, pp. 1794-1806, 2022. https://doi.org/10.1109/TCSS.2022.3181271

[9] P. Nitu, J. Coelho, and P. Madiraju, "Improvising personalized travel recommendation system with recency effects," Big Data Mining and Analytics, vol. 4, no. 3, pp. 139-154, 2021. https://doi.org/10.26599/BDMA.2020.9020026

[10] Q. Gao, F. Zhou, K. Zhang, F. Zhang, and G. Trajcevski, "Adversarial human trajectory learning for trip recommendation," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 4, pp. 1764-1776, 2023. https://doi.org/10.1109/TNNLS.2021.3058102

[11] H. Liu, Y. Tong, J. Han, P. Zhang, X. Lu and, and H. Xiong, "Incorporating multi-source urban data for personalized and context-aware multi-modal transportation recommendation," IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 2, pp. 723-735, 2022. https://doi.org/10.1109/TKDE.2020.2985954

[12] F. Huang, J. Xu, and J. Weng, "Multi-task travel route planning with a flexible deep learning framework," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 3907-3918, 2021. https://doi.org/10.1109/TITS.2020.2987645

[13] W. Wang, N. Kumar, J. Chen, Z. Gong, X. Kong, and W. Wei., "Realizing the potential of the internet of things for smart tourism with 5G and AI," IEEE Network, vol. 34, no. 6, pp. 295-301, 2020. https://doi.org/10.1109/MNET.011.2000250

[14] Z. Lv, D. Chen, R. Lou, and H. Song, "Industrial security solution for virtual reality," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6273-6281, 2021. https://doi.org/10.1109/JIOT.2020.3004469

[15] J. Pirker, and A. Dengel, "The potential of 360° virtual reality videos and real VR for education - a literature review," IEEE Computer Graphics and Applications, vol. 41, no. 4, pp. 76-89, 2021. https://doi.org/10.1109/MCG.2021.3067999

[16] S. R. Dubey, "A decade survey of content-based image retrieval using deep learning," IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 5, pp. 2687-2704, 2022. https://doi.org/10.1109/TCSVT.2021.3080920

[17] R. Fernandez-Beltran, B. Demir, F. Pla, and A. Plaza, "Unsupervised remote sensing image retrieval using probabilistic latent semantic hashing," IEEE Geoscience and Remote Sensing Letters, vol. 18, no. 2, pp. 256-260, 2021. https://doi.org/10.1109/LGRS.2020.2969491

[18] Y. Liu, L. Ding, C. Chen, and Y. Liu, "Similarity-based unsupervised deep transfer learning for remote sensing image retrieval," IEEE Transactions on Geoscience and Remote Sensing, vol. 58, no. 11, pp. 7872-7889, 2020. https://doi.org/10.1109/TGRS.2020.2984703

[19] H. Zhai, S. Lai, H. Jin, X. Qian, and T. Mei, "Deep transfer hashing for image retrieval," IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 2, pp. 742-753, 2021. https://doi.org/10.1109/TCSVT.2020.2991171

[20] M. Jankowski, D. Gündüz, and K. Mikolajczyk, "Wireless image retrieval at the edge," IEEE Journal on Selected Areas in Communications, vol. 39, no. 1, pp. 89-100, 2021. https://doi.org/10.1109/JSAC.2020.3036955

[21] H. Lu, M. Zhang, X. Xu, Y. Li, and H. T. Shen, "Deep fuzzy hashing network for efficient image retrieval," IEEE Transactions on Fuzzy Systems, vol. 29, no. 1, pp. 166-176, 2021. https://doi.org/10.1109/TFUZZ.2020.2984991

[22] C. Liu, J. Ma, X. Tang, F. Liu, X. Zhang, and L. Jiao, "Deep hash learning for remote sensing image retrieval," IEEE Transactions on Geoscience and Remote Sensing, vol. 59, no. 4, pp. 3420-3443, 2021. https://doi.org/10.1109/TGRS.2020.3007533

[23] C. Yan, B. Gong, Y. Wei, and Y. Gao, "Deep multi-view enhancement hashing for image retrieval," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 43, no. 4, pp. 1445-1451, 2021. https://doi.org/10.1109/TPAMI.2020.2975798

[24] Z. Xia, L. Wang, J. Tang, N. N. Xiong, and J. Weng, "A privacy-preserving image retrieval scheme using secure local binary pattern in cloud computing," IEEE Transactions on Network Science and Engineering, vol. 8, no. 1, pp. 318-330, 2021. https://doi.org/10.1109/TNSE.2020.3038218

[25] P. Li, L. Han, X. Tao, X. Zhang, C. Grecos, A. Plaza, and P. Ren, "Hashing nets for hashing: a quantized deep learning to hash framework for remote sensing image retrieval," IEEE Transactions on Geoscience and Remote Sensing, vol. 58, no. 10, pp. 7331-7345, 2020. https://doi.org/10.1109/TGRS.2020.2981997

[26] L. Zhang, Z. He, Y. Yang, L. Wang, and X. Gao, "Tasks integrated networks: joint detection and retrieval for image search," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44,

no. 1, pp. 456-473, 2022. https://doi.org/10.1109/TPAMI.2020.3009758

[27] N. Pellas, A. Dengel, and A. Christopoulos, "A scoping review of immersive virtual reality in STEM education," IEEE Transactions on Learning Technologies, vol. 13, no. 4, pp. 748-761, 2020. https://doi.org/10.1109/TLT.2020.3019405

[28] F. Hu, Y. Deng, W. Saad, M. Bennis, and A. H. Aghvami, "Cellular-Connected Wireless Virtual Reality: Requirements, Challenges, and Solutions," IEEE Communications Magazine, vol. 58, no. 5, pp. 105-111, 2020. https://doi.org/10.1109/MCOM.001.1900511

[29] M. Melo, G. Gonçalves, P. Monteiro, H. Coelho, J. Vasconcelos-Raposo, and M. Bessa, "Do multisensory stimuli benefit the virtual reality experience? a systematic review," IEEE Transactions on Visualization and Computer Graphics, vol. 28, no. 2, pp. 1428-1442, 2022. https://doi.org/10.1109/TVCG.2020.3010088

[30] L. Zhang, and J. Chakareski, "UAV-assisted edge computing and streaming for wireless virtual reality: analysis, algorithm design, and performance guarantees," IEEE Transactions on Vehicular Technology, vol. 71, no. 3, pp. 3267-3275, 2022. https://doi.org/10.1109/TVT.2022.3142169

[31] X. Liu, Y. Deng, C. Han, and M. D. Renzo, "Learning-based prediction, rendering and transmission for interactive virtual reality in ris-assisted terahertz networks," IEEE Journal on Selected Areas in Communications, vol. 40, no. 2, pp. 710-724, 2022. https://doi.org/10.1109/JSAC.2021.3118405

[32] O. Postolache, D. J. Hemanth, R. Alexandre, D. Gupta, O. Geman, and A. Khanna, "Remote monitoring of physical rehabilitation of stroke patients using IoT and virtual reality," IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 562-573, 2021. https://doi.org/10.1109/JSAC.2020.3020600

[33] H. Oagaz, B. Schoun, and M. -H. Choi, "Performance improvement and skill transfer in table tennis through training in virtual reality," IEEE Transactions on Visualization and Computer Graphics, vol. 28, no. 12, pp. 4332-4343, 2022. https://doi.org/10.1109/TVCG.2021.3086403

[34] K. Bang, Y. Jo, M. Chae, and B. Lee, "Lenslet VR: thin, flat and wide-fov virtual reality display using fresnel lens and lenslet array," IEEE Transactions on Visualization and Computer Graphics, vol. 27, no. 5, pp. 2545-2554, 2021. https://doi.org/10.1109/TVCG.2021.3067758

[35] F. Guo, F. R. Yu, H. Zhang, H. Ji, V. C. M. Leung, and X. Li, "An adaptive wireless virtual reality framework in future wireless networks: a distributed learning approach," IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 8514-8528, 2020. https://doi.org/10.1109/TVT.2020.2995877

Hybrid Machine Learning Classifier Models for Kidney Disease Detection

T. Mangayarkarasi[1], D. Najumnissa Jamal[2]
[1]Research Scholar, B.S. Abdur Rahman Crescent University, and Associate Professor, Electronics and Instrumentation Control Engineering, Sri Sairam Engineering College, Chennai, TamilNadu, India
[2]Professor and head, Electronics and Instrumentation Engineering, B.S. Abdur Rahman Crescent University, Chennai, TamilNadu, India
E-mail: mangairaajkumar@gmail.com, najumnissa.d@crescent.education

Keywords: hybrid model, decision tree, random forest, support vector machine, parameter tuning

Received: January 1, 2024

Detecting kidney disease at an early stage is crucial for timely intervention and improved patient outcomes. In recent years, machine learning classifiers have shown promise in enhancing the accuracy and efficiency of diagnosing kidney disease. This research paper delves into the comparative analysis of Support Vector Machine (SVM) classifier, Random Forest classifiers, and a Hybrid model combining SVM and Decision Tree for kidney disease detection. The introduction of each classifier, including SVM's classification mechanism, advantages, and preferred usage scenarios, as well as Random Forest's approach to combating overfitting through ensemble learning and parameter tuning considerations, sets the stage for a comprehensive evaluation. Additionally, exploring the benefits, challenges, and synergistic strengths of a Hybrid model in leveraging SVM's robustness and Decision Tree's interpretability is essential for understanding its potential in kidney disease detection. By investigating the common features utilized for kidney disease detection and assessing the accuracy and implications of early detection using machine learning models, this paper aims to contribute to the advancement of medical diagnostics. Furthermore, the study will evaluate and compare the performance of SVM, Random Forest, and Hybrid classifiers, examining the metrics employed for model effectiveness assessment and addressing any limitations or biases inherent in interpreting the results for kidney disease detection. Through this research, we aim to provide valuable insights into the application of machine learning classifiers in medical diagnostics, particularly in the context of kidney disease detection.

Povzetek: Predlagan je hibridni model strojnega učenja, ki združuje SVM in odločitveno drevo za zgodnje odkrivanje ledvičnih bolezni.

1 Introduction

Detecting kidney disease is crucial for early intervention and prevention of progression to kidney failure. Common features used for this purpose include assessing the number of filtering units (glomeruli) in the kidney and evaluating the condition of the tubules that collect urine [1]. Additionally, identifying the presence of fluid-filled sacs, known as cysts, in the kidneys is another key feature used in detection [1]. Monitoring the kidney's ability to eliminate waste from the blood and maintain the body's chemical balance is also essential in the detection process [1]. Various diagnostic tests play a vital role in identifying kidney disease, such as urine tests that reveal abnormalities and provide insights into the underlying cause of chronic kidney disease [1]. Imaging tests like ultrasounds or CT scans help assess the size, structure, visible damage, inflammation, or stones in the kidneys, aiding in the diagnosis process [1]. Furthermore, routine blood work can indicate the early stages of chronic kidney disease, making it an important tool in early detection and management [1]. Blood pressure monitoring and kidney function testing with urine and blood tests are also common practices in the detection and monitoring of kidney disease [1]. Early detection through these features and tests is essential as kidney disease often progresses without showing specific signs or symptoms until irreversible damage has occurred [1]. Machine learning models have shown promise in predicting kidney disease by utilizing various diagnostic tests and tools. Blood and urine tests play a crucial role in diagnosing kidney disease by assessing the levels of waste products like creatinine and urea in the blood, as well as detecting abnormalities that may indicate underlying issues [2][1]. Additionally, tests such as the estimated glomerular filtration rate (eGFR) and urine albumin test are commonly used to evaluate chronic kidney disease (CKD) and determine its severity [3]. These tests provide essential information about kidney function and can help healthcare providers identify the stage of CKD a patient is in, ranging from very mild to kidney failure [4]. Moreover, imaging tests like ultrasounds, MRIs, and CT scans are employed to visualize the kidneys and detect any potential blockages or abnormalities that may contribute to kidney disease [5]. By incorporating the results of these diagnostic tests into machine learning models, healthcare professionals can

enhance the accuracy of predicting kidney disease and tailor treatment plans to individual patients based on their specific diagnostic profile. Early detection of kidney disease using classifiers presents a promising avenue for improving patient outcomes and preventing disease progression. Given the variability in symptoms associated with kidney disease, including swelling, itchiness, and changes in urination frequency, timely consultation with a healthcare provider is crucial when suspecting such conditions [4]. Importantly, kidney disease may not exhibit any symptoms in its early stages, underscoring the significance of proactive screening and detection methods [4]. By leveraging classifiers for early detection, healthcare professionals can promptly identify individuals at risk and initiate interventions to prevent further deterioration of kidney function [4]. Such timely interventions have the potential to slow down kidney damage and, in some cases, avert the progression to kidney failure, highlighting the critical role of early detection in mitigating the impact of kidney disease on patients' health outcomes [4].

2 Machine learning approaches

Machine learning algorithms have revolutionized the field of healthcare by offering innovative solutions for disease diagnosis and prediction. In the context of kidney disease detection, Support Vector Machine (SVM) classifier, Random Forest classifiers, and the Hybrid (SVM and Decision Tree) machine learning classifier models have shown promising results. This section delves into the intricacies of these models and their application in the early diagnosis of chronic kidney disease (CKD) to enhance preventive healthcare strategies.

2.1 Support vector machines

Support Vector Machines (SVM) are a valuable tool in the realm of supervised learning, serving purposes in both regression and classification tasks. The fundamental principle of SVM involves plotting data points in a multi-dimensional space, where each feature corresponds to a specific coordinate within that space [6]. Support Vector Machine (SVM) is a powerful machine learning algorithm used for linear or nonlinear classification, regression, and even outlier detection [6]. In the realm of healthcare, particularly in the domain of kidney disease detection, SVM plays a crucial role. The research work [7] aims to assist in the prevention of chronic kidney disease (CKD) by utilizing machine learning techniques to diagnose CKD at an early stage. SVM can be used for both regression and classification tasks, but generally, they work best in classification problems [8]. The ability of SVM to handle complex classification tasks makes it a valuable tool in the early detection of kidney diseases. SVM is favored when computational resources are limited, as it requires less power to operate effectively compared to some other classifiers [8]. Furthermore, SVM shines when dealing with non-linearly separable data, making it the preferred choice in such scenarios over other classifiers that struggle with this type of data [9]. In fact, SVM has been found to outperform Naive Bayes specifically when data is not linearly separable, showcasing its superior performance in such cases [9]. Another advantage of SVM is its ease of interpretation, making it a preferred option when transparency and explainability are crucial factors in model selection [9]. Moreover, SVM is known for being less prone to over-fitting, ensuring more robust and generalize models compared to some other classifiers [10]. Particularly, SVM is well-suited for high-dimensional and unstructured datasets, such as image and text data, where it tends to outperform logistic regression, further solidifying its preference in these contexts [10]. The overall findings of SVM algorithm implemented in literature and its gap analysis is described in table 2.1.

2.2 Random forest

Random forest is a supervised learning algorithm that builds an ensemble of decision trees, usually trained with the bagging method [11]. In the context of medical data classification for kidney disease detection, a feature ranking based approach is developed and implemented using Random Forest classifiers [12]. Despite its popularity, the Random Forest Algorithm comes with its own set of advantages and disadvantages [13]. By leveraging the strengths of Random Forest classifiers, healthcare professionals can enhance the accuracy and efficiency of kidney disease diagnosis. Random Forest, utilizes various strategies to tackle the prevalent issue of over-fitting. One key approach employed by Random Forest is to increase the number of trees in the forest, as it has been shown that having a greater number of trees leads to higher accuracy and helps prevent over-fitting. By ensuring that individual trees in the forest are built with randomness, the algorithm reduces correlations between them, subsequently diminishing the risk of bias and over-fitting. Additionally, Random Forest implements feature bagging during the training phase, which helps prevent the dominance of any single feature, fostering diversity among the trees and contributing to a more resilient model. Furthermore, the algorithm controls the randomness of sample selection and feature choice, mitigating the risk of over-fitting by sampling features for the best split at each node and utilizing bootstrap aggregating to randomly sample subsets of the training data. Moreover, Random Forest's use of "majority rules" output serves as another mechanism to handle overfitting, ensuring that the final prediction is based on the collective decisions of multiple trees, rather than being influenced by a single tree that may have overfit the data. Overall, through a combination of

strategies such as increasing the number of trees, utilizing randomness in tree construction, feature bagging, and majority voting, Random Forest effectively manages the issue of overfitting, making model overfitting nearly impossible. The overall findings of random forest algorithm implemented in literature and its gap analysis is described in table 2.2.

Table 2.1 SVM algorithm gap analysis

	Findings	Gaps
Support Vector Machines (SVM)	- Effective in handling complex classification tasks, especially with non-linear separable data. - Efficient in computational resource usage. - Less prone to overfitting, ensuring robust and generalizable models. Easier to interpret, which is crucial for healthcare applications.	- Struggles with scalability for very large datasets due to computational complexity. - Requires careful tuning of parameters, which can be computationally intensive. - Sensitive to noisy data and outliers, which can affect performance.

Table 2.2 Random Forest algorithm gap analysis

	Findings	Gaps
Random Forest	- Achieves high accuracy and effectively prevents overfitting through increasing the number of trees, randomness in tree construction, feature bagging, and majority voting. - Excels in determining feature importance. Demonstrates resilience and robustness in various data scenarios.	- Often less interpretable than simpler models, which can be a drawback in healthcare applications. - Resource-intensive, particularly with a large number of trees. Can still overfit on particularly noisy datasets if not carefully managed.

Table 2.3 Hybrid model algorithm gap analysis

	Findings	Gaps
Hybrid Model (SVM and Decision Tree)	- Combines SVM and Decision Tree algorithms to optimize classification, leveraging SVM for crucial datapoints near decision boundaries. - Significantly enhances performance metrics such as prediction accuracy, MSE, and RMSE compared to individual models. Adaptable and can be tailored to various applications.	- Increased complexity can lead to longer training times and higher computational costs. - Integration of SVM and Decision Tree requires seamless integration, which can be technically challenging. Effectiveness heavily depends on data quality and may require extensive preprocessing and feature engineering.

2.3 Hybrid model

The hybrid tree model combines the strengths of SVM and Decision Tree algorithms to optimize the classification process for kidney disease detection. By utilizing SVM to classify crucial datapoints near decision boundaries, the hybrid model ensures efficient classification while maintaining accuracy [14]. This hybrid approach enhances the speed and precision of classification tasks, particularly in scenarios where quick decision-making is essential for early disease detection [14]. The synergy between SVM and Decision Tree algorithms in the hybrid model offers a comprehensive solution for accurate and timely kidney disease diagnosis [14]. Integrating Support Vector Machine (SVM) and Decision Tree in a hybrid model offers a multitude of advantages that outweigh the

limitations of each individual model. This integration not only addresses the shortcomings of the individual models but also enhances the classification accuracy significantly [15]. By leveraging the unique mechanisms of SVM and Decision Tree, the hybrid model can capitalize on the strengths of each model, leading to improved performance in terms of classification and prediction accuracy [15]. Furthermore, the hybrid model aids in the acquisition of optimal parameters, resulting in enhanced prediction accuracy, Mean Squared Error (MSE), and Root Mean Squared Error (RMSE) [16]. Research has shown that the hybrid model, combining SVM and Decision Tree, outperforms Logistic Regression (LR) and standalone SVM models, demonstrating superior generalization prediction accuracy, MSE, and RMSE [17]. This amalgamation of SVM and Decision Tree in a hybrid model showcases the potential for more robust and accurate predictive modeling compared to using either model in isolation. The hybrid model, a fusion of Support Vector Machine (SVM) and Decision Tree classifiers, is designed to capitalize on the strengths of each to enhance overall processing performance [18]. By incorporating the Euclidean distance and H-EOM metric, the hybrid model effectively harnesses the robust capabilities of SVM to improve classification accuracy and efficiency [19]. Studies have showcased the effectiveness of this approach, particularly with the H-SVM classifier, which has outperformed other traditional classifiers by effectively merging the attributes of SVM and Decision Tree methodologies [18]. In a different context, Wang et al. adopted a similar strategy by combining the predictions of neural network, support vector regression, and decision tree models to forecast the outcomes of optimizations in a plasma arc process for tar reforming, demonstrating the versatility and utility of hybrid models in diverse applications [20].A novel hybrid model algorithm combining SVM and decision tree algorithm implemented in this research work with its expected gap analysis is given in table 2.3. Overall findings and gap analysis are tabulated in table 2.4.

3 Challenges in integrating SVM and decision tree in a single classifier model

Integrating Support Vector Machine (SVM) and Decision Tree in a single classifier model poses certain challenges that need to be addressed. The hybrid tree model incorporates SVM's assistance specifically for classifying essential data points located near the decision boundary, while the less critical data points are handled by a rapid decision-making process. This approach aims to leverage the strengths of both SVM and Decision Tree algorithms to enhance classification accuracy and model performance. Previous studies have explored a range of machine learning algorithms, including logistic regression, random forest, gradient boosting, and SVM, to investigate the effectiveness of different approaches in classification tasks. Additionally, hybrid models have been proposed that combine Gaussian Naïve Bayes, gradient boosting, and decision tree as base classifiers, supplemented by random forest as a meta-classifier. One research initiative introduces the concept of a hybrid support vector machine (H-SVM) classifier, utilizing SVM as the foundational element in the hybrid model. Moreover, the integration of SVM and logistic regression in a hybrid model has been evaluated, showcasing the potential benefits of combining these techniques in a unified framework. Despite these advancements, the challenge remains in effectively merging the distinct methodologies of SVM and Decision Tree to create a cohesive and efficient classifier model that optimizes performance and accuracy in classification tasks. The intention of our research work is to examine the kidney disease from patient's images and indicate the menace of kidney disease via support vector machine, ensemble Random Forest and hybrid algorithm. The objective of our proposed work is discussed below,

- To identify the kidney disease using kidney affected patient's images as input.
- To implement conventional machine learning algorithms and hybrid-based algorithm in predicting kidney disease along with classification.
- To evaluate the overall performance of Proposed models.
- To classify the kidney images via two-level classifiers which distinguish images into normal from abnormal, and multi-label classifiers which categorize the kidney input images into several classes namely cyst, calculi, tumor from normal individuals.

Table 2.4 Over all findings and gap analysis from literature review

S. No	Title of the Article	Journal Details	Findings	Gap Analysis
1	Machine Learning Techniques for Kidney Disease Prediction	Journal of Healthcare Informatics Research [17],[20]	Demonstrates the use of various machine learning models like SVM, Random Forest, and Hybrid models for kidney disease prediction.	Lacks a comprehensive evaluation of hybrid models, especially in integrating SVM and Decision Trees.
2	Early Detection of Chronic Kidney Disease using	Journal of Medical Systems [6]	Highlights the importance of early detection using SVM and Random Forest.	Limited comparison with hybrid models and insufficient statistical analysis for validation.

	Machine Learning Algorithms			
3	A Hybrid Machine Learning Model for Predicting Kidney Disease	Health Informatics Journal [14]	Shows the effectiveness of hybrid models combining SVM and Decision Trees.	Needs detailed analysis on overfitting prevention and real-world dataset validation.
4	Improving the Accuracy of Kidney Disease Diagnosis with Machine Learning	International Journal of computing Business Research [18]	Focuses on improving diagnosis accuracy with Random Forest and SVM.	Does not address hybrid model integration and its comparative performance.
5	Comparative Analysis of Machine Learning Algorithms for Kidney Disease Detection	Computers in Biology and Medicine [23]	Compares SVM, Random Forest, and other algorithms for kidney disease detection.	Lacks a detailed discussion on hybrid models and overfitting issues.

4 Proposed methodology

In this section, we are introducing workflow of our proposed methods along with how the novel machine learning models utilized in kidney disease prediction and classification. The proposed workflow integrates multiple machines learning models, including SVM (Support Vector Machine), Ensemble Random Forest, and a Hybrid Model (combining SVM and Decision Tree), to enhance the prediction and classification accuracy of kidney diseases. The Hybrid Model combines SVM and Decision Tree to enhance prediction capabilities. Consideration of Overfitting and Model Complexity

Overfitting concerns

- Complexity of Hybrid Models: The integration of multiple models can lead to increased model complexity, which in turn can risk overfitting.

- Regularization techniques: To mitigate overfitting:

- Use regularization methods such as L2 regularization for the SVM.
- Prune the Decision Trees to avoid overly complex trees that fit the training data too closely.

- Validation strategies:

- Cross-validation: Employ k-fold cross-validation to ensure the model generalizes well to unseen data.
- Early stopping: Monitor performance on a validation set during training and stop when performance degrades, indicating potential overfitting.
- Ensemble methods: Usage of ensemble techniques like bagging and boosting to combine multiple models and reduce variance.

Implementation measures

- Hyperparameter Tuning: Perform grid search or random search to find the optimal hyperparameters for SVM and Decision Tree.
- Balanced Dataset: Ensure the dataset is balanced to prevent the models from being biased towards the majority class.
- Robust Evaluation Metrics: Besides accuracy, consider metrics such as precision, recall, and F1-score, especially in the case of imbalanced datasets.

By addressing overfitting and leveraging the strengths of both SVM and Decision Tree, the hybrid model aims to provide a robust solution for kidney disease prediction and classification, ensuring high accuracy and reliability in real-world applications.

The integration works as follows too depicted in figure 1.:

The outline of the proposed novel algorithm that integrates SVM (Support Vector Machine), Ensemble Random Forest, and a Hybrid Model (SVM and Decision Tree) for predicting kidney disease. This algorithm leverages the strengths of each model to improve overall prediction accuracy.

Step 1: Data preprocessing

a) Data collection: Gather a comprehensive dataset related to kidney disease with features such as age, blood pressure, blood tests, urine tests, etc.
b) Data cleaning: Handle missing values, outliers, and noisy data.
c) Feature engineering: Create new features if necessary and perform

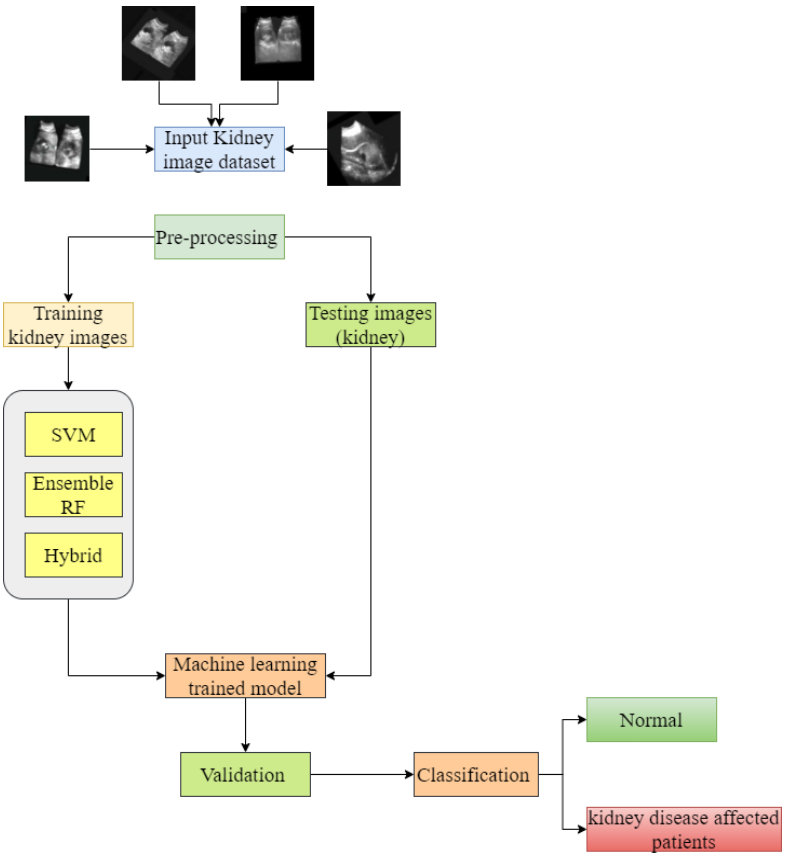


Figure 1: Proposed workflow for kidney disease identification and classification

a) feature selection to keep only the most relevant features.
b) Normalization/Standardization: Normalize or standardize the features to ensure they are on a similar scale.

Step 2: Model training

A. Split Data: Divide the dataset into training (70%) and testing (30%) sets.
B. Train base models:
   a. SVM: Train an SVM classifier using the training set.
   b. Random Forest: Train an ensemble Random Forest classifier using the training set.

Step 3: Hybrid model

A. Train hybrid model:
   a. SVM with Decision Tree: Combine SVM and Decision Tree to create a hybrid model. This can be done by training an SVM and using its predictions as additional features for a Decision Tree classifier.

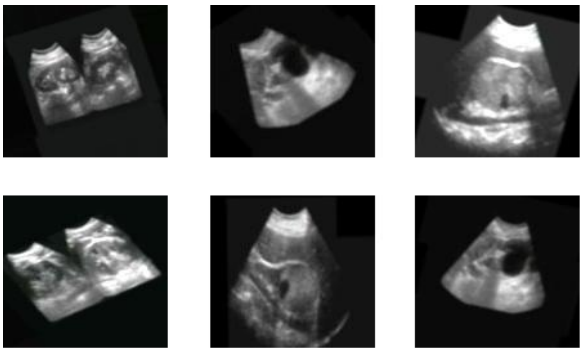


Figure 2: Sample input images for finding kidney abnormal region

B. Sequential training:
   a. Step 1: Train the SVM on the preprocessed training data to create a robust model that handles high-dimensional data efficiently.
   b. Step 2: Use the SVM's output predictions as input features for training the Decision Tree. This step allows the Decision Tree to capture non-linear relationships and interactions that the SVM might miss.

C. Synergistic effects:
    a. Strengths of SVM: Handles high-dimensional data well, finds the optimal hyperplane for classification, and is effective in cases where the number of dimensions exceeds the number of samples.
    b. Strengths of Decision Tree: Provides clear interpretability, captures non-linear interactions, and can model complex decision boundaries.
    c. By combining these two, the hybrid model benefits from the SVM's ability to separate classes in a high-dimensional space and the Decision Tree's capacity to refine these predictions with non-linear decision boundaries.

Step 4: Model integration

A. Stacking Ensemble: Use a stacking ensemble technique to integrate the predictions from the SVM, Random Forest, and Hybrid Model.
B. Train a meta-classifier (e.g., Logistic Regression) using the predictions from the SVM, Random Forest, and Hybrid Model as input features.

Step 5: Model evaluation

A. Evaluate Models: Use the testing set to evaluate the performance of the individual models (SVM, Random Forest, Hybrid Model) and the final stacked model.
    a. Calculate metrics such as accuracy, precision, recall, F1-score, and ROC-AUC.
B. Comparison: Compare the performance of the stacked model against the individual models to ensure the ensemble approach improves prediction accuracy.

Step 6: Deployment

Deploy Model: Once satisfied with the performance, deploy the stacked model for real-time kidney disease prediction.

This algorithm leverages the strengths of different models to improve kidney disease prediction accuracy, providing a robust solution.

5 Evaluation

When assessing the efficacy of SVM, Random Forest, and Hybrid classifiers for identifying kidney disease, it is imperative to employ robust evaluation metrics. A total of 520 samples with cyst, tumor, calculi and normal are taken and it is shown in table 5.1. These metrics serve to quantify the models' performance by comparing their predictions with the actual ground truth values, thereby determining the correctness and reliability of the outcomes [18][19]. To conduct a thorough analysis, multiple models are assessed against chosen evaluation metrics within a structured evaluation framework.

Table 5.1: kidney disease categories with number of samples

Categories of kidney disease	Number of samples
Cyst	180
Tumor	109
Calculi	99
Normal	132

This systematic approach allows for a comprehensive comparison of different classifiers, facilitating the identification of the most effective model for kidney disease detection [21][22][23]. When comparing the effectiveness of different classifier models, various metrics play a crucial role in providing a comprehensive evaluation. Metrics like accuracy, precision, recall, F1 score, and the area under the ROC curve are commonly employed to gauge the performance of classifier models from different angles, allowing for benchmarking and comparison purposes [19]. These metrics offer distinct perspectives on the model's behavior and effectiveness, aiding in the selection of the best-performing classifier [19]. The multilevel classifier confusion matrix is utilized to analyze the confusion matrix in order to detect several types of kidney abnormalities such as tumours, cysts, calculi, and normal via pictures of kidney patients. This multilevel classifier aids in the classification of images into many labels. Distinguishing two classes using confusion matrix is common. For example, to detect the aberrant region created in kidney pictures, we categorize the pictures of kidney into four classes with four labels shown in table 5.2. The confusion matrix, which records the occurrence quantity between real and anticipated values, is used by the multi label classifier to classify actual images into various classes.

Inferences-

- The confusion matrix of ensemble based random forest is shown in figure 3 Here, truly predicted the disease as 27, false negative as 0, false positive value as 2 and true negative as 20.

Table 5.2: Multi label classifiers for kidney disease identification using confusion matrix

Actual value	Classes	Predicted Value: Normal	Calculi	Tumour	Cyst
	Normal	TN	FP	TN	TN
	Calculi	FN	TP	FN	FN
	Tumour	TN	FP	TN	TN
	Cyst	TN	FP	TN	TN

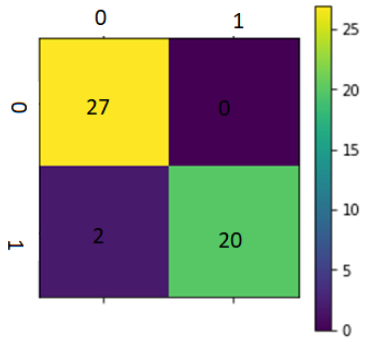


Figure 3: CM for ensemble based random forest algorithm

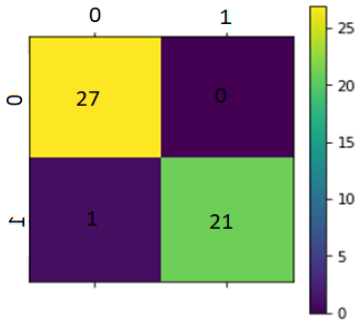


Figure 4: CM for SVM algorithm

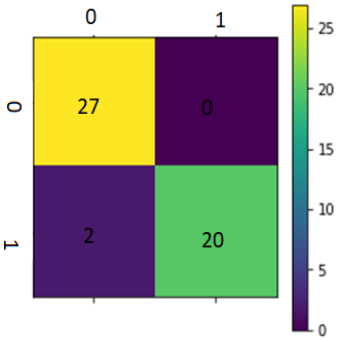


Figure 5: CM for hybrid algorithm

- For detecting kidney disease and also classifying images into two classes using confusion matrix for SVM approach which is shown in figure 4. The values predict the classes correctly namely TP value is 27, FN is 0, FP is 1 and TN is 21.
- The confusion matrix of proposed hybrid algorithm which appropriate to detect the disease via TP as 27, FN is 0, FP is 2 and TN is 20 are depicted in figure 5.
- Table 5.3 clearly indicates the need for Multilabel Classifier.

Table 5.3: Performance metrics -two label classifier

	Random Forest	SVM	Hybrid approach (SVM + Decision Tree)
Precision	1	1	1
Recall	0.931	0.964	0.931
F-Score	0.964	0.981	0.964

Multi-label classifier results

The classifier which distinguishes the kidney images into several classes namely class 0, class 1, class 2, and class 3 represented as calculi, cyst, normal and tumor kidney images. Here the comparison has done among three algorithms such as ensemble random forest, SVM and hybrid algorithm in predicting kidney disease and also classifying images into several classes namely tumor, cyst, calculi and normal. Table 5.7 demonstrates three machine learning approaches in terms of accuracy along with two-level and multi label classifiers.

- Detection of Kidney Stones / Calculi, classification accuracy has been improved using Hybrid Algorithm
- Detection of Kidney Cyst- Classification Accuracy for Hybrid Algorithm is less when compared to SVM classifier
- Detection of Kidney Tumor- Classification Accuracy for Hybrid Algorithm is less when compared to SVM classifier
- F-score has an improved metric which shows abnormality detection of any type, Hybrid algorithm gives better performance
- Obtained values of Precision, in classifying kidney stones, shows Hybrid Algorithm has positively classified TP for that particular abnormality.

After image classification has done, the representation of images is shown in figure 6.

6 Impact and clinical relevance

The proposed workflow and hybrid machine learning algorithm for kidney disease identification and classification have significant implications for clinical practice and patient care. Below are key areas where this impact and relevance are most evident:

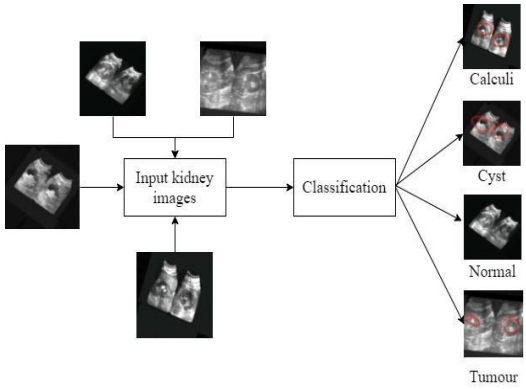


Figure 6: Classification to detect the affected region of kidney

Table 5.4: Detection of calculi kidney disease

	Random Forest	**SVM**	**Hybrid approach (SVM + Decision Tree)**
Accuracy	91.3	86.9	89.1
Precision	0.894	0.894	1
Recall	0.894	0.809	0.791
F-Score	0.917	0.894	0.833

Table 5.5: Detection of Cyst kidney disease

	Random Forest	**SVM**	**Hybrid Combine (SVM + Decision Tree)**
Accuracy	92	93.6	92
Precision	0.972	0.944	0.972
Recall	0.897	0.944	0.897
F-Score	0.883	0.943	0.883

Enhanced diagnostic accuracy

- **Improved prediction accuracy**: By leveraging the strengths of SVM, Random Forest, and a Hybrid Model, the proposed approach ensures higher accuracy in predicting various kidney diseases. This leads to more reliable diagnoses, reducing the risk of misdiagnosis.
- **Precision and recall**: High precision and recall metrics mean fewer false positives and false negatives, respectively. Clinicians can be more confident in the diagnostic results, which is critical for timely and appropriate treatment.

Table 5.6: Detection of tumor kidney disease

	Random Forest	**SVM**	**Hybrid Combine (SVM + Decision Tree)**
Accuracy	95.9	97.9	95.9
Precision	1	1	1
Recall	0.931	0.964	0.931
F-Score	0.964	0.981	0.964

Table 5.7: Comparison of classification accuracy among proposed algorithms with two label and multi label classifiers

Proposed Machine learning algorithm	**Two-level classifier**	**Multi label classifier**
Ensemble Random Forest	95.9	83.65
Support Vector Machine	97.9	91.3
Hybrid (SVM+DT)	95.9	82.69

b. Early detection and prevention

- **Early intervention**: Accurate early detection of kidney diseases such as calculi, cysts, and tumors enable early intervention, which can significantly improve patient outcomes. Early treatment can slow disease progression and improve quality of life.
- **Preventive measures**: Identifying at-risk individuals through precise prediction models allows for the implementation of preventive measures, potentially reducing the incidence of severe kidney disease complications.

c. Personalized treatment plans

- **Tailored treatments**: The detailed and accurate classification of kidney disease types supports the development of personalized treatment plans. Each patient's specific condition can be addressed with a customized approach, enhancing treatment effectiveness.
- **Monitoring and adjustments**: Accurate predictions enable ongoing monitoring and timely adjustments to treatment plans, ensuring they remain effective as the disease progresses or responds to therapy.

d. Resource optimization

- **Efficient use of resources**: By providing accurate and early diagnoses, the proposed model helps optimize the use of medical resources. Fewer diagnostic tests and follow-ups are needed, which reduces healthcare costs and saves time for both patients and healthcare providers.
- **Prioritization**: Healthcare facilities can prioritize patients based on the severity and type of kidney disease detected, ensuring those in critical need receive prompt attention.

e. Clinical decision support

- **Supporting clinicians**: The integration of machine learning models into clinical workflows acts as a decision support system, aiding clinicians in making informed decisions based on data-driven insights.
- **Reducing human error**: Machine learning models help reduce human error in diagnosis, providing consistent and objective assessments that support clinical judgment.

f. Research and development

- **Advancing medical research**: The data and insights generated from these predictive models can contribute to medical research, helping to uncover new patterns and correlations in kidney disease progression and treatment response.
- **Innovation in healthcare**: The use of advanced machine learning models in clinical practice promotes innovation, encouraging the development and adoption of new technologies in healthcare.

g. Patient empowerment

- **Patient awareness**: Accurate and early predictions can empower patients with knowledge about their health status, encouraging proactive health management and adherence to treatment plans.
- **Improved patient outcomes**: With better diagnostic tools and personalized treatments, patients experience better health outcomes and improved quality of life.

The integration of SVM, Random Forest, and a Hybrid Model for kidney disease prediction and classification presents a robust, accurate, and clinically relevant approach to managing kidney health. By enhancing diagnostic accuracy, supporting early detection, and enabling personalized treatment plans, this workflow has the potential to significantly improve patient care and outcomes. Additionally, it optimizes healthcare resources and supports clinical decision-making, making it a valuable tool in modern medical practice.

7 Conclusion

A diagnostic decision support system is required to aid doctors in determining the chronic state of kidney disease patients. We devised a mechanism to assist clinicians in treating individuals with kidney disease. Support Vector Machine is a system that was created using machine learning techniques (SVM). This proposed work focused on detecting kidney disease affected patients by applying machine learning techniques like SVM, ensemble random forest and hybrid algorithm upon kidney images dataset as input. Moreover, classification has done to identify the affected regions on kidney images to find whether it is either cyst or tumor or calculi in terms of accuracy and confusion matrix measures. Our experimental results reveal that among these machine learning algorithms, SVM generates high accuracy of 91.3% for Multi label classifiers and 97.9% for two label classifiers. This approach is supposed to assist doctors in accurately determining the chronic state of kidney disease patients. But the approaches still produce ambiguity in multi label classification since the image dataset is comparatively less which necessitates the implementation of Transfer learning techniques.

Acknowledgement

We render our Sincere thanks to Dr. Vezhaventhan, Urologist at Saanvi Fertility Center and Urology Hospital Chennai, Tamil Nadu, India for his support, in providing medical images especially Ultrasound Kidney Images to carry out our research. His guidance and Clinical inputs helped us to proceed with our research objectives to a great extent.

References

[1] Romagnani P, Remuzzi G, Glassock R, Levin A, Jager KJ, Tonelli M, Massy Z, Wanner C, Anders HJ, “chronic kidney disease”, Nature reviews Disease primers, 2017 Nov 23;3(1):1-24 https://doi.org/10.1038/nrdp.2017.89

[2] Chen TK, Knicely DH, Grams ME, “chronic kidney disease diagnosis and management: a review”, Jama, 2019, Oct 1;322(13):1294-304. https://doi.org/10.1001/jama.2019.14745

[3] Byvatov E, Fechner U, Sadowski J, Schneider G. “Comparison of support vector machine and artificial neural network systems for drug/nondrug classification”, Journal of chemical information and computer sciences. 2003 Nov 24;43(6):1882-9. https://doi.org/10.1021/ci0341161

[4] Alam MZ, Rahman MS, Rahman MS, “A Random Forest based predictor for medical data classification using feature ranking”, Informatics in Medicine Unlocked, 2019 Jan 1;15:100180, https://doi.org/10.1016/j.imu.2019.100180

[5] Kumari A, Mehta AK, "A hybrid intrusion detection system based on decision tree and support vector machine", 2020, IEEE 5th International conference on computing communication and automation (ICCCA) 2020 Oct 30 (pp. 396-400). IEEE, https://doi.org/10.1109/iccca49541.2020.9250753

[6] Polat H, Danaei Mehr H, Cetin A, "Diagnosis of chronic kidney disease based on support vector machine by feature selection methods", Journal of medical systems. 2017 Apr; 41:1-1, https://doi.org/10.1007/s10916-017-0703-x

[7] Hussein Abdel-Jaber, Ahmed Abdel-Wahab Rakha, Anas Abdualqader Hadi, Nesrine Atitallah, Ali Wagdy Mohamed, "ML-Based Stroke Detection Model using Different Feature Selection Algorithms", An International journal of computing and informatics, Vol 48, No 17 (2024), https://doi.org/10.31449/inf.v48i17.6096

[8] Ruaa Sadoon, Adala Chaid, "Classification of Pulmonary Diseases Using a Deep Learning Stacking Ensemble Model", An International journal of computing and informatics, Vol 48, No 14 (2024), https://doi.org/10.31449/inf.v48i14.6145

[9] Charbuty B, Abdulazeez A., "Classification based on decision tree algorithm for machine learning", Journal of Applied Science and Technology Trends. 2021 Mar 24;2(01):20-8, https://doi.org/10.38094/jastt20165

[10] *Dalila Cherifi, Abderraouf Djaber, Mohammed-Elfateh Guedouar, Amine Feghoul, Zahia Zineb Chelbi, Amazigh Ait Ouakli* ,"Covid-19 Detecting in Computed Tomography Lungs Images using Machine and transfer Learning", An International journal of computing and informatics, Vol 47, No 8 (2023), https://doi.org/10.31449/inf.v47i8.4258

[11] Rustam Z, Sudarsono E, Sarwinda D, "Random-forest (RF) and support vector machine (SVM) implementation for analysis of gene expression data in chronic kidney disease (CKD)", IOP Conference Series: Materials Science and Engineering 2019 Jun 1 (Vol. 546, No. 5, p. 052066), https://doi.org/10.1088/1757-899x/546/5/052066

[12] Subasi A, Alickovic E, Kevric J, "Diagnosis of chronic kidney disease by using random forest", In CMBEBIH 2017: Proceedings of the International Conference on Medical and Biological Engineering, 2017 (pp.589-594). Springer Singapore, https://doi.org/10.1007/978-981-10-4166-2_89

[13] Zhao J, Gu S, McDermaid A, "Predicting outcomes of chronic kidney disease from EMR data based on Random Forest Regression", Mathematical biosciences, 2019, Apr 1;310:24-30, https://doi.org/10.1016/j.mbs.2019.02.001

[14] Wainstein M, Rahimi AK, Katz I, Healy H, Pirabhahar S, Turner K, Shrapnel S, "A comparison between a Random Forest model and the Kidney Failure Risk Equation to predict progression to kidney failure", medRxiv. 2023 May 17:2023-05, https://doi.org/10.1101/2023.05.16.23290068

[15] Chaudhuri AK, Sinha D, Banerjee DK, Das A, "A novel enhanced decision tree model for detecting chronic kidney disease", Network Modeling Analysis in Health Informatics and Bioinformatics. 2021 Dec; 10:1-22, https://doi.org/10.1007/s13721-021-00302-w

[16] Ahmad M, Tundjungsari V, Widianti D, Amalia P, Rachmawati UA, "Diagnostic decision support system of chronic kidney disease using support vector machine", 2017, second international conference on informatics and computing (ICIC) 2017 Nov 1 (pp. 1-4). IEEE, https://doi.org/10.1109/iac.2017.8280576

[17] Vardhan GK, Vimala GS, "Efficient detection of kidney disease using novel support vector machine in comparison with decision tree classifier", AIP Conference Proceedings 2023 Nov 21 (Vol. 2821, No. 1). AIP Publishing, https://doi.org/10.1063/5.0166591

[18] Almustafa KM, "Prediction of chronic kidney disease using different classification algorithms", Informatics in Medicine Unlocked. 2021 Jan 1; 24:100631, https://doi.org/10.1016/j.imu.2021.100631

[19] Ali A. Abaker, Fakhreldeen A. Saeed, "A Comparative Analysis of Machine Learning Algorithms to Build a Predictive Model for Detecting Diabetes Complications", An International journal of computing and informatics , Vol 45, No 1 (2021), https://doi.org/10.31449/inf.v45i1.3111

[20] Akter S, Habib A, Islam MA, Hossen MS, Fahim WA, Sarkar PR, Ahmed M, "Comprehensive performance assessment of deep learning models in early prediction and risk identification of chronic kidney disease", IEEE Access. 2021 Nov 19; 9:165184-206, https://doi.org/10.1109/access.2021.3129491

[21] De Guia JD, Concepcion RS, Bandala AA, Dadios EP, "Performance comparison of classification algorithms for diagnosing chronic kidney disease", 2019, IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM) 2019 Nov 29 (pp. 1-7). IEEE, https://doi.org/10.1109/hnicem48295.2019.9073568

[22] Iftikhar H, Khan M, Khan Z, Khan F, Alshanbari HM, Ahmad Z, "A comparative analysis of machine learning models: a case study in predicting chronic kidney disease", Sustainability. 2023 Feb 2;15(3):2754, https://doi.org/10.3390/su15032754

[23] Oluwashola David Adeniji, Samuel Oladele Adeyemi, Sunday Adeola Ajagbe, "An Improved Bagging Ensemble in Predicting Mental Disorder using Hybridized Random Forest - Artificial Neural Network Model", An International journal of computing and informatics, vol-46, No 4(2022), https://doi.org/10.31449/inf.v46i4.3916

Research on Operation and Anomaly Detection of Smart Power Grid Based on Information Technology Using CNN+Bidirectional LSTM

Yong Zhang*, Yueda Gao, Zhe Zhao
E-mail: zhangy_y@hotmail.com
Electric Energy Measurement Branch of Inner Mongolia Power (Group) Co., Ltd., Inner Mongolia 010020, China
* Corresponding author

Keywords: smart grid, abnormal power consumption, intelligent algorithm, integrated learning

Received: August 30, 2024

The accurate detection of abnormal users in the grid is conducive to maintaining the stability of the smart grid. This paper briefly introduces the smart power grid and the intelligent algorithm used to detect users with abnormal power consumption in the power grid. The intelligent algorithm combined the bidirectional long short-term memory (LSTM) and a convolutional neural network (CNN) to extract the features from the power consumption data of the users and then used the adaptive boosting (AdaBoost) model to classify the users. The field operation test was carried out in a small substation. The proposed method was compared with the single bidirectional LSTM and CNN methods. The findings showed that the proposed method had the best performance in the simulation experiment, with a precision of 98.7%, a recall rate of 97.9%, and a false drop rate of 3.6%, and its receiver operator characteristic (ROC) curve deviated the most from the diagonal line and had the largest area enclosed. In the field operation test, the proposed method obtained a lower and more stable false detection rate (approximately 3.6%).

Povzetek: Raziskava je omogočila izdelavo CNN+Bidirectional LSTM za zaznavanje anomalij v pametnem omrežju, kar omogoča stabilno in učinkovito identifikacijo nepravilne porabe električne energije.

1 Introduction

With the rapid advancement of information technology and the optimal adjustment of energy structure, the smart grid has emerged as a crucial development direction of future power systems, gathering increasing attention [1]. Characterized by information, automation, and intelligence, the smart grid can realize real-time monitoring, intelligent scheduling, and efficient management of the power network [2]. In the operation process of the smart grid, the power transported by the power grid will produce technical and non-technical losses. The former refers to the inherent loss of all equipment in the power grid and is an unavoidable loss, while the latter is caused by abnormal power consumption, equipment failure, and network system failure [3]. Abnormal power consumption is the main cause of non-technical loss of the smart grid and will affect the stability and security of the smart grid. Therefore, rapid and accurate detection of abnormal power consumption in the smart grid is conducive to maintaining its stability [4]. Artificial intelligence has been making significant breakthroughs in various new fields, such as the perception of real-world signals. In these areas, artificial intelligence has occasionally surpassed human capabilities and will continue to do so even more in the future. Artificial intelligence can also be applied to the management of smart grids. The relevant research, as shown in Table 1, is all related to improving the performance of smart grids. Some studies focus on demand distribution calculation in smart grids, some on the interaction efficiency between users and intelligent systems in smart grids, and some on intelligent controllers in smart grids. This paper focuses on identifying abnormal electricity users in smart grids by using a convolutional neural network (CNN) to extract electricity consumption features from users and then using bidirectional long short-term memory (LSTM) for identification. By utilizing a deep learning algorithm to improve the efficiency and accuracy of identifying abnormal users in smart grids, it provides an effective reference for enhancing the stable operation of smart grids.

Table 1: Related research

Author	Research content	Research results
Deng et al. [5]	They proposed a dual decomposition-based distributed approach to improve demand response in smart grid.	The test results verified the effectiveness of the proposed algorithm.
Jo et al. [6]	They proposed a lightweight privacy-protecting metering protocol for bidirectional communication between smart grid users and power	The test results showed that the protocol can further improve the speed of message authentication.

	systems.	
Grilo et al. [7]	They developed a solution for extracting relevant data from specific locations in low-voltage power grids and efficiently transmitting the data to intelligent controllers via wireless sensor networks.	The experimental results showed the effectiveness of the proposed method.

This paper briefly introduces the smart power grid and the intelligent algorithm used to detect users with abnormal power consumption in the power grid. The intelligent algorithm integrated the bidirectional LSTM with a CNN to extract the features from the power consumption data of users and then used the adaptive boosting (AdaBoost) model to classify these users. Moreover, simulation experiments were carried out in a laboratory. A field operation test was carried out in a small substation.

2 The detection method of abnormal operation in the smart power grid

2.1 Smart grid

With the expansion of the power grid scale, traditional power management approaches have been unable to meet the needs of power grid operation. However, with the progress of information technology and the Internet, it has become easier to collect and analyze operational data of power grids [9], giving rise to smart grids. Compared with the conventional power grid, the smart grid can use the sensors installed on the equipment to automatically collect and analyze the operation data produced by the power grid, then intelligently schedule the power grid, and detect the anomalies in the power grid [10].

Figure 1 presents the basic architecture of smart grid operation monitoring. The corresponding sensing facilities are installed in power grid equipment such as power transmission lines, transformer equipment, distribution station equipment, and smart meters. The sensing facilities collect real-time operation data from the corresponding power grid equipment and then transmit the data to the smart grid control center via the Internet. The control center analyzes and processes the collected data [11].

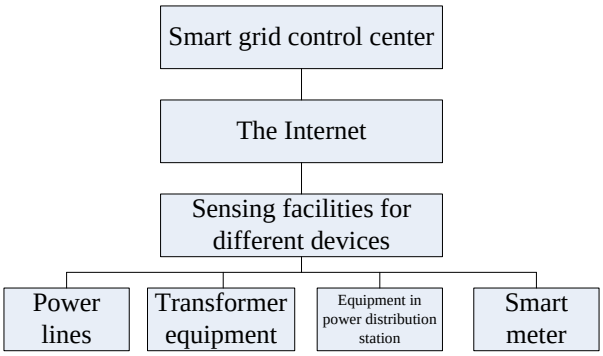


Figure 1: Basic architecture of smart grid operation monitoring.

2.2 Detection of abnormal power consumption

The smart grid will produce technical loss and non-technical loss during operation. The former is the unavoidable loss of power grid equipment during operation, while the latter is the power loss caused by other reasons, including abnormal power consumption and equipment failure, among which abnormal power consumption is the main reason [12]. The causes of abnormal power consumption include illegally stealing electricity, privately pulling wires, private change of electricity meters, and other informal means. The main goal of these informal means of electricity consumption is to pay for less electricity or for temporary convenience. Therefore, during the smart grid operation, it is necessary to detect abnormal users from the grid in time [13].

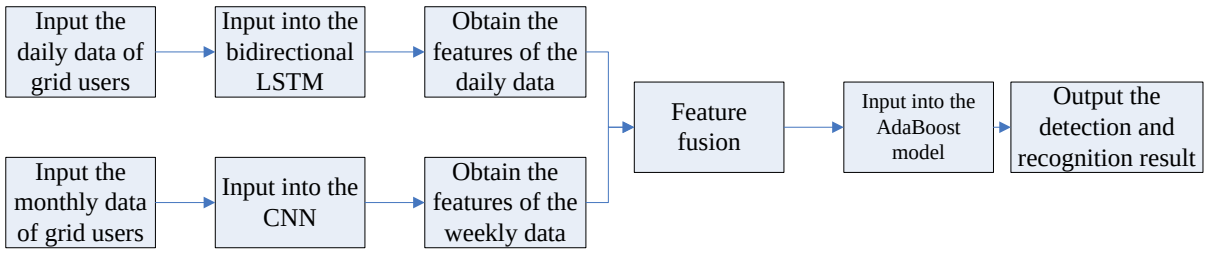


Figure 2: Abnormal power consumption detection process based on bidirectional LSTM+CNN.

The scale of the smart grid is huge; hence, the amount of data collected by sensors is very large. It is difficult to carry out statistical analysis of big data by manual alone, and it is necessary to use computers to assist in processing [14]. This paper employs a deep learning algorithm to detect users with abnormal power consumption in the smart grid. The power consumption data generated by users in the process of using a smart grid has different time scales, such as daily data, weekly data, and monthly data. The data at different time scales have different hidden

characteristics. Although the data at a single time scale can also reflect the users with abnormal power consumption, it is not comprehensive enough. Therefore, this paper uses different deep learning algorithms to extract the features from the electricity consumption data at different time scales, and then fuses the features for the detection and identification of abnormal users. As shown in Figure 2, this paper selects the bidirectional LSTM to extract the daily data features from power grid users and the CNN to extract the monthly data features. After the fusion, the AdaBoost model [15] is employed to detect and identify abnormal users among power grid users. The specific process is described as follows.

① The daily data of power grid users collected by the device sensor is input into the bidirectional LSTM. The computational formula of the one-directional LSTM is:

$$\begin{cases} f_t = f(W_f \cdot [h_{t-1}, x_t] + \theta_f) \\ i_t = f(W_i [h_{t-1}, x_t] + \theta_i) \\ \widetilde{C}_t = \tanh(W_C [h_{t-1}, x_t] + \theta_C) \\ C_t = f_t \cdot C_{t-1} + i \cdot \widetilde{C}_t \\ o_t = f(W_o [h_{t-1}, x_t] + \theta_o) \\ h_t = o_t \cdot \tanh(C_t) \end{cases}, \quad (1)$$

where $\widetilde{C}_t$ and C_t are the temporary state and updated state of the current memory unit, h_t is the hidden data state input at the current time, x_t is the current input, f_t, i_t, and o_t are the output of three gated units, forget, input, and output, at the current time, W_f, W_i, and W_o are the weight in corresponding gated units, and θ_f, θ_i, and θ_o are the bias in corresponding gated units.
The formula of the bidirectional LSTM is:

$$\begin{cases} h_i^+ = \overrightarrow{LSTM}(W_1^+ x_i, W_2^+ h_{i-1}^+) \\ h_i^- = \overleftarrow{LSTM}(W^- x_i, W_2^- h_{i+1}^-) \\ h_i = h_i^+ \oplus h_i^- \end{cases}, \quad (2)$$

where $\overrightarrow{LSTM}()$ is the calculation function of the hidden layer of the forward LSTM, i.e., the application of equation (1), $\overleftarrow{LSTM}()$ is the calculation function of the hidden layer of the backward LSTM, which is the application of equation (1) (its only difference is reversely inputting x_t), h_i^+, h_i^-, h_i are the current forward LSTM hidden layer output, the current backward LSTM hidden layer output, and the current final output, x_i is the current input, $W_1^+, W_2^+, W_1^-, W_2^-$ are weights of the forward and backward LSTM calculations [16].

② The weekly data of power grid users collected by the device sensor is input into a CNN in the form of two-dimensional arrangement for convolutional feature extraction. The convolutional formula of the CNN is:

$$x_j^l = f\left(\sum_{j \in M} x_i^{l-1} \cdot W_{ij}^l + b_j^l \right), \quad (3)$$

where x_j^l is the feature map of the convolver output, x_i^{l-1} is the feature output of the i-th convolutional kernel in the last convolutional layer after pooling, W_{ij}^l is the weight parameter between the i-th convolutional kernel and the j-th convolutional kernel, b_j^l is the bias of j convolutional kernels of l layers, M is the number of convolutional kernels, and $f(\bullet)$ is an activation function.

③ In the first two steps, the bidirectional LSTM finally outputs hidden state h_i, and the CNN finally outputs the convolution feature. They are processed into features of the same dimension, and then the two features are fused.

④ The fused features are input into the AdaBoost model for recognition and detection. When training the AdaBoost model, the weight of the samples with classification errors is increased, and then the new weak classifier is trained by random sampling according to the weights. The above steps of "sampling according to weights - training weak classifiers - increasing the weight of samples with classification error" are repeated, and multiple weak classifiers are obtained. The weight of weak classifiers and the updated formula of the weight of training samples are:

$$\begin{cases} \alpha_m = \dfrac{1}{2} \log \dfrac{1 - e_m}{e_m} \\ w_{m+1,i} = \dfrac{w_{m,i} \exp(-\alpha_m y_i G_m(x_i))}{Z_m} \\ Z_m = \sum_{i=1}^{N} w_{m,i} \exp(-\alpha_m y_i G_m(x_i)) \end{cases}, \quad (4)$$

where α_m is the weight of the m-th classifier, e_m is the classification error of the m-th classifier, $w_{m,i}$ is the weight of sample i when training the m-th classifier, y_i is the result label of sample i, $G_m(x_i)$ is the computation function of the m-th classifier, x_i is the input of sample i, and Z_m is the normalization factor.

3 Simulation experiment

3.1 Experimental environment

The simulation experiment was carried out in laboratory servers, which were configured as Windows 11 operating system, Core i7 processor, and 32G memory.

3.2 Experimental data

The dataset used was from the open dataset provided by the State Grid Corporation of China (http://www.sgcc.com.cn/). The dataset selected in this

paper covered the period from May 1, 2015, to June 1, 2018. The dataset contained 35,689 users, of whom 93.5% were normal users. Abnormal users accounted for 6.5%. The public dataset from the State Grid Corporation of China was collected from real grid users, so the proportion of normal and abnormal users was realistic, with only a small number of abnormal users. The dataset with the unbalanced proportion of normal and abnormal users was not suitable for training intelligent algorithms, and it was easy to cause the intelligent algorithms to be biased. Therefore, this paper used SMOTE to balance the sample number, and after that, the ratio of normal users to abnormal users was 1:1. The basic process of the SMOTE algorithm is as follows: ① The Euclidean distance between each sample in the default bond set and other samples in that set was calculated, and a neighbor sample set was obtained for each sample based on the Euclidean distance. ② For each sample, several samples were randomly selected from the neighbor sample set. ③ New samples were generated according to the following formula:

$$x_{new} = x + rand(0,1) \cdot (x - x_m), \quad (5)$$

where x refers to the original sample in the default bond set, x_m is the random sample in the neighbor sample set of x, $rand(0,1)$ is a random number between 0 and 1, and x_{new} is the newly generated sample.

3.3 Experimental setup

The relevant parameters of the abnormal electricity detection and recognition algorithm proposed in this paper are shown in Table 2. Moreover, in order to verify the effectiveness of the proposed algorithm, it was compared with a single bidirectional LSTM and a single CNN. The relevant parameters of the two algorithms were consistent with those of the corresponding part of the proposed algorithm.

Table 2: Relevant parameters of the proposed algorithm.

	Structure	Parameter	Structure	Parameter
Bidirectional LSTM	Input layer	An input with 1,125 dimensions	Forward hidden layer	One layer, 256 nodes, the sigmoid activation function
	Backward hidden layer	One layer, 256 nodes, the sigmoid activation function	Output layer	An output with 256 dimensions
CNN	Input layer	An input with 7 × 161 dimensions	Convolution layer 1	Eight 3 × 1 convolution kernels, a step length of 2
	Pooling layer 1	A pooling box with a specification of 3×1, a step length of 2	Convolution layer 2	Sixteen 3 × 1 convolution kernels, a step length of 1
	Pooling layer 2	A pooling box with a specification of 3×1, a step length of 1	Output layer	An output with 256 dimensions
AdaBoost	Weak classification learner	Linear predictor	Number of classifiers	50
	Error threshold	0.1		

In addition to training and testing the algorithm using the open dataset, this study also conducted a one-month field test in a local small-scale substation and compared the predicted results of the algorithm with the measured results of the substation. The above two single algorithms for comparison were also tested for a one-month field test.

3.4 Evaluation indicator

This paper used the precision, recall rate, false detection rate, and receiver operator characteristic (ROC) curve as the evaluation indicators of the detection performance of the algorithm. The formula of precision, recall rate, and false drop rate is:

$$\begin{cases} P = \dfrac{TP}{TP + FN} \\ R = \dfrac{TP}{TP + FP} \\ W = \dfrac{FP + FN}{TP + FP + TN + FN} \end{cases}, \quad (6)$$

where P refers to precision, R refers to the recall rate, and W is the false drop rate.

The formula for calculating the true and false positive case rates of the ROC curve is:

$$\begin{cases} TPR = \dfrac{TP}{TP + FN} \\ FPR = \dfrac{FP}{TN + FP} \end{cases}, \quad (7)$$

where TPR is the true positive rate and FPR is the false positive rate.

3.5 Test results

Figure 3 shows the performance of the three abnormal power user detection algorithms. It can be seen that there was little difference in precision, recall rate, and false detection rate between a single bidirectional LSTM and a single CNN. The AdaBoost recognition algorithm based on bidirectional LSTM+CNN had significantly better detection and recognition performance than the other two algorithms.

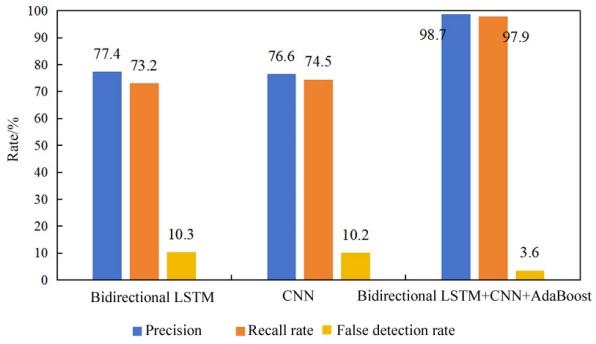


Figure 3: Performance of three abnormal user detection algorithms.

In addition to the above three evaluation indicators, the ROC curve was also used to evaluate the detection algorithm, and the final result is shown in Figure 4. The ROC curve reflects the positive and false detection rates of a prediction model under different recognition thresholds. When the prediction model cannot make predictions and can only give random results, its ROC curve is a diagonal line. When the prediction model is ideal, its ROC curve is a broken line coincident with axes $x=0$ and $y=1$. In other words, for a prediction model, the closer its ROC curve is to the diagonal line, the worse its prediction performance will be; the closer it is to the broken line, the better its prediction performance will be. It can be seen that the performance of a single bidirectional LSTM was close to that of a single CNN, while the bidirectional LSTM+CNN+AdaBoost detection algorithm had better prediction performance.

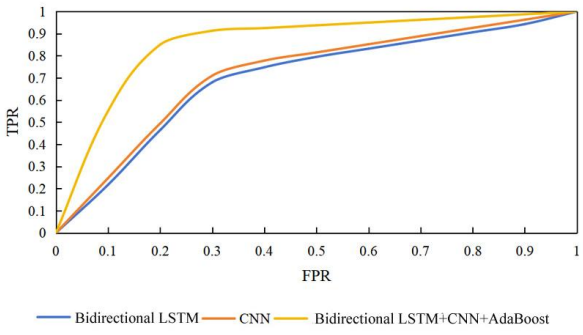


Figure 4: The ROC curves of three detection algorithms.

Finally, the three detection algorithms were deployed in a small substation for one month, and the changes in the false detection rates of the three detection algorithms during the field operation period are shown in Figure 5. With the passage of field operation time, the false detection rates of a single bidirectional LSTM and a single CNN gradually increased, and the CNN increased more. The proposed method had a stable false detection rate, which was lower than that of the other two detection algorithms.

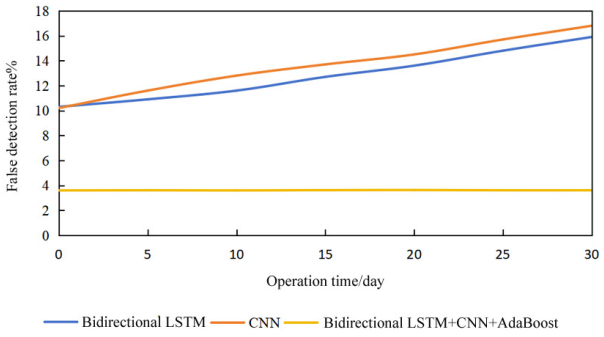


Figure 5: False detection rates of three detection algorithms in the one-month substation field operation.

4 Discussion

With the rapid development of technology, the smart grid, as an important component of modern power systems, is increasingly being emphasized for its stability and security. By integrating computation, communication, and physical environment, smart grids enable efficient management and monitoring of power networks. However, the complexity of smart grids also brings many challenges, especially in anomaly detection. Traditional detection methods often suffer from low accuracy and slow response, making it difficult to meet the requirements of modern power systems. The emergence of deep learning algorithms with data mining capabilities provides a new approach for processing and analyzing operational data in smart grids. As a deep learning model, the CNN has shown excellent performance in areas such as image processing and video analysis. In smart grids, the CNN can be applied to feature extraction and classification of power data. Key features can be extracted from massive amounts of power data through training the CNN model. The convolutional layer structure of the CNN possesses the ability to extract local features, enabling it to capture subtle variations in power data and improve the recognition capability for abnormal power data. The LSTM is a special type of recurrent neural network that can handle long sequence data, while the bidirectional LSTM further considers reverse sequences based on the LSTM. In the smart grid, a bidirectional LSTM can be used for processing and analyzing time series data. By capturing the temporal dependencies in power data, the bidirectional LSTM enables the detection of abnormal user behavior in the grid.

This paper combined a CNN and a bidirectional LSTM to analyze electricity consumption data from users in the smart grid and detect users with abnormal electricity usage.

Afterward, simulation experiments were conducted in the laboratory using power grid data collected from the State Grid Corporation of China. Subsequently, a one-month actual test was carried out in a local small-scale substation. This paper demonstrated that combining a CNN and a bidirectional LSTM yielded higher performance in identifying abnormal power grid users than using only a bidirectional LSTM or a CNN alone. During the actual operation process of the small-scale substation, our algorithm maintains lower and more stable false detection rates. The reason is that the CNN can extract local features of power data, while bidirectional LSTM can extract time series features of power data. Compared with a single bidirectional LSTM or a single CNN, it can obtain more comprehensive power data features. In addition, the AdaBoost model combines multiple weak classifiers into a strong classifier to further improve the recognition performance of the algorithm.

5 Conclusions

This paper briefly introduces the smart grid and the intelligent algorithm used to detect users with abnormal power consumption. This algorithm combined the bidirectional LSTM with the CNN to extract the features from the power consumption data of the users. Then, the AdaBoost model was employed to classify the users. A field operation test was carried out in a small substation. The proposed method was compared with a single bidirectional LSTM and a CNN. The precision, recall rate, and false detection rate were not much different between the single bidirectional LSTM and single CNN, and the performance of the proposed was obviously better than the other two algorithms. The ROC curves showed that the performance of the single bidirectional LSTM was close to that of the single CNN, while the predictive performance of the proposed detection algorithm was better. In the field operation, the false detection rate of the single bidirectional LSTM and single CNN gradually increased, and the CNN increased more; the proposed method had a more stable and smaller detection rate than the other two algorithms.

References

[1] Khan A R, Mahmood A, Safdar A, Khan ZA, Khan NA (2016). Load forecasting, dynamic pricing and DSM in smart grid: A review. *Renewable & Sustainable Energy Reviews*, 54(FEB.), pp. 1311-1322. https://doi.org/10.1016/j.rser.2015.10.117

[2] Collier SE (2017). The Emerging Enernet: Convergence of the Smart Grid with the Internet of Things. *IEEE Industry Applications Magazine*, 23(2), pp. 12-16. https://doi.org/10.1109/MIAS.2016.2600737

[3] Shan X, Dai Z, Zhang Z, Zhang Y, Bi X, Ge C (2015). Research on and Application of Integrated Smart Alarm Based on Smart Grid Dispatching and Control Systems. *Dianli Xitong Zidonghua/Automation of Electric Power Systems*, 39(1), pp. 65-72. https://doi.org/10.7500/AEPS20140930016

[4] Wang X, Liang Q, Mu J, Wang W, Zhang B (2015). Physical layer security in wireless smart grid. *Security & Communication Networks*, 8(14), pp. 2431-2439. https://doi.org/10.1002/sec.751

[5] Gams M, Kolenik T (2021). Relations between Electronics, Artificial Intelligence and Information Society through Information Society Rules. *Electronics*, 10(4), pp. 1-16. https://doi.org/10.3390/electronics10040514

[6] Deng R, Lu R, Xiao G, Chen J (2015). Fast Distributed Demand Response With Spatially and Temporally Coupled Constraints in Smart Grid. *IEEE Transactions on Industrial Informatics*, 11(6), pp. 1597-1606. https://doi.org/10.1109/TII.2015.2408455

[7] Jo H J, Kim I S, Lee D H (2016). Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems. *IEEE Transactions on Smart Grid*, 7(3), pp. 1732-1742. https://doi.org/10.1109/TSG.2015.2449278

[8] Grilo A, Casaca A, Nunes M, Bernardo A, Rodrigues P, Almeida JP (2017). A management system for low voltage grids. *2017 IEEE Manchester PowerTech*, IEEE, Manchester, UK. https://doi.org/10.1109/PTC.2017.7980826

[9] Gholian A, Mohsenian-Rad H, Hua Y (2016). Optimal Industrial Load Control in Smart Grid. *IEEE Transactions on Smart Grid*, 7(5), pp. 2305-2316. https://doi.org/10.1109/TSG.2015.2468577

[10] Li Q, Zhu Y, Ding J, Li W, Sun W, Ding L. (2024). Deep Reinforcement Learning Based Resource Allocation for Fault Detection with Cloud Edge Collaboration in Smart Grid. *CSEE Journal of Power and Energy Systems*, 10(3), pp. 1220-1230. https://doi.org/10.17775/CSEEJPES.2021.02390

[11] Good N, Ellis K A, Mancarella P (2017). Review and classification of barriers and enablers of demand response in the smart grid. *Renewable & Sustainable Energy Reviews*, 72, pp. 57-72. https://doi.org/10.1016/j.rser.2017.01.043

[12] Chen K L, Chen Y R, Tsai Y P, Chen N (2017). A Novel Wireless Multifunctional Electronic Current Transformer Based on ZigBee-Based Communication. *IEEE Transactions on Smart Grid*, 8(4), pp. 1888-1897. https://doi.org/10.1109/TSG.2015.2510325

[13] Luo X (2017). Design and Implementation of Wireless Voltage Monitoring System Based on Zigbee. *Chinese Journal of Electron Devices*, 12(3), pp. 83-96. https://doi.org/10.4018/IJITWE.2017070108

[14] Sharma J, Bhattacharya PP, Jha MK (2016). Performance Analysis of IEEE 802.15.4 in Different NLOS Environments of Smart Grids. *International Journal of Sensors Wireless Communications & Control*, 2016, 6(3):216-220. https://doi.org/10.2174/2210327906666160928121906

[15] Gao Y, Zhang J, Chen Z, Chen X (2024). Anomaly Detection Algorithm of Power System Based on Graph Structure and Anomaly Attention. *Computers, Materials & Continua*, 79(4), pp. 493-507. https://doi.org/10.32604/cmc.2024.048615

[16] Syu J H, Srivastava G, Fojcik M, Cupek R, Lin JCW (2023). Energy grid management system with anomaly detection and Q-learning decision modules. *Computers and Electrical Engineering*, 2023, 107, pp. 108639-1-108639-11. https://doi.org/10.1016/j.compeleceng.2023.108639

Enhancing Searchable Symmetric Encryption Performance through Optimal Locality

Aya A. Alyousif[1*], Ali A. Yassin[2], Hussein M. Mohammed[3]
[1] Department of Medical Instrumentation Engineering Techniques, Shatt Al-Arab University College, Basra, Iraq
[2] Department of Computer Science, Education College for Pure Sciences, University of Basrah, Basrah, Iraq
[3] Directorate General of Education Basrah, Ministry of Education, Basrah, Iraq
Email: ayah.abdulhussain@sa-uc.edu.iq[1], ali.yassin@uobasrah.edu.iq[2] , hussain.mazin@sa-uc.edu.iq[3]
[*]Corrsponding author

Keywords: information retrieval, searchable symmetric encryption, inverted index, locality, cloud server

Received: March 17, 2024

Both individuals and institutions place great importance on maintaining the security and privacy of their data, when stored in the cloud server. To achieve this, they often turn to searchable symmetric encryption (SSE), which is considered a crucial technology for safeguarding user data. However, SSE has encountered some challenges, particularly in the case of large databases. One such issue is poor performance, which can be attributed to poor locality. This means that the cloud server must visit a large number of locations during the search process, resulting in slow retrieval times. The main problem however, is not just poor locality. In many cases, optimization methods intended to improve performance can actually lead to increased storage requirements for the encrypted index stored on the cloud server or reduced efficiency when reading data. These issues must be addressed in order for SSE to continue to be an effective tool for protecting sensitive information. In this paper, we introduce a secure and searchable scheme that effectively addresses the issues mentioned above, while also enhancing the performance of information retrieval through an improved encrypted inverted index storage mechanism. Our scheme achieves optimal locality at $O(1)$, and read efficiency at $O(1)$, thereby significantly increasing the speed of retrieval. Through experimentation with real-world data, we have demonstrated the practicality, accuracy, and security of our approach, making it a reliable solution for secure and efficient information retrieval.

Povzetek: Predlagana je optimizirana metoda za izboljšanje učinkovitosti iskanja v šifriranih podatkih z uporabo izboljšanega obrnjenega indeksa, ki dosega optimalno lokalnost in povečuje hitrost ter varnost pridobivanja informacij.

1 Introduction

In the modern age, the need for data storage has greatly increased. With technology advancing rapidly, we are generating data faster than ever, and businesses, individuals, and organizations all need efficient ways to store, manage, and access this data. Consequently, cloud storage has become a popular choice, offering many benefits over traditional data storage methods[1][2].

Cloud storage refers to storing data on remote servers accessible via the internet from any connected device. This method allows data to be centrally stored and easily accessed from anywhere with an internet connection. Cloud storage is flexible, letting users adjust their storage needs up or down as required, without the limitations of physical storage devices. It is ideal for businesses and individuals needing to store large amounts of data securely. Cloud storage providers ensure high reliability by using redundant storage systems and multiple data centers in different locations, making data always accessible, even during hardware failures or natural disasters. This reliability is crucial for businesses relying on data for critical operations, ensuring their data is secure and available when needed.

Despite the numerical advantages of cloud storage, it is not without challenges, and security is the biggest challenge for cloud storage [3]. To ensure the security of data stored on cloud servers, various methods need to be employed, including access control, network security, and encryption [4]. Access control is a mechanism that restricts access to data based on user identity, role, or authorization. Network security involves securing the network infrastructure used for data transmission. Encryption, on the other hand, is the process of transforming data into code to prevent unauthorized access. Encryption can be applied both in transit and at rest, thus ensuring that data remains secure during transmission and storage.

To secure data stored in the cloud, various encryption techniques are used to prevent unauthorized access. Symmetric encryption is widely used and involves a single key for both encrypting and decrypting data. In contrast, asymmetric encryption uses different keys for encryption and decryption, offering more security but at a slower speed. Hashing is another method, commonly used for

securing passwords, which converts data into a fixed-size string that cannot be reversed. A newer technique, Searchable Symmetric Encryption (SSE) [5], allows users to search encrypted data without exposing it. SSE comes in two types: deterministic, which offers consistent results but less security, and probabilistic, which provides better security but less predictability.

Table 1: List of symbols

Character	Description
W	Word
nw	Number of W
M	Words in DB, $M = \{W_1, \ldots, W_{nw}\}$
id	Identifier
Ndb	Total of identifiers DB
n	Total of identifiers W
N	$\sum_{i=1}^{nw} \lvert db(W) \rvert$ where $db(W) = \{id_1, .., id_n\}$
c	Counter
H_T	A hash table is a data structure that allows efficient storage and retrieval of key-value pairs. It comprises a pair of algorithms, are "Add" and "Get"[11].
Add	Algorithm adds pairs of $(key, value)$ to H_T
Get	value=Get(key)
S_t	String
$\check{S}_t$	Encrypted string
sk_e	Derivative key used for encryption and decryption of S_t
La	Label is used to store and retrieve $\check{S}t$ in HT, $Add(La, \check{S}_t)$, $\check{S}_t = Get(La)$
Enc	Function to encryption S_t
Dec	Function to decryption $\check{S}_t$
L_{id}	List to store identifiers

These encryption methods are crucial for protecting cloud data and must be carefully implemented to prevent data breaches or attacks.

Searchable symmetric encryption (SSE) presents several challenges[6]. The process, which involves searching encrypted data, requires creating and maintaining an index for each keyword, making it complex. Moreover, there are security risks, such as the possible leakage of sensitive data. A recent challenge in SSE is a significant drop in performance and retrieval efficiency when dealing with large databases [7]. Researchers have found that this issue is not due to flaws in the encryption itself but is related to how the secure index is stored in memory. During a search, the index may cause the cloud server to perform many continuous memory transitions, known as "poor locality," " [[7], [8], [9], [10], [11]] which can slow down the retrieval process and degrade SSE performance. While some researchers are working to improve locality to boost performance, this can lead to increased storage requirements for the encrypted index on the cloud server or reduce the

efficiency of data reading. The contributions of our approach can be summarized as follows:

Firstly, our scheme significantly improves the performance of information retrieval for all databases, regardless of their size, by enhancing locality. Secondly, our scheme achieves an optimal locality of $O(1)$, meaning that the cloud server only needs to access one memory location during each search operation, as opposed to many locations. Thirdly, our proposed scheme is highly secure, as the server searches for the required data and sends it to the data owner without decrypting it, thereby enhancing resistance to various attacks that symmetric searchable encryption is vulnerable to. Fourthly, our scheme has better reading efficiency $O(1)$, as the cloud server only responds with the requested data when the user queries it. Finally, our scheme has no significant negative impact on the storage of the encrypted index in the cloud server.

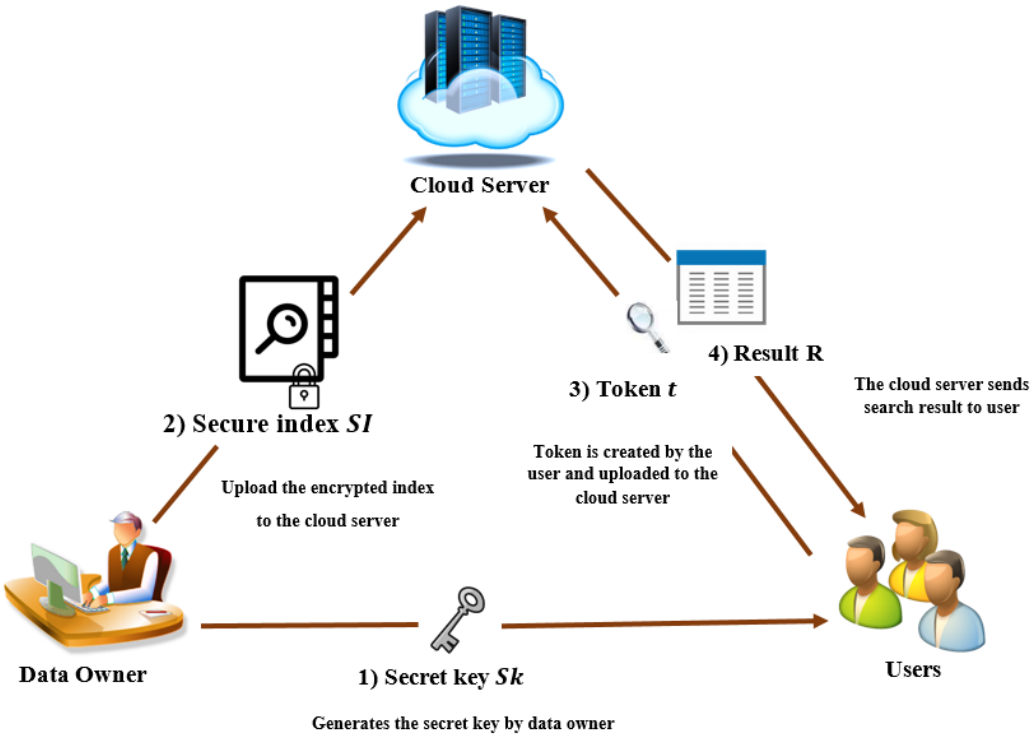


Figure 1: Searchable symmetric encryption

Table 2: Searchable symmetric encryption algorithm

Algorithm	Description
Key generation phase: $sk \leftarrow Gen_{sk}(1^{\lambda})$	The key generation algorithm takes the security parameter1^{λ} as input and generates the secret key as its output.
Constructing secure index: $SI \leftarrow Enc\_DB(sk, DB)$	The secure index SI is created in this algorithm by taking the secret key sk and the database DB as input.
Token generator: $t \leftarrow Trpdr\_W(sk, W)$	The token t in this algorithm is created by the user to search for a specific word W or data.
Search: $R \leftarrow Search\_t(t, SI)$	In this algorithm, the cloud server searches for the required word in SI and returns the result R to the user. If the result is encrypted, the user will need to use $Find\_ids$ algorithm.
Find identifiers: $IDS \leftarrow Find\_ids(sk, R)$	The user employs this algorithm to retrieve the final outcome, which comprises word identifiers IDS after carrying out any essential processing and decrypting R

2 Searchable symmetric encryption (SSE)

SSE is a technology designed to enable searching over encrypted data while maintaining its confidentiality [[12], [13], [14]]. It involves three key components: the data owner DW, the cloud server CS, and the users. The process of SSE consists of several steps. Initially, the data owner selects a secret key for encryption and decryption. Next, they construct a secure index based on the words in their database. This index is then encrypted with the secret key chosen earlier. When a user wishes to search for data, they generate an encrypted search query known as a token. This token is encrypted using the same secret key that was used to encrypt the index and is sent to the cloud server. Upon receiving the token, the cloud server uses the encrypted index to search for the requested data[15]. The cloud server either decrypts the data and sends it to the user or sends it encrypted so that the user can decrypt it later. The Table 2. summarizes the steps involved in Searchable Symmetric Encryption algorithms:

Table 3: Comparison with previous schemes based on storage, locality, and read efficiency

Related works	Storage	Locality	Read efficiency
Curtmola et al. [14]	$O(N)$	$O(n)$	$O(1)$
Kamara et al. [21]	$O(N)$	$O(n)$	$O(1)$
David cash et al. [17]	$O(N)$	$O(n)$	$O(1)$
Chase and Kamara [18]	$O((\text{Max}\lvert db(W)\rvert)Ndb)$	$O(1)$	$O(1)$
P. van Liesdonk et al.[19]	$O(nw\ Ndb)$	$O(n)$	$O(1)$
Kamara and Papamanthou [22]	$O(nw\ Ndb)$	$O(n\ log\ Ndb)$	$O(Ndb\ logNdb)$
David cash et al. [8]	$O(N\ log\ N)$	$O(log\ N)$	$O(1)$
Asharov et al. (Scheme 3) [9]	$O(N\ log\ N)$	$O(1)$	$O(1)$
Demertzis and Papamanthou [10]	$O\ (N\ s)$	$O(L_d)$ Where L_d is a tunable locality	$O(\frac{N^{\frac{1}{s}}}{L})$
Asharov et al. (Pad-and-split scheme) [11]	$O(N\ log\ N/\ log\ L)$	$O(L_d)$ Where L_d depends on the scheme in which it is implemented within its framework	$O(1)$
Alyousif et al.[23]	$N = \sum_{i=1}^{nw}(\sum_{j=1}^{nq} St)$	$O(nq)$	$O(1)$

	where nq is number of QR codes for the word and St is a string		
Our work	$O(N)$	$O(1)$	$O(1)$

3 Related works

In the year 2000, a novel technology emerged that facilitated the searching of encrypted data without the need for decryption [16]. The system was dubbed Searchable Symmetric Encryption and provided users with the ability to search for specific keywords within encrypted data while maintaining content security. SSE's inception marked a significant milestone in the field of data security and privacy. Following the introduction of this new technology, extensive research was conducted in various areas, including performance optimization. Studies have shown that the reduction in performance is not due to the technology itself, but rather to the memory positions that the server accesses while processing user requests. As the encrypted index size grows, the number of positions accessed also increases, resulting in a slower response time [17]. This case is called poor locality. Known constructions can be classified into two approaches. The first approach has linear space and constant read efficiency, but its poor locality is highlighted in references [14] and [17]. This scheme involves allocating an array of size N and uniformly mapping N elements from the DB into it. To retrieve a list of identifiers that contain a specific W, the approach stores each identifier in the array alongside a pointer to the next identifier in the list. Unfortunately, this approach requires the cloud server to access random positions in the array, with the number of identifiers associated with the word,

which results in inefficiency due to the need to move to a large number of different positions. The second approach has excellent read efficiency and locality, but it comes at the cost of a significant amount of extra space [[18], [19], [20], [21]]. The basic idea behind this approach is to allocate a sufficiently large array A and then map each list of W identifiers uniformly into a contiguous interval in A, based on the length of the W identifiers. There should be no overlaps among different lists. To retrieve a list for a given W efficiently, the cloud server only needs to access one random position and read all consecutive identifier entries, which leads to optimal read efficiency and locality.

However, the positions of the lists in the array reveal information about the structure of the underlying DB. To hide this information, padding must be applied, resulting in a polynomial increase in space usage. We have to highlight that there is often a problem with storage capacity, which is often large due to locality optimization, or bad locality itself which can have a detrimental effect on cloud server response time. And sometimes there is a negative impact on the efficiency of reading the data as well. It is difficult, if not impossible, to construct a construction that is ideally locality with limited storage space without compromising its data read efficiency. This issue was discussed by Cash and Tessaro in 2014[8], where they also determined the minimum tradeoff required between these three criteria. Also, Cash and Tessaro developed a new construction that enhances locality to $O(log\ N)$ with storage capacity $O(N\ log\ N)$. In 2016, Gilad Asharov et al. improved construction locality for Cash and Tessaro locality, achieving locality of $O(1)$ [9] while maintaining the same storage capacity. Demertzis and Papamanthou [10] developed two constructions in 2017. The first construction offered optimal locality and required $O(N\,S)$ space, where S represents the number of levels employed to store data. However, this construction resulted in a slight reduction in read efficiency, and the storage space needed was still significant. The second construction, which operated within the same storage space as the first, allowed for tunable locality, enabling the DW to select a parameter through which to create their index. In 2021, Asharov et al. achieved remarkable progress by introducing two frameworks [11]: pad-and-split and statistical-independence.

The last work that we will talk about is one of our previous works [23] that aims to improve locality using QR code technology. The work achieved good results compared to previous works, but the locality was not ideal O(1) rather, it depends on the number of QR codes for the word. The following table summarizes the most important previous works in terms of the three main important characteristics: locality, storage efficiency, and reading efficiency.

4 Proposed scheme

In this section, we will explain our scheme in detail. First, the data owner generates a secret key, sk, using a

CONSTRUCTION.
Let $= \{db(W_1),\ldots,db(W_{nw})\}$,
; For $W \in M$ let $db(W) = M = \{W_1,\ldots,W_{nw}\}$
$\{id_1,..,id_n\}$ and Ndb is total of identifiers DB
:$sk \leftarrow Gen_{sk}(1^{\lambda})$
Compute sk with PRF
:$H\_T \leftarrow Enc\_DB(sk, DB)$
1. Initialize empty H_T
2. For every $W \epsilon M$
Sort $db(W)$
$S_t =$ " ", i=1
For from i *to* Ndb
If i mod 2 is not equal 0
If i and $i+1$ in $db(W)$
Add "A" to S_t
Else if i and $i+1$ not in $db(W)$
Add "D" to S_t
Else if i in $db(W)$ and
$i+1$ not in $db(W)$
Add "B" to S_t
Else if i not in $db(W)$ and
$i+1$ in $db(W)$
Add "C" to S_t
$sk_e = PRF_{sk}(2 \| w)$
$\check{S}_t = Enc_{sk_e}(S_t)$ by AES256
Compute $La = PRF_{sk}(1 \| W)$
Add $(La, \check{S}_t)$ to H_T

Pseudo-Random Function (PRF). A PRF is a deterministic algorithm that produces outputs that seem random, despite being generated from a specific input. PRFs are commonly used in cryptography to improve security, as their output is difficult to distinguish from true randomness, even against powerful adversaries[[24], [25],[26]]. The secret key, sk, will be used for both encryption and decryption. Below, we present the complete construction of our scheme.

The next step involves the data owner DW creating a secure index SI for the database DB. In our approach, SI is equivalent to H_T,, which is based on the words M in the database and their corresponding identifiers $db(W) = \{id_1,..,id_n\}$. The DW then arranges the identifiers $db(W)$ for each word W in the group M in ascending order and prepares an empty string $S_t =$ "" for the next step.

Next, we examine all identifiers in odd positions within the database. For each of these odd-positioned identifiers, we check the state of the corresponding word as well as the adjacent even-positioned identifier, recording the results in S_t. There are four possible scenarios, labeled A, B, C, and D, depending on whether the word appears in the odd or even positions.

1. Case A: If the word appears in the identifiers that is located in the odd and even positions together.

:$t \leftarrow Trpdr\_W(sk, W)$
1. Input sk and W
2. Compute $t = PRF_{sk}(1 \| W) = La$
$\check{S}_t \leftarrow Search\_t(t, H\_T)$:
$\check{S}_t = Get\ (La)$
:$L_{id} \leftarrow Find\_ids(sk, \check{S}_t)$
1. $sk_e = PRF_{sk}(2 \| W)$
2. $S_t = Dec_{sk_e}(\check{S}_t)$
3. Initialize L_{id}=[] list and $i = 1$
c=0
For from $i = 1$ to $Ndb/2$
if $S_t[i]$ equal "A"
c=c+1, add c to L_{id}
c=c+1, add c to L_{id}
Else if $S_t[i]$ equal "D"
c=c+2
Else if $S_t[i]$ equal "B"
c=c+1, add c to L_{id}
c=c+1
Else if $S_t[i]$ equal "C"
c=c+1
c=c+1, add c to L_{id}

2. Case D: The opposite of Case A is when the word does not appear in either identifier located in the odd and even positions.
3. Case B: If the word appears in the identifier located in an odd position but not in the identifier located in an even position.
4. Case C: Conversely, the opposite of Case B is when the word does not appear in the identifier located in an odd position but appears in the identifier located in an even position.

Once we have constructed S_t that indicates the presence or absence of the word in its identifiers, we will generate two keys. The first key $sk_e = PRF_{sk}(2 \| w)$ will be used to encrypt S_t, $\check{S}_t = Enc_{sk_e}(S_t)$, ensuring that it remains secure and confidential. The second key $La = PRF_{sk_e}(1 \| W)$ will serve as a label to identify $\check{S}_t$ when it is stored in the hash table.

After encrypting S_t with the first key, we store the encrypted result, $\check{S}_t$, in a hash table using La as a label. We then add $(La, \check{S}_t)$ to H_T, which allows us to easily retrieve $\check{S}_t$ when needed while keeping it secure from unauthorized access or tampering. Once H_T is constructed, the data owner DW can upload it to the cloud server CS. When a user wants to search for a word W, they generate a token t using the second key La, which was created during the index construction, and send it to CS. This step is essential for enabling secure data searches on CS. When CS receives t from the user, it uses t to retrieve $\check{S}_t$ from H_T and then sends $\check{S}_t$ to the user.

After the user receives $\check{S}_t$, he begins to decrypt it after recalculating the first key $sk_e = PRF_{sk}(2 \| w)$,

$S_t = Dec_{sk_e}(\check{S}_t)$. The next step is to set up a counter c and a list L_{id} to keep track of the end result. Subsequently, every letter in S_t is examined to ascertain if the word exists in the identifiers, and the identifiers are determined based on these cases.

5 Security analysis

In this part, we discussed the resistance of our scheme, the most famous types of attacks on SSE.

- **Frequency analysis attack**

A frequency analysis attack is a well-known ciphertext attack. It is based on examining the frequency of individual letters or groups of letters in a ciphertext. [6]. Therefore, it exploits the frequency of encrypted data uploaded to SI, which is either term frequency TF or term frequency-inverse TF_IDF. TF is defined as the number of times a word W appears in a document id, and $TF - IDF$ is the product of the term frequency (TF) and the inverse document frequency (IDF). IDF is calculated by dividing the total number of documents Ndb by the number of documents that contain the word n.

If the cloud server CS can access this critical information, it can execute this attack and identify the keyword being searched for.

Based on the above, we can conclude that our work is secure against this type of attack because the values stored in the cloud server CS are encrypted and do not directly reveal the original identifiers. Instead, they are transformed into an obscure text that enables the user to access the identifiers later.

- **IKK attack**

The IKK attack utilizes disclosed partial information to determine the plaintext words associated with the user search trapdoors. Consequently, this attack primarily depends on the leakage of access pattern information, which is defined as the outcome of the cloud server's CS search for t in SI, For instance, let's consider our database focuses on computer science, and a user submits three queries as trapdoors:t1, t2, and t3, representing the words "Hardware," "software," and "information," respectively. Once the communication between the user and CS is completed, the CS examines the obtained results, which are the sets of identifiers corresponding to the trapdoors. The CS can then calculate the probability of any two of these keywords appearing in the same document by observing the number of documents that are returned for those corresponding trapdoors. By continuing the search and leaking the access pattern to obtain more probabilities, the server can determine the keywords that correspond to the trapdoors [6]. However, after clarifying this attack, we can assert that our scheme resists the IKK attack because the search results by the CS are encrypted, and the access pattern does not reveal any significant information. Thus, the CS cannot access the identifiers corresponding to the trapdoors [27].

- **Keyword guessing attack (KGA)**

Keyword guessing attack is an attack on the encrypted index stored on the server, where the attacker attempts to guess the keyword being searched in order to use it later to find its identifiers [28]. This attack can be mitigated by various precautionary measures, such as encrypting the keywords themselves and keeping the encryption key secret and secure. Both of these measures are implemented in our scheme. Therefore, we can state that our work is resistant to KGA attacks.

- **Man-in-the-middle attack**

This type of attack happens when the communication channel between the user and the CS is not secure, allowing the attacker to impersonate one of the parties [29].Our work resists a Man-in-the-middle attack, due to the secret channel between the two parties (user and server), as the copy of the secret key exists only with the user and the server.

6 Experimental results

In this section, we evaluate our scheme using a real-world database of Wikipedia articles. We executed our experiments on a Windows 64-bit machine running an Intel Core i5 CPU clocked at 1.6 GHz and 8GB RAM. The database contains 2,050 identifiers $Ndb = 2{,}050$ and 525,430 words $W = 525{,}430$. Additionally, we chose a database that supports locality to enable us to observe the effect on retrieval time due to its significant number of identifiers. Python was our language of choice for the implementation of the code, owing to its numerous features and popularity in the scientific community.

Comparison with previous studies

In this section, we will conduct a comparative analysis of our work with four previous studies that share a similar objective: to improve performance through locality. These studies are [[8], [9], [10], [30]] and we conducted all of these works at the beginning before starting the comparison process.

To compare the studies, we focused on the search time required for retrieving three words that vary in the number of identifiers. The first word, $W1$, has the highest number of identifiers ($n = 2025$), the second word, $W2$, has an average number of identifiers ($n = 1015$), and the last word, W3, has a very small number of identifiers ($n = 4$). The outcomes of acquiring $W1$ and $W2$ clearly demonstrate the disparity between our work and the prior works in terms of search speed, as shown in Fig. 2. Meanwhile, the results of retrieving W3 demonstrate that while our approach enhances the search of words with a substantial number of identifiers, it does not adversely impact the search of words with fewer identifiers as shown in Fig. 3. To ensure a fair comparison with previous works that did not include a $Find\_ids$ phase, we have included the time required for this phase along with the research time.

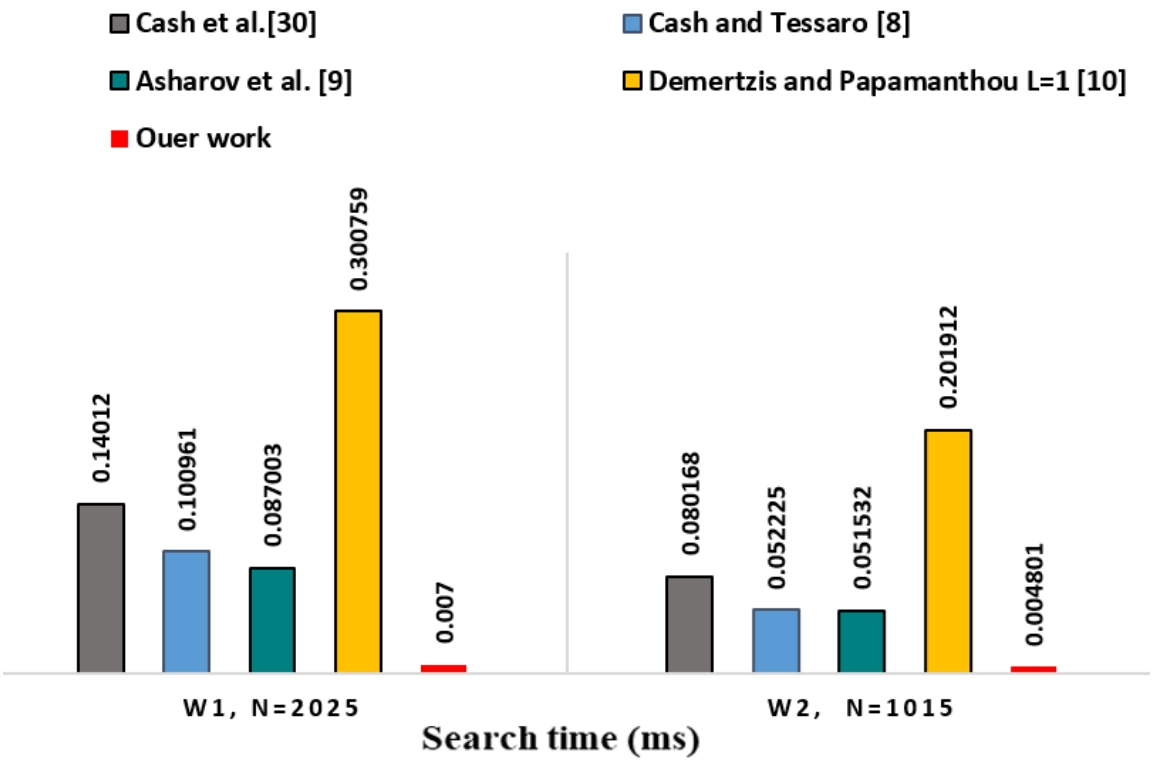


Figure 2: Comparing the search time required to find $W1$ and $W2$ in our scheme to that of previous schemes.

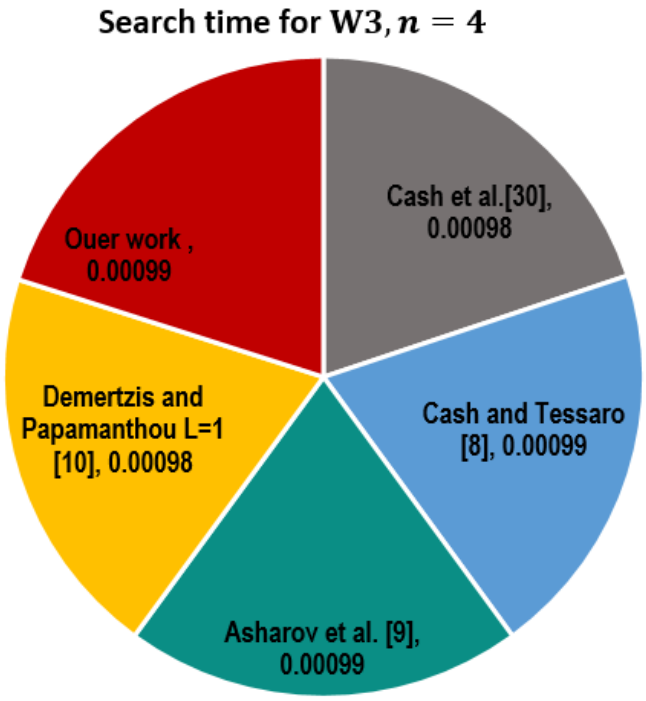


Figure 3: Comparison of search time for W3 in our scheme versus previous

6 Discussion

The primary reason for these promising results is the locality enhancements we integrated into our scheme,

which significantly decreased the number of memory locations the cloud server needs to access to respond to a user's query. For example, in the work of Cash et al. [30], the cloud server had to traverse 2025 different memory locations to retrieve identifiers for the first word, whereas in our scheme, it only needs to access one location. Furthermore, the improved locality results in fewer decryption operations. In our scheme, decryption is performed once to obtain the identifiers, whereas in other schemes, multiple decryptions are required, affecting the overall speed of the results. Another factor contributing to these positive outcomes is that the cloud server in our schemes interacts with a single hash table, while in Asharov et al. (Scheme 3) [9], Cash and Tessaro [8], and Demertzis and Papamanthou [10], it manages multiple hash tables.

7 Conclusions

Our primary goal for this work is to enhance the overall performance of SSE. We are addressing a problem related to large DB, specifically the issue of poor locality caused by the many moves in memory by the cloud server during the search phase. We have made changes to SI storage mechanism, resulting in a significant improvement in the search performance. Our modification has optimized the locality to $O(1)$ without impacting the reading efficiency, which remains at $O(1)$. Additionally, this change has not resulted in significant increase in the storage space of the encrypted index.

Our work provides a high level of security since the server does not decrypt the data. Instead, it sends the encrypted data to the user, who decrypts it. Moreover, the values stored on the server are all equal in size and do not reveal the identifiers themselves. These values serve as evidence to obtain the identifiers later.

References

[1] M. Malathi, “Cloud computing concepts,” in *2011 3rd International Conference on Electronics Computer Technology*, 2011, vol. 6, pp. 236–239. doi: 10.1109/ICECTECH.2011.5942089.

[2] G. Boss, P. Malladi, D. Quan, L. Legregni, and H. Hall, “Cloud computing,” *IBM white Pap.*, vol. 321, pp. 224–231, 2007.

[3] T. Dillon, C. Wu, and E. Chang, “Cloud computing: issues and challenges,” in *2010 24th IEEE international conference on advanced information networking and applications*, 2010, pp. 27–33. doi: 10.1109/AINA.2010.187.

[4] J. R. Vacca, *Cloud computing security: foundations and challenges*. CRC press, 2016.

[5] Y. Wang, J. Wang, and X. Chen, “Secure searchable encryption: a survey,” *J. Commun. Inf. networks*, vol. 1, pp. 52–65, 2016, doi: https://doi.org/10.1007/BF03391580.

[6] D. V. N. Siva Kumar and P. Santhi Thilagam, “Searchable encryption approaches: attacks and challenges,” *Knowl. Inf. Syst.*, vol. 61, no. 3, pp. 1179–1207, 2019, doi: https://doi.org/10.1007/s10115-018-1309-4.

[7] G. Sen Poh, J.-J. Chin, W.-C. Yau, K.-K. R. Choo, and M. S. Mohamad, “Searchable symmetric encryption: designs and challenges,” *ACM Comput. Surv.*, vol. 50, no. 3, pp. 1–37, 2017, doi: {10.1145/3064005}.

[8] D. Cash and S. Tessaro, “The locality of searchable symmetric encryption,” in *Annual international conference on the theory and applications of cryptographic techniques*, 2014, pp. 351–368. doi: https://doi.org/10.1007/978-3-642-55220-5_20.

[9] G. Asharov, M. Naor, G. Segev, and I. Shahaf, “Searchable symmetric encryption: optimal locality in linear space via two-dimensional balanced allocations,” in *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, 2016, pp. 1101–1114. doi: {10.1145/2897518.2897562}.

[10] I. Demertzis and C. Papamanthou, “Fast searchable encryption with tunable locality,” in *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, pp. 1053–1067. doi: {10.1145/3035918.3064057}.

[11] G. Asharov, G. Segev, and I. Shahaf, “Tight tradeoffs in searchable symmetric encryption,” *J. Cryptol.*, vol. 34, no. 2, pp. 1–37, 2021, doi: https://doi.org/10.1007/s00145-020-09370-z.

[12] E.-J. Goh, “Secure indexes,” *Cryptol. ePrint Arch.*, 2003.

[13] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in *International conference on applied cryptography and network security*, 2005, pp. 442–455.

[14] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 79–88. doi: {10.1145/1180405.1180417}.

[15] R. Zhang, R. Xue, and L. Liu, “Searchable encryption for healthcare clouds: A survey,” *IEEE Trans. Serv. Comput.*, vol. 11, no. 6, pp. 978–996, 2017, doi: 10.1109/TSC.2017.2762296.

[16] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in *Proceeding 2000 IEEE symposium on security and privacy. S&P 2000*, 2000, pp. 44–55. doi: 10.1109/SECPRI.2000.848445.

[17] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, and M. Steiner, “Highly-scalable searchable symmetric encryption with support for boolean queries,” in *Annual cryptology conference*, 2013, pp. 353–373. doi: https://doi.org/10.1007/978-3-642-40041-4_20.

[18] M. Chase and S. Kamara, “Structured encryption and controlled disclosure,” in *International conference*

on the theory and application of cryptology and information security, 2010, pp. 577–594. doi: https://doi.org/10.1007/978-3-642-17373-8_33.

[19] P. Van Liesdonk, S. Sedghi, J. Doumen, P. Hartel, and W. Jonker, "Computationally efficient searchable symmetric encryption," in *Workshop on Secure Data Management*, 2010, pp. 87–100. doi: https://doi.org/10.1007/978-3-642-15546-8_7.

[20] K. Kurosawa and Y. Ohtaki, "How to update documents verifiably in searchable symmetric encryption," in *c*, 2013, pp. 309–328. doi: https://doi.org/10.1007/978-3-319-02937-5_17.

[21] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 965–976. doi: {10.1145/2382196.2382298}.

[22] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *International conference on financial cryptography and data security*, 2013, pp. 258–274. doi: https://ia.cr/2013/832.

[23] A. A. Alyousif and A. A. Yassin, "Locality Improvement Scheme Based on QR Code Technique within Inverted Index," *Informatica*, vol. 47, no. 7, 2023.

[24] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*, 1996, pp. 1–15. doi: https://doi.org/10.1007/3-540-68697-5_1.

[25] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.

[26] Y. Watanabe *et al.*, "How to make a secure index for searchable symmetric encryption, revisited," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 105, no. 12, pp. 1559–1577, 2022, doi: 10.1587/transfun.2021EAP1163.

[27] D. Cash, P. Grubbs, J. Perry, and T. Ristenpart, "Leakage-abuse attacks against searchable encryption," in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 2015, pp. 668–679. doi: {10.1145/2810103.2813700}.

[28] Y. Miao, Q. Tong, R. H. Deng, K.-K. R. Choo, X. Liu, and H. Li, "Verifiable searchable encryption framework against insider keyword-guessing attack in cloud storage," *IEEE Trans. Cloud Comput.*, vol. 10, no. 2, pp. 835–848, 2020, doi: 10.1109/TCC.2020.2989296.

[29] S. Gangan, "A review of man-in-the-middle attacks," *arXiv Prepr. arXiv1504.02115*, 2015, doi: https://doi.org/10.48550/arXiv.1504.02115.

[30] D. Cash *et al.*, "Dynamic searchable encryption in very-large databases: Data structures and implementation," *Cryptol. ePrint Arch.*, 2014, doi: 10.14722/ndss.2014.23264.

Anomaly Detection in Network Access-Using LSTM and Encoder-Enhanced Generative Adversarial Networks

Jian Hu[1*], Yingjun He[1], Wenqian Xu[2,3], Yixin Jiang[2,3], Zhihong Liang[2,3], Yiwei Yang[2,3]
[1]Yunnan Power Grid Information Center, China Southern Power Grid, Kunming 650217, China
[2]Electric Power Research Institute, China Southern Power Grid, Guangzhou 510663, China
[3]Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou 510663, China
[*]E-mail: hjian127@163.com
[*]Corresponding Author

Keywords: generative adversarial networks, anomalous access, detection algorithms, models

Received: September 29, 2024

Along with the continuous development of information technology, the database has become an important module for enterprises and individuals to apply computers, and some important data are stored in the database, which also leads to the database becoming the target of malicious intruders. The abnormal access behavior detection algorithm for data can quickly identify abnormal access situations, timely intervention and processing to ensure data security. Based on this, this paper proposes an abnormal defense behavior detection algorithm based on generative adversarial network, the new algorithm has the applicability as well as two derivative models of generative adversarial network for network abnormal access detection with high efficiency. In this paper, we experiment the classification accuracy of network anomaly detection algorithm, i.e., F1, by using three models, namely, the original Generative Adversarial Network (GAN), Generative Adversarial Network using Long and Short-Term Memory Network (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder (GAN+Encoder), and the result of this paper shows that the GAN+Encoder model is the most effective. And based on these three models of the generator and discriminator loss trends are compared, as well as through the iteration of 50 times of training results show that the GAN + Encoder model is relatively simple, and the training time is shorter and more efficient.

Povzetek: Razvita je metoda GAN+Encoder za zaznavanje anomalij v omrežnem dostopu, ki omogoča krajši čas učenja in boljšo prilagodljivost pri prepoznavanju nenavadnega dostopa.

1 Introduction

In today's digital age, network security has become a crucial issue. With the continuous development and popularization of the internet, abnormal access behavior is also increasing, bringing huge risks to individuals, businesses, and society. Traditional methods for detecting abnormal access behavior often suffer from issues such as low accuracy and poor adaptability when facing complex and ever-changing network environments. Generative Adversarial Networks (GANs), as an emerging deep learning technology, have shown great potential in the field of anomaly access behavior detection. Generative Adversarial Networks (GANs) are a type of deep learning model consisting of a generator and a discriminator. Its basic principle originates from the zero-sum game of game theory, which learns the distribution of data through the adversarial process between the generator and discriminator. Since Ian Goodfellow et al. proposed GAN in 2014, it has developed into one of the most cutting-edge technological fields in the field of deep learning [1]. With the continuous deepening of research in the field of generative adversarial networks, problems such as models being too free and uncontrollable, models not converging, and models collapsing in the original generative adversarial networks (GANs) have gradually been exposed. Researchers have continuously proposed new generative adversarial network derived models to address these issues. So far, there have been hundreds of derivative models of generative adversarial networks, and various new derivative models are still being proposed [2]. Generative adversarial networks have achieved great success in multiple fields. For example, in the field of image generation, GAN can generate realistic facial photos, animal photos, comic characters, etc; In the field of style transfer, GAN can transform one form of image into another, such as converting photos into oil paintings, three-dimensional into anime, etc. These successful applications provide rich ideas and methods for GAN in the field of anomaly detection.

Currently, some scholars have conducted research on database anomaly access detection based on log records generated by user access to databases. Due to the large number of system log files and the presence of redundant information, traditional feature engineering manually extracts features from relational entities, which is cumbersome and time-consuming, making it

very difficult to establish detection models and resulting in low efficiency in anomaly detection. Therefore, based on the network anomaly access detection algorithm of generative adversarial networks, this article proposes two derivative models of generative adversarial networks, namely the LSTM based generative adversarial model and the encoder based generative adversarial model. And through the comparative analysis of the three models, the advantages of the encoder-based generative adversarial model are highlighted, in order to be able to provide a more novel reference for the field of anomaly detection.

2 Generative adversarial network

In the process of training the generative adversarial network, the generator tries hard to "deceive" the discriminator so that it decides that the generated data is real data, and the discriminator also needs to try its best to make the correct judgment between the real sample and the generated sample, so the two form an adversarial relationship, and the ultimate goal of the GAN is to generate the generator to generate enough fake samples to match the real one. fake samples. The loss function of the original generative adversarial network is as follows:

$$\min_G \max_D V(D,G) = \mathrm{E}_{x\sim p_{data}(x)}[\log D(x)] + \mathrm{E}_{x\sim p_z(z)}[\log(1-D(G(z)))] \quad (1)$$

Where $p_z(z)$ denotes that the input z of the generator is sampled from a certain distribution, usually taking a -some simple distribution, such as Gaussian distribution, uniform distribution. $G(z;\theta_g)$ denotes a parameterized θ_g network G, whose purpose is to map a simple distribution to the data space. $D(x;\theta_d)$ denotes a parameterized θ_d network D, whose output ranges from 0 to 1 to indicate the probability of generating samples from the real probability from the data. The discriminator $D(x;0_d)$ is designed to distinguish whether its input sample x is from the generator or from the real data, defining the real data distribution as label y=1 and the data generated from the generator as label y=0 [3]. The probability that the output of the discriminator is 1 (real data) can then be defined as.

$$p(y=1|x) = D(x;\theta_d) \quad (2)$$

The probability that the output of the discriminator is 0 (generator generated data) can be defined as:

$$p(y=0|x) = 1 - D(x;\theta_d) \quad (3)$$

For the generator, its goal is to minimize the loss function of the above equation (1), that is to say, to generate samples as close as possible to the real data, and then make the discriminator produce a misjudgement, so that its output tends to.

3 Detection of abnormal access behavior based on adversarial network

3.1 Network anomalous access detection model

Adversarial network-based anomalous access behavior detection is a method that uses the adversarial network technique in deep learning to detect anomalous access behavior. It detects abnormal access behavior by training an adversarial network to generate normal access behavior data and comparing it with real access behavior data. In contrast, adversarial network-based anomalous access behavior detection methods can take advantage of the powerful fitting ability of deep learning technology to achieve accurate detection of anomalous behavior [4].

The overall structure of the primitive GAN-based network anomalous access detection model is shown in Figure 1, a network anomaly detection model is mainly composed of two parts: model training as well as anomaly detection. The upper half of Figure 1 shows the training process of the generative adversarial network, the Generator uses Noise to generate "fake data", the discriminator is trained by the real sample data in the Training Data as well as the fake data generated by the Generator. The closer the result is to 1, the more the discriminator is true, otherwise it is false. The second half of Figure 1 is the anomaly detection stage, where the test data is input into the discriminator, and the trained discriminator will determine whether this data is anomalous or not.

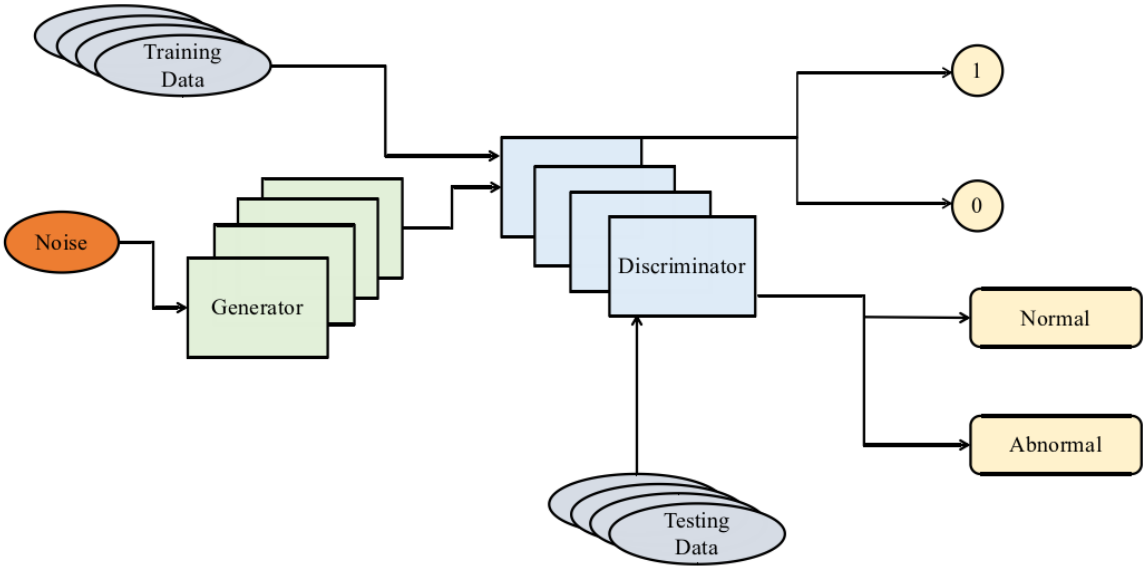


Figure 1: General framework of GAN-based network anomaly access detection

Although the original generative adversarial model can be used to complete the detection of abnormal network access data, however, due to the generative adversarial network itself has the problem that the discriminator is too strong and the generator is too weak which makes the model difficult to be trained, so the original generative adversarial model needs to be adapted and adjusted. In this paper, two GAN-based network anomalous access detection models are designed. The first method uses the advantage of LSTM in processing time series to design LSTM-based generative adversarial model, so as to achieve the optimization effect on the original model. The second method is to add an encoder (Encoder) in the generative adversarial model, and learn jointly with the generator in the generative adversarial network through the Encoder [5, 6].

3.1 Generative adversarial model based on LSTM

Figure 2 shows the model architecture of a generative adversarial model based on LSTM. The left half of the figure is a GAN framework, where the generator and discriminator are obtained through iterative adversarial training. On the right is the anomaly detection process, where the discriminator trained with GAN calculates the discrimination score, the generator calculates the reconstruction score, and then combines them.

Firstly, this article constructs the generator and discriminator of GAN as two Long Short-Term Memory (LSTM) neural networks, as shown in the left half of Figure 3-2. According to the original GAN framework, the generator takes a sequence from a random latent space as its input to generate fake access data, and passes the generated sequence samples to the discriminator, which attempts to distinguish the generated (i.e., "fake") data sequence from the actual (i.e., "true") normal training data sequence. This model does not handle each data stream separately, but considers the entire dataset simultaneously in order to capture potential interactions between variables in the model.

In order to utilize the advantages of LSTM in processing time series in this method, both the generator and discriminator of GAN are long short-term memory neural networks (LSTM). After sufficient rounds of training iterations, the trained discriminator and generator can be used to detect anomalies in the data. The advantage of using GAN is that it can train both a discriminator and a generator simultaneously. This article uses discriminators and generators to jointly train and identify network anomalies.

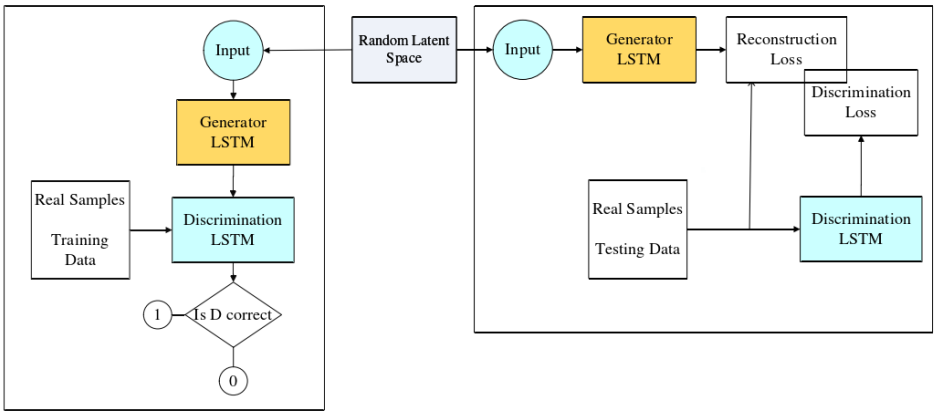


Figure 2: Generative adversarial model based on LSTM

3.2 Encoder based generative adversarial model

A GAN trained to adapt to a normal sample distribution should be able to reconstruct a normal sample from some potential representation. However, since GANs can only implicitly model data distributions, using them for anomaly detection requires a complex optimization process to recover the potential representation of a given input example, which is a very time-consuming approach for large datasets or real-time applications. Therefore, this article designs a GAN model based on an encoder for anomaly detection, with the aim of learning the encoder while training the GAN to achieve better anomaly detection performance.

This model is based on the GAN method and simultaneously learns an encoder E that maps the input sample X to a latent representation Z, a generator G, and a discriminator D during training, which can avoid the problem of high computational complexity in recovering latent representations during testing. Unlike the discriminator in conventional GANs that only considers real or generated samples, in this case, discriminator D also considers potential representations (generator input or encoder). The structure of the encoder based generative adversarial model is shown in Figure 3.

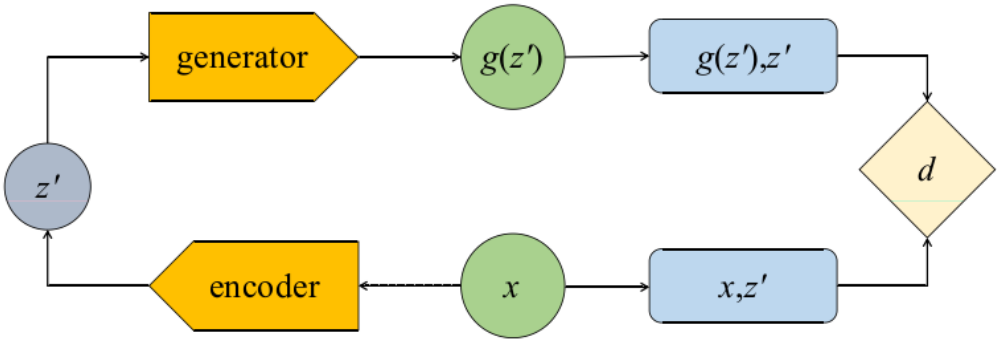


Figure 3: Encoder+GAN model structure

There are different strategies for training encoders, where G and E are jointly learned. In order to optimize the training process of the original GAN, this paper defines V (D, E, G) as equation (4):

$$V(D,E,G)=E_{X-PX}\left[E_{Z-PE(\cdot|X)}\left[\log D(x,z)\right]\right]+\left[E_{X-PG(\cdot|z)}\left[1-\log D(x,z)\right]\right] \quad (4)$$

Here PX (X) is the distribution of the data, Pz (z) is the distribution on the latent representation, PE (z | x) and PG (x | z) are the distributions of the encoder and generator, respectively. After training the model on normal data to generate G, D, and E, this paper defines a score function A $_{(x)}$, which is a combination of reconstruction loss L_G and discriminator-based loss L_D. The specific form of detecting whether example x is abnormal is:

$$A(x)=aL_G(x)+(1-a)L_D(x) \quad (5)$$

Where a represents the weight of the reconstruction loss in the overall loss of the model, and 1-a represents

the weight of the discriminator loss. Among them,

$$L_G(x) = \| xG(E(x)) \|_1 , \text{L}_\text{D}\ (\text{x})$$

are defined in two ways. Firstly, taking the cross-entropy loss of x's discriminator as an example: it captures the discriminator's confidence in the distribution of samples from real data. The second method of defining L_D has a "feature matching loss", were

$$L_D(x) = \| f_D(X, E(x)) - f_D(G(E(x), E(x))) \|_1$$

evaluates whether the reconstructed data has features similar to the real sample in the discriminator, and samples with larger $A_{(x)}$ values are considered more likely to be abnormal.

4 Experimental results and analysis

4.1 Experimental data

To verify the effectiveness of the proposed method, this paper uses the publicly available dataset KDDCUP1999Data1 as experimental data and analyzes the experimental results using the two model evaluation metrics mentioned earlier. The experimental environment is as follows: using the industry's mainstream deep learning framework Tensor Below to implement data loading and model training, and conducting experiments using PyCharm software.

The samples in the KDDCUP1999 dataset are network connections, each network connection is labeled as normal and abnormal, and the abnormal types are mainly categorized into the following four types:

(1) Denial-of-service attack (DOS, denial-of-service);

(2) The remote computer is not authorized to access the local computer (R2L, the remote computer is not authorized to access the local computer);

(3) super user has unauthorized access (U2R, super user has unauthorized access);

(4) port monitoring or scanning (surveillance and probing) [7].

In this paper, K-fold cross validation method is used for the training set and test set. The dataset is randomly divided into mutually exclusive subsets, and the k subsets are randomly divided into two groups, one with k-1 subsets and the other with one subset. In each kind of grouping result, the group with k-1 subsets is treated as a training set and the other as a test set, generating predictions, which are averaged. In this paper k is chosen as 12 during the processing of the dataset [8, 9].

4.2 Network transmission data anomaly identification method

4.2.1 Preprocessing of network transmission data

Before data anomaly identification, certain preprocessing of network transmission data is required. This study applies the normalization method to control the network transmission data between 0 and 1, with the expression:

$$Y = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (6)$$

Due to the large volume of network transmission data, coupled with the fact that the subsequent construction of the model requires a training set and a test set, a Gaussian mixture model is applied in this section to partition the network transmission data set. Gaussian mixture model can effectively partition the network transmission data set into 2 sets, respectively, the training set (dark circle) and the test set (light circle), which are recorded as sets Y1 and Y2, laying a solid foundation for the realization of the subsequent network transmission data anomaly identification.

4.2.2 Network transmission data anomaly identification model construction

Based on the preprocessed network transmission data collection, LSTM, a deep learning technique, is introduced to construct a network transmission data anomaly identification model, which provides support for the realization of the research objectives.

The Encoder+GAN based network transmission data anomaly identification model is specifically shown in Fig. 4.

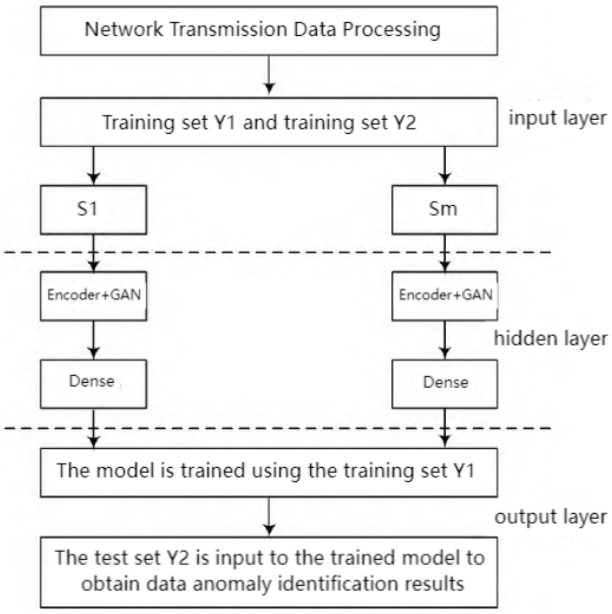


Figure 4: Schematic diagram of network transmission data anomaly identification model

Due to the network transmission data in the time dimension there is a back and forth relationship, with time series characteristics, coupled with the data

transmission is a more complex process, but also subject to a variety of factors directly or indirectly, resulting in the existence of anomalous data with a certain degree of uncertainty, and LSTM has a better convergence of the time series data processing, so this is the basis for the construction of the network transmission data anomaly identification model.

4.2.3 Network transmission data input remodeling

Because the LSTM neural network contains long-term and short-term memory unit states in the above model, it has certain requirements on the input data form, therefore, it is necessary to reshape the network transmission data to make it meet the requirements of the model input, and maximize the recognition accuracy of the anomalous data.

Setting the network transmission data as

$$Y = \{y_1, y_2, ..., y_m\},$$

LSTM neural network long-term and short-term memory unit association length is LC and LD respectively, then the expression of input data after reshaping is:

$$z_i = \frac{y_i}{\alpha_c \cdot L_c} + \frac{y_i}{\alpha_D \cdot L_D} \quad (7)$$

The entire network transmission data is reshaped and processed using Eq. (7) to obtain the set of input data $S = \{s_1, s_2, ..., s_m\}$

for constructing the model, in preparation for the implementation of network transmission data anomaly identification.

4.2.4 Network transmission data anomaly identification

The gradient descent method is applied to formulate the training procedure for constructing the model, determine the abnormal data discrimination rules, input the test set into the trained recognition model, and its output is the abnormal data recognition result.

The training process of network transmission data anomaly identification model based on gradient descent method is shown below:

1) Initialize the parameters of the recognition model, set the initial step size to 0.001 and the initial decay rate to 0.9.

2) Collect a random sample data q in the training set Y_1, which is noted as $\{y_1, y_2, ..., y_q\}$, and its corresponding model output target is R_j.

3) Calculate the gradient values g and update the biased first-order moment estimate H and biased second-order moment estimate K.

4) Correct the biased first-order moments and second-order moments to obtain new estimates, denoted as H vs K.

5) Calculate the updated parameters.

6) Repeat steps 2) to 5) until the maximum number of iterations is satisfied, and output the parameters of the final recognition model. The anomalous data discrimination parameter is calculated as:

$$\Gamma = \sqrt{\frac{1}{n-1}\sum_{t-1}^{n}[y(t) - \hat{y}(t)]^2} \quad (8)$$

Where: Γ denotes the anomalous data discriminating parameter; $y(t)$ and $\hat{y}(t)$ denote the model fitting value and the actual value, respectively.

Based on the calculation results of Eq. (8), the rules of abnormal data discrimination are formulated: when Γ is greater than or equal to 0.43, it is recognized that the data transmitted by the network are abnormal data; when Γ is less than 0.43, it is recognized that the data transmitted by the network are normal data. Substituting the relevant parameter values and abnormal data discrimination rules obtained from the above training into the network transmission data abnormality identification model, the training and improvement of the identification model can be completed. The test set is used as the input of the identification model, and the output of the model is the result of abnormal data identification, thus realizing the accurate identification of network transmission data abnormality, providing a more effective guarantee for the security of network transmission data, and facilitating the querying of demand data to a certain extent.

4.3 Anomaly detection results and analysis based on classification accuracy

In order to verify the performance of the network anomaly access detection method based on generative adversarial network proposed in this paper, this paper uses One-ClassSVM, Isolation Forest Algorithm, Local Anomaly Factor Algorithm and Covariance Estimation Algorithm for comparison experiments [10].

Before analyzing the experimental results, this paper selects the same number of network anomaly access data from the preprocessed data and uses a variety of traditional algorithms as a comparison experiment. The experimental results are shown in Table 1:

Table 1: Classification accuracy of traditional machine learning methods

Model	Precision	Recall	F1
Isolation Forest	0.4415	0.3260	0.3750
One-Class-SVM	0.7457	0.8523	0.7954
Local Outlier Factor	0.7913	0.8045	0.7743
Covariance estimation	0.7879	0.7736	0.7851

From the experimental results, it can be seen that among all the machine learning methods, the use of Isolation Forest for anomaly detection has the worst effect, and the accuracy rate of detecting network anomalies is even less than half, while the accuracy rate of using One-Class SVM, Local Anomaly Factor Algorithm, and Covariance Estimation Algorithm is relatively similar, and among them, the Local Anomaly Factor Algorithm has the best experimental results. Among all the machine learning methods, the highest accuracy was achieved using the Local Outlier Factor method. Although the experimental results show that the results are not bad when using traditional machine learning algorithms for network anomalous access detection, however, for the Internet as a whole, every time one more network attack goes undetected, its potential damage increases exponentially [11]. In this paper, we propose a network anomaly detection algorithm based on generative adversarial networks, and the accuracy rates under different models and parameters are shown in Table 2:

Table 2: Classification accuracy of the network abnormality detection algorithm based on GAN

Model	Parameter	Precision	Recall	F1
GAN(Feature Matching)	w=0.1	0.7382	0.7500	0.7741
GAN(Cross-E)	w= 0.1	0.7859	0.7984	0.7921
GAN(Feature Matching)	w=0.3	0.7292	0.7408	0.7349
GAN(Cross-E)	w=0.3	0.7858	0.7984	0.7920
GAN + LSTM(Cross-E)	w =0.1	0.7983	0.8650	0.8303
GAN + LSTM(Feature Matching)	w= 0.1	0.7719	0.8467	0.8134
GAN + LSTM(Cross-E)	w =0.3	0.7959	0.8646	0.8300
GAN + LSTM(Feature Matching)	w=0.3	0.7597	0.8250	0.7954
GAN + Encoder(Cross-E)	w=0.1	0.9508	0.9659	0.9583
GAN + Encoder(Feature Matching)	w= 0.1	0.9492	0.9643	0.9567
GAN + Encoder(Cross-E)	w=0.3	0.9507	0.9658	0.9582
GAN + Encoder(Feature Matching)	w=0.3	0.9104	0.9249	0.9176

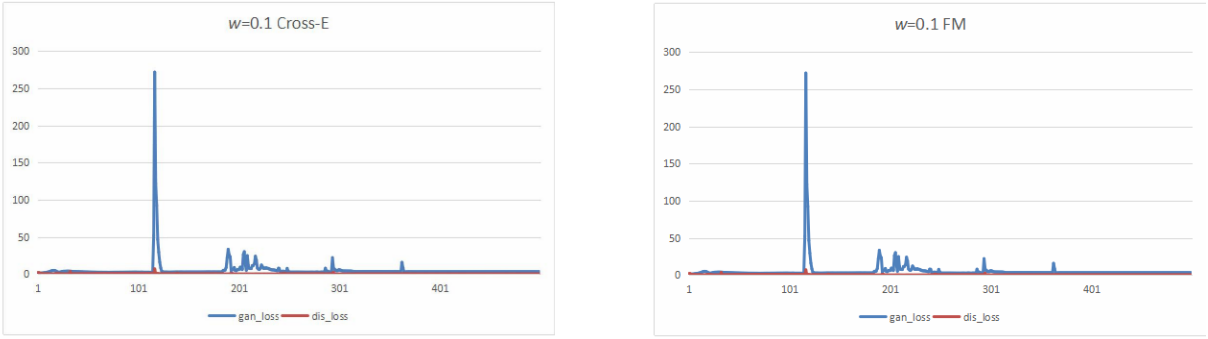
In this case, the accuracy rate is the percentage of data points that are correctly detected as anomalous. A higher accuracy rate means that the model can accurately find out the abnormal data with better results. Among the three models, the accuracy rate of GAN + Encoder is higher than the other two models, which is around 0.9. Recall is the ratio between data points that are correctly detected as anomalous and all anomalous data points. The higher the recall, the more comprehensively the model is able to identify anomalous data. Among the three models, the GAN + Encoder model has the highest value, which indicates better results. F1 value is a combined assessment of accuracy and recall, which is used to measure the overall performance of the model. Higher F1 values represent better anomaly detection ability of the model. Among the three models, GAN + Encoder has a relatively high F1, which shows the advantage of its detection ability.

In Table 2, w is the weight, which indicates the proportion of the generator's loss to the overall loss of the generative adversarial model, and the corresponding loss weight of the discriminator is 1-w. Through the experimental results, it is not difficult to see that the experimental results are the best when w is taken to be 0.1, and the classification accuracy rate is in a decreasing trend with the increasing w. On the other hand, this paper uses two kinds of loss functions, cross-entropy and feature matching, and experiments are conducted with different loss functions under each parameter, and the results show that in the process of using generative adversarial network for network anomalous access detection, cross-entropy as a loss function is more effective for classification compared to feature matching. When the original generative adversarial network is used, the anomaly detection

effect that can be achieved is similar to the result of using local anomaly detection methods, and when the discriminator and generator in the GAN use LSTM, it can produce a certain enhancement to the accuracy of classification. Finally, when the GAN+Encoder method is used, for anomalous access detection Data Table 2 GAN-based Network Anomaly Detection Algorithm achieves the best accuracy in terms of classification accuracy, which is best compared to other classification models [12].

4.4 Anomaly detection results and analysis based on generator discriminator loss

In this paper, a total of three different generative adversarial network models are used for anomaly detection, which are the original Generative Adversarial Network (GAN), Generative Adversarial Network using Long and Short-Term Memory Networks (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder (GAN+Encoder). The strengths and weaknesses of the models can be observed through the loss variations of the generators and discriminators of these three models.



(a) (b)

Figure 3: Trend of GAN loss change. (a)Loss variation of GAN with loss function Cross-E (b) Loss variation of GAN with loss function as FM

As shown in Figure 3, Figure 3a shows the loss variation of GAN using Cross-Entropy as the loss function, and Figure 3b shows the loss variation of GAN using Feature Matching as the loss function. When using the same parameters to train the original GAN, it can be found that the generator loss will first become larger and larger, this is due to the initial period of training the model discriminator is stronger, the generator is weaker, at this time the discriminator can easily distinguish between the real data and the fake data generated by the generator, so at this time, the loss of the discriminator is very small, and the generator's loss is larger, and continues to show an upward trend. However, in the process of continuous adversarial training, the generator gradually learns how to generate more "realistic" fake data, and then the generator loss begins to decline, and eventually converge to a smaller value, until the generator and discriminator losses converge [13].

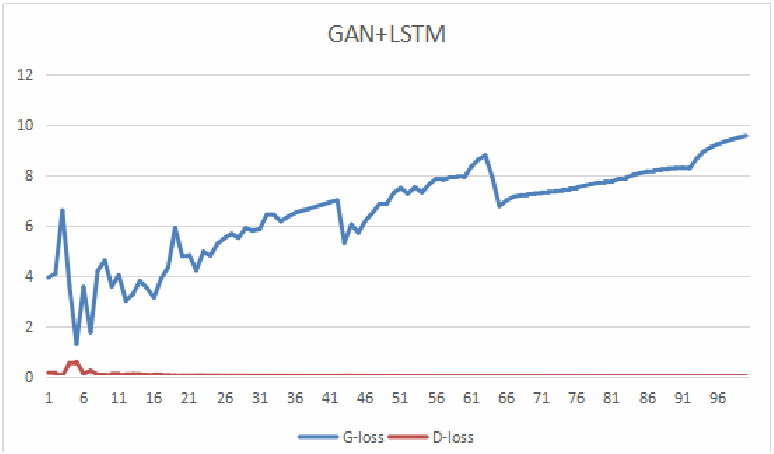
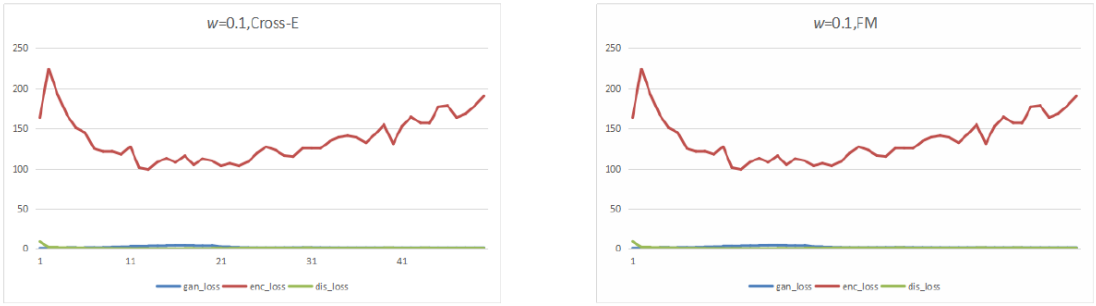


Figure 4: Loss variation of GAN+LSTM

Figure 4 shows the training loss variation of the generative adversarial network model based on Long Short-Term Memory Network (LSTM), unlike the original GAN, the generator and the discriminator of this model are all using LSTM. Through many experiments, it is found that the model's performance is the best at this time when the number of times of training is set to about 100 times. Meanwhile, compared with the original GAN, the loss of the generator and the discriminator tends to converge faster after using the GAN+LSTM model, which means that the model's classification effect is better after adding the LSTM. However, due to the increased complexity of the model, each iteration of training takes longer [14].

Figure 5 shows the loss variation of the generative adversarial network model with the addition of the Encoder. From Figure 5, it is not difficult to see that although the loss of the encoder is very large and constantly showing an upward trend, but the loss of the generator converges very quickly, at this time, only need to train about 50 times to make the model has a very good detection effect.



(a) (b)

Figure 5: Loss variation trend of Encoder+GAN. (a) The loss function is the loss variation (b) Encoder+GAN loss variation of Encoder+GAN of Cross-E with loss function as FM

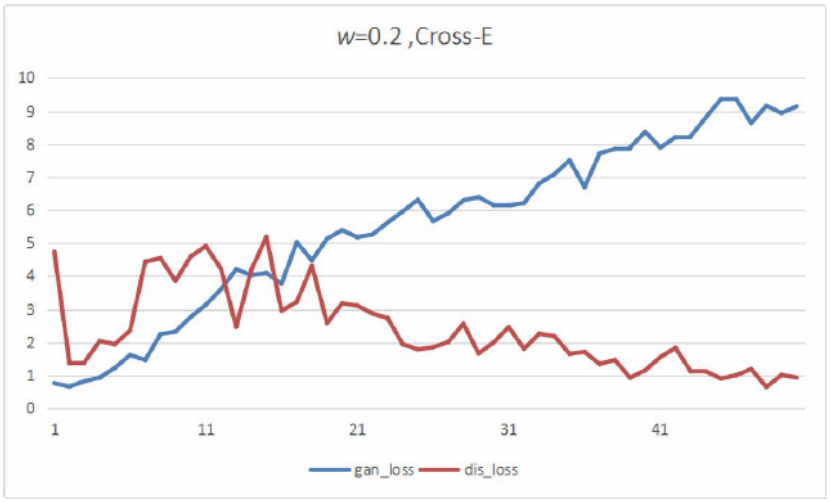


Figure 6: Training results of GAN after 50 iterations

As shown in Figure 6, in order to compare the model enhancement effect, when using the original GAN for 50 times of training, at this time it is not difficult to find that the loss of the generator is extremely large and rising, while using the GAN + Encoder at this time, the loss of the generator and discriminator has converged. At the same time compared to the GAN + LSTM model, the use of GAN + Encoder model is relatively simple, and the training time is shorter, more efficient.

5 Discussion

The research on network anomaly access detection technology is crucial in the field of intrusion detection. However, currently this technology is facing issues such as high false alarm rates, insufficient detection coverage, and inadequate detection accuracy and efficiency, which urgently require in-depth research. This article proposes a novel detection mechanism based on generative adversarial networks to address the challenge of dealing with network intrusion datasets with rich types of anomalies but limited sample sizes encountered by

traditional methods. By training the GAN model, the generator generates data through continuous adversarial training, thereby enhancing the discriminative ability of the discriminator.

This article also explores the problem of mismatched generator and discriminator capabilities during GAN training, and proposes two variant models of GAN that help the generator loss function converge faster, significantly reducing training time and improving training quality. However, due to the large number of network connection features contained in the processed data samples, the computational complexity of the GAN model is high, making it difficult to quickly achieve result output in a single machine environment. Therefore, this study suggests adopting a distributed server cluster architecture to improve program running efficiency.

In this study, the classification accuracy and F1 results of the three models, the original Generative Adversarial Network (GAN), Generative Adversarial Network using Long Short-Term Memory Network (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder (GAN+Encoder), were analyzed experimentally in comparison to the original Generative Adversarial Network (GAN), and the Generative Adversarial Network using Long Short-Term Memory Network (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder, and the F1 results show that GAN+Encoder model is the best. This is due to the fact that this model is based on stemming approach while learning an encoder E mapping input samples X to potential representations Z, a generator G, and a discriminator D during the training period, which avoids high computational complexity problems in recovering potential representations during testing. Experiments on the loss trends of the generator and discriminator based on these three models, as well as the results of training through 50 iterations show that the GAN+Encoder model is relatively simple, and has a shorter and more efficient training time. However, there are still some challenges and limitations of the method, such as the comprehensiveness of data collection, the effectiveness of feature extraction, and the robustness of the network. Future research can further explore these issues to achieve more efficient and reliable anomalous access behavior detection.

Funding

This work was sponsored in part by China Southern Power Grid Corporation technology project (059300KC2212000).

Conflict of interest

The authors declare that they have no competing interests.

Data availability statement

The data used to support the findings of this study are all in the manuscript.

References

[1] Xu XY, Fan WW, Wang SY, Zhou F. (2024). WBIM-GAN: A generative adversarial network based wideband interference mitigation model for synthetic aperture radar. *Remote Sensing*, 16(5), 910. https://doi.org/10.3390/rs16050910

[2] Vijaykumar R, Mueer Ahmad M, Ismail MA, Ahmad I, Neelum N. (2024). Deep learning-driven virtual furniture replacement using GANs and spatial transformer networks. *Mathematics*, 12(22), 3513. https://doi.org/10.3390/math12223513

[3] Zhang YL, Wang TK, Du K, Chen P, Wang HX, Sun HH. (2024). General network framework for mixture raman spectrum identification based on deep learning. *Applied Sciences*, 14(22), 10245. https://doi.org/10.3390/app142210245

[4] Zhu W, Guo QS, Yang N, Tong Y, Zheng CB. (2024). An improved generative adversarial network for generating multi-scale electronic map tiles considering cartographic requirements. *ISPRS International Journal of Geo-Information*, 13(11), 398. https://doi.org/10.3390/ijgi13110398

[5] Riaz M, Dilpazir H, Naseer S, Mahmood H, Anwar A, Khan J, Benitez IB, Ahmad T. (2024). Secure and fast image encryption algorithm based on modified logistic map. *Information*, 15(3), 172. https://doi.org/10.3390/info15030172

[6] Khemaissia R, Derdour M, Ferrag MA, Bouhamed MM. (2023). PrSChain: A blockchain based privacy preserving approach for data service composition. *Informatica*, 47(9). https://doi.org/10.31449/inf.v47i9.5081

[7] Zhu YH, Li Y, Wei TY. (2024). Classification and identification of frequency-hopping signals based on jacobi salient map for adversarial sample attack approach. *Sensors*, 24(21), 7070. https://doi.org/10.3390/s24217070

[8] AlKhonaini A, Sheltami T, Mahmoud A, Imam M. (2024). UAV detection using reinforcement learning. Sensors, 24(6), 1870. https://doi.org/10.3390/s24061870

[9] Xie Q, Huang JJ. (2024). Improvement of a conditional privacy-preserving and desynchronization-resistant authentication protocol for IoV. *Applied Sciences*, 14(6), 2451. https://doi.org/10.3390/app14062451

[10] Taurshia A, Kathrine JW, Andrew J, Eunice RJ. (2024). Securing internet of things applications using software-defined network-aided group key management with a modified one-way function tree. *Applied Sciences*, 14(6), 2405. https://doi.org/10.3390/app14062405

[11] Sun L, Chen P, Xiang W, Chen P, Gao WY, Zhang KJ. (2019). SmartPaint: a co-creative drawing

system based on generative adversarial networks. *Frontiers of Information Technology & Electronic Engineering*, 20 (12): 1644-1657. https://doi.org/10.1631/FITEE.1900386

[12] Xia LM, Wang H, Guo WT. (2019). Gait recognition based on generative adversarial image complementation network (English). *Journal of Central South University*, 26 (10): 2759-2770. https://www.cnki.com.cn/Article/CJFDTotal-ZNGY201910013.htm

[13] Hu YD, Sun L, Mao XQ, Zhang S. (2024). EEG data augmentation method for identity recognition based on spatial-temporal generating adversarial network. *Electronics*, 13(21), 4310. https://doi.org/10.3390/electronics13214310

[14] Xiao YJ, Xu WY, Jia ZH, Ma ZR, Qi DL. (2017). A non-intrusive power consumption-based anomaly detection scheme for programmable logic controllers (in English). *Frontiers of Information Technology & Electronic Engineering*, 18 (04): 519-535. https://doi.org/10.1631/FITEE.1601540

SBPM Model for Analyzing Students' Learning Behavior Based on Fine Grained Emotion Analysis and Emotion Assessment

Xianzhong Wang, Jian Li*
Beihai Campus, Guilin University of Electronic Technology, Beihai 536000, China
*E-mail: zzbzzk2504@163.com
*Corresponding Author

Keywords: sentiment analysis, behavior prediction, student, fine-grained, emotional dictionary, mini-batch gradient descent

Received: August 30, 2024

Different students have different learning behaviors, and their attitudes towards learning are directly reflected in their learning behavior. To improve students' self-learning ability and enhance the teaching level of universities, this study constructs an emotional change trend evaluation model based on fine-grained emotion analysis technology during the learning process. Based on the output results of the model, predictive analysis is conducted on students' learning behavior. The results showed that the designed emotional evaluation model could achieve an accuracy of over 80% in analyzing the trend of students' emotional changes, and the calculation time was only about 15 seconds. The proposed student learning behavior prediction model could reduce the average percentage error to 0.15% when predicting and analyzing students' learning behavior. The proposed student learning behavior prediction model consistently maintained an F1 score above 0.95 and an accuracy rate of over 97% in predicting students' learning behavior. The research model can accurately analyze the emotional changes of students during the learning process and predict and analyze their learning behavior. Universities can correct students' learning behavior based on the output results of the model, effectively improving students' learning efficiency and enhancing the teaching level of universities.

Povzetek: Uveden je model SBPM za napovedovanje študentskega vedenja na podlagi podrobne analize čustev. Model dosega visoko natančnost in pomaga izboljšati učno učinkovitost ter prilagoditi pedagoške strategije univerz.

1 Introduction

The continuous advancement of educational technology has made the analysis and understanding of Students' Learning Behavior (SLB) increasingly important. By analyzing SLBs, teachers can understand each student's unique needs and learning styles, and design personalized learning plans and teaching strategies accordingly [1, 2]. Learning Behavior Analysis (LBA) can also help students understand their learning habits and efficiency, thereby encouraging them to adopt more effective learning strategies and cultivate their ability for self-directed learning. LBA can not only assist teachers and students but also provide data support for education administrators to make more informed decisions on resource allocation, curriculum design, and policy formulation [3, 4]. In recent years, educational and psychological research has gradually recognized that students' emotional states and behavioral patterns have a significant impact on their learning outcomes. By analyzing nonverbal signals such as students' language, facial expressions, and body language, it is possible to identify and understand students' emotional states in more detail. Understanding students' emotional states can help teachers understand their emotional changes promptly and provide a basis for adjusting teaching strategies [5, 6]. Traditional teaching methods and evaluation systems often fail to fully reflect students' learning status and needs. Fine-grained Sentiment Analysis (FGSA) is an advanced emotion recognition technique that focuses on identifying and understanding an individual's specific emotional state in a particular context. Therefore, to improve the quality of education and student learning outcomes, this study establishes a Sentiment-change-trend-based Behavioral Prediction Model (SBPM) based on the FGSA method to analyze SLB.

This study innovatively utilizes the FGSA method to construct a multi-polar emotion assessment model for analyzing students' emotional changes. Based on the analysis results of the model, an SBPM model is constructed to predict and analyze SLB. The main contribution is the design of a fine-grained multi-level sentiment evaluation model. Based on the results of this model, predicting and analyzing SLB can help educators and participants develop more efficient teaching and learning methods.

2 Related works

FGSA is an emerging emotion analysis technology. Luo et al. employed deep learning sentiment analysis to ascertain the experiences of diverse guests who had evaluated Chinese economy hotels. The location factor

received the highest praise, while negative emotions were mostly focused on facility details. This study provided a new method for understanding customer experience and discussed the significance of management theory and practice [7]. Wang Y et al. proposed a method of automatically constructing a fine-grained sentiment dictionary to improve the performance of sentiment analysis. This dictionary achieved significantly better F1 scores in emotion and sentiment analysis on multiple datasets [8]. Zhu S et al. proposed a customer hearing system that combines sentiment analysis and redesign mechanisms to improve the accuracy of product redesign. The system enhanced accuracy through ontology and professional knowledge and has been successfully applied to smartphone cases, verifying its effectiveness and providing reliable product redesign strategies [9]. Wang Z et al. proposed the MiMuSA method to enhance the granularity and interpretability of sentiment analysis. This method imitated the process of human language comprehension and identified multiple types of emotions through a multi-level modular structure. MiMuSA outperformed existing methods in accuracy and F1 Score [10]. Zhang H et al. proposed a lightweight regression model that combines statistical distribution and autoencoder to improve fine-grained financial prosperity analysis. This model significantly outperformed the baseline in news and Weibo data, with low computational overhead, while emphasizing the importance of dictionary methods [11] (Table 1).

Table 1: Summary of surveys related to fine-grained sentiment analysis

Author	Achievement	Deficiency
Luo J et al.	Discussed the role of sentiment analysis in hotel management	Not considering the emotional impact of hotel services on customers
Wang Y et al.	Constructed a new fine-grained sentiment dictionary	The new dictionary has low universality and is only applicable to certain fields
Zhu S et al.	Optimized the design strategy of smartphones using customer sentiment analysis	Not considering the usage habits of different customers
Wang Z et al.	Improved interpretability of FGSA	Only focus on the interpretability of language sentiment analysis
Zhang H et al.	Established a fine-grained emotional financial analysis model	The sentiment dictionary used does not focus on emotions with small fluctuations

SLB can reflect students' learning status. Fan J et al. proposed a deep learning recommendation method based on a multi-attention mechanism to improve the MOOC learning experience and reduce dropout rates. This model could effectively analyze learning behavior and recommend personalized MOOCs, improving the interpretability of recommendations [12]. Ikawati Y et al. proposed a learning style prediction model based on the ensemble tree method by analyzing Moodle logs and ILS questionnaire data to improve the efficiency of e-learning and personalized teaching. This model significantly improved classification accuracy compared to the single tree model [13]. Wang J et al. proposed a comprehensive review and classification method using natural driving research combined with computer vision technology to study driver distraction and safety issues. This method effectively identified driver behavior and revealed technological gaps in future research [14]. Mizael T M et al. proposed four contributions from Brazilian researchers to explore the relationship between racial issues and behavioral analysis in Brazil. These contributions underscored the perils of racial bias, stereotypes, and systemic racism, as well as novel approaches to measuring bias. They also advocated for enhanced international collaboration [15]. Wilder D A et al. proposed the role of response effort as an independent variable in addressing target responses in behavioral analysis. Clinical applications could reduce bad behavior and increase ideal behavior, while organizational applications could improve safety and recovery efficiency. The impact mechanism and future research directions were discussed [16] (Table 2).

Table 2: Survey summary of learning behavior analysis

Author	Achievement	Deficiency
Fan J et al.	Established a MOOC recommendation model based on LBA	Not paying attention to the impact of emotional changes on SLB
Ikawati Y et al.	Established a learning style prediction model	Not paying attention to students' emotional changes
Wang J et al.	Established a behavior analysis model based on computer vision	Not paying attention to changes in target emotions
Mizael T M et al.	Established a behavior analysis model based on historical factors	Only focus on historical legacy factors
Wilder D	Corresponding behavior	Not considering the impact

A et al.	analysis models were established based on response efforts	of personal emotional factors on behavior

In summary, existing research is deficient in its consideration of emotional states and their impact on learning behavior. This deficiency results in an inability to fully reflect the true learning status and needs of students. Moreover, the limited universality and applicability of the dictionaries used in sentiment analysis limit the wide applicability of the analysis results. In addition, existing research often overlooks students' personal usage habits and multidimensional emotional analysis. This results in an inability to fully capture the subtleties of emotional fluctuations and a deficiency in the comprehensive analysis and forecasting of students' emotional trajectories. These restrictions have affected a deeper understanding and effective intervention of SLB. Accordingly, the study assesses students' multi-level emotional states by developing a multi-polar emotional dictionary and anticipates SLB states based on the assessment outcomes. This approach aims to facilitate more precise methods for examining students' emotional and behavioral patterns.

3 Construction of a SLB prediction model based on emotion analysis

3.1 Construction of student emotional assessment model based on FGSA

The construction of a student emotional assessment model is aimed at evaluating and analyzing the emotional state of students, and analyzing the trend of student emotional changes based on the results of students' multi-polar emotional assessment. FGSA can identify and distinguish subtle differences in human emotions. When using this method to construct a student emotion assessment model, it is necessary to build an emotion dictionary [17]. According to the natural emotion differentiation method, human emotional perception can be divided into eight basic emotions. Based on eight basic emotional feelings, scholars have constructed a multi-level emotional dictionary. However, when translated into other language dictionaries, this dictionary contains a large number of synonyms that cannot reflect emotional levels. Therefore, it is necessary to perform synonym matching and weighting on the dictionary. The synonym matching and weighting method for the designed dictionary is shown in Figure 1.

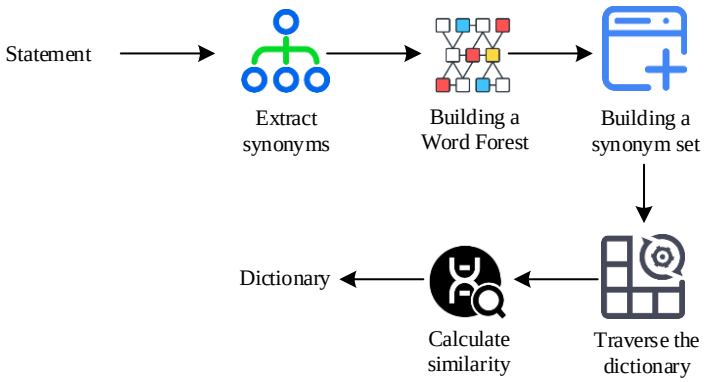


Figure 1: Dictionary synonym matching and empowerment process

The matching of synonyms is a fundamental step in building a multi-level emotion dictionary. The study chooses a synonym matching algorithm based on WordNet, which is a linguistic database that provides synonym relationships between words and a hierarchical structure of word meanings. When matching and weighting synonyms, it is necessary to calculate the similarity of word meanings. When calculating the similarity of word meanings, the first is to extract emotional words from the dictionary and use them as matching target words for synonyms. In the matching interval for extracting target words, some emotional words are selected to form a synonym set, and then the similarity between the extracted target words and the synonym set is calculated according to equation (1) [18, 19]. For the calculation of word meaning similarity, the cosine similarity algorithm is used in the study. Cosine similarity is a similarity measure that measures the angle between two non-zero vectors, suitable for distance calculation in high-dimensional spaces. The calculation of word meaning similarity comprehensively considers the similarity of word meanings and their structural distance in the dictionary. Through this method, synonyms can be more accurately identified and matched, providing a foundation for building a multi-level emotion dictionary.

$$sim\left(w_i, w_j\right) = m_l \cos\left(\frac{p \cdot \pi}{180}\right)\left(\frac{p-q+1}{p}\right) \quad (1)$$

In equation (1), p is the number of nodes contained in the first branch layer of synonyms. $sim(w_i, w_j)$ is the similarity between the target word and the matching word. q is the branch distance between the target word and the matching word in the first branch layer. The setting of this parameter reflects the emphasis on the distance factor in synonym similarity calculation. A smaller q value means a shorter distance, resulting in a higher similarity score. m_l is the similarity coefficient at the same level as the target word. The above operation is repeated until all sentiment words in the initial dictionary are traversed. Then, based on the similarity calculation results, the initial dictionary is divided into three different similarity subsets: high, medium, and low, as shown in equation (2).

$$\begin{cases} C(w_i, N)_g, & sim(w_i, w_j) \in [0.85,1] \\ C(w_i, N)_z, & sim(w_i, w_j) \in [0.65,0.85] \\ C(w_i, N)_d, & sim(w_i, w_j) \in [0,0.65] \end{cases} \quad (2)$$

In equation (2), $C(w_i, N)_g$ is a high similarity subset. $C(w_i, N)_z$ is a subset of medium similarity. $C(w_i, N)_d$ is a low similarity subset.

All elements in the high similarity subset are weighted to extract the emotional strength of the target word similarity. When setting the weights in the similarity subset, the coefficient is 0.85. The weight of the elements in the similarity subset is 0.85 times the weight of the extracted target word. The low similarity subset is directly deleted. Students' emotions during the learning process will constantly change as the course progresses. In the multi-polar sentiment dictionary, the emotional changes of students are shown in Figure 2.

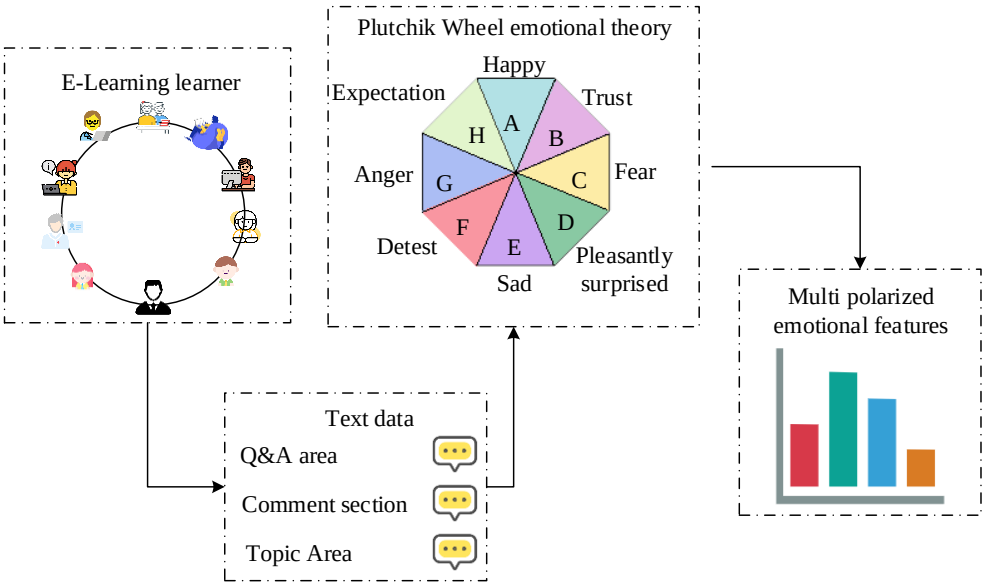


Figure 2: The emotional changes in different stages of learning

The data collection for FGSA mainly comes from text data of students' online Q&A and discussions. The preprocessing process first involves data cleaning, including merging text, constructing a set of language segments, and segmenting them according to the length of the course. Subsequently, the merged segments are subjected to sentence segmentation and word segmentation, and a sentence word vector is constructed after removing stop words. In terms of feature extraction, the study uses a multi-polar sentiment dictionary to match and modify sentiment words, while considering factors such as punctuation marks, sentiment word strength, emoticons, degree adverbs, negative words, transitional conjunctions, and progressive conjunctions. By calculating the quantitative value of sentiment strength in sentences, a multi-level sentiment vector is constructed to analyze students' emotional changes at different learning stages [20]. Data cleaning requires merging the text and constructing a set of segments based on different course levels, as shown in equation (3).

$$U(L_i) = \{prgh_1, \cdots, prgh_T\} \quad (3)$$

In equation (3), $U(L_i)$ is a set of language segments for a student. $prgh_T$ is the first student to

participate in the discussion of text merging paragraphs in the course. T is the length of the course. After merging the texts, the paragraphs are divided according to equation (4).

$$S(prgh_t)=\{stat_1,\cdots,stat_j\} \quad (4)$$

In equation (4), $S(prgh_t)$ is the statement set. j is the statement index. After completing the sentence segmentation, the sentence is segmented and stop words are removed to construct a sentence word vector, as shown in equation (5).

$$V(stat_j)=\{word_1,\cdots,word_o\} \quad (5)$$

In equation (5), $V(stat_j)$ is a word vector. $word$ is a word. o is a word index. Finally, based on the multi-polar sentiment dictionary, sentiment words are matched and modified. After processing the raw data, the stage specific emotional intensity of students can be quantified based on their learning stage. The quantitative calculation of the emotional intensity of a statement is shown in equation (6).

$$p(stat_j)=\begin{cases}\sum_{o=1}^{O}\left(w_j\prod_{k=1}^{K}\varepsilon_k\mu+sym_{E\_fc}(\omega)+sym_{E\_fc}(\delta)\right)\sigma, & if \quad \sigma \quad appeared\\ \sum_{o=1}^{O}\left(w_j\prod_{k=1}^{K}\varepsilon_k\mu+sym_{E\_fc}(\omega)+sym_{E\_fc}(\delta)\right)\tau, & if \quad \tau \quad appeared\end{cases} \quad (6)$$

In equation (6), $p(stat_j)$ is the quantified value of emotional intensity. $sym_{E\_fc}(\delta)$ is the intensity of punctuation modification. w_j is the emotional intensity of emotional words. O is the number of sentiment words in the sentence. $sym_{E\_fc}(\omega)$ is the intensity of modification in emoticons. ε_k is the modifier strength of degree adverbs. μ represents the strength of negative word modification. σ is the modifying strength of transitional conjunctions. τ is the modifying strength of progressive conjunctions. The quantitative calculation of emotional intensity integrates various factors such as emotional words, facial expressions, and degree adverbs. The weight setting of each parameter is based on linguistic and psychological research to ensure accurate quantification of emotional intensity. According to equation (6), the multi-level emotion vector of students during the course hours can be calculated, as shown in Figure 3.

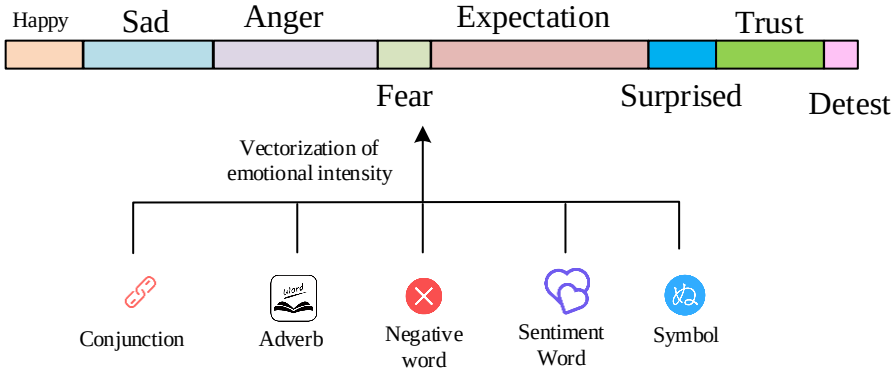


Figure 3: Phdic multi-level emotion vectorial representation of learners

Happiness and sadness, anger and tragedy, expectation and surprise, trust and disgust are four pairs of bidirectional emotions. If the calculation result of the sentence sentiment vector is negative, the corresponding sentiment will be reversed to the corresponding bidirectional sentiment. A multi-polar emotional state change chain is established based on students' dominant emotions at different stages. The expression for judging students' emotional tendencies based on the emotional chain is shown in equation (7). This equation is used to determine students' emotional tendencies at a specific stage of learning. By analyzing the frequency of different types of emotions, it is possible to identify the dominant emotions in a specific learning stage, which is crucial for understanding students' emotional trends and predicting their learning behavior.

$$Sent_{tend}(L_i)=\max(Dmt_{pst,I}-freq) \quad (7)$$

In equation (7), $Sent_{tend}(L_i)$ represents the emotional inclination of the student. I is the frequency of dominant emotions in the current course progress. The setting of emotional tendency parameters is based on the analysis of the trend of students' emotional state changes.

Studying the frequency of dominant emotions at different stages to determine students' emotional tendencies can help predict changes in their behavior.

3.2 Construction of learning behavior prediction model based on SBPM

Based on FGSA, the results of student multi-polar emotional assessment can be used to analyze students' emotional trends. The emotion assessment model first identifies students' emotional states through FGSA techniques. This technology can identify and distinguish specific emotions of students in specific learning contexts, such as happiness, sadness, anger, etc. By constructing a multi-level emotion dictionary and quantifying the emotional intensity of sentences, the model can track students' emotional changes at different learning stages and identify patterns of rising, falling, or fluctuating emotions. A predictive model is constructed by combining students' emotional trends with learning behavior data, thereby enabling the prediction of their learning behavior based on their emotional state. If the student can graduate smoothly, there is no need to intervene in their learning behavior. If there are certain difficulties for students to graduate successfully, their learning behavior can be adjusted based on the results of emotional analysis. The algorithm logic is shown in Figure 4.

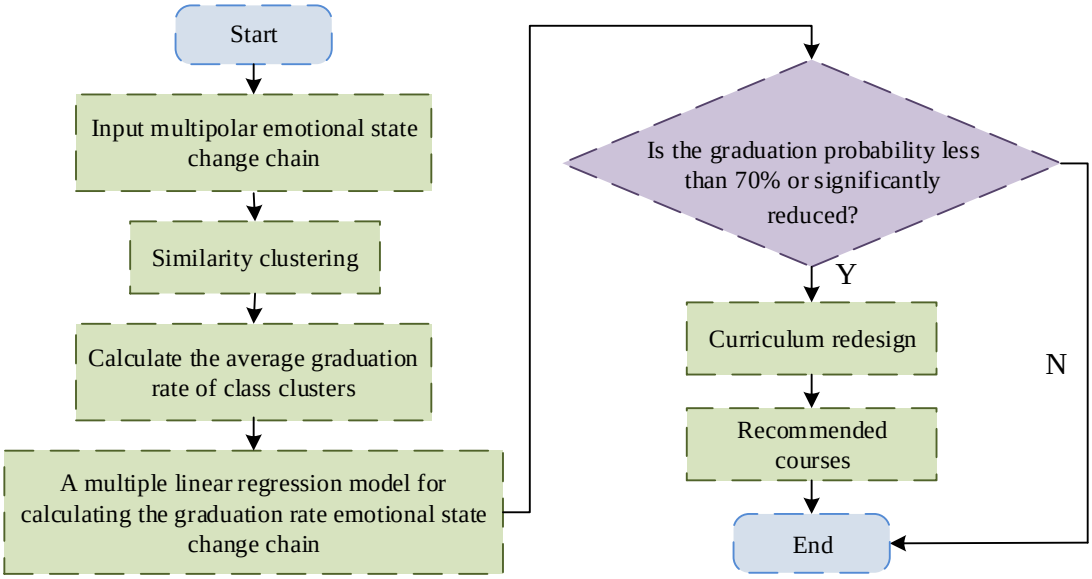


Figure 4: Algorithmic logic of the SBPM model

The construction of the SBPM model is intended to facilitate the analysis of SLB states by leveraging the emotional results of the student emotional assessment state model. This analysis is designed to assist educators in adapting their instructional content to align with students' emotional needs. When using the SBPM model to analyze the graduation rates of different students, it is necessary to perform similarity clustering on student emotions to calculate the average graduation probability of different students. When calculating the graduation probabilities of different students, it is needed to first normalize the student data to weaken the impact of extreme situations on the final calculation results. The normalization formula is shown in equation (8) [21, 22].

$$Dmt_{pst} - c(L_i) = \frac{Dmt_{pst}(v_1), \cdots, Dmt_{pst}(v_T)}{\max\left(Dmt_{pst}(v_t)\right) - \min\left(Dmt_{pst}(v_t)\right)} \tag{8}$$

In equation (8), $Dmt_{pst} - c(L_i)$ is the chain of changes in students' emotional states. $Dmt_{pst}(v_t)$ is the emotional intensity value. When determining whether a student can graduate, it is necessary to decompose their graduation status into levels based on the similarity of their multi-polar emotions. This study uses the cosine similarity method to calculate the cosine similarity between different students, as shown in equation (9) [23].

$$dist\left(Dmt_{pst}-c\left(L_i\right),Dmt_{pst}-c\left(L_j\right)\right)=\frac{\sum_{t=1}^{T}Dmt_{pst,i}\left(v_t\right)Dmt_{pst,j}\left(v_t\right)}{\sqrt{\sum_{t=1}^{T}Dmt_{pst,i}\left(v_t\right)^2}\sqrt{\sum_{t=1}^{T}Dmt_{pst,j}\left(v_t\right)^2}} \quad (9)$$

In equation (9), $dist\left(Dmt_{pst}-c\left(L_i\right),Dmt_{pst}-c\left(L_j\right)\right)$ is the similarity between student i and j. $Dmt_{pst,i}\left(v_t\right)$ is the normalized emotional intensity of i during class t. Student clustering analysis needs to be based on the similarity calculation results. During clustering analysis, the clustering radius is calculated using equation (10).

$$R=\Gamma\left(n\right)\frac{1}{\sqrt{\pi^n}}\frac{1}{n}\sqrt{\prod_{i=1}^{n}\prod_{j=1}^{n}dist\left(Dmt_{pst}-c\left(L_i\right),Dmt_{pst}-c\left(L_j\right)\right)} \quad (10)$$

In equation (10), R is the clustering radius. n is the size of the sample set. $\Gamma\left(n\right)$ is the gamma function. Finally, with the goal of increasing the probability of students graduating, a predictive model function can be constructed. The constructed prediction target multiple linear regression model is shown in equation (11).

$$Gp\left(L_i\right)=\beta_0+\sum_{t=1}^{T}\beta_t Dmt_{pst}-c\left(L_i\right)\left[t\right] \quad (11)$$

In equation (11), $Gp\left(L_i\right)$ is the student graduation probability output by the model. β is the partial regression coefficient. $Dmt_{pst}-c\left(L_i\right)\left[t\right]$ is the element value in the chain of students' multi-polar emotional state changes. When using this model to predict and analyze the graduation probability of students, the model loss needs to be considered, and the constructed loss function is shown in equation (12). This equation defines the loss function of the model, which measures the difference between the predicted and actual values of the model. The loss function is the main objective of optimization during the model training process. By minimizing the loss function, the model parameters can be adjusted to improve the accuracy of predictions.

$$Loss\left(\beta_0,\ldots,\beta_T\right)=\sum_{i=1}^{n}\left(Gp\left(L_i\right)-Gpat\left(L_i\right)\right)^2 \quad (12)$$

In equation (12), $Loss\left(\beta_0,\ldots,\beta_T\right)$ is the model loss. $Gpat\left(L_i\right)$ is the actual probability of students graduating. The research model is designed with universities as the target users, with a large number of students. Concurrently, students exhibit a spectrum of emotional fluctuations, rendering the data samples inherently multidimensional. This complexity precludes the application of conventional numerical computation techniques for model resolution. Mini-batch Gradient Descent (MBGD) uses a small batch of data samples per iteration to calculate the average gradient, rather than using the entire training set like Batch Gradient Descent (BGD) or only one sample like Stochastic Gradient Descent (SGD) [24, 25]. This method strikes a balance between computational efficiency and convergence speed, but it uses a fixed learning rate to solve the model, resulting in lower solving efficiency. Learning Rate Warm Restarts (LRWR) is a strategy for dynamically adjusting learning rates. It allows the learning rate to periodically increase and decrease during the training process, rather than simply decaying linearly or exponentially according to a predetermined decay strategy. Accordingly, this study proposes to enhance the MBGD with LRWR and refine the coefficients of the SLB prediction model through the implementation of the proposed algorithm, thereby optimizing the model's computational precision and efficiency. The improved MBGD algorithm flow is shown in Figure 5.

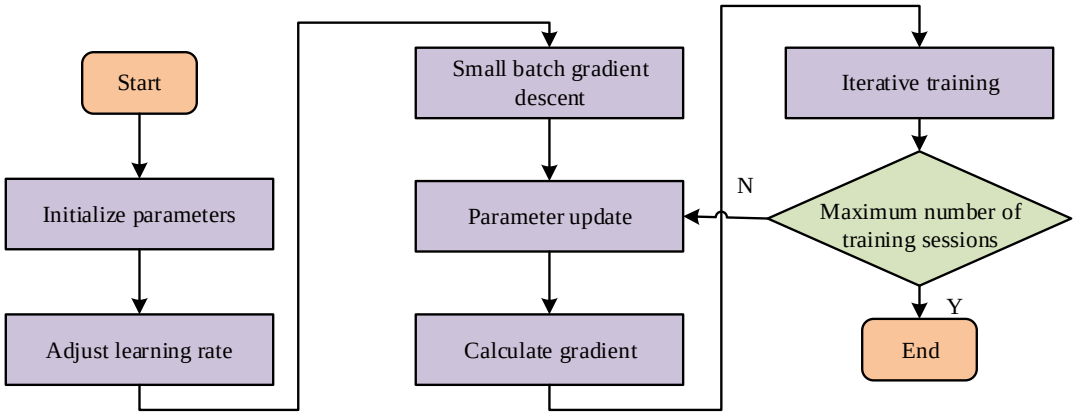


Figure 5: Model solving process for improving the MBGD algorithm based on LRWR

Improving the MBGD algorithm requires initializing the model parameters, adjusting the initial learning rate, and determining the batch size when solving the model. The data samples are divided based on batch size. Before each iteration of training starts, the order of the dataset is randomly shuffled, and small batches of data are sampled according to batch size to begin iterative training. During the training process, it is necessary to calculate the gradient and update the algorithm parameters based on the gradient. Finally, the above steps are repeated until the algorithm performance meets the requirements or reaches the maximum number of iterations. In this algorithm, when updating the learning rate, this study uses the sigmoid function to slow down the learning rate to reduce the problem of algorithm efficiency caused by a fixed rate decrease in the learning rate. When using the above method to update the partial regression coefficients of the model, the update function formula is shown in equation (13).

$$\beta_{t\_updt} = \beta_t + \frac{Lr_t}{b}\sum_{k=i}^{i+b-1}\left(Gp(L_k) - Gpat(L_k)\right)\times Dmt_{pst} - c(L_k)[t] \quad (13)$$

In equation (13), β_{t_updt} is the updated value of the partial regression coefficient. b is the sampling interval for students. In the development of the SBPM model, the parameter adjustment steps include initializing the model parameters, setting an appropriate initial learning rate, and determining the batch size in MBGD. Subsequently, the dataset is divided into small batches of samples and the order of the dataset is randomly shuffled before each iteration to enhance the model's generalization ability. During the iterative training process, the gradient of each small batch of data is calculated and the model parameters are updated. At the same time, the learning rate and batch size are dynamically adjusted based on the performance evaluation results to optimize the model. Furthermore, a learning rate hot restart strategy is employed to facilitate periodic adjustments to the learning rate, thereby preventing the phenomenon of local minima. Additionally, a sigmoid function is utilized to decelerate the learning rate, thus enhancing the efficiency of the solution process. Finally, when the model loss drops to the preset threshold or reaches the maximum number of iterations, training is stopped to ensure that the model is both accurate and efficient.

4 Simulation analysis of SLB prediction model based on emotion analysis

4.1 Analysis of student emotional assessment model based on FGSA

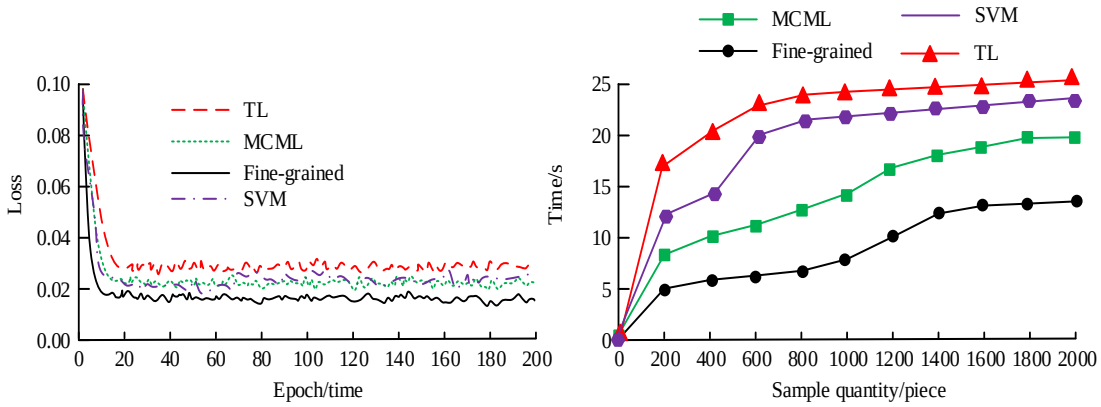
When conducting simulation analysis on the student emotional assessment model, this study randomly selects discussion texts from 2,500 students in a university during 12 hours of a certain course on an electronic learning platform as data samples. Among them, there are a total of 18,564 text data records. Table 3 shows the specific experimental configuration for training and simulation testing of the model.

Table 3: Experimental environment of student emotion assessment model simulation

Item	Type	Item	Type
Operating system	windows10	Programming Language	Java
Memory	2T	Programming type	Single threaded

			compilation
CPU	i7-7700k	Simulation platform	MATLAB
Equipped with RAM	16GB	Programming Library	Apache NetBeans

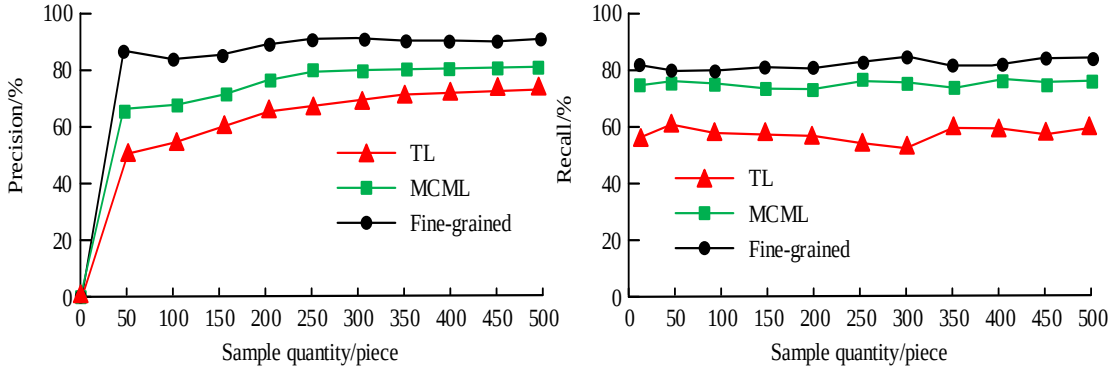
The research model (FGSA) is mainly used for sentiment classification. Pan W et al. proposed an emotion splitting model based on Multi-class Machine Learning (MCML) model. Cao Z et al. proposed an emotion classification method based on Transfer Learning (TL). To verify the effectiveness of the research model, the performance of three algorithms is compared. The changes in model loss value and evaluation efficiency are shown in Figure 6.



(a) Comparison results of model loss values (b) Comparison results of model efficiency

Figure 6: Model loss value of several computational efficiency comparison

Figure 6 (a) shows the changes in loss values for the three models. FGSA completes convergence in the 10th iteration and the loss value after model convergence can be reduced to below 0.02. Both MCML and TL converge at the 20th iteration, with MCML able to reduce the loss value to around 0.25, while TL maintains the loss value at around 0.03 after convergence. The convergence effect of the SVM benchmark model is also lower than that of the research model. FGSA has a faster convergence speed and a lower loss value after convergence. Figure 6 (b) shows the comparison results of emotion classification efficiency among three models. As the number of data samples increases, the time required for all three models to complete sentiment classification is also increasing. When the data volume increases to 2,000, FGSA takes about 12s to complete the sentiment classification task, MCML takes about 17s to complete the classification of all data, and TL takes more than 20s. Compared to MCML, the efficiency of FGSA has increased by nearly 30%. The SVM model also maintains a time consumption of around 20 seconds to complete the emotion classification task. Figure 7 compares the accuracy and recall of three models.



(a) Comparison results of model precision values (b) Comparison results of model recall values

Figure 7: Comparison of model precision and recall rate

Figure 7 (a) shows a comparison of the accuracy of three models. The accuracy of FGSA basically does not change with the number of data samples, and overall remains around 0.82. The accuracy of MCML and TL both increases with the increase of data sample size, with the highest accuracy of MCML being about 0.78 and the

accuracy of TL being about 0.61. Figure 7 (b) shows the recall rates of the three models, which are largely unaffected by the number of data samples. The recall rate of FGSA remains at around 0.81, while MCML is slightly lower at around 0.78, and TL is much lower than these two models, with a recall rate of only around 0.60. Compared with other current emotion classification algorithms, the FGSA model always maintains a higher level of accuracy and recall when evaluating student emotions.

4.2 Construction of learning behavior prediction model based on SBPM

When conducting simulation analysis on the SBPM model, the experimental environment used is consistent with the student sentiment assessment model. The experimental data for this model also come from online learning platforms. To verify the applicability of the model in different environments, this study extracts data from online learning platforms of universities. In addition to the data from the simulation analysis of the student emotional assessment model, data from students of different grades in another university are also extracted. In this study, the first extracted data will be named Data 1, and the second extracted data will be named Data 2. Table 4 shows the parameter information of all algorithms, including the SBPM model.

Table 4: Algorithm parameter setting

Name	Value	Name	Value
Sampling interval	10	Duration of class hours	12
Convergence threshold	0.01	Data 1	2500
Iterations	10000	Data 2	2500

By modifying the sampling interval, the quantity of data utilized on each occasion that the model parameters are updated can be regulated. A smaller sampling interval can accelerate the model's adaptation speed to new data, but it may lead to increased fluctuations during the training process. A larger sampling interval can make the model update smoother and help the model converge stably. The implementation of an appropriate convergence threshold is an effective method for ensuring that the model terminates its training process at a predetermined level of accuracy. This approach helps to prevent the unnecessary expenditure of computational resources and the potential overfitting of the model to the training data. Setting an upper limit on the number of iterations can prevent overfitting of the model on the training data. By limiting the number of iterations, the complexity of the model can be controlled to some extent, enabling the model to have better generalization ability on unseen data. The choice of batch size directly affects the stability and convergence speed of model training. Through experiments and parameter tuning, a suitable batch size can be selected to enable the model to converge quickly and maintain good generalization performance during training. The algorithm used in the SBPM model is the MBGD algorithm, which is a common gradient descent algorithm. Therefore, when selecting the comparison algorithm, this study compares the performance of the original MBGD, SGD, and traditional Gradient Descent algorithm (GD). The Mean Square Percent Error (MSPE) results of different algorithms on two datasets are displayed in Figure 8.

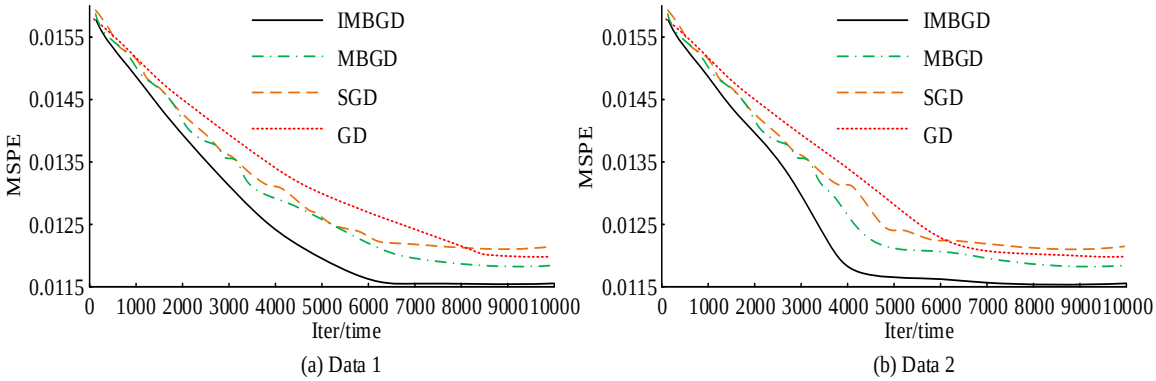


Figure 8: Comparison results of MSPE values for different algorithms

Figures 8 (a) and (b) show the MSPE convergence of four algorithms on Data 1 and Data 2. In Figure 8 (a), as the iteration increases, the MSPE values of all algorithms decrease accordingly. After the MBGD algorithm converges, its MSPE value can be reduced to around 0.0115. The MSPE values of the remaining algorithms after convergence are around 0.012. In Figure 8 (b), on the Data 2 dataset, the convergence speed of all algorithms will accelerate, and the MSPE value of the converged algorithm will also decrease to a certain extent. Figure 9 shows the efficiency comparison of four algorithms on two datasets.

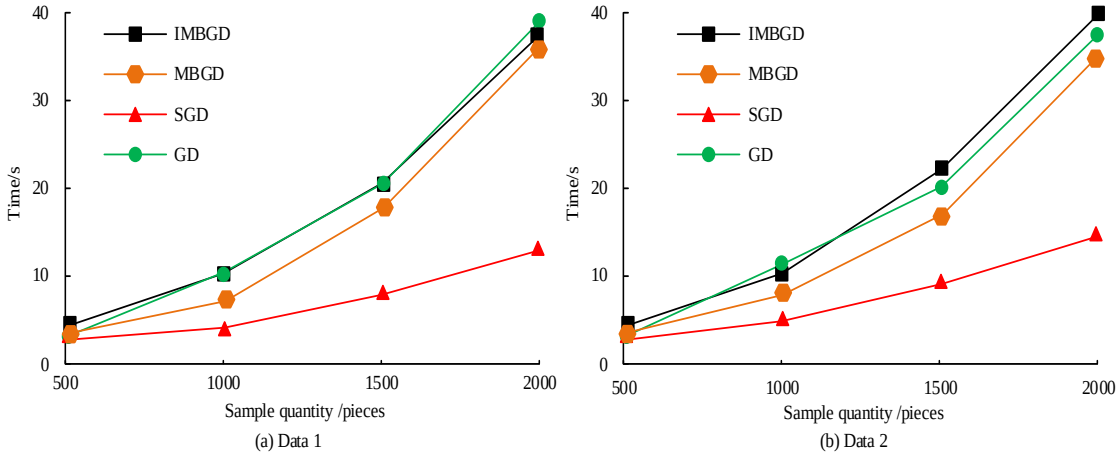


Figure 9: Time-cost comparison results for the different algorithms

Table 5: Comparing the results of the F1 to and accuracy of the four algorithms

Model	Date 1		Data 2	
	F1	Accuracy (%)	F1	Accuracy (%)
IMBGD	0.964	97.4	0.959	98.4
MBGD	0.918	92.3	0.906	91.1
SGD	0.906	91.1	0.911	92.1
GD	0.867	89.7	0.877	90.7

Figure 9 (a) shows the time cost of the algorithm on Data 1 and Data 2. In Figure 9 (a), SGD takes the shortest time to complete LBA tasks, while the time difference between other algorithms is relatively small. SGD only takes about 10 seconds to complete LBA for 2,000 samples, while other algorithms take around 35 seconds. In Figure 9 (b), SGD has the shortest time consumption, the rest of the time costs have increased to a certain extent, while MBGD has the most significant increase in time cost. The study further compares the F1 values and accuracy of four models, and the results are shown in Table 5. By comparing the F1 scores and accuracy of different models on different datasets, the generalizability of the research model in the field of education can be further validated.

As shown in Table 5, the IMBGD algorithm achieves an F1 value of 0.95 or above, while maintaining an accuracy of over 97% in both datasets. The F1 values of the other three algorithms remain around 0.90, while the accuracy remains around 90%. The performance of the IMBGD algorithm is significantly better than the other three algorithms. In Data 1 and Data 2, this study randomly selects 10 students who are predicted to be unable to graduate, analyzes their graduation probabilities, and compares their graduation probabilities after receiving recommended learning behaviors, as shown in Figure 10.

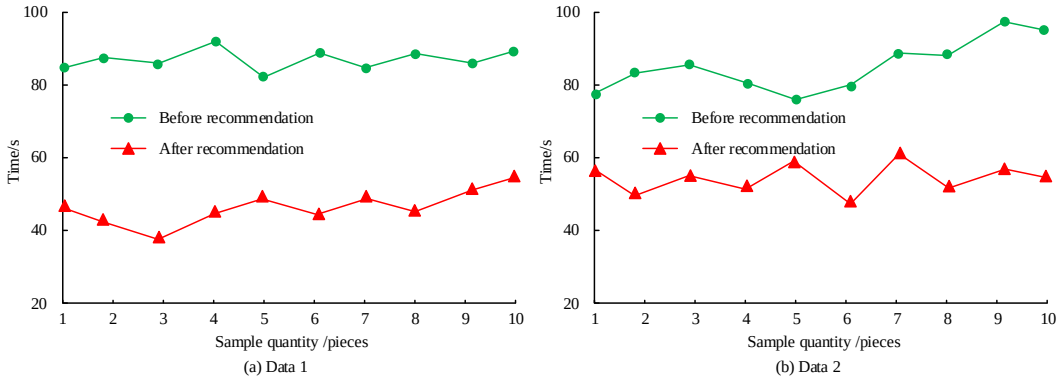


Figure 10: Comparison of student graduation probability change

Figures 10 (a) and (b) show the changes in graduation rates of 10 students in two datasets after receiving learning behavior recommendations. In Figure 10 (a), the graduation rate of students remains around 50% before accepting the school's recommendations for changing their learning behavior. After accepting the

school's advice and correcting their own learning behavior, the graduation rate of all students has reached over 80%, and even some students have a graduation rate of 90%. In Figure 10 (b), the graduation rate is similar to the changes in students in Data 1, and the changes are more pronounced. Taking X High School as an example, the study selects 10 different classes and uses the designed model to predict the learning behavior of students in these classes. Based on the predicted learning behavior results, the students' learning courses are adjusted. The results are shown in Table 6.

Table 6: Practical application effect of the design model in X High school

Class ID	Class graduation rate (%)	Class ID	Class graduation rate (%)
1	98	6	100
2	100	7	100
3	99	8	98
4	98	9	100
5	100	10	99

As shown in Table 6, after applying the research model to this experimental class, the graduation rate of all classes can reach 98% or above. This suggests that the research model can also be effectively applied in practical settings to predict SLB, allowing for the adaptation and optimization of course content based on current learning behaviors, with the aim of enhancing students' learning outcomes.

5 Discussion

The study has achieved significant results in the field of SLB analysis by combining FGSA and SBPM. The FGSA model provides key inputs for the SBPM model by accurately identifying and quantifying students' emotional changes during the learning process. Compared with existing methods, the research model achieved an accuracy of over 80% in emotion recognition, largely due to the construction of a multi-level emotion dictionary and the application of synonym matching and weighting methods. Compared with the SOTA solution mentioned in related work, the research model performed well in both accuracy and recall of sentiment analysis. For example, compared with MCML and TL models, the research model has improved efficiency by nearly 30% in sentiment classification tasks and has lower loss values. The observed performance differences stem from multiple factors. Firstly, the research model emphasizes the granularity of emotion analysis during the construction process, which enables the model to more accurately capture subtle changes in students' emotions. Secondly, advanced optimization strategies are adopted in the model training, which help the model to break out of local minima and find better solutions during the training process. The model fully considers individual differences among students during design and improves its applicability and accuracy through personalized emotional assessment and behavior prediction. In education, accurate prediction of learning behavior can help teachers and educational administrators better understand students' learning needs, thereby designing more effective teaching strategies and intervention measures. In addition, the potential of this model in improving student learning efficiency and graduation rates provides universities with a new tool to optimize educational resource allocation and curriculum design. In the long run, this emotion-based learning behavior prediction method is expected to play a greater role in personalized education and lifelong learning.

6 Conclusion

To improve the level of higher education and enhance students' study habits, this study constructed a student emotional assessment model based on FGSA technology. This model could analyze the emotional trends of students during the learning process. Based on the trend of student emotional changes output by the emotional assessment model, this study constructed an SLB predictive analysis model. The model used cluster analysis to preprocess the sample data and constructed an objective function based on the linear regression equation. When solving the objective function, an improved MBGD algorithm was used. The results showed that the research model achieved an accuracy of over 80% in analyzing students' emotions, while also stabilizing the algorithm's recall rate at around 80%. The emotional evaluation model could reduce the loss value to below 0.02 when analyzing students' emotions while keeping the calculation time within 15 seconds. The student LBA prediction model could reduce the loss value to around 0.0115 when predicting and analyzing SLB, but the time consumption was relatively high, requiring more than 35s. After providing special tutoring to students based on SLB prediction analysis results, the graduation rate of students could significantly increase. Universities could provide additional tutoring and correction to students based on the predicted results of SLB, effectively improving the teaching level of universities. However, the designed SLB prediction model has a high computational time when analyzing predictive learning behavior. In the future, the model-solving method will be further optimized to reduce the time cost of model-solving.

Funding statement

The Basic Research ability Improvement Project of young and middle-aged teachers in Guangxi Universities in 2024, "Research on Job Stress on turnover intention of

College Teachers - Based on the moderated mediating Effect" (Project No. 2024KY0189).

References

[1] Ahmad Z, Bangyal W H, Nisar K, Haque M R, Khan M A. (2022). Comparative analysis using machine learning techniques for fine grain sentiments. *Journal on Artificial Intelligence*, 4(1): 49-60. https://doi.org/10.32604/jai.2022.017992

[2] Zhang W, Wang H, Song M, Deng S. (2023). A method of constructing a fine-grained sentiment lexicon for the humanities computing of classical chinese poetry. *Neural Computing and Applications*, 35(3): 2325-2346. https://doi.org/10.1007/s00521-022-07690-8

[3] Clay C J, Schmitz B A, Balakrishnan B, Hopfenblatt J P, Evans A, Kahng S. (2021). Feasibility of virtual reality behavior skills training for preservice clinicians. *Journal of Applied Behavior Analysis*, 54(2): 547-565. https://doi.org/10.1002/jaba.809

[4] Kimball R T, Greer B D, Fuhrman A M, Lambert J M. (2023). Relapse and its mitigation: Toward behavioral inoculation. *Journal of Applied Behavior Analysis*, 56(2): 282-301. https://doi.org/10.1002/jaba.971

[5] Wang Y, Yang N, Miao D, Chen Q. (2023). Dual-channel and multi-granularity gated graph attention network for aspect-based sentiment analysis. *Applied Intelligence*, 53(11): 13145-13157. https://doi.org/10.1007/s10489-022-04198-5

[6] Mao R, Liu Q, He K, Li W, Cambria E. (2022). The biases of pre-trained language models: An empirical study on prompt-based sentiment analysis and emotion detection. *IEEE Transactions on Affective Computing*, 14(3): 1743-1753. https://doi.org/10.1109/TAFFC.2022.3204972

[7] Luo J, Huang S, Wang R. (2021). A fine-grained sentiment analysis of online guest reviews of economy hotels in China. *Journal of Hospitality Marketing & Management*, 30(1): 71-95. https://doi.org/10.1080/19368623.2020.1772163

[8] Wang Y, Huang G, Li M, Li Y, Zhang X, Li H. (2023). Automatically constructing a fine-grained sentiment lexicon for sentiment analysis. *Cognitive Computation*, 15(1): 254-271. https://doi.org/10.1007/s12559-022-10043-1

[9] Zhu S, Qi J, Hu J, Huang H. (2021). Intelligent product redesign strategy with ontology-based fine-grained sentiment analysis. *AI EDAM*, 35(3): 295-315. https://doi.org/10.1017/S0890060421000147

[10] Wang Z, Hu Z, Ho S B, Cambria E, Tan A H. (2023). MiMuSA-mimicking human language understanding for fine-grained multi-class sentiment analysis. *Neural Computing and Applications*, 35(21): 15907-15921. https://doi.org/10.1007/s00521-023-08576-z

[11] Zhang H, Li Z, Xie H, Lau R Y, Cheng G, Li Q, et al. (2022). Leveraging statistical information in fine-grained financial sentiment analysis. *World Wide Web*, 25(2): 513-531. https://doi.org/10.1007/s11280-021-00993-1

[12] Fan J, Jiang Y, Liu Y, Zhou Y. (2022). Interpretable MOOC recommendation: a multi-attention network for personalized learning behavior analysis. *Internet Research*, 32(2): 588-605. https://doi.org/10.1108/INTR-08-2020-0477

[13] Ikawati Y, Al Rasyid M U H, Winarno I. (2021). Student behavior analysis to predict learning styles based felder silverman model using ensemble tree method. *EMITTER International Journal of Engineering Technology*, 9(1): 92-106. https://doi.org/10.24003/EMITTER.V9I1.590

[14] Wang J, Chai W, Venkatachalapathy A, et al. (2021). A survey on driver behavior analysis from in-vehicle cameras. *IEEE Transactions on Intelligent Transportation Systems*, 23(8): 10186-10209.

[15] Mizael T M, Coelho C L, Rodrigues W C, et al. (2021). Racial issues and behavior analysis: Experiences and contributions from Brazil. *Behavior and Social Issues*, 30(1): 495-513. https://doi.org/10.1007/s42822-021-00071-1

[16] Wilder D A, Ertel H M, Cymbal D J. (2021). A review of recent research on the manipulation of response effort in applied behavior analysis. *Behavior modification*, 45(5): 740-768. https://doi.org/10.1177/0145445520908509

[17] Chan J Y L, Bea K T, Leow S M H, Phoong S W, Cheng W K. (2023). State of the art: a review of sentiment analysis based on sequential transfer learning. *Artificial Intelligence Review*, 56(1): 749-780. https://doi.org/10.1007/s10462-022-10183-8

[18] Anderson R, Taylor S, Taylor T, et al. (2022). Thematic and textual analysis methods for developing social validity questionnaires in applied behavior analysis. *Behavioral Interventions*, 37(3): 732-753. https://doi.org/10.1002/bin.1832

[19] Sadoughi M, Hejazi S Y. (2023). The effect of teacher support on academic engagement: The serial mediation of learning experience and motivated learning behavior. *Current Psychology*, 42(22): 18858-18869. https://doi.org/10.1007/s12144-022-03045-7

[20] Yang X, Zhang S, Liu J, Gao Q, Dong S, Zhou C. Deep learning for smart fish farming: applications, opportunities and challenges. *Reviews in Aquaculture*, 2021, 13(1): 66-90. https://doi.org/10.1111/raq.12464

[21] Gams M, Kolenik T. (2021). Relations between electronics, artificial intelligence and information society through information society rules. *Electronics*, 10(4): 514. https://doi.org/10.3390/electronics10040514

[22] Chang C W, Chang C Y, Lin Y Y. (2022). A hybrid

CNN and LSTM-based deep learning model for abnormal behavior detection. *Multimedia Tools and Applications*, 81(9): 11825-11843. https://doi.org/10.1007/s11042-021-11887-9

[23] Sharma T, Kaur K. (2023). A deep learning-fuzzy based hybrid ensemble approach for aspect level sentiment classification. *Informatica*, 47(6). https://doi.org/10.31449/inf.v47i6.4607

[24] Yuan Z. (2024). Consumer behavior prediction and enterprise precision marketing strategy based on deep learning. *Informatica*, 48(15). https://doi.org/10.31449/inf.v48i15.6260

[25] Cao Z, Zhou Y, Yang A, Peng S. (2021). Deep transfer learning mechanism for fine-grained cross-domain sentiment classification. *Connection Science*, 33(4): 911-928. https://doi.org/10.1080/09540091.2021.1912711

Attention-CNN with Multi-Task Learning for Chinese Named Entity Recognition

Yanhong Fu[1*], Fuwang Chen[2]
[1]School of Preschool Education, Nanyang Vocational College of Agriculture, Nanyang 473061, China
[2]School of Information Engineering, Nanyang Vocational College of Agriculture, Nanyang 473061, China
E-mail: fuyanhong0309@163.com
[*]Corresponding author

Keywords: attention mechanism, convolutional neural networks, chinese named entity recognition, bidirectional encoder representation from transformer, multi-task learning

Received: February 20, 2025

Named entity recognition serves as a cornerstone in natural language processing and has garnered extensive research attention due to its significance in various downstream applications. Owing to the intricate nature of Chinese texts, characterized by complex syntactic structures and the lack of explicit word boundaries, conventional NER methodologies often encounter difficulties in simultaneously optimizing recognition accuracy and computational efficiency. To address this issue, the study proposes a named entity recognition algorithm that integrates attention mechanisms with Convolutional Neural Networks, incorporates into a Transformer-based bidirectional encoder framework for training. A multi-head self-attention mechanism is employed to capture the global semantic information of the text, and multi-task learning is introduced to construct the final model. When evaluated on datasets with sample sizes of 200, 1000, and 3000, the proposed model consistently outperforms the baseline models in terms of precision, recall, and F1 score. Specifically, under the low-resource setting with 200 samples, the model achieves a precision of 98.62%, a recall of 98.10%, and an F1 score of 98.36%. In terms of inference efficiency, the model processes at a speed of 2618 tokens per second. The experimental results indicate that this method can be widely applied in various fields such as information extraction and text understanding, providing strong technical support for related research.

Povzetek: Model AC-MTL združuje pozornostne mehanizme, konvolucijske nevronske mreže in večopravilno učenje za kitajsko prepoznavo imenovanih entitet. Povezuje globalni pomen in lokalne značilnosti, odlikujeta ga robustnost in natančnost.

1 Introduction

Chinese Named Entity Recognition (CNER) is a fundamental task in Natural Language Processing (NLP), aiming to automatically identify entities with specific meanings within Chinese text. As Chinese information technology continues to advance, Named Entity Recognition (NER) has become a crucial technology in various applications, including information extraction, sentiment analysis, knowledge graph construction, intelligent question answering, and machine translation [1]. CNER is increasingly being utilized across various sectors, including finance, healthcare, e-commerce, and law. It provides crucial support for cross-domain data integration, information extraction, and intelligent applications [2]. With the rise of deep learning technologies, NER methods based on Convolutional Neural Networks (CNN), Recurrent Neural Networks, and Transformers have gradually become the mainstream in research [3]. However, CNER still faces significant challenges due to the unique structure of the Chinese language. Traditional NER methods based on dictionaries and machine learning still suffer from low universality and poor cross-regional recognition performance [4]. Bidirectional Encoder Representations from Transformers (BERT), built on the Transformer architecture, effectively captures deep contextual information from text, thereby improving the accuracy and generalization of entity recognition in complex contexts [5]. The Multi-Head Self-Attention Mechanism (MHSA) is particularly well-suited for capturing long-range dependencies and contextual relationships in Chinese text, enhancing NER accuracy by considering the global semantic information across the entire sentence [6]. To address the issues of low generalizability and suboptimal recognition performance in CNER, a novel recognition approach—Attention-Enhanced Convolutional Neural Network (Attention-CNN)—was proposed to improve recognition accuracy and optimize computational efficiency. The study also introduces Multi-Task Learning (MTL) to develop the final CNER hybrid model, named Attention-CNN with Multi-Task Learning for Chinese Named Entity Recognition (AC-MTL). By combining the advantages of MHSA and CNN, this study aims to simultaneously process global semantics and local features. The AC-MTL model provides an effective and feasible new

method to improve the performance and accuracy of CNER.

2 Related works

With the advent of the information age, CNER has emerged as a crucial task in natural language processing, aiming to extract specific types of entities—such as person names, locations, and organizations—from unstructured text [7]. The lack of clear word boundaries in Chinese, combined with semantic ambiguity, nested entities, and long-distance dependencies, has long made CNER a challenging problem. Early research in NER primarily relied on statistical learning approaches such as Conditional Random Fields (CRF) and Hidden Markov Models (HMM), which were heavily dependent on hand-crafted features and lacked generalizability in complex scenarios [8]. Later on, deep learning approaches took center stage. Notably, the BiLSTM-CRF framework proposed by Huang et al. significantly improved sequence labeling performance and became a widely adopted baseline in NER research [9]. In recent years, the development of pre-trained language models has driven substantial advances in NER performance. Devlin et al.'s BERT model, which employs a deep bidirectional Transformer to capture contextual semantics, demonstrated strong performance across various NLP tasks and has been extensively applied to NER [10]. Several BERT-based adaptations have been introduced to better model Chinese-specific linguistic features. For example, Chay-intr et al. introduced a Lattice Attention Encoding (LATTE) method for character-based word segmentation that achieved promising results on standard datasets in Chinese, Japanese, and Thai [11]. These studies underscore BERT's potential for modeling word boundaries, contextual dependencies, and semantic richness in Chinese NER tasks.

Beyond foundational architectures, the integration of attention mechanisms and multi-task learning has become a prominent direction for boosting NER performance. For instance, Patel and Ezeife proposed a novel aspect-based opinion mining system, BERT-MTL, which introduces auxiliary tasks to enable shared representation across multiple subtasks, simultaneously handling aspect term and category extraction. This approach not only improves accuracy but also significantly reduces training time [12]. The GlobalPointer method further overcomes the limitations of CRF in recognizing overlapping entities. Zhai et al. developed a CNER framework that utilizes an Efficient GlobalPointer model to effectively address entity nesting, along with a context shielding window mechanism [13]. These works validate the effectiveness of structural integration strategies in enhancing NER capabilities. In terms of applied CNER, several studies have extended the task to domain-specific text, including medical, agricultural, and railway documents. Models combining CNNs and attention mechanisms have shown promising performance by leveraging convolutional layers for local feature extraction and attention mechanisms for capturing global dependencies [14]. Yang et al. proposed a BERT-based CNER model tailored for complex filtering in COVID-19 epidemiological investigation texts, resulting in notable improvements in both accuracy and F1 score [15]. Zhao et al. introduced a high-performance NER model for agricultural texts by incorporating multi-level glyph feature modeling and self-attention mechanisms. This model achieved an F1 score of 95.56% and enriched target word representations through hierarchical glyph feature learning [16]. A summary and comparison of these studies are provided in Table 1.

Table 1: Structured summary of related work

Author(s)	Dataset / Domain	Method	Key results	Major contribution
Huang et al. [9]	CoNLL/multi-task labeling	BiLSTM-CRF	Multi-task average F1>91%	Introduced a classic deep structured model for sequence labeling; became a standard NER baseline.
Devlin et al. [10]	Multilingual pre-training corpora	BERT: Bidirectional Transformer	Significant improvement in F1	Proposed the BERT pre-trained language model, establishing a new paradigm for NER tasks.
Chayintr et al. [11]	BCCWJ/CTB6/BEST2010	LATTE (Lattice+ GNN+Attention)	Improved word segmentation accuracy	Addressed multi-granularity semantic ambiguity using lattice-based encoding and attention mechanisms.
Patel and Ezeife [12]	SemEval-14 ABSA	BERT-MTL (Multi-task Learning)	Improved multi-task accuracy	Enhanced generalization and training efficiency between subtasks through shared BERT representations.
Zhai et al. [13]	Medical texts/CMeEE and others	Knowledge Distillation+Efficient GlobalPointer	F1 score exceeds existing best results	Proposed an efficient GlobalPointer architecture to handle nested entities and redundant information while balancing accuracy and speed.
Yang et al. [15]	COVID-19 epidemiological texts	BERT+BiLSTM+IDCNN+CRF	F1 score exceeds existing best results	Constructed a multi-level architecture for complex medical text modeling, improving CNER accuracy.
Zhao et al. [16]	Agricultural chinese texts	ALBERT+CNN+BiLSTM+Self-Attention+CRF	F1=95.56%	Enhances the generalization ability of named entity recognition in agricultural texts by leveraging multi-level glyph features.

In summary, the development of CNER has evolved from statistical learning methods to deep learning, and further toward integrated pre-trained architectures and multi-task modeling. Deep learning approaches that incorporate self-attention mechanisms and convolutional neural networks have demonstrated superior performance in capturing complex data patterns and modeling global contextual information. The primary challenge at present lies in how to jointly model character-level semantics, word boundaries, and contextual dependencies while achieving accurate entity classification and boundary recognition. To address this, the study proposes the AC-MTL model, which integrates attention mechanisms with CNN structures. This design aims to achieve a better balance between global semantic understanding and local feature extraction, particularly when dealing with complex entities and long-form texts, thereby enhancing the model's adaptability in Chinese named entity recognition tasks.

3 CNER model based on attention mechanism and CNN

3.1 CNER design based on CNN and attention mechanism

With the development of the internet, artificial intelligence has become ubiquitous in people's lives, bringing convenient and intelligent technologies for societal advancement [17]. NER serves the purpose of automatically identifying entities such as person names, organizations, and locations in text [18, 19]. In service, NER needs to accurately and quickly recognize specific entities, whereas traditional NER methods often suffer from insufficient accuracy. CNN, a feedforward neural network that utilizes convolutional operations and a deep architecture, is widely applied in tasks like object detection and image recognition [20]. In NER tasks, CNNs can be employed to extract local contextual features from embedded character sequences. The standard processing pipeline involves four main steps. First, the input Chinese sentence is encoded by a pre-trained language model such as BERT into a two-dimensional embedding matrix $X \in R^{n \times d}$, where n denotes the sentence length and d represents the dimensionality of each character's embedding vector. This embedded sequence is then passed through a one-dimensional convolutional layer. The convolutional layer applies multiple sets of filters with varying kernel sizes—specifically, window sizes of 3, 5, and 7—sliding along the sequence dimension to capture local features at different granularities. Each filter generates a feature map, and all resulting feature maps are concatenated to form a richer representation. Following the convolution operation, a max-pooling layer is applied to reduce the length of the feature maps and retain the most salient features. The pooled output is subsequently fed into a fully connected layer or a CRF layer for final entity label prediction. Unlike the two-dimensional convolution used in image processing tasks, the convolution operation in this model is performed only along the temporal (sequence) dimension, and thus constitutes a one-dimensional convolution. This approach effectively captures local structural features in Chinese, such as radicals, part-of-speech combinations, and character patterns, thereby enhancing the model's ability to understand short-range entity structures. When the convolutional layer processes the sequence, the dimensions are adjusted, and the padding size is shown in Equation (1).

$$paddingSize = \frac{f-1}{2} \tag{1}$$

In Equation (1), f represents that the convolutional kernel size is odd. The formula used to calculate the convolution output size is provided in Equation (2).

$$\begin{cases} w_{out} = \dfrac{w + 2 \times paddingSize - f}{s} + 1 \\ h_{out} = \dfrac{h + 2 \times paddingSize - f}{s} + 1 \end{cases} \tag{2}$$

In Equation (2), w and h represent the width and height of the input image, while s is the stride. To reduce the output dimensions, a pooling operation is performed as shown in Equation (3).

$$\begin{cases} \mathrm{C}_i = \mathrm{Conv1D}(\mathrm{A}_i, \mathrm{W}, b) \\ \mathrm{C}_{\max} = \max(\mathrm{C}_1, \mathrm{C}_2, ..., \mathrm{C}_k) \end{cases} \tag{3}$$

In Equation (3), A_i represents the input processed by MHSA, and C_i is the output after convolution. In the field of natural language processing, CNN is widely used to extract features such as the structural components of Chinese characters. CNN can also handle long Chinese sentences or capture potential word properties. However, since CNN performs better in learning local features and cannot fully consider global semantics, it may encounter issues with inaccurate recognition of Chinese, as its operational scope is limited. The core idea of the attention mechanism is to focus on specific locations while ignoring less important information, similar to how humans focus their attention on specific parts of an object to enhance feature learning from semantic information [19]. Among the different types of attention mechanisms, MHSA has multiple attention heads, and when processing semantic information, it not only extracts local features clearly but also processes them in parallel, allowing global features to be expressed more distinctly [20]. The principle of the MHSA mechanism is shown in Figure 1.

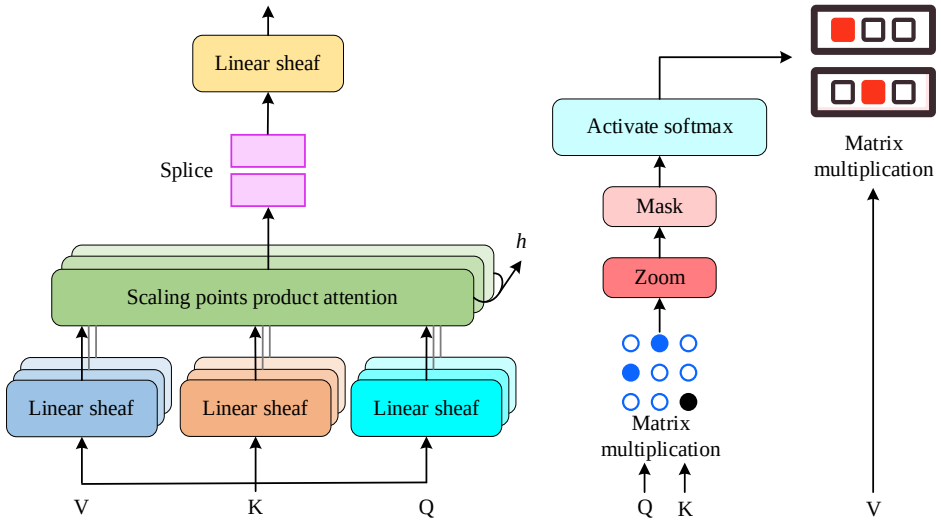


Figure 1: Diagram of the multi-head attention mechanism.

As shown in Figure 1, MHSA is capable of focusing on the most important tasks at the moment by gathering various pieces of information. First, for each sequence, a query vector (Q), a key vector (K), and a value vector (V) are assigned. These vectors are then processed through linear layers for individual linear transformations. After that, they are aggregated into scaled dot-product attention, where the attention distribution is calculated. Subsequently, operations like concatenation are performed, followed by another round of linear transformations. When the Q and K vectors undergo attention via matrix multiplication and masking, the resulting scores are processed by the softmax function. All the outcomes are then added to the V vector, and after the final matrix multiplication, the output is obtained. The attention computation during linear transformations is expressed in Equation (4).

$$\begin{cases} Q = XW^Q \\ K = XW^K \\ V = XW^V \end{cases} \tag{4}$$

In Equation (4), X represents the word vector $X = \{x_1, x_2, x_3, \ldots, x_n\}$. Due to the parallel computing capability of MHSA during CNER, it effectively captures global semantic information. Therefore, the study proposes combining MHSA with CNN to form Attention-CNN, which improves the accuracy of text CNER. The structure of CNER based on Attention-CNN is shown in Figure 2.

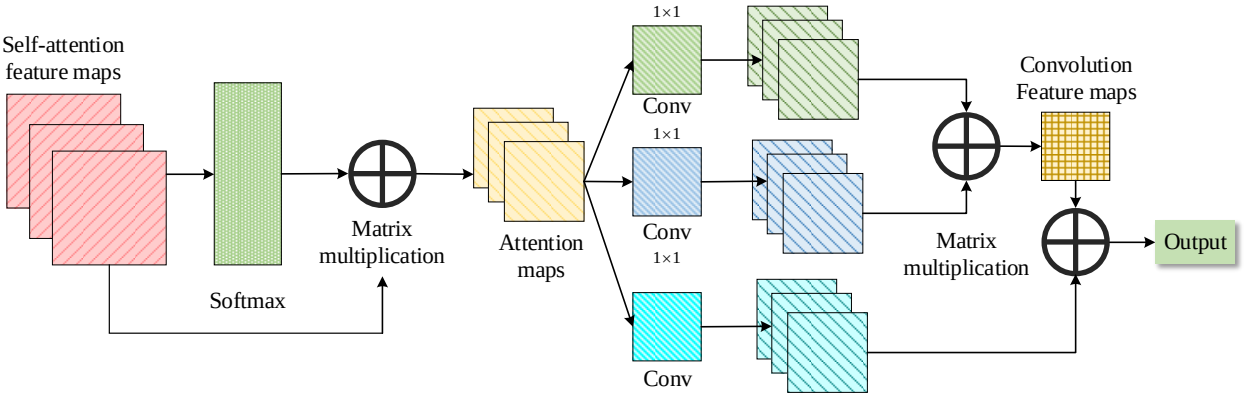


Figure 2: Structure of CNER based on Attention-CNN.

As shown in Figure 2, Attention-CNN structure in CNER has MHSA at the front end, which identifies Chinese entities in the text. Its multiple heads perform parallel computation of attention scores, and after matrix multiplication and softmax function mapping, the output of the MHSA feature map is obtained. This output is then used as the input for CNN, where convolution operations are applied with different kernels, followed by max pooling to reduce dimensions. The process of convolution and pooling is repeated, and after further matrix and function calculations, the final recognition result is output through the maximum probability at the fully connected layer. The more optimal results are selected, and CNN is used to further extract the optimal solution, resulting in the best overall output. Additionally, position encoding solves the problem of lacking sequential order information when the model processes

words at different positions. The expression is shown in Equation (5).

$$\begin{cases} \mathrm{PE}(pos, 2i) = \sin\left(\dfrac{pos}{10000^{\frac{2i}{d}}}\right) \\ \mathrm{PE}(pos, 2i+1) = \cos\left(\dfrac{pos}{10000^{\frac{2i}{d}}}\right) \end{cases} \tag{5}$$

In Equation (5), pos represents the position, and i represents the dimension. Further clarification of the scaled dot-product attention is shown in Equation (6).

$$\mathrm{Attention}(Q, K, V) = \mathrm{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)\mathrm{V} \tag{6}$$

In Equation (6), d_k represents the key dimension, which is used for scaling. The combined formulation of MHSA is given in Equation (7).

$$\mathrm{MultiHead}(Q, K, V) = \mathrm{Concat}(\mathrm{head}_1, \mathrm{head}_2, ..., \mathrm{head}_h)W^O \tag{7}$$

In Equation (7), head represents the output of each head.

3.2 Attention-CNN model design for CNER

After completing the design of the Attention-CNN algorithm, the study proceeds to apply it for modeling CNER in text. Existing NER models predominantly focus on surface-level lexical recognition and often fail to capture the deeper semantic features inherent in Chinese characters. This work leverages the parallel computation capability of the attention mechanism to extract global semantic features of Chinese characters and further utilizes CNNs to perform high-precision local extraction of salient features, thereby improving both the accuracy and efficiency of Chinese NER. The character-level embeddings are trained within the BERT framework to enhance the expressive capacity of Chinese representations. BERT is a bidirectional language model capable of performing classification, question answering, and other natural language processing tasks [21, 22]. In this study, the BERT-Base Chinese model is adopted along with its built-in WordPiece tokenizer, which segments the original Chinese character stream into subword units and maps them to vocabulary indices. No additional stopword filtering is applied, and all function words and grammatical particles are retained during training to preserve the full semantic context. The expression for each character vector after BERT training is shown in Equation (8).

$$\begin{cases} e_b = \left(e_{b1}, e_{b2}, \ldots, e_{bn}\right) = BERT\left(s_1, s_2, \ldots, s_n\right) \\ S = \left\{s_1, s_2, \ldots, s_n\right\} \end{cases} \tag{8}$$

In Equation (8), S represents a sentence, n represents the length of a sentence, and s_n and e_b represent the low-dimensional character vector and the character vector obtained after training, respectively. Then, the Attention-CNN CNER model will be established, and the model architecture is shown in Figure 3.

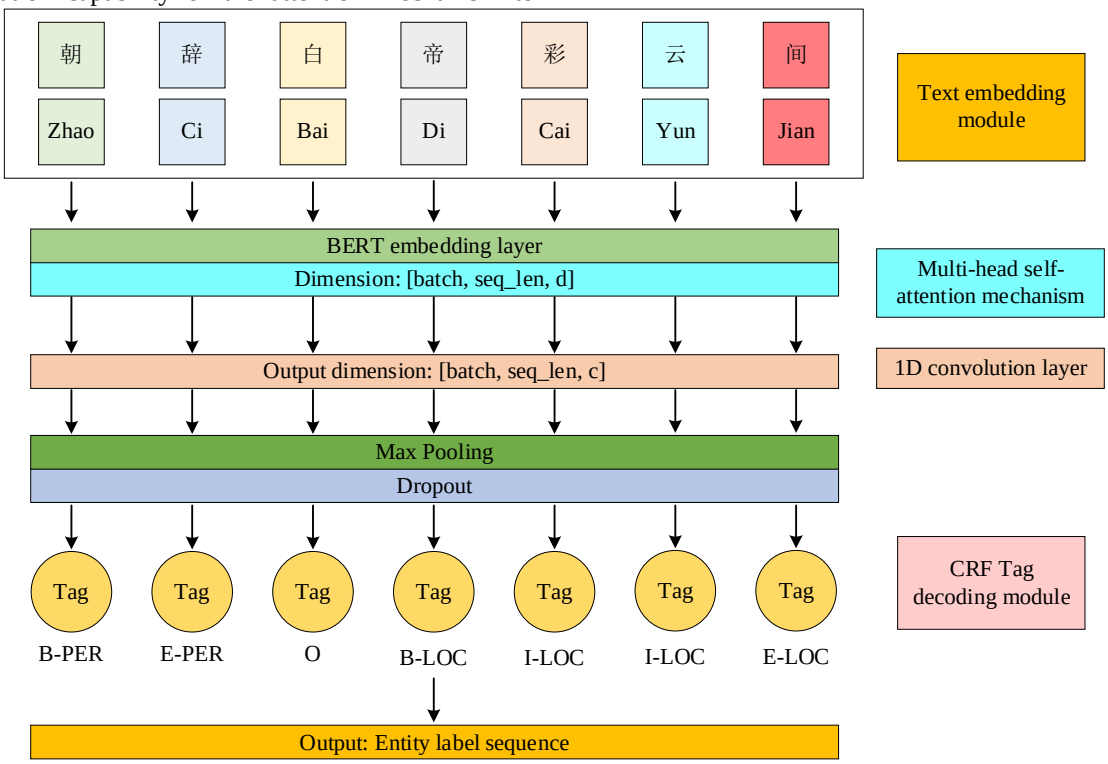


Figure 3: Attention-CNN model architecture for CNER.

In Figure 3, the Attention-CNN model consists of four modules. First, the Chinese character and pinyin vectors are input into the Chinese semantic feature embedding module, where the four tones in Chinese are represented by [1, 4] for tone values. Then, the attention mechanism is used to globally and parallelly compute the

attention scores for the features such as the Chinese characters and pinyin, allowing more accurate extraction of global semantic features. Next, in the CNN phase, the Chinese semantic features undergo convolution operations, and the final output of the Chinese character labels is sent to the CRF for decoding. In the CRF, PER denotes person names, B indicates the beginning of a label, I represent the intermediate stage of the label, and E signifies the end of the label, O denotes non-entity tokens such as prepositions, while LOC represents location names. The expression for the vector after the character feature fusion operation is shown in Equation (9).

$$E_i = concat\left(\left[e_i^c, e_i^p\right]\right) \tag{9}$$

In Equation (9), e_i^c and e_i^p represent the corresponding character and pinyin vectors of Chinese. The output expression obtained after h attention heads of Multi-Head Self-Attention undergo linear transformation is shown in Equation (10).

$$\begin{cases} h_i = f\left(W_i^q q, W_i^k k, W_i^v v\right) \\ Multihead\left(h\right) = W_o \begin{bmatrix} h1 \\ \vdots \\ hn \end{bmatrix} \end{cases} \tag{10}$$

In Equation (10), W and f represent the learnable parameter matrix and scaled dot-product attention, respectively. Next, convolution operations are performed to connect the convolutional layers, followed by information fusion, as shown in Equation (11).

$$\begin{cases} S' = Conv1D\left(hs_T^P\right) \\ S'' = GeLU\left(Maxpool1D\left(S + S'\right)\right) \end{cases} \tag{11}$$

In Equation (11), S and S' represent the 1D convolution and max pooling, respectively, while S'' represents the entity scoring matrix after convolution processing. After updating the weights, the results obtained by parallel computations in the MHSA are concatenated, as shown in Equation (12).

$$Multi-Head\left(Q,K,V\right) = \left(Head_j \oplus \ldots \oplus Head_h\right) \tag{12}$$

After the computation in Equation (12), higher-precision text content features are obtained. The optimal sequence decoded by the CRF is shown in Equation (13).

$$y^* = \arg\max_y \sum_{i=1}^{n} \left(A_{y_{i-1}, y_i} + P_{i, y_i}\right) \tag{13}$$

In Equation (13), A denotes the transition matrix and P represents the emission score matrix. The Attention-CNN CNER model progressively extracts entity-related features from the text while effectively capturing global key semantic information, thereby enhancing the accuracy of label classification. In specific textual domains, the NER task is often inherently related to other tasks; however, traditional models typically focus on single-task learning. NER naturally correlates with tasks such as entity type classification and sentiment polarity detection. To improve the model's comprehension of semantic nuances, this study adopts a multi-task learning framework, which shares parameters in both the attention and convolutional layers while jointly optimizing multiple related tasks. Therefore, in the final model, MTL is introduced to improve the recognition accuracy, even with limited data. The MTL framework is shown in Figure 4 [23, 24].

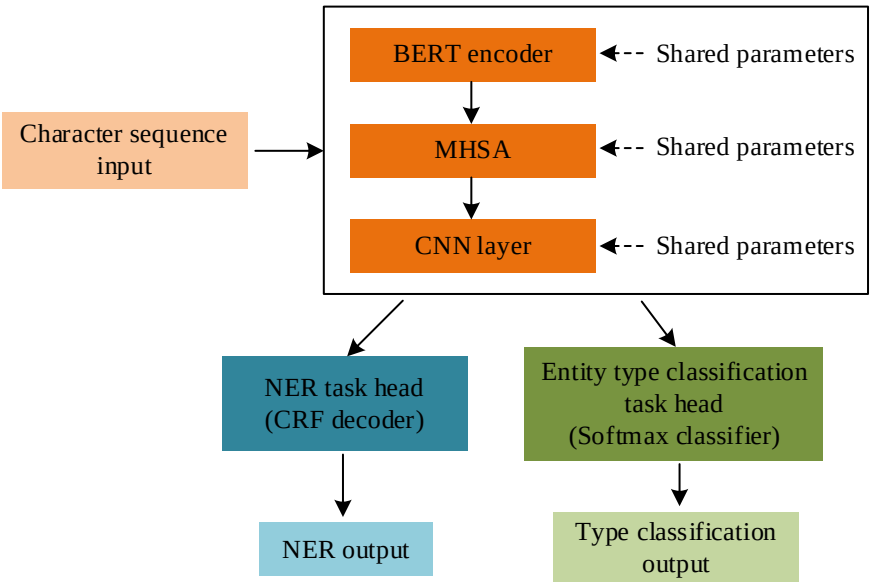


Figure 4: MTL framework with a shared backbone and task-specific branches.

As shown in Figure 4, the MTL module uses soft parameter sharing technology. Although tasks share the underlying feature extraction parts of the convolutional layer and attention mechanism, tasks such as NER, sentiment analysis, and text classification typically have specific output layers and task goals. Therefore, they require independent, task-specific parameters. This design allows for the use of shared lower-level feature

extraction capabilities while ensuring that the individual requirements of each task are met, rather than using hard parameter sharing where all tasks would use the same network layers and weights. When constructing the final model, a Dropout layer is typically added within the CNN framework to prevent overfitting. The Dropout operation is expressed in Equation (14).

$$C_{dropout} = C_{max} \cdot \text{Dropout}(p) \quad (14)$$

In Equation (14), p represents the dropout probability. The operational flow of the AC-MTL document CNER model, which combines Attention-CNN and MTL techniques, is shown in Figure 5.

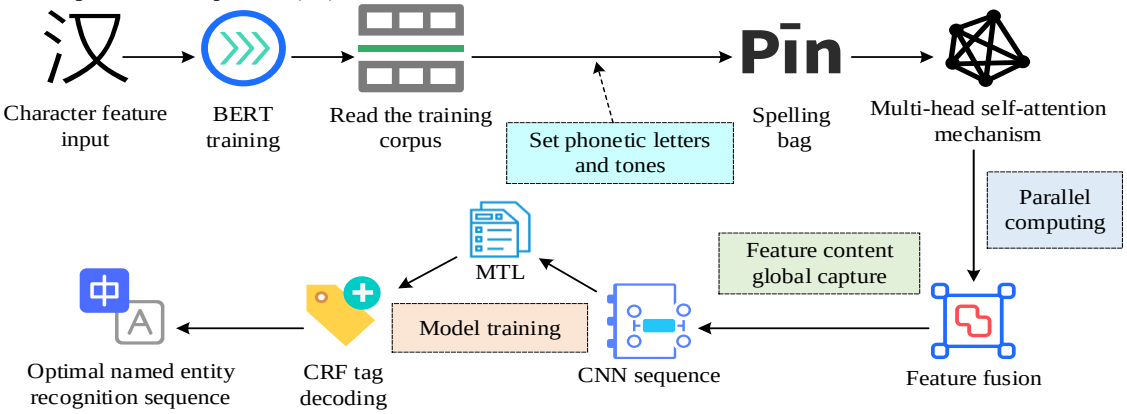


Figure 5: Flowchart of AC-MTL operation combining Attention-CNN and MTL techniques.

As shown in Figure 5, when the AC-MTL model is running, the first step is to input Chinese character features, which are pre-trained in the BERT module. After that, the trained character features proceed to the next step of corpus reading, where pinyin letters and tone values need to be set. Then, during the Attention phase, parallel computation of attention scores, dot-product scaling, and other operations are performed, followed by feature fusion. After Attention extracts the global semantic features, the data proceeds to the CNN sequence stage. Next, after convolution and max-pooling operations, feature combinations and transformations are processed through the fully connected layer. The model is then trained with multi-task learning, followed by CRF label decoding to obtain the final optimal Chinese named entity sequence.

4 Performance analysis of CNER model integrating attention and CNN with MTL

4.1 Comprehensive evaluation of AC-MTL on Chinese NER Tasks

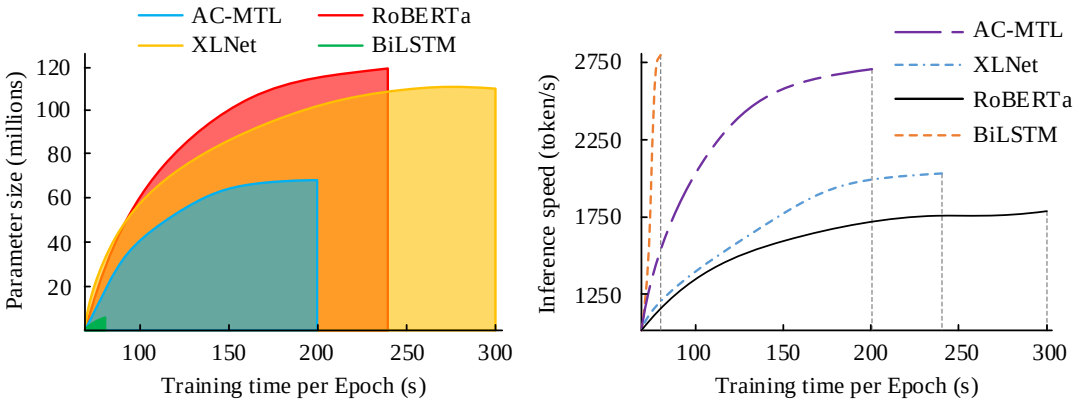
To evaluate the effectiveness of the proposed AC-MTL model, experiments were conducted on a workstation equipped with an Intel Xeon Gold 6248R processor, 128 GB of memory, and an NVIDIA Tesla V100 GPU. The operating system used was Ubuntu 18.04, with PyTorch 1.8.1 as the deep learning framework, CUDA version 11.1, and driver version 450.80.02. The hyperparameters of the AC-MTL model were set based on prior empirical studies and experimental validation. The learning rate was set to $5e^{-5}$, a common starting value for BERT fine-tuning which ensured stable convergence without needing extensive tuning. The batch size was set to 32 to balance training efficiency and GPU memory constraints. The number of training epochs was set to 50, with early stopping applied to prevent overfitting. The dropout rate was set to 0.1, which was the standard value used in Transformer architectures to prevent overfitting. Additionally, the initial weight of the primary task in the multi-task loss function was set to 0.7 to emphasize its central role. This value was empirically validated to deliver favorable performance across multiple experimental settings. The Adam optimizer was employed due to its fast convergence and stability, making it a mainstream choice for deep learning tasks and particularly suitable for Transformer-based text modeling.

To assess the model's performance in Chinese named entity recognition, AC-MTL was compared against baseline CNER models based on BiLSTM, RoBERTa, and XLNet architectures. For a fair comparison, RoBERTa and XLNet were fine-tuned by adding a CRF decoding layer and training with BIO-labeled sequences on the same dataset, to meet the requirements of the NER task. The experiments utilized the Weibo dataset and a subset of the Microsoft Research Asia (MSRA) dataset. The MSRA subset contained 200 samples specifically selected to evaluate performance under low-resource conditions. A stratified sampling strategy was adopted to divide each dataset, ensuring that the distribution of named entity labels was consistent across the training set (70%), validation set (15%), and test set (15%). Four models were used for Chinese NER, and their performance was measured by precision, recall, and F1 score. The results are presented in Table 2.

Table 2: Overall performance comparison of CNER models

Sample size	Model	Precision (%)	Recall (%)	F1 Score (%)
200	AC-MTL	98.62	98.10	98.36
	XLNet	96.21	95.89	95.54
	RoBERTa	88.53	85.37	86.92
	BiLSTM	82.48	82.64	82.73
1000	AC-MTL	98.40	97.90	98.15
	XLNet	97.16	96.29	96.64
	RoBERTa	88.24	88.71	89.44
	BiLSTM	81.76	81.46	82.17
3000	AC-MTL	98.54	98.19	98.79
	XLNet	97.46	95.27	96.26
	RoBERTa	86.89	87.04	87.28
	BiLSTM	82.40	81.67	81.64

As shown in Table 2, under sample sizes of 200, 1000, and 3000, the AC-MTL model consistently maintained a leading position across all three-performance metrics: precision, recall, and F1 score. In the low-resource setting with only 200 samples, AC-MTL achieved a precision of 98.62%, recall of 98.10%, and an F1 score of 98.36%, significantly outperforming XLNet, RoBERTa, and BiLSTM, showing its strong adaptability to limited data. When the sample size increased to 1000, AC-MTL still maintained the highest precision at 98.40% and recall at 97.90%, resulting in an F1 score of 98.15%, which was notably higher than RoBERTa's 89.44% and BiLSTM's 82.17%. It was also worth noting that although XLNet showed some improvement in recall under medium- to high-resource settings, its overall precision stability and combined performance stayed below AC-MTL's. This suggested that AC-MTL achieved a better balance between high-accuracy recognition and error tolerance. Subsequently, the study evaluated the model's runtime efficiency, as illustrated in Figure 6.



(a) Model size of different models (b) Inference time of different models

Figure 6: Inference speed and parameter size comparison among CNER models.

As shown in Figure 6(a), AC-MTL maintained high performance while keeping its parameter size at 64 million, which was significantly smaller than RoBERTa's 118 million and XLNet's 105 million—representing a model compression rate exceeding 40% relative to both. In contrast, although BiLSTM had the smallest parameter size, it lacked deep semantic modeling capability and thus exhibited functional limitations. Through the integration of modular structures and task-guided mechanisms, AC-MTL effectively reduced redundant parameters while preserving both global semantic understanding and local feature representation, achieving a well-balanced trade-off between structural compactness and expressive power. In Figure 6(b), the inference efficiency of each model was further compared using token-level processing speed as the evaluation metric. AC-MTL reached a throughput of 2618 tokens per second, demonstrating significantly faster inference than RoBERTa and XLNet, and approaching the speed of the lightweight BiLSTM model. This improvement was primarily attributed to the introduction of convolutional modules and task decoupling optimizations within the encoding structure of AC-MTL, which collectively enhanced computational efficiency during inference. Overall, AC-MTL exhibited superior performance in both parameter compactness and inference speed. These are two key factors for real-world deployment, making it a practical and deployable solution for resource-constrained environments.

4.2 Ablation study: validating the structural design of AC-MTL

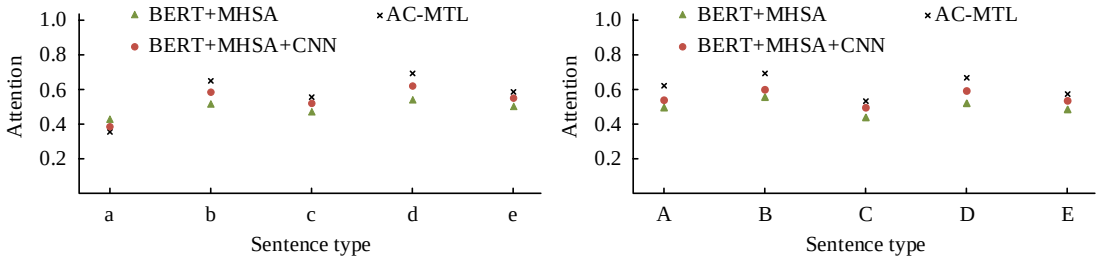
To verify the actual contribution of each core structural module within the AC-MTL model to overall

performance, a systematic ablation study was conducted to compare the effects of different component combinations, as detailed in Table 3.

Table 3: Ablation results of AC-MTL on key structural components

Model architecture	Precision (%)	Recall (%)	F1-score (%)
BERT+CNN	95.14	94.12	94.75
BERT+MHSA	96.23	94.85	95.32
BERT+MHSA+CNN	97.37	96.22	96.74
AC-MTL	99.54	98.19	98.79

As shown in Table 3, the AC-MTL model achieved the highest performance when all structural components were retained, with a precision of 99.54%, a recall of 98.19%, and an F1 score of 98.79%. Compared to the model with only the BERT+MHSA+CNN structure, the F1 score increased by 2.05 percentage points, indicating that the multi-task learning mechanism significantly improved overall performance. In contrast, simplified models that retained only the CNN or MHSA module yielded F1 scores of 94.75% and 95.32%, respectively—substantially lower than the full AC-MTL configuration. This suggested that relying solely on local feature extraction or global semantic modeling was insufficient and that the synergy of module integration was critical for optimal performance. The study further evaluated attention scores across three model structures using two sentence segments. Segments a, b, c, d, and e corresponded to the Chinese sentences: He is a Beijinger. He graduated from Beijing Jiaotong University. He still works in Beijing. The pace of development in Beijing is fast. I also want to study in Beijing. Segments A, B, C, D, and E represented Chinese sentences: Innovation is the core driving force behind enterprise development. Only through continuous exploration of new technologies and new models could one stand out in the fierce market competition. In the field of scientific research, innovation meant breaking free from the constraints of conventional thinking and capturing every spark of inspiration that could lead to transformative change with keen insight. The essence of education lay in cultivating innovative talents. Through diversified curricula and practical activities, students' creativity and spirit of exploration could be effectively stimulated. The sustainable development of cities could not proceed without the integration of innovative concepts. From the application of green energy to the construction of intelligent transportation systems, the power of innovation was evident everywhere. Cultural heritage required innovative expression. By leveraging digital technology and interdisciplinary fusion, traditional culture could be revitalized and given new life in the modern era. The detailed comparative results were illustrated in Figure 7.



(a) The attention weight assigned to the token Beijing(Chinese)

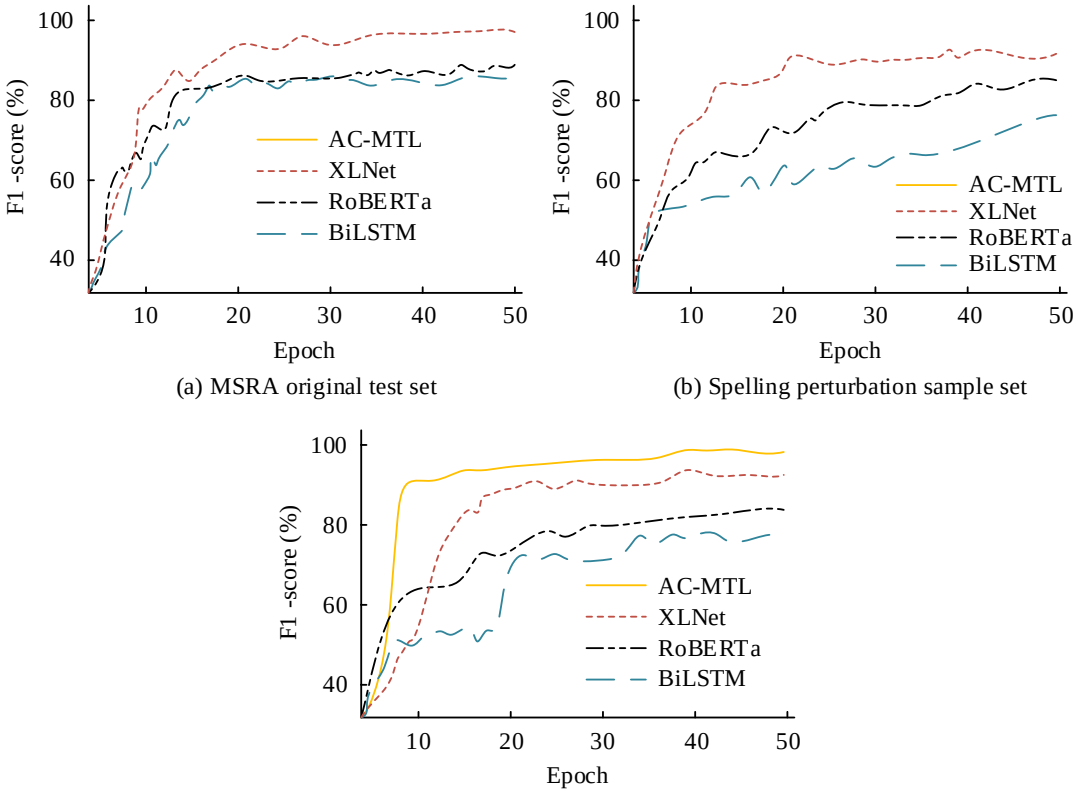
(b) The attention weight assigned to the token Innovation(Chinese)

Figure 7: Attention score comparison for tokens under different model architectures.

In Figure 7(a), the AC-MTL model consistently achieved higher attention scores across all positions compared to the other two baseline models. Notably, it reached 0.63 in sentence b and 0.67 in sentence d, demonstrating more precise semantic recognition of nested entities and core thematic terms. In contrast, the BERT+MHSA model exhibited relatively uniform attention distribution toward the token Beijing, lacking focused differentiation, while the addition of CNN introduced some improvement but still fell short of the structural enhancement achieved by AC-MTL. Overall, AC-MTL demonstrated stronger discriminative capacity and contextual understanding in allocating attention to high-frequency geographical terms under polysemous conditions. In Figure 7(b), AC-MTL exhibited the strongest semantic focus in all contexts. Specifically, it scored 0.68 in sentence B ("scientific thinking") and 0.66 in sentence D ("sustainable development"), surpassing BERT+MHSA in both cases. This indicated that the model had a superior ability to capture the semantic salience of abstract policy-related terms within complex syntactic structures. Notably, even in peripheral semantic scenarios such as "mode of expression," AC-MTL maintained a relative advantage, whereas BERT+MHSA achieved only 0.46. These overall trends suggested that AC-MTL possessed enhanced contextual aggregation and semantic stability when dealing with abstract, highly context-dependent lexical disambiguation, thereby validating the effectiveness of its structural design in recognizing semantically ambiguous words.

4.3 Interpretability and robustness analysis of AC-MTL

To further evaluate the stability and interpretability of the AC-MTL model in practical applications, the study conducted robustness analysis under various types of perturbation scenarios. The model was tested on datasets with noise-injected samples derived from the original corpus, and the resulting F1 scores were shown in Figure 8.



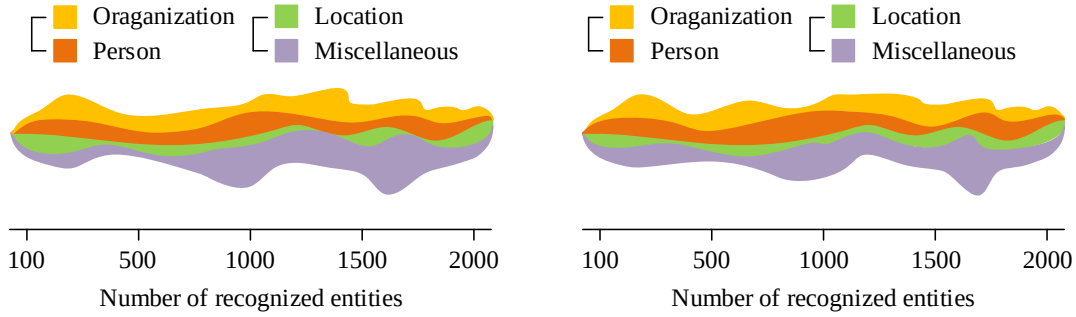
(a) MSRA original test set

(b) Spelling perturbation sample set

(c) Weibo short texts

Figure 8: Robustness of AC-MTL under noisy and informal input conditions.

In Figure 8(a), during training on the standard MSRA test set, the F1 score of the AC-MTL model increased rapidly within the first five epochs and stabilized, eventually converging at 98.79%, significantly outperforming XLNet (96.26%) and RoBERTa (87.28%). This demonstrated both a faster convergence speed and a higher performance ceiling. Notably, AC-MTL reached its major performance plateau by epoch 10, whereas the baseline models required at least 20 epochs to approach a similar level. This indicating that AC-MTL's structural design was more efficient in capturing semantic features and entity boundaries. In Figure 8(b), despite larger fluctuations during training on the spelling-perturbed dataset, AC-MTL maintained strong stability and noise resistance, with a final F1 score of 96.54%, substantially higher than other models. In Figure 8(c), on the Weibo short-text dataset, AC-MTL almost fully converged after just four epochs and stabilized at an F1 score of 98.35%. In contrast, XLNet achieved only 92.78% on this dataset and showed considerable volatility throughout training, reflecting its limited adaptability to unstructured and contextually ambiguous language. Supported by multi-task learning signals, AC-MTL exhibited superior contextual modeling capabilities, allowing it to maintain high recognition accuracy and convergence stability even under fragmented input conditions. Figure 9 presented a validation of AC-MTL's performance in identifying different thematic categories in legal text cases.



(a) AC-MTL (b) Actual Statistics

Figure 9: Distribution of recognized thematic entities in legal texts.

As shown in Figure 9(a), the vertical axis represented the number of entities mentions identified as belonging to each thematic category, while the theme river illustrated the aggregation trend of topic recognition as the text progressed. The thematic stream recognized by the AC-MTL model across 2,000 legal text cases was shown, with each colored band represented a different theme category identified by the model, including organizations, person names, locations, and domain-specific terms. The AC-MTL model demonstrated the ability to accurately identify and distinguish between different types of entities, with a smooth distribution of recognized themes that effectively covered a wide range of entity categories present in the text. Figure 9(b) presented the actual thematic distribution across the 2,000 legal text cases. The distribution generated by the AC-MTL model closely matched the true distribution, with minimal fluctuations between the two. As the number of cases increased, the recognition trends became increasingly aligned. This indicated that the AC-MTL model had strong recognition capabilities and was able to extract and differentiate themes from complex texts with high accuracy, further underscoring its effectiveness in the context of legal document analysis. Finally, to further investigate the limitations of the model, an error analysis was conducted by categorizing 100 misclassified samples produced by the AC-MTL model. The distribution of common misclassification types was presented in Figure 10.

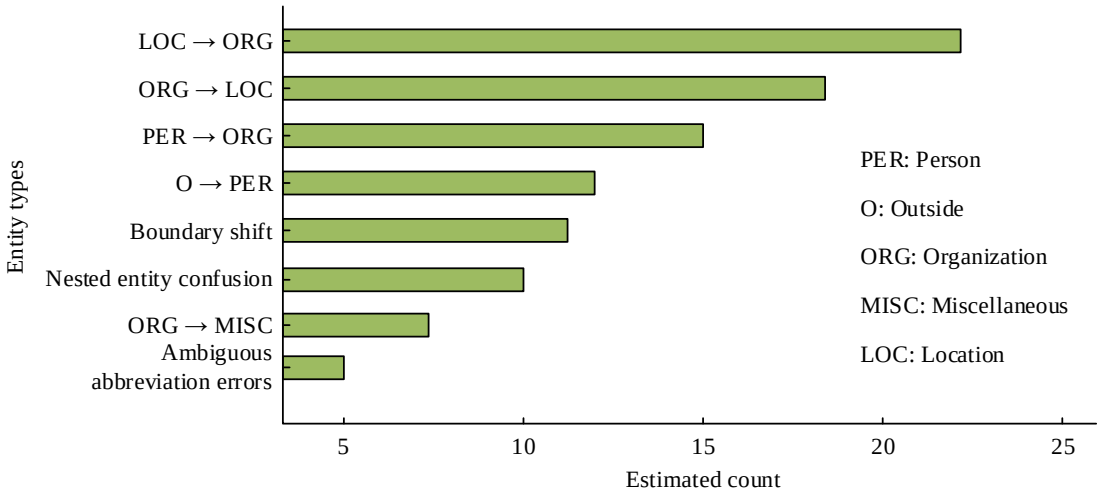


Figure 10: Distribution of common misclassification types in AC-MTL output.

As illustrated in Figure 10, the most frequent misclassification types involved confusion between location and organization entities (LOC ⇔ ORG), which reflected the semantic overlap in Chinese place names and institutional titles. Errors related to person names also occurred, especially when user handles or role-based nicknames were interpreted as named entities. Boundary-related mislabeling and nested entity conflicts occurred in complex expressions, suggesting that further improvements in fine-grained boundary detection might be necessary.

5 Discussion

The proposed AC-MTL model demonstrated outstanding performance in CNER tasks, particularly in maintaining high robustness and accuracy when faced with limited data resources and noisy textual environments. Experimental results confirmed that the integration of attention mechanisms with convolutional neural networks, along with the adoption of a multi-task learning strategy, effectively compensated for the deficiencies of traditional methods in modeling long-range dependencies while enhancing local feature extraction capabilities. This reflected the model's

structural design in terms of both scientific rigor and engineering practicality. Firstly, performance evaluations indicated that AC-MTL consistently outperformed mainstream baseline models such as XLNet, RoBERTa, and BiLSTM across datasets of varying sizes. Even in a low-resource scenario with only 200 samples, the model achieved an F1 score of 98.36%, showing strong generalization capability in data-scarce conditions. Secondly, in terms of inference efficiency, AC-MTL attained a processing speed of 2618 tokens per second, approaching that of the lightweight BiLSTM while significantly surpassing both XLNet and RoBERTa, thereby highlighting its computational advantage for real-world deployment.

The effectiveness of individual modules within the AC-MTL architecture was further validated through ablation experiments. While combinations such as BERT+CNN or BERT+MHSA showed some recognition ability, they fell short in holistic semantic modeling and precise feature localization. Only through the synergistic integration of BERT, MHSA, and CNN—each enhanced by a multi-task learning framework—enabled the model to achieve substantial performance gains. This soft parameter-sharing MTL framework enabled information sharing across multiple subtasks such as entity boundary recognition and type classification, significantly enhancing semantic discrimination capability. Visualization of attention weights revealed that AC-MTL was particularly adept at capturing syntactic and semantic cores when processing polysemous and abstract lexical items (e.g., “Beijing” or “innovation”), showing clearer focus compared to BERT+MHSA and BERT+CNN structures. Moreover, the model’s stable performance on Weibo short texts and spelling-perturbed corpora demonstrated its adaptability to unstructured input, making it suitable for real-world applications such as social media analysis and legal document mining.

Nevertheless, certain limitations remained. In contexts with highly sparse information or pronounced semantic ambiguity, the model still suffered from inaccurate boundary detection or entity type confusion. Additionally, although AC-MTL exhibited strong generalization, its reliance on large-scale pre-trained models like BERT posed challenges for deployment in resource-constrained environments, necessitating further compression and optimization. In conclusion, AC-MTL excelled in both theoretical design and empirical performance, offering an efficient, robust, and extensible approach to Chinese named entity recognition. Given its modular architecture and strong performance in capturing both global semantics and local features, the AC-MTL model held significant potential for adaptation across multilingual NER tasks and domain-specific applications such as biomedical text mining, cross-lingual knowledge extraction, and low-resource language processing, where robust entity recognition remained a persistent challenge.

6 Conclusion

To address the limitations of existing methods in handling complex textual environments, this study proposes a Chinese named entity recognition approach that integrates attention mechanisms with convolutional neural networks, and further designs the AC-MTL model by incorporating BERT and multi-task learning techniques for legal document entity recognition. On the standard MSRA test set, the AC-MTL model achieved an F1 score of 98.79%, and on a spelling-perturbed sample set, it reached an F1 score of 96.54%, both outperforming the baseline models XLNet and RoBERTa. When applied specifically to legal document cases, the thematic distribution recognized by the model across 2,000 samples closely matched the actual distribution, demonstrating its strong potential for domain-specific applications and generalization. Although the current method performs well in recognizing named entities in long-form texts, it may still encounter errors in scenarios with high semantic ambiguity or sparse contextual information. Future optimization may proceed in two directions: first, by incorporating larger and more domain-adapted pre-trained language models for targeted fine-tuning; and second, by exploring the integration of external knowledge graphs or entity linking mechanisms to enhance its practical applicability in tasks such as question answering, information extraction, and sentiment analysis.

References

[1] Abdullah M H A, Aziz N, Abdulkadir S J, Alhussian H S A, Talpur N. Systematic literature review of information extraction from textual data: recent methods, applications, trends, and challenges. IEEE Access, 2023, 11(1): DOI: 10535-10562. 10.1109/ACCESS.2023.3240898

[2] Pan X, Xue Y. Advancements of artificial intelligence techniques in the realm about library and information subject—A case survey of latent Dirichlet allocation method. IEEE Access, 2023, 11(2): 132627-132640. DOI: 10.1109/ACCESS.2023.3334619

[3] Shishehgarkhaneh M B, Moehler R C, Fang Y, Hijazi A A, Aboutorab H. Transformer-Based named entity recognition in construction supply chain risk management in Australia. IEEE Access, 2024, 12(3): 41829-41851. DOI: 10.1109/ACCESS.2024.3377232

[4] Almutiri T, Nadeem F. Markov models applications in natural language processing: a survey. I.J. Information Technology and Computer Science, 2022, 2(1): 1-16. DOI: 10.5815/ijitcs.2022.02.01

[5] Eker K, Pehlivanoğlu M K, Eker A G, Syakura M A, Duru N. A comparison of grammatical error correction models in English writing. IEEE Access, 2023, 56(13): 218-223. DOI: 10.1109/UBMK59864.2023.10286642

[6] Yu Z, Shi X, Zhang Z. A multi-head self-attention transformer-based model for traffic situation prediction in terminal areas. IEEE Access, 2023, 11(7): 16156-16165. DOI: 10.1109/ACCESS.2023.3245085

[7] Xiong W. Web News Media retrieval analysis integrating with knowledge recognition of semantic grouping vector space model. Informatica, 2024, 48(5): 41-54. DOI: 10.31449/inf. v48i5.5377

[8] Peng F, McCallum A. Information extraction from research papers using conditional random fields. Information Processing & Management, 2006, 42(4): 963-979. DOI: 10.1016/j.ipm.2005.09.002

[9] Huang Z, Xu W, Yu K. Bidirectional LSTM-CRF models for sequence tagging. arXiv preprint arXiv:1508.01991, 2015. DOI: 10.48550/arXiv.1508.01991

[10] Devlin J, Chang M W, Lee K, Toutanova K. Bert: Pre-training of deep bidirectional transformers for language understanding. Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers), Minneapolis, Minnesota, 2019: 4171-4186. DOI: 10.18653/v1/N19-1423

[11] Chayintr T, Kamigaito H, Funakoshi K, Okumura M. Latte: Lattice attentive encoding for character-based word segmentation. Journal of Natural Language Processing, 2023, 30(2): 456-488. DOI: 10.5715/jnlp.30.456

[12] Patel M, Ezeife C I. BERT-based multi-task learning for aspect-based opinion mining. International conference on database and expert systems applications, Springer International Publishing, Cham, 2021: 192-204. DOI: 10.1007/978-3-030-86472-9_18

[13] Zhai Z, Fan R, Huang J, Xiong, Zhang L, Wan J, Zhang L. A named entity recognition method based on knowledge distillation and efficient Global Pointer for Chinese medical texts. IEEE Access, 2024, 12(4): 83563-83574. DOI: 10.1109/ACCESS.2024.3405997

[14] Ranjan R, Daniel A K. CoBiAt: A sentiment ClassificatiCobiat: A sentiment classification model using hybrid Convnet-Dual-lstm with attention mechanismon model using hybrid ConvNet-Dual-LSTM with attention mechanism. Informatica, 2023, 47(4): 523-536. DOI: 10.31449/inf. v47i4.3911

[15] Yang C, Sheng L, Wei Z, Wang W. Chinese named entity recognition of epidemiological investigation of information on COVID-19 based on BERT. IEEE Access, 2022, 10(3): 104156-104168. DOI: 10.1109/ACCESS.2022.3210119

[16] Zhao P, Wang W, Liu H, Han M. Recognition of the agricultural named entities with multifeature fusion based on Albert. IEEE Access, 2022, 10(9): 98936-98943. DOI: 10.1109/ACCESS.2022.3206017

[17] Gonçalves T, Rio-Torto I, Teixeira L F, Cardoso J S. A survey on attention mechanisms for medical applications: are we moving toward better Algorithms? IEEE Access, 2022, 10(7): 98909-98935. DOI: 10.1109/ACCESS.2022.3206449

[18] Yang Z, Ma J, Chen H, Zhang J, Chang Y. Context-aware attentive multilevel feature fusion for named entity recognition. IEEE transactions on neural networks and learning systems, 2022, 35(1): 973-984. DOI: 10.1109/TNNLS.2022.3178522

[19] Biswas S, Poornalatha G. Opinion mining using multi-dimensional analysis. IEEE Access, 2023, 11(5): 25906-25916. DOI: 10.1109/ACCESS.2023.3256521

[20] Haque M Z, Zaman S, Saurav J R, Haque S, Islam M S, Amin M R. B-ner: A novel bangla named entity recognition dataset with largest entities and its baseline evaluation. IEEE Access, 2023, 11(1): 45194-45205. DOI: 10.1109/ACCESS.2023.3267746

[21] Liu Y, Wen F, Zong T, Li T. Research on joint extraction method of entity and relation triples based on hierarchical cascade labeling. IEEE Access, 2022, 11(3): 9789-9798. DOI: 10.1109/ACCESS.2022.3232493

[22] Rafi T H, Ko Y W. HeartNet: Self multihead attention mechanism via convolutional network with adversarial data synthesis for ECG-based arrhythmia classification. IEEE Access, 2022, 10(7): 100501-100512. DOI: 10.1109/ACCESS.2022.3206431

[23] Chen X, Cong P, Lv S. A long-text classification method of Chinese news based on BERT and CNN. IEEE Access, 2022, 10(5): 34046-34057. DOI: 10.1109/ACCESS.2022.3162614

[24] Shen Y, Liu Q, Fan Z, Liu J, Wumaier A. Self-supervised pre-trained speech representation based end-to-end mispronunciation detection and diagnosis of Mandarin. IEEE Access, 2022, 10(6): 106451-106462. DOI: 10.1109/ACCESS.2022.3212417

IoT-Enabled Hierarchical Architecture for Intelligent Home-Based Elderly Care: A Multi-Objective Optimization Approach

Jiaoqian Xiao*
Changzhi Medical College, Changzhi 046000, Shanxi, China
*E-mail: 15197901237@163.com

Keywords: intelligent elderly care, internet of things, ecosystem, home-based elderly care, data acquisition

Received: March 13, 2025

With the acceleration of global aging process, the contradiction between the home care needs of disabled elderly and limited nursing resources is becoming increasingly prominent. To address monitoring blind spots, delayed responses, and lack of personalized services in traditional elderly care models, a smart elderly care ecosystem based on the Internet of Things is constructed. By integrating data collection, transmission, and intelligent service modules through a layered architecture design, a multi-modal sensor network is deployed to fuse physiological parameters, behavioral trajectories, and environmental data. The research involves deploying Raspberry Pi 4B edge nodes in 15 households of disabled elderly individuals, integrating wearable devices, ultra-wideband positioning tags, and environmental sensors, totaling 23-28 units per household. The sampling frequency is 1 Hz during the day and 0.017 Hz at night, with an average data volume of 12.7 GB per day. The core algorithm includes an improved LZW compression algorithm that reduces data redundancy through differential preprocessing and dynamic dictionary elimination, a dynamic priority scheduling mechanism that uses a random forest classifier to identify event urgency and predicts pre-allocated bandwidth based on LSTM behavior, and a multi-objective particle swarm optimization algorithm for balancing energy consumption and load distribution. The proposed system was deployed in home-based elderly care for disabled individuals. The results showed that the improved compression algorithm and dynamic priority scheduling mechanism reduced the compression rate by 40.09% and shortened the transmission delay of key data in network jitter scenarios by 61.3% at a sampling frequency of 6 times/min. After introducing a multi-objective optimization load balancing strategy, the day and night energy consumption were reduced by 30.8% and 27.5%, respectively. In the 12-month controlled experiment, a single-group pre-post design was adopted, with 30 participants aged 72.5±6.8 years. Based on the MIT-BIH arrhythmia database and the UR fall dataset, the training set was constructed to verify that the prediction accuracy of chronic diseases increased to 81.5% (the original baseline was 67.7%, $p<0.001$), the incidence of bedsores decreased by 78.9% (the original baseline was 37%), and the nursing cost decreased by 62.1% (the original baseline was 9,354 RMB/month). The study proposes a technical approach to mitigate resource mismatches in home-based elderly care services by constructing a closed-loop management system of "monitoring-warning-intervention", promoting the intelligent elderly care towards ecological and precise direction.

Povzetek: Članek predstavi večnivojsko IoT-arhitekturo za pametno domačo oskrbo starejših, ki združuje večmodalno zaznavanje, stiskanje ILZW, dinamično razvrščanje prednosti (RF+LSTM) in večciljno PSO-optimizacijo. Sistem zmanjša porabo energije ter izboljša točnost napovedi bolezni.

1 Introduction

With the intensification of global population aging, the number of disabled elderly people is also increasing year by year. This not only poses a huge challenge to the social welfare system, but also brings unprecedented pressure to the home-based elderly care model for disabled individuals. The family-based care model for disabled elderly is difficult to bear the main responsibility of home-based elderly care due to factors such as shrinking family size and changes in intergenerational relationships, while institutional elderly care faces problems such as limited resources, high costs, and shortage of manpower [1]. Therefore, exploring new elderly care models and technological solutions tailored to disabled individuals has become an urgent task. The rapid development of new quality productive forces such as information technology, Artificial Intelligence (AI), big data, and the Internet of Things (IoT) provides new opportunities for the intelligent upgrading of elderly care services for disabled populations. IoT refers to a network system that connects various physical devices, vehicles, buildings, daily necessities and other objects through the Internet to collect and exchange data [2]. As an emerging elderly care model for disabled individuals, intelligent elderly care integrates disabled elderly people,

communities, medical staff, medical institutions, governments, and service agencies through modern technology to form a targeted intelligent service system. Due to the limitations of physical functions, disabled elderly people have a more urgent need for elderly care services [3]. However, there are still many shortcomings in current elderly care services in meeting the personalized needs.

The primary goal of the research is to address three core issues in the home-based care scenario for disabled elderly individuals: insufficient real-time monitoring, lack of dynamic response mechanisms, and resource allocation. In terms of real-time sensor monitoring, traditional single-point sensors struggle to capture the dynamic associations between physiological, behavioral, and environmental multi-modal data, leading to delayed health risk predictions. Regarding the response mechanism, existing systems lack hierarchical transmission strategies based on event urgency, resulting in excessive delays in critical tasks under high-concurrency scenarios. In terms of resource allocation, there is a mismatch between the supply of nursing resources and the personalized needs of the elderly, and service scheduling lacks support from multi-objective optimization.

A multi-mode data collection network integrating physiological monitoring, behavior tracking, and environmental perception is established to address the above issues, improving the sensitivity of abnormal sign recognition. The LZW compression algorithm and dynamic priority scheduling mechanism are optimized to reduce the transmission delay of critical data. A blockchain driven multi-agent collaboration framework and service orchestration strategy are used to optimize nursing resources.

The study employs three types of validation methods to assess target achievement. In the algorithm performance comparison experiment, on the standard dataset (MIT-BIH arrhythmia database), ILZW is compared with traditional LZW and ISRLE algorithms, with an expected compression rate of ≤15%. In high packet loss and mixed jitter scenarios, the expected data recovery rate is ≥85%. In network performance stress tests, Mininet-WiFi simulates NB-IoT bandwidth limitations, with an expected end-to-end latency for emergency events of ≤800ms. In a multi-device concurrent (20 terminals) scenario, the expected critical task failure rate is ≤1.0%. In the health management control experiment, a single-group pre-post design (N=30) is used, with an expected monthly reduction in bedsores incidence of ≥70%. From the nursing time statistics and consumable records, the expected monthly reduction in nursing costs is ≥50%.

The innovation of the research lies in designing a hierarchical architecture intelligent elderly care ecosystem based on IoT technology. By integrating physiological monitoring, behavior tracking, and environmental perception into a multi-modal sensor network, and combining the Improved Lempel-Ziv-Welch (ILZW) algorithm and intelligent hierarchical transmission mechanism, efficient data processing and transmission have been achieved. A multi-objective optimization strategy is adopted to balance energy consumption and load, ensuring the stability and efficiency of the system. The contribution of the research lies in providing a systematic solution to the resource allocation problem in home-based elderly care, and providing reference for the technological iteration and social service collaboration in the field of smart elderly care.

2 Related works

Intelligent elderly care utilizes advanced information technology and IoT technology to improve the quality of life of elderly people, help them live more independently, and provide better support for caregivers and family members. He et al. proposed an intelligent elderly care space design based on the Kano model to improve the quality of home-based elderly care. The results indicated that this design made the method more approachable and shortened the psychological distance between the elderly and the intelligent elderly care space [4]. Yin et al. developed a new intelligent elderly care service model to address the worsening population aging. The results indicated that the intelligent elderly care service model could reduce the burden of family elderly care, which was an effective way to actively respond to population aging [5]. Yang et al. designed an intelligent nursing bed based on a low-cost resource constrained micro-controller to cope with the nursing pressure brought about by the increasing global aging population. The results showed that the gesture recognition accuracy of the device was 96.65% [6]. Ghosh analyzed the current application status of AI technology in the field of addressing malnutrition in the elderly. Deploying nutrient intake monitoring systems based on AI still posed challenges due to regional differences in dietary habits and personalized hospital menus [7]. Mohan et al. reviewed the application of AI, the IoT, and sensor technology in the prevention of falls among the elderly. The results indicated that AI and IoT technology were the best solutions for preventing falls in the elderly [8].

With the development of cloud computing, big data, and AI technologies, the application scenarios of the IoT are constantly expanding. Li et al. discussed the current application status and development prospects of IoT technology in the field of mental health services. The results indicated that IoT technology could improve the quality of life of patients with mental disorders, but it also faced challenges on patient privacy and security [9]. Ni et al. proposed an intelligent monitoring system based on the Medical IoT to improve the medical monitoring efficiency of elderly patients and patients with chronic diseases. Real-time data such as location, weight of infusion urine bags and heart rate were collected through low-cost sensors and transmitted to the cloud server via wireless network. Medical staff could check the patient's status with the help of mobile applications, reducing human resource consumption and improving the flexibility of diagnosis and treatment [10]. SanchezIborra et al. proposed a hierarchical integration TinyML solution to achieve intelligent perception in the distributed IoT.

Heterogeneous terminal decision-making was integrated through a two-layer edge computing architecture and applied to intelligent agriculture scenarios. This method reduced the frequency of wireless transmission while lowering energy consumption and response delay, and enhanced data privacy protection, providing an efficient solution for edge intelligence in resource-constrained environments [11]. Almasoudi et al. evaluated IoT information security in the health care for people with disabilities from strategy, technology, organization, personnel, and environment to identify assets, threats, and protective measures, combining the confidentiality, integrity, and availability assessment and safety performance. Case studies showed that this method could be flexibly updated, revealing the correlations between various elements and providing an extensible evaluation framework for medical IoT security research [12]. Wang et al. proposed a solution based on the IoT and edge computing technology to improve the information processing efficiency of the expressway intelligent transportation system. The results indicated that this approach outperformed traditional intelligent transportation systems in monitoring response speed, congestion rate, and accident rate prediction [13]. The comparison of relevant studies is shown in Table 1.

Table 1: Comparison analysis of relevant studies

Author (Year)	Method/Technology	Dataset/Application Scenario	Accuracy/Performance	Latency	Energy Consumption	Limitations
He et al. (2023) [4]	Kano model-based smart elderly care space design	Simulation environment (no specific dataset)	Psychological distance reduced by 38%	Not mentioned	Not mentioned	No validation of real-user scenario adaptability
Yin et al. (2023) [5]	Novel intelligent elderly care service model	Community pilot (N=200)	Family burden reduced by 52%	Not mentioned	Not mentioned	Lacks dynamic resource scheduling
Yang et al. (2024) [6]	Low-cost microcontroller-based smart nursing bed	Lab gesture dataset (N=50)	Gesture recognition accuracy 96.65%	≤200 ms	0.8 W	Lacks real-time health monitoring
Ghosh (2024) [7]	AI-based nutrition monitoring system review	Multi-regional hospital menu data (N=300)	Personalized menu matching rate 68%	Not mentioned	Not mentioned	Limited generalization due to dietary habits
Mohan et al. (2024) [8]	AIoT-enabled fall prevention review	Public fall dataset (URFD)	Average recall rate 89.7%	Not mentioned	Not mentioned	Lacks dynamic priority scheduling
Li et al. (2024) [9]	IoT-based mental health services	Mental disorder patients (N=120)	Quality of life improved by 23%	Not mentioned	High device dependency	Weak privacy protection mechanisms
Ni et al. (2023) [10]	Medical IoT smart monitoring system	Hospital infusion monitoring (N=80)	Infusion anomaly detection rate 94%	120 ms	2.1 W	Limited to clinical settings, not adaptable to home environments
SanchezIborra (2023) [11]	Hierarchical TinyML edge intelligence solution	Smart agriculture dataset (N=1500)	Energy consumption reduced by 40%	≤500 ms	0.5 W	Untested in complex home network jitter scenarios
Almasoudi (2023) [12]	Healthcare IoT security assessment framework	Disabled care case studies (N=45)	Security compliance score 92%	Not mentioned	Not mentioned	Unquantified data misuse risks
Wang and Shang (2024) [13]	Edge computing-based traffic monitoring	Highway monitoring data (10 km)	Response latency reduced by 45%	85 ms	12.3 W	Not optimized for resource-constrained home elderly care scenarios
Proposed Approach (2025)	Multimodal IoT ecosystem	Real home scenarios (N=30)	Chronic disease prediction accuracy 81.5%	235 ms	Daytime/Nighttime energy consumption ↓30.8%/27.5%	Needs enhanced privacy protection techniques

In summary, most existing studies (such as smart nursing beds and fall prevention systems) focus on optimizing a single function, lacking dynamic hierarchical response mechanisms for emergencies (such as abnormal heart rates and falls). This results in significant delays in critical tasks during high-concurrency scenarios, making it difficult to meet the real-time requirements of home environments. Moreover, current technologies (such as edge computing for traffic monitoring and agricultural IoT solutions) are often designed for industrial or urban settings, which do not suit the frequent network jitter and strong device heterogeneity of home environments, making it challenging to balance energy consumption and stability. The research on msental health monitoring and nutritional management relies heavily on manually annotated data, lacking a closed-loop feedback mechanism that can dynamically capture real-time changes in disabled elderly individuals. These limitations

make it difficult for existing technologies to achieve an ecological closed-loop management system of "monitoring-warning-intervention." To address the insufficient dynamic response capability in existing technologies, this study combines Random Forest (RF) classification with Long-Term Short-Term Memory (LSTM) networks for contextual reasoning, enabling preemptive transmission of urgent tasks and reducing key data transmission latency in bandwidth-constrained scenarios. Additionally, to tackle the challenge of network heterogeneity in home environments, a multi-objective optimization load balancing strategy is designed, using Particle Swarm Optimization (PSO) to dynamically coordinate service quality, energy consumption, and load balancing, thereby reducing equipment energy consumption over time. A blockchain-driven ecological closed-loop architecture is constructed, incentivizing collaboration among hospitals, pharmaceutical companies, and other stakeholders through quantified data contribution, and forming a "risk-sharing-data-sharing-benefit-repayment" model.

3 Methods and materials

3.1 Architecture design of intelligent elderly care system based on IoT

When building an IoT-based home care ecosystem for disabled elderly, the research first focuses on the design and technical implementation of the system architecture to ensure efficient operation and meet the diverse needs. The research adopts a modular and layered design approach, dividing the system into three main modules: data acquisition layer, data transmission layer, and intelligent service layer. Through IoT technology, the collaborative work among these modules is achieved, providing real-time and reliable home-based elderly care support for the elderly [14]. The architecture of the home intelligent elderly care IoT system for disabled elderly is shown in Figure 1.

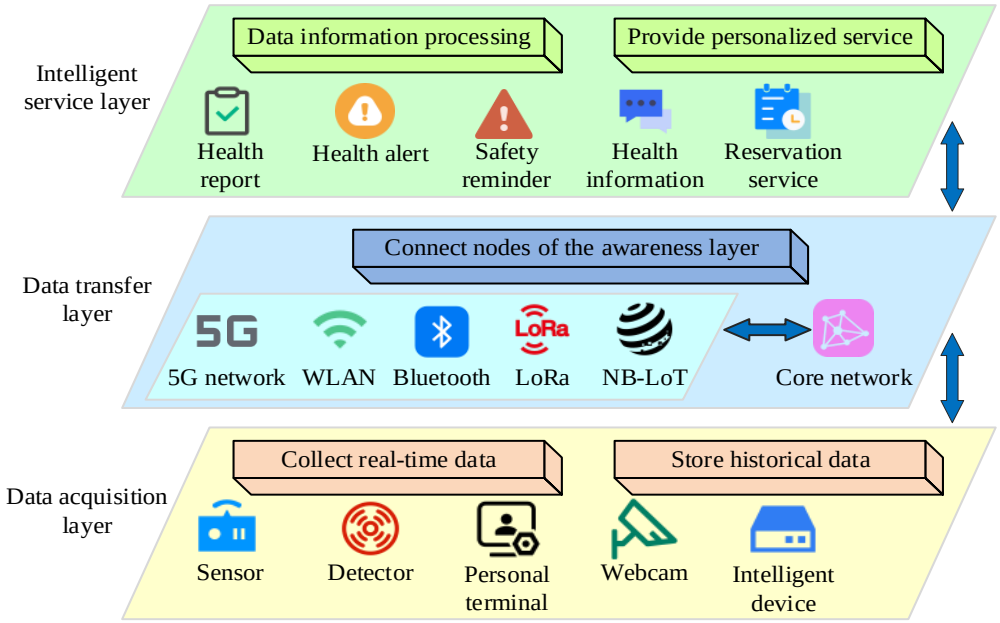


Figure 1: Architecture of intelligent home care IoT system for disabled elderly

In Figure 1, the data acquisition layer focuses on the deployment and optimization of sensor networks. By configuring multiple intelligent sensors, various physical data in the environment of disabled elderly people can be collected. Intelligent sensors include physiological parameter monitoring devices, such as wearable heart rate and blood oxygen monitors. Environmental sensing devices include smoke and gas leak sensors, behavior tracking devices such as infrared motion sensors and pressure pads [15]. In the data acquisition layer, physiological monitoring employs Photoplethysmography technology due to its non-invasive and low-power characteristics, ensuring long-term wear comfort. Environmental sensing uses a combination of electrochemical sensors and Micro-Electro-Mechanical Systems, reducing bandwidth usage and supporting local calibration. Behavioral tracking utilizes ultra-wideband technology, leveraging its high-precision positioning at the 10 cm level and strong penetration capabilities to adapt to complex home environments. To improve the pertinence of data collection and reduce resource waste, a data collection strategy based on spatial partitioning is designed, which divides the home environment into sub areas with clear functions. This strategy optimizes sensor deployment based on the characteristics and needs of activity areas such as bedrooms, living rooms, kitchens, bathrooms, and corridors. The activity trajectory and lifestyle habits are analyzed to identify regional functions. Floor plan and ultra wideband indoor positioning technology are used to divide boundaries and evaluate priority based on the needs of the elderly [16]. Through continuous 30-day behavioral monitoring of 12 disabled

elderly individuals, their daily activity range is mainly concentrated within a 0.5-1.5 m space. A grid that is too small can lead to high sensor density, while a grid that is too large can reduce the accuracy of fall detection. The study compares different grid densities through pre-experiments. When the grid size is reduced to 0.5 m×0.5 m, the positioning accuracy is improved to 0.12 m, but the number of devices increased by 120%, and the average daily energy consumption is 68%. When the grid expands to 2 m×2 m, the number of devices decreases by 55%, but the missed critical event rate increases to 15%. A 1 m×1 m grid achieves the optimal balance between positioning accuracy and sensor deployment cost. Therefore, the sensors are arranged in a 1 m×1 m grid pattern. Sensor positions are determined based on activity frequency and demand weights. During the day, elderly people are more active, moving an average of 12 times per hour, while at night, their activity frequency drops to 1.5 times per hour. Through simulation experiments comparing data integrity and energy consumption under different sampling frequencies, 1 Hz daytime sampling can cover 95% of critical events (such as abnormal heart rates), while nighttime sampling once per minute only misses 2% of low-risk events. Additionally, maintaining 1 Hz sampling at night increases the device's daily energy consumption by 81%, but the detection rate of critical events improves by only 0.8%. If the daytime sampling frequency is reduced to 0.5 Hz, the error rate in reconstructing activity trajectories rises from 7.2% to 19.5%. Therefore, the device performs high-frequency sampling at 1 time/s during the day and low-frequency sampling at 1 time/min at night to reduce redundancy in data collection and energy consumption of the device.

To ensure the fast and secure transmission of multi-source data, this study constructs a data transmission layer through a hybrid network architecture, utilizing various network communication methods such as narrowband IoT and wireless LAN to adapt to communication needs in different scenarios. The maximum data throughput supported by the system is 10 Mbps, and each edge node can access 30 terminal devices simultaneously. 20% of the reserved bandwidth is reserved for dynamic load balancing to cope with peak traffic. At the protocol level, NB-IoT is based on the 3 GPP Release 13 standard, supporting a single-link transmission rate of 62.5 kbps for uplink and 26.15 kbps for the downlink. WLAN uses the IEEE 802.11 n protocol, with a theoretical bandwidth of 150 Mbps and an actual coverage radius of 50 m (indoor). The NB-IoT base station supports up to 50,000 device connections per cell (in compliance with 3 GPP TS 36.211 specifications), while the LoRa gateway operates at a bandwidth of 125 kHz, with the transmission rate ranging from 0.3 kbps to 50 kbps (LoRaWAN TS001-1.0.4), covering a radius of 1.5 km (urban environment). The system coordinates multiple protocols through an adaptive channel allocation mechanism (TDMA + CSMA/CA) to ensure the success rate of critical data transmission.

The intelligent service layer aims to adapt to the aging as its core goal, reducing operational complexity through multi-modal hardware interaction design, ensuring that disabled elderly people can intuitively and conveniently use system functions, while providing various services such as health alerts, safety warnings, appointment arrangements, health status reports, and medical consultations. In the intelligent service layer, edge computing nodes handle real-time tasks locally, reducing cloud transmission pressure. The cloud platform uses AWS IoT Core, leveraging its encryption and device shadow functions to ensure data security and offline caching. Human-computer interaction employs an offline voice engine and thin-film piezoresistive sensors to balance internet availability with durability for frequent use.

In the process of data transmission, data compression technology is introduced to optimize bandwidth utilization. Small fluctuations in physiological parameters can indicate early symptoms of atrial fibrillation or precursors to respiratory failure. Using lossy compression may lead to distortion of characteristic waveforms, posing a risk of false-negative diagnoses. Additionally, according to ISO 27799: 2016 Health Information Security Management Standard Clause 8.3, raw physiological data must be maintained at the bit level for audit trail purposes. Lossy compression results in irreversible data loss. Regarding the physiological data of disabled elderly individuals, the IZWL algorithm is used for lossless compression [17]. The algorithm flow is shown in Figure 2.

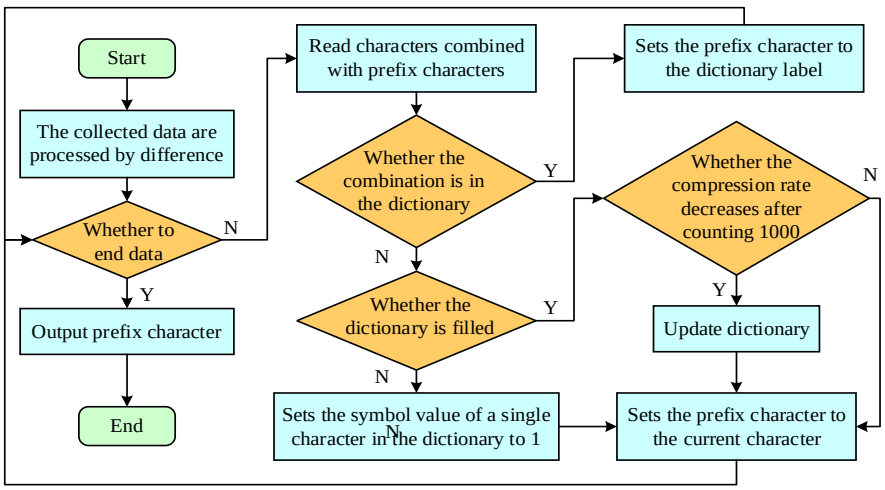


Figure 2: Improved LZW flow

As shown in Figure 2, in the ILZW algorithm, the data collected by the sensors is first preprocessed for differences, and the data repetition rate is improved by calculating the differences between adjacent data. Then, a dictionary with appropriate size is selected and the hash storage is taken instead of traditional sequential storage to improve search efficiency and compression speed. During the compression process, the dictionary is updated when a decrease in compression rate is detected, while commonly used single characters are saved and infrequently used dictionary entries are released to increase space utilization. In addition, the dictionary is not updated immediately after it is filled, but is adjusted according to the data duplication situation, and only updated when the compression rate increases.

Regarding the dictionary update frequency, this study introduces an adaptive triggering mechanism based on data repetition rate changes in the ILZW algorithm. When the data repetition rate decreases by more than 5% over ten consecutive compression processes, the system automatically triggers a dictionary update operation and uses a Markov prediction model to prioritize the elimination of dictionary entries that have not been referenced for nearly 30 minutes. When device resources are limited, the dictionary storage space is changed from a static array in traditional LZW to a linked hash table using a hash index structure. The least recently used (Least Recently Used, LRU) algorithm is employed to cache the access sequence of dictionary entries, thereby reducing memory fragmentation. Additionally, the study implements variable-length encoding for character compression, optimizing the byte count of a single dictionary entry from a fixed 3 bytes to a dynamic 1-4 bytes encoding, further reducing resource consumption.

To optimize bandwidth utilization, a priority scheduling mechanism is utilized to prioritize the key data transmission with high real-time requirements, such as abnormal heart rate alarm data, while compressing non-emergency data such as environmental monitoring and sending them in batches. The architecture and workflow of the priority scheduling mechanism are shown in Figure 3.

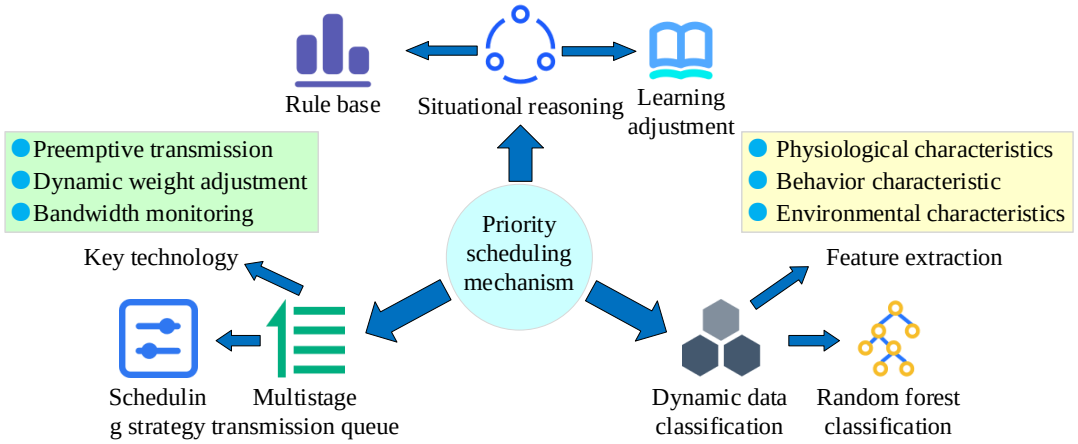


Figure 3: Architecture and workflow of priority scheduling mechanism

In Figure 3, the priority scheduling mechanism designed in the research works together through three core modules: dynamic data classification, multi-level queue management, and real-time contextual inference, to achieve intelligent hierarchical guarantee of data transmission. In dynamic data classification, feature extraction is performed on the raw sensor data stream, including physiological characteristics, behavioral characteristics, and living environment characteristics of disabled elderly people. The RF method is used to train datasets and annotate historical events such as falls and heart rate abnormalities. The acceleration variance, continuous heart rate anomaly, and residential environment temperature mutation rate of wearable devices are assigned different importance weights, and classification labels are output according to high, medium, and low priority. In multi-level transmission queue management, emergency situations such as fall alarms and cardiac arrest are set as high priority. Sleep apnea and high-temperature warning are set to medium priority. Temperature, humidity, lighting data, etc. are set as low priority. When a high priority event is identified, the current transmission task is immediately suspended, independent transmission paths are divided, and preemptive transmission is performed. The network utilization is calculated in real-time. When the bandwidth usage exceeds 80% and lasts for 5 seconds, the low priority queue is paused.

The RF training dataset is used to annotate historical events such as falls and abnormal heart rate. RF suppresses sensor data noise through multi-tree integration and voting mechanisms, adapting to the heterogeneity of physiological, behavioral, and environmental characteristics. Compared with XGBoost and CNN, RF is faster in inference speed for edge devices, meeting the real-time response requirement of fall detection within 50 ms. Additionally, RF supports variable-length time series data input, eliminating the need for fixed-window preprocessing required by CNN, making it suitable for deployment on low-power microcontrollers. The dataset

includes 12,850 groups of annotated event data, covering six categories of priority events (falls, abnormal heart rate, etc.). Among them, 7,320 groups come from the clinical monitoring records of the geriatrics department at a hospital from 2021 to 2023. 3,610 groups are collected in real-time through sensor networks deployed in 15 households with disabled elderly individuals. The remaining 1,920 groups are from public datasets (the MIT-BIH Arrhythmia Database and the UR Fall Detection Dataset). The historical event data with annotations is divided into training, validation, and independent test sets in a ratio of 7:2:1, maintaining consistent sample proportions across categories. The training is conducted using Python's Scikit-learn library. During the training phase, the RF classifier model undergoes stratified 10-fold cross-validation to optimize model hyperparameters. In each fold of validation, the average accuracy of the model is calculated. The final model achieves an accuracy of 92.4% (±1.2%) on the independent test set.

To further evaluate the performance of the RF classifier, the study quantifies the model through feature importance score and confusion matrix. The study calculates the feature importance score based on the reduction of Gini impurity, and screens out the top 5 features with the highest contribution to classification, as shown in Table 2.

Table 2: Characteristic contribution

Feature category	Weighted score
Acceleration variance of wearable devices	0.32
The number of consecutive abnormal heart rates	0.28
The temperature fluctuation rate of the living environment	0.19
Standard deviation of nighttime activity duration	0.12
Gradient of light intensity variation	0.09

From Table 2, the contribution of acceleration variance to fall event detection is the highest, accounting for 32%, which verifies its core role in emergency event classification. In the confusion matrix verification, multiple classification confusion matrices are generated on the independent test set, and key indicators are shown in Table 3.

Table 3: Key indicator confusion matrix

True\Predicted	Fall (High-Priority)	Heart rate anomaly (High)	Sleep apnea (Medium)	Environmental anomaly (Low)	Normal (Low)
Fall	284	5	2	1	0
Heart rate anomaly	8	189	3	0	0
Sleep apnea	3	2	145	4	1
Environmental Anomaly	0	1	6	92	2
Normal	1	0	2	5	381

In Table 3, the model performs excellently in classifying five types of events. For high-priority events, the recall rate for fall detection is 98.3%, with an accuracy of 96.2%. The recall rate for abnormal heart rate is 94.5%, indicating that the model can accurately identify emergencies. For medium-priority events, the recall rate for apnea is 93.5%, with misjudgments mainly due to similar characteristics to high-priority events. For low-priority events, the recall rate for environmental abnormalities is 89.3%, with a normal state accuracy rate of 98.9% and a false positive rate of ≤2.8%. The overall classification accuracy is 91.7%, with a Macro-F1 value of 0.902, verifying the model's balanced performance across multiple categories. For task segmentation within the same priority category, a sub-priority dynamic evaluation model is designed to achieve refined scheduling through event urgency quantification indicators. Taking high-priority tasks as an example, the system extracts three core features: Response Time Threshold (RTT), Anomaly Gradient Physiological parameter (APG), and Historical Impact Factor (HIF), to construct an evaluation system. In RTT, the gold standard response time for cardiac arrest events is defined as ≤4 minutes (RTT=1), and the effective intervention time for fall alarms is defined as ≤10 minutes (RTT=2). Absolute time windows are allocated to different events using hardware timers. For APG, the rate of change in real-time heart rate relative to baseline values (ΔHR/minute) is calculated when heart rate is abnormal. When ΔHR> 50 bpm, it is marked as APG=1 (extremely critical). When 20 bpm <ΔHR ≤ 50 bpm, it is marked as APG=2 (high-risk). For HIF, based on the handling results of similar events over the past 30 days, if a timely response leads to complications, HIF=1. If a successful intervention is made, HIF=2. By integrating these features using a fuzzy logic controller, a sub-priority coefficient in the 0-1 range is output, with smaller values indicating higher priority.

In real-time situational reasoning, the long short-term memory network is used to learn the daily activity patterns of the elderly, and a relevant rule library is established. By predicting the behavior status for the next hour in real time, the transmission strategy of relevant data is preloaded. LSTM employs a two-layer stacked architecture. Based on the 24-hour activity trajectory data collected from ultra-wideband positioning systems, an input sequence with a time step of 60 is constructed using a sliding window mechanism (each time step corresponds to a 24-minute behavior segment). The network structure includes two 64-unit LSTM layers, which use layer normalization to enhance temporal feature extraction capabilities. The output layer predicts the behavior state for the next hour through a Sigmoid function. The training data comes from a behavioral trajectory dataset of 300 disabled elderly people for 6 consecutive months (with a total sample size of 2.16 million). The loss function L

adopts the improved weighted binary cross entropy loss, as shown in equation (1).

$$L = -\frac{1}{N}\sum_{i=1}^{N}[\tau y_i \log(\hat{y}_i) + (1-y_i)\log(1-\hat{y}_i)] + \lambda \|\mathbf{W}\|_2 \quad (1)$$

In equation (1), N represents the total number of samples in the training batch, used to average the loss for each sample. y_i is the true label of the i-th sample. $\hat{y}_i$ indicates the prediction probability of the model for the i-th sample. τ is the positive class weight, used to amplify the loss contribution of rare anomalies, alleviating the class imbalance, and $\tau = 2.5$. λ is the regularization coefficient, controlling the strength of the L2 regularization term to prevent over-fitting. $\|\mathbf{W}\|_2$ is the L2 norm of the weight matrix, used to constrain model complexity. The model is deployed on NVIDIA Jetson Nano edge devices.

The collaborative mechanism between the rule base and situational reasoning learning achieves dynamic adjustment through a three-stage closed loop. First, the rule weights are dynamically updated based on LSTM learning from a 12-month historical event database to generate a priority weight evolution matrix. When the real-time inference result deviates from the pre-set value in the rule base by more than 15%, Bayesian optimization is triggered to adjust the priority threshold. Situational reasoning takes a reinforcement learning framework to update the convolution kernel parameters of the situational feature extractor every 24 hours, enhancing the ability to capture spatiotemporal features of complex behavioral patterns. The resource allocation strategy optimizes the bandwidth distribution ratio of the transmission queue according to the network utilization real-time heat map. When the number of concurrent medical devices exceeds 5, the TCP window size of the low-priority queue is automatically reduced from 64 KB to 16 KB, combined with an adaptive bandwidth compression algorithm to reduce transmission latency for emergency events.

3.2 Construction of an intelligent home care ecosystem for disabled elderly

In the process of building an intelligent elderly care ecosystem based on the IoT, it is crucial to adapt to the personalized needs of disabled elderly people and optimize system performance. The research method starts from two aspects: requirement identification and system adjustment, combined with design strategies and relevant technical means, to ensure that the system can flexibly respond to the specific situations, while maintaining long-term stable operation of the system. In terms of personalized demand adaptation, a data-driven framework for demand mapping and service customization is proposed, as shown in Figure 4.

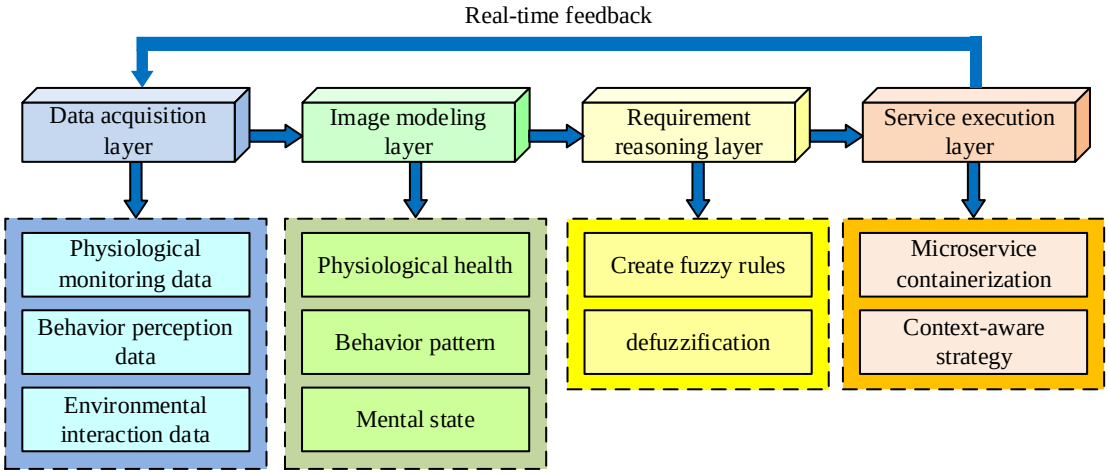


Figure 4: A data-driven framework for requirement mapping and service customization

From Figure 4, the framework first deploys multi-modal sensors to collect real-time physiological indicators, behavioral trajectories, and environmental data. The Dempster-Shafer evidence theory is used to fuse multi-source data, eliminate noise, and construct a unified temporal database [18]. By utilizing feature engineering to extract key indicators and combining online principal component analysis to dynamically update personalized state portraits, a multi-dimensional feature space covering physiology, behavior, and psychology is formed. The study employs a sliding window mechanism and an incremental learning strategy to achieve real-time personalized state mapping. Data windows are rolled every 5 minutes, with a capacity of 1,440 time-series data points. By extracting statistical features of physiological indicators, behavioral trajectories, and environmental parameters within the window, a user dynamic profile is constructed. To address data drift issues, online principal component analysis is used for dimensionality reduction and feature space updates. The study dynamically adjusts model parameters using the rank-1 correction formula of the covariance matrix, as shown in equation (2).

$$C_{new} = \delta C_{old} + (1-\delta)\frac{1}{V}\sum_{i=1}^{V}(x_i - \mu)(x_i - \mu)^T \quad (2)$$

In equation (2), C_{new} and C_{old} represent the covariance matrices before and after updates, respectively. δ is the forgetting factor and $\delta = 0.8$, used to reduce the weight of historical covariance matrices and control the model's adaptability to data drift. V is the sliding window

size and $V = 1440$. x_i is the original observation value of the i-th data sample within the window. μ is the mean vector of all data within the window, used for centering processing. The time complexity for a single update is O(d) (where d is the feature dimension and d=15), which is much lower than the $O(d^3)$ required for batch principal component analysis, making it suitable for real-time data stream processing.

The behavioral trajectory data collected by the sensor is first modeled using LSTM for temporal feature extraction, identifying behavior patterns related to psychological states. In the feature engineering phase, a behavioral feature vector is constructed, including behavioral entropy values, social activity levels, and environmental interaction frequencies. This vector is annotated and trained using the Simplified Geriatric Depression Scale (GDS-15) and the UCLA Loneliness Scale from psychometrics, forming a mapping model from behavioral data to psychological states. The output of the model is then fused through Dempster-Shafer evidence theory, ultimately forming a comprehensive state profile in multidimensional feature space that encompasses "physiological-behavior-psychological" aspects.

Based on a fuzzy logic inference engine, continuous data is transformed into fuzzy sets. Meanwhile, it matches the rule base constructed with expert experience to output demand categories and priority ratings. Specifically, the study normalizes three types of indicators: Physiological Abnormality Index (PAI), Behavioral Deviation (BD), and Environmental Risk Score (ERS), to the [0, 1] interval and processes them through triangular membership functions for fuzzification. For example, the high-risk membership function $\eta_{\text{high}}(x)$ for PAI is shown in equation (3).

$$\eta_{\text{high}}(x) = \begin{cases} 0 & x < 0.7 \\ \dfrac{x - 0.7}{0.2} & 0.7 \le x < 0.9 \\ 1 & x \ge 0.9 \end{cases} \tag{3}$$

In equation (3), x is the input value of PAI, which is quantitatively calculated from physiological indicators such as heart rate variability and blood oxygen saturation to assess the health risk level of disabled elderly individuals. The membership functions for BD and ERS are designed according to the fuzzy logic inference engine. The implementation method is consistent with that of PAI membership function. Mamdani fuzzy inference is used, and the center of gravity method is applied to resolve fuzziness, outputting a priority score ranging from 0 to 100. High priority ≥ 80, medium priority 50-79, and low priority <50. Some of the core rules in the rule base are shown in Table 4.

Table 4: Some of the core rules in the rule base

Rule ID	Conditions (Input Variables)	Priority Level	Weight	Example Scenarios	Conflict Resolution
R1	PAI≥0.9 (High-Risk) and BD≥0.7 (High Deviation)	Emergency	1.0	Heart rate surge (0.92) +Prolonged immobility (0.85)	Independent transmission path, preemptive response
R2	ERS≥0.8 (High-Risk) and PAI ≥0.7 (Medium-Risk)	Emergency	0.9	Excessive CO (0.85) +Respiratory anomaly (0.78)	Priority stacking of service combinations
R3	0.7≤PAI<0.9 (Medium-Risk) and 0.5≤ERS<0.8 (Medium-Risk)	High	0.7	Sleep apnea (0.75) +High-temperature alert (0.65)	Dynamic load balancing allocation
R4	BD<0.3 (Low Deviation) and ERS<0.4 (Low-Risk)	Low	0.2	Normal activity (0.15) +Stable environment (0.25)	Delayed processing or batch transmission

In Table 4, the rule base covers the dynamic mapping relationship between input conditions and output priority. For example, when PAI ≥ 0.9 and BD ≥ 0.7, the system determines it as an emergency event (weight 1.0) and directly triggers a preemptive response for fall alarm services. The library contains a total of 52 expert experience rules, which achieve service orchestration through weighted summation and dynamic conflict resolution mechanisms. The service orchestration layer adopts a micro-service architecture and deploys functional modules such as fall detection and voice broadcasting in Kubernetes containers to optimize resource scheduling strategies [19]. Service orchestration divides the system into independent service modules, each communicating through RESTful API. The average code length per service is less than 500 lines, and the deployment image size is less than 100 MB. Kubernetes automatically adjusts the number of replicas based on load. For example, the fall detection service reduces to one replica when concurrent traffic drops at night and expands to three replicas during the day, thereby improving resource utilization. Through Kubernetes containerized deployment, the system can dynamically allocate computing resources based on real-time needs, while achieving independent updates and version management of service modules. The fault isolation mechanism ensures that a single-point service failure does not affect other functions. Combined with the mixed integer programming model to optimize service

combinations, it meets the diverse needs of elderly individuals living at home, ensuring low latency and high efficiency.

The constraint of the mixed integer programming model is used to realize the service combination with low latency and high energy efficiency. The model is shown in equation (4).

$$\min \sum_{s=1}^{S} c_s \cdot n_s + \sum_{t=1}^{T} d_t \cdot l_t \tag{4}$$

In equation (4), n_s represents the number of deployment replicas for service s, and $s \in \{1,2,\ldots,S\}$. c_s is the unit operating cost of service s, determined by service complexity and resource consumption. d_t is the delay sensitivity coefficient of task t, reflecting the task's tolerance to delay. The coefficient for emergency alarm tasks is 10. For every 1ms increase in delay, the cost increases by 10 units. l_t is the end-to-end delay of task t, and $t \in \{1,2,\ldots,T\}$. Under the constraints of mixed integer programming models, low latency and high-efficiency service composition can be achieved. The closed-loop feedback mechanism analyzes service performance through gradient boosting tree analysis, such as response speed, elderly satisfaction, etc., and corrects inference rules and weight parameters in reverse to continuously improve system adaptability. In terms of system optimization, a multi-objective optimization based load balancing strategy is proposed to address the diversity and potential instability of IoT equipment in home environments. The framework of this strategy is shown in Figure 5.

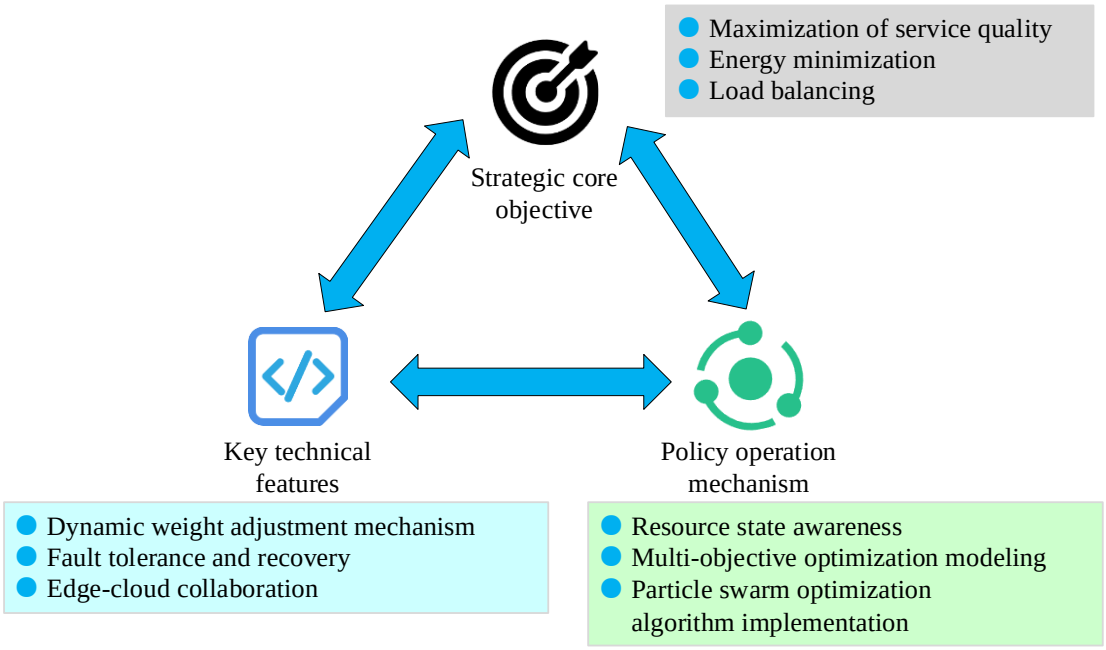


Figure 5: Load balancing policy framework based on multi-objective optimization

As shown in Figure 5, this strategy aims to minimize energy consumption, and balance load. By monitoring the network in real-time, it continuously collects key indicators such as computing load, communication delay, and remaining power of IoT equipment. Future task requirements are predicted based on historical data. The objective function of energy consumption minimization and load balancing is shown in equation (5).

$$\begin{cases} \min E = \sum_{j}^{n} (P_j \cdot T_j) \\ \min L = \sqrt{\frac{1}{n} \sum_{j=1}^{n} (C_j - \bar{C})^2} \end{cases} \tag{5}$$

In equation (5), E and L are the total energy consumption of the system and the load balancing index, respectively. n is the total number of edge nodes. P_j and T_j are the average power and active time of node j, respectively. C_j and $\bar{C}$ are the real-time load and its average value of node, respectively. The constraints are shown in equation (6).

$$\begin{cases} E_j \geq E_{\min} \\ C_j \leq C_{\text{th}} \end{cases} \tag{6}$$

In equation (6), $E_{\min}$ is the threshold of remaining power of the device, and $E_{\min} = 20\%$. C_{th} is the threshold of node load, and $C_{\text{th}} = 80\%$. Simultaneously, the task is divided into three categories: urgent, routine, and backend, and the priority scheduling rule is established for each task. Urgent tasks are prioritized for allocation to low delay nodes, while routine tasks are dynamically allocated based on load balancing principles, and backend tasks are delayed or handed over to the cloud. The PSO algorithm is used to simulate the intelligent search process of biological populations, iteratively evaluating the comprehensive performance of different resource allocation schemes in dimensions such as service

quality, energy consumption, and load balancing, and gradually approaching the optimal solution [20]. In the PSO algorithm, each particle represents the task allocation scheme, and the dimension is the number of edge nodes. The position $X_{ij} \in (0,1)$ of the particle indicates whether the task is assigned to the node. The fitness function is shown in equation (7).

$$\text{Fitness} = \beta \cdot (\frac{E}{E_0}) + \gamma \cdot L \tag{7}$$

In equation (7), β and γ are fixed weights (experimentally verified to achieve optimal energy consumption and load balancing), and $\beta = 0.6 / \gamma = 0.4$. E_0 is the initial total energy consumption. The algorithm takes 20 particles, with a maximum of 100 iterations, and an acceleration constant $c_1 = c_2 = 2.0$. Parameter selection is based on the sensitivity analysis results from reference [20], aiming to balance convergence speed and global search capability. Within 50 iterations, the objective function value stabilizes, with a standard deviation less than 5%, indicating that the convergence meets real-time scheduling requirements. The time complexity of the PSO algorithm is O(N T D), where D=2 (dimension of the objective function). The average time for a single optimization at an edge node is 12.3ms (edge node computation), meeting real-time requirements. The system triggers the PSO algorithm by monitoring network utilization in real-time. First, it suspends low-priority queues to release bandwidth resources. By dynamically adjusting the particle swarm parameters, the inertia weight is temporarily increased to 0.7 to accelerate the search.

The algorithm introduces a dynamic weight mechanism, which automatically increases the energy-saving weight when the device has low power, and focuses on optimizing response speed during peak service periods, achieving flexible trade-offs between multiple objectives. At the critical technical level, edge nodes handle real-time tasks and cache data, globally optimize resource parameters in the cloud, and combine backup path switching to ensure service continuity in fault scenarios. The home intelligent elderly care ecosystem for disabled elderly is shown in Figure 6.

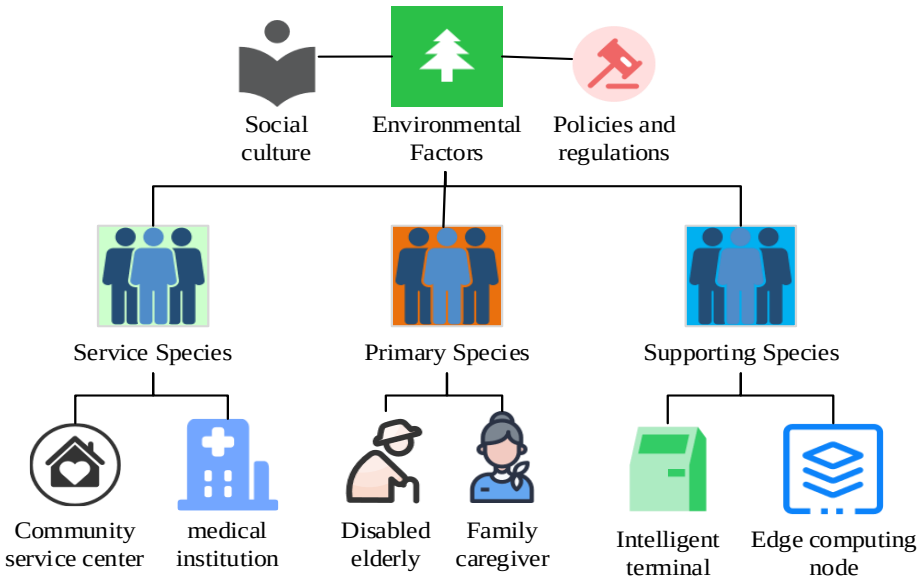


Figure 6: Ecosystem of smart home care for the disabled elderly

In Figure 6, the intelligent elderly care ecosystem is a collaborative network that integrates technology, services, and environmental elements with disabled elderly people as the core, and achieves sustainable operation through dynamic resource allocation and value exchange. The system population consists of a core population, a support population, and a service population. The core population includes the elderly and family caregivers, who generate driving data through wearable equipment and interactive behaviors. Family caregivers report abnormal behaviors of elderly individuals through mobile applications. The system triggers priority scheduling after verifying with sensor data. Health reports generated by the system are annotated, and feedback data is used to optimize feature weights in the fall detection algorithm through a gradient enhanced tree model, improving prediction accuracy. When family caregivers submit medication adherence reports, the system synchronously updates the R&D database of pharmaceutical companies and the risk assessment model of insurance companies, forming a collaborative value stream of "family-enterprise-insurance."

The support population is composed of IoT hardware, edge computing nodes, and network technology to achieve multi-modal data collection. The service population connects hospitals, communities, supermarkets, and other institutions, and maps demand to cross domain services based on reinforcement learning. The community service center receives health monitoring data from the system in real-time through block links. This includes abnormal physiological indicators of elderly individuals, high-risk behavioral events, and environmental alerts. It also coordinates medical resources and public services within the community. For example,

when the system predicts that an elderly person has a fall risk exceeding the threshold over the next 2 hours, the community service center will dispatch the nearest community nurse with a portable monitor to intervene.

Environmental factors ensure that the system complies with social ethics through policy interfaces and cultural adaptation modules. This ecosystem supports the ecological cycle through information flow and value flow. Information flow relies on online learning to achieve cross institutional knowledge sharing, while blockchain records data contribution for incentive distribution. Information flow includes real-time vital signs stream, behavioral pattern analysis stream, and environmental control command stream. The real-time vital signs stream transmits data such as heart rate and blood oxygen collected by wearable devices, with an end-to-end average delay of 83 ms, meeting the requirement for emergency response within 100 ms. The behavioral pattern analysis stream transmits behavioral trajectory segments generated by ultra-wideband positioning systems, with a peak delay of 1.2 s and a daily update cycle of 15 minutes per session. The environmental control command stream issues temperature control commands in JSON format, with an average delay of 210 ms and a feedback delay of 380 ms. The study aims to achieve sustainable motivation for multi-party collaboration through designed incentive mechanisms. The system records the data contribution values of all participants through blockchain, with quantifiable metrics including the volume of sensor data uploaded, service response frequency, and collaboration node efficiency. The government dynamically allocates subsidies based on contribution values. For example, communities receive an additional 5% of their annual budget for every 100 care tasks completed. Pharmaceutical companies pay 0.5% of their R&D revenue as data usage fees for each 100,000 anonymized health data entries. Families with data contribution values exceeding 500 can redeem free health check-ups or drug discount coupons. Pharmaceutical companies, due to shortened R&D cycles from the data, must return 12% of cost savings in the form of "medication points," where 1 point equals 1 RMB and can be used to offset medication costs. Hospitals reduce the annual fall rate among insured users to <5%, and insurance companies pay hospitals 3% of their annual premiums as a collaboration reward.

An economic closed loop is built through value streams. In the quantification of insurance industry value, the system dynamically adjusts premium strategies by reducing health risk events. Based on the proportion of risk reduction, insurers offer a 5%-8% premium discount, with a discount rate of 2% for every 10% decrease in risk rate. In practice, the cumulative discount rate can reach up to 8%. Pharmaceutical companies accelerate R&D through anonymized health trend data, while agreeing to purchase equipment worth 0.5 million RMB for every 10,000 RMB saved in R&D costs, forming a sustainable ecosystem model of "risk sharing-data sharing-benefit feedback." This ecological architecture breaks through the linear logic of traditional IoT by establishing multi-directional feedback and adaptive adjustment mechanisms, truly integrating technology into the social collaboration system, improving service accuracy, and reducing system resource redundancy. The system deployment hardware is shown in Table 5.

Table 5: System deployment hardware equipment

Device Category	Device Model	Quantity	Unit Price (RMB)	Function Description
Physiological Monitoring Sensors	HUAWEI Watch D	3 units	1,999	Real-time collection of physiological parameters (heart rate, blood oxygen, body temperature, etc.), supporting Bluetooth 5.0 communication.
	Sleepace Rest Smart Mattress	1 unit	3,999	Monitors sleep cycles, body movement frequency, and respiratory rate; transmits data through Wi-Fi.
Environmental and Behavioral Sensors	HC-SR501 Infrared Sensor	5 units	25	Detects human activity trajectories, deployed in living rooms, corridors, and other areas.
	FlexiForce A201 Pressure Mat	3 units	150	Monitors pressure distribution in sitting/lying positions, placed on seats and bedding surfaces.
	MQ-7/MQ-2 Gas Sensors	2 units	80	Detects CO and smoke concentrations, deployed in kitchens and bedrooms.
Positioning and Communication Equipment	Ultra-Wideband (UWB) Positioning Tag	6 units	300	Achieves centimeter-level positioning accuracy with UWB technology (coverage: 10m).
	Raspberry Pi 4B (8GB)	1 unit	899	Edge computing node integrating sensor gateway and local data processing modules.
Interactive Devices	Voice Interaction Terminal	1 unit	1,299	Supports voice commands for emergency calls, health inquiries, and other functions.
Network Equipment	Wi-Fi 6 Router	1 unit	599	Provides 2.4G/5G dual-band coverage and supports Mesh networking expansion.
Others	Smart Pill Box	1 unit	199	Monitors medication adherence with integrated RFID tag recognition.

The hardware devices in Figure 5 are arranged in a grid pattern (1m×1m grid) in the home environment. In the bedroom of the disabled elderly person, pressure pads are laid along the edge of the bed to monitor the pressure distribution during sitting and lying positions in real time. Smart mattresses are deployed under the bed to collect sleep cycles and respiratory rates. Gas sensors are installed near the headboard to monitor CO and smoke concentrations in real time. An infrared sensor is placed at the entrance of the bathroom to detect human entry and exit activities, while humidity sensors are installed on the ceiling to dynamically monitor environmental humidity to prevent slipping risks. A Ultra-Wideband (UWB) positioning base station is installed in the corner of the wall to achieve centimeter-level positioning with the UWB tags worn by the elderly. Infrared sensors are deployed in the corridor area to track daily activity trajectories. Gas sensors are installed near the gas pipes in the kitchen to provide real-time warnings of gas leaks. Temperature sensors are installed in the cabinet area to monitor abnormal high temperatures to prevent fires. The Raspberry Pi 4B edge computing node is placed in the center of the living room as the sensor gateway and local data processing core. The total deployment cost for a single household is approximately 11,842 RMB.

3.3 Data security and privacy

Regarding user data security issues, the study adopts a three-tier privacy protection mechanism to ensure data safety. The SHA-256 algorithm is used at the data collection end to irreversibly encrypt sensitive information such as names, ID numbers, and addresses, retaining only non-identifiable data directly related to health management (such as age, gender, and medical history codes). All sensor data, after preprocessing by edge nodes, is accessible to authorized researchers for the anonymized dataset, while healthcare institutions must obtain temporary keys approved by an ethics committee to access the data. Data transmission takes TLS 1.3 protocol encryption, and storage servers are deployed in data centers that meet ISO 27001 standards. Physical storage devices undergo regular security audits, and decommissioned equipment is physically destroyed. Considering the possible sensor deception problem, a unique digital certificate is assigned to each IoT device. The edge node verifies the legitimacy of the device through two-way TLS protocol, and the device signature based on elliptic curve digital signature algorithm is attached during data collection to prevent forged data.

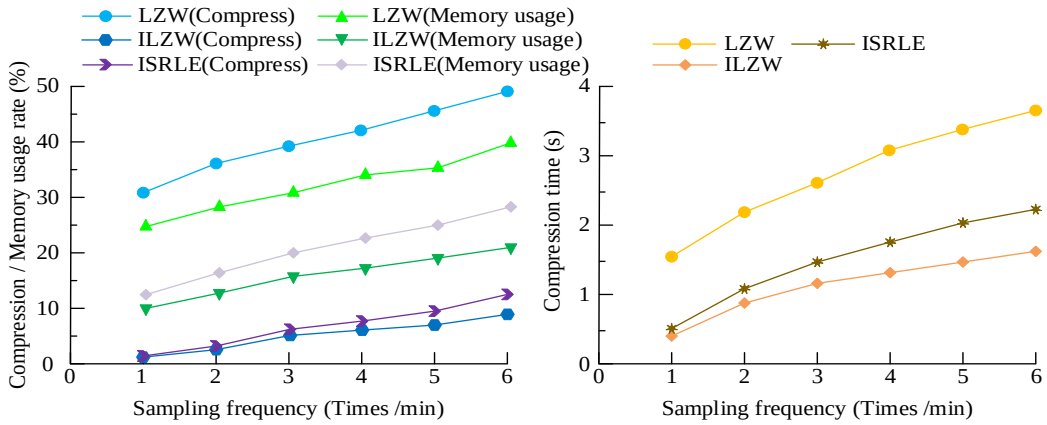
In response to the threat of network hijacking, the communication link is encrypted using TLS1.3 protocol, with keys rotated daily, and traffic anomalies are monitored in real-time through an LSTM model. For designs not fully encrypted, the primary considerations are the compatibility of resource-constrained devices and the real-time nature of emergency services. Low-power sensors take lightweight Corrected Block Tiny Encryption Algorithm to encrypt key fields, prioritizing alarm data transmission, with encryption concentrated at edge nodes. Non-sensitive data is transmitted in plaintext after de-identification, while sensitive data is protected through both AES-256 and homomorphic encryption, ensuring a balance between data integrity and privacy security [21].

Considering the potential conflict of interest, the study records all data contributions and service responses on the blockchain, labels data streams, and ensures that responsibility is traceable. When data abuse is detected, the smart contract automatically freezes access to it and triggers an audit process. In potential ethical issues, the system provides an informed consent form at deployment, clearly labeling data sharing parties and exit clauses. Any new service provider must obtain written authorization before joining. Family members can track in real-time which institutions access and use the data through a blockchain browser, with the system generating monthly data usage reports via email.

4 Results

4.1 Key technology performance optimization verification

To verify the effectiveness of the ILZW algorithm in lossless compression of data, the DHT11 humidity sensor is used to collect indoor humidity data at different frequencies for 3 days, and the collected data is compressed using the algorithm. At each sampling frequency, the compression algorithm is tested independently for 100 times, and the compression rate, memory occupancy rate and compression time are recorded for each run. The final result is the average of 100 runs. The performance of the current latest Improved Shared Run Length Coding (ISRLE) data compression method at different sampling frequencies is shown in Figure 7 [22]. In the performance testing of the ILZW algorithm, a sampling frequency of up to 6 times per minute is used, aiming to simulate the comprehensive frequency after data preprocessing at edge nodes. In practical applications, after initial screening by edge nodes to filter out duplicate and invalid signals, the transmission frequency of some non-urgent data is below 6 times per minute, forming a gradient data transmission system with one time per minute at night. Figures 7 (a) and 7 (b) show the data compression rate, memory usage, and compression time of different methods, respectively.



(a) Data compression rate and memory usage of LZW algorithm before and after improvement

(b) Compression time of LZW algorithm before and after improvement

Figure 7: Performance of each method at different sampling frequencies

In Figure 7 (a), with the increase of device sampling frequency, the data compression rate and memory usage of the LZW algorithm before and after improvement also increased. The data compression rate and memory usage of ILZW were lower than LZW throughout the entire testing process. When the sampling frequency was 6 times/min, the data compression rate and memory usage of ILZW were 8.92% and 21.87%, respectively, while the data compression rate and memory usage of LZW were 49.01% and 39.98%, respectively. The data compression rate and memory usage of the ISRLE method were basically the same as those of the ILZW when the sampling frequency was low. As the sampling frequency gradually increased, the gap between ISRLE and ILZW widened. At a sampling frequency of 6 times /min, the data compression rate and memory usage of ISRLE were 12.51% and 27.52%, respectively, which were 3.59% and 5.65% higher than the research method. As shown in Figure 7 (b), the compression time of ILZW at different sampling frequencies was lower than that of the comparison method. At the sampling frequency of 6 times /min, the compression time of ILZW was 1.65 s, while that of ISRLE and LZW was 2.24 s and 3.72 s, respectively. The compression time of the research method was reduced by 55.65% compared with the traditional method. The improved algorithm reduces data compression rate and compression time by optimizing preprocessing and storage strategies.

In terms of algorithm complexity, the time complexity of the traditional LZW algorithm is O(n), where n is the length of the input data. The ILZW algorithm optimizes the average time complexity to O(n/k) through a hash storage structure and dynamic dictionary adjustment strategy, where k is the length of repeated pattern units formed during the preprocessing stage through difference calculation ($k \geq 2$). The time complexity of ISRLE is O(n), but it requires additional processing for shared repetitive patterns. In terms of space complexity, the traditional LZW takes a fixed dictionary, resulting in a space complexity of O(m), where m is the maximum number of entries that the dictionary can store. The ILZW reduces the space complexity to $O(m/\alpha)$ through hash indexing and dictionary item elimination mechanisms, with $\alpha = 1.25$ being the experimental-determined dictionary space compression coefficient. The space complexity of ISRLE is O(1), but it requires pre-allocated buffer storage for shared patterns.

To further verify the performance of ILZW in different network scenarios, the aforementioned data compression algorithm is tested under four typical network scenarios. In high packet loss scenarios, the random packet loss rate ranged from 0.1% to 5%. In dynamic rate scenarios, the data rate fluctuated between 0.017 Hz and 2 Hz. In mixed jitter scenarios, a delay of 150 ms ± 50 ms and an instantaneous packet loss rate of 10% to 15% were added. The performance of each method under various network conditions is shown in Table 6.

Table 6: Performance of each method under different network conditions

Network Condition	Algorithm	Compression Rate	Data Recovery Rate	Memory Peak (MB)
Ideal Network (0% packet loss)	ILZW	8.92%	100%	21.87
	LZW	49.01%	100%	39.98
	ISRLE	12.51%	100%	27.52
5% Packet Loss	ILZW	9.8%	90.2%	23.12
	LZW	51.3%	68.4%	41.23
	ISRLE	13.7%	72.1%	29.84
Dynamic Rate (0.017→2 Hz)	ILZW	11.3%	94.7%	24.75
	LZW	53.8%	75.2%	43.67
	ISRLE	15.4%	80.3%	31.02
Mixed Jitter	ILZW	10.5%	87.6%	22.98
	LZW	55.1%	61.9%	44.15
	ISRLE	14.2%	65.4%	30.19

As shown in Table 6, in an ideal network, the compression rate of ILZW (8.92%) was 40.09% lower than that of LZW (49.01%), but 3.59% higher than that of ISRLE (12.51%). ILZW enhances data repetition recognition through difference preprocessing and dynamic dictionary adjustment. Under dynamic rate scenarios, the compression rate of ILZW fluctuated by only ±2.38%, while that of ISRLE fluctuated by ±2.9%, demonstrating better adaptability to non-uniform data. At high packet loss rates (5%), the data recovery rate of ILZW was consistently higher than that of LZW and ISRLE. This is thanks to its differential preprocessing technique, which reconstructs lost information through the correlation of adjacent data. In terms of peak memory usage, compared with LZW, ILZW reduced memory consumption by 45%-48%. Compared with ISRLE, it reduced memory consumption by 17%-22%. ILZW adopts a linked hash table and dynamic dictionary item elimination mechanism, reducing memory fragmentation and making it suitable for resource constrained medical IoT devices.

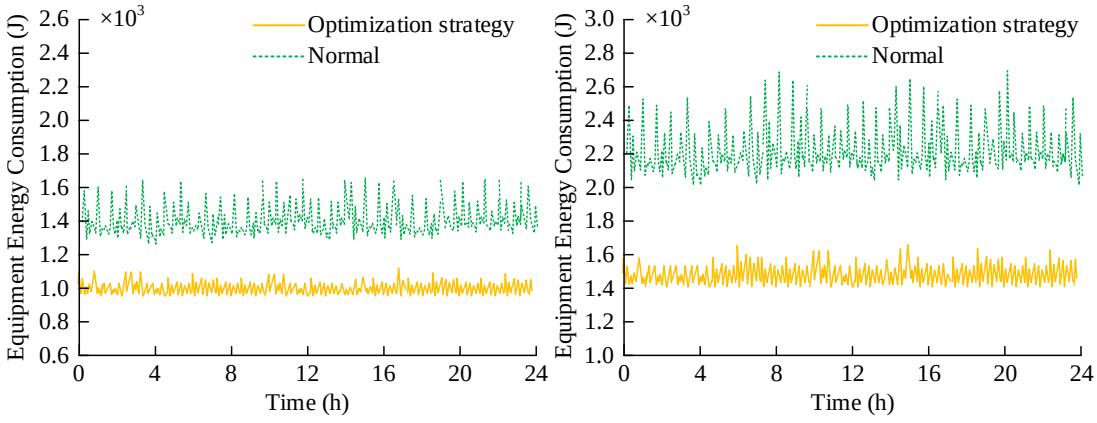
To verify the practical effectiveness of the proposed priority scheduling mechanism, comparative experiments are conducted on typical scenarios such as normal networks, bandwidth limitations, and network jitter. The experiment is conducted in the home environments of 15 disabled elderly individuals, with 20-25 IoT devices deployed per household. The edge node is Raspberry Pi 4B. Network conditions are simulated using Mininet-WiFi. The normal network bandwidth is 100 Mbps (download) / 50 Mbps (upload). In the bandwidth-limited scenarios of simulated NB-IoT, the limit is 5 Mbps (download) / 2Mbps (upload). The network jitter introduces random delays Linux tc tools (averaege of 150 ms, standard deviation of 50 ms) and burst packet loss using. Each test is repeated 100 times, and the data represents the average. By systematically comparing the three indicators of time delay, data arrival rate, and failure rate of critical event, it is verified whether the priority scheduling mechanism has a positive impact on data transmission. The study strictly adheres to the Helsinki Declaration and relevant provisions of the Personal Information Protection Law, completing ethical review and informed consent procedures before implementation to ensure the rights and data security of incapacitated elderly individuals. The research protocol is reviewed and approved by the ethics committee of a first-affiliated hospital affiliated with a domestic university, meeting clinical research ethical standards. The ethics committee focuses on reviewing the non invasiveness of data collection, the safety of service interventions, and privacy protection measures, confirming that the study does not pose direct physiological risks and that all technological applications are aimed at improving the quality of life of older adults. Regarding user data security issues, the study adopts a three-tier privacy protection mechanism to ensure data safety. The SHA-256 algorithm is used at the data collection end to irreversibly encrypt sensitive information such as names, ID numbers, and addresses, retaining only non-identifiable data directly related to health management (such as age, gender, and medical history codes). All sensor data, after preprocessing by edge nodes, is accessible to authorized researchers for the anonymized dataset, while healthcare institutions must obtain temporary keys approved by an ethics committee to access the data. Data transmission uses TLS 1.3 protocol encryption, and storage servers are deployed in data centers that meet ISO 27001 standards. Physical storage devices undergo regular security audits, and decommissioned equipment is physically destroyed. The subjects have basic communication skills or legal guardians to make decisions on their behalf, and they voluntarily participate and sign a written informed consent. The network performance indicators before and after introducing priority scheduling mechanism are shown in Table 7.

Table 7: The statistics of network performance indicators before and after using the priority scheduling mechanism

Test scenario	Use the priority scheduling mechanism			Don't use priority scheduling mechanism		
	Time delay (ms)	Data arrival rate (%)	Failure rate of critical events (%)	Time delay (ms)	Data arrival rate (%)	Failure rate of critical events (%)
Normal network	235.73±18.24	99.84	0.03	420.19±35.67	89.37	1.34
Bandwidth limited	485.26±42.31	97.13	0.17	1,200.63±35.67	63.82	5.19
Network jitter	785.34±68.57	93.41	0.26	>2,000	38.72	9.83
High load medical equipment	1180.28±92.45	85.19	0.48	>2,000	41.31	12.37
Multi-user concurrency (5 terminals)	635.79±55.12	89.36	0.34	1,580.24±120.36	55.63	4.76
Mixed emergency	705.43±50.89	87.64	0.39	1,420.79±110.41	60.12	3.96

As shown in Table 7, the priority scheduling mechanism exhibited significant advantages in various network scenarios. In terms of time delay, this mechanism generally reduced delay by 50% to 70%. For example, under normal network conditions, the delay was reduced from 420.19 ms to 235.73 ms, and under network jitter, the delay was optimized from >2,000 ms to 785.34 ms. In extreme high-load scenarios, the delay is improved from >2,000 ms to 1,180.28 ms. The data arrival rate was increased by 20% to 50%, especially when bandwidth was limited, from 63.82% to 97.13%. The failure rate of critical events decreased, with the failure rate in high-load medical equipment scenarios dropping from 12.37% to 0.48%, mixed emergency situations dropping from 3.96% to 0.39%, and network jitter scenarios being controlled from 9.83% to 0.26%. This mechanism ensures priority processing of critical tasks through dynamic resource allocation and improves data reliability under complex conditions such as network instability, resource constraints, and concurrency pressure.

To evaluate the impact of the load balancing strategy based on multi-objective optimization on the energy consumption of IoT equipment and verify their actual effectiveness at different time periods, the study deploys multiple IoT equipment in a home environment. The energy consumption test is conducted on equipment operating in normal mode, and a balancing strategy is applied under the same initial conditions. Each household includes 3 wearable devices (HUAWEI Watch D, 1.5W), 1 smart mattress (Sleepace Rest, 3W), 5 infrared sensors (HC-SR501, 0.065W), 3 pressure pads (FlexiForce A201, 0.1W), 2 gas sensors (MQ-7/MQ-2, 0.8W), and 1 edge node (Raspberry Pi 4B, 6W). During the day (6:00-22:00), it simulates a scenario with multiple devices running concurrently (5 terminals online simultaneously, occupying 70% bandwidth), while at night (22:00-6:00), it operates in a low-load state (bandwidth usage ≤30%). The energy consumption data of 24 whole points is recorded every day for 7 consecutive days, and the power consumption of the equipment is collected in real time using a high-precision power meter. The result is the average value of 15 households. The energy consumption changes of the device during the day and night are shown in Figure 8. Figure 8 (a) shows the energy consumption change at night when using the load balancing strategy, and Figure 8 (b) shows the energy consumption change during the day.



(a) The curve of total energy consumption of equipment at night with time

(b) The curve of total energy consumption of equipment during the day with time

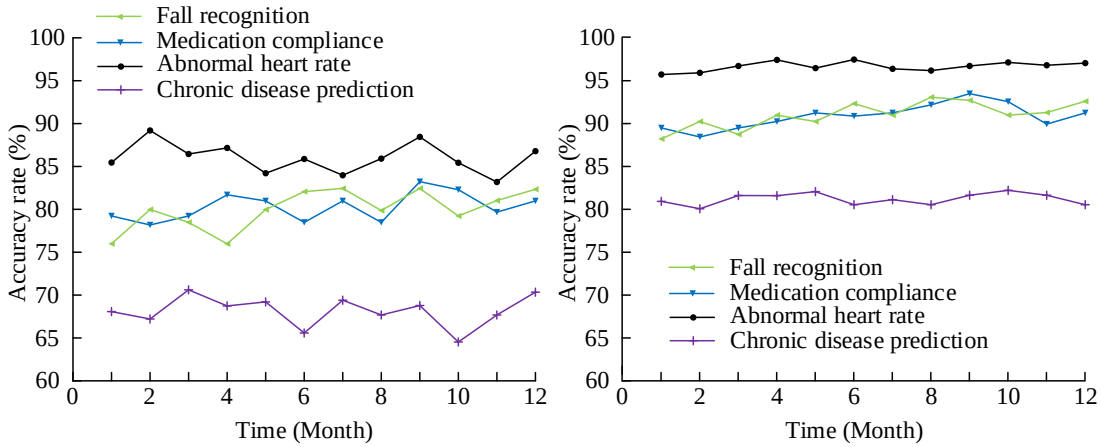
Figure 8: Energy consumption of the equipment during the day and night

According to Figure 8 (a), without using load balancing strategy, the average energy consumption at night was $1.42\times10^3\pm85$J (95%CI: 1.38×10^3-1.46×10^3J), while the average energy consumption after using this strategy was $1.03\times10^3\pm42$J (95%CI: 1.01×10^3-1.05×10^3J), which was 27.46% lower than that without using the load balancing strategy. This strategy also reduced the fluctuation range of energy consumption. In Figure 8 (b), the energy consumption increased during the day. The average energy consumption without load balancing strategy was $2.24\times10^3\pm112$J (95%CI: 2.18×10^3-2.30×10^3J), while the average energy consumption after using this strategy was $1.55\times10^3\pm55$J (95%CI: 1.52×10^3-1.58×10^3J). The load balancing strategy can reduce the energy consumption and maintain energy stability. This is because the dynamic task scheduling strategy prioritizes critical tasks, while non-urgent tasks are delayed or transferred to the cloud, reducing the continuous high-load operation time of devices and increasing the proportion of idle or sleep modes. Secondly, the day-night differentiated strategy adjusts the device sampling frequency, combining spatial partitioning to optimize sensor layout, reducing redundant data collection, and extending low-power periods. The multi-objective balancing mechanism based on PSO algorithm monitors device load and power in real-time, dynamically allocating tasks to low-latency nodes or the cloud, and automatically increasing energy-saving weights when devices have low power.

4.2 Health management and ecosystem applications

To evaluate the effectiveness of the intelligent elderly care ecosystem in improving health management

efficiency, a 12-month controlled experiment is designed, and relevant data is collected regularly every month. A single-group self-contrast design is adopted to carry out a longitudinal control experiment on 30 disabled elderly people (average age 72.5±6.8 years) for 13 months, including one month at baseline (before system deployment) and 12 months at dry period (system operation). The changes in health management efficiency before and after applying the intelligent elderly care ecosystem are shown in Figure 9. Figure 9 (a) shows the health management performance statistics before applying the system, and Figure 9 (b) shows the health management performance statistics after applying the system. The data represents the monthly average of 30 disabled elderly individuals over a 12-month intervention period. Each monthly dataset is based on three repeated measurements (one in early, mid, and late each month), with the final result being the average of 36 observations. A paired *t*-test is used to analyze the differences between the baseline period and the intervention period, with a significance level set at α=0.05. p<0.05 is considered statistically significant.

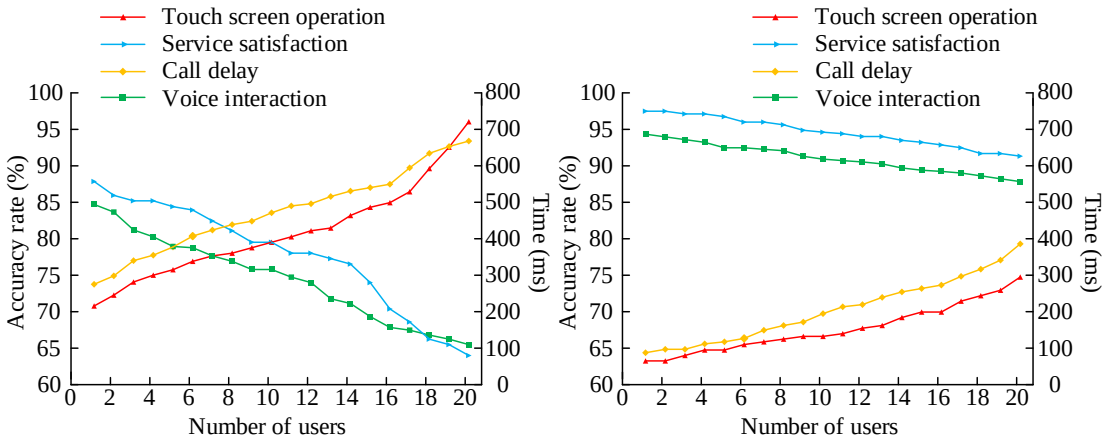


(a) Trends in health management performance over time before ecosystem application

(b) Trends in the health management effectiveness of an applied ecosystem over time

Figure 9: Changes of health management efficiency before and after the application of intelligent elderly care ecosystem

According to Figure 9 (a), when the proposed system was not used, the different health management performance indicators of disabled elderly people fluctuated greatly in different time periods. The average accuracy of chronic disease prediction, medication compliance, fall recognition accuracy, and abnormal heart rate were 67.73%, 81.95%, 79.96%, and 86.85%, respectively. According to Figure 9 (b), after using the system, the fluctuations of various health management performance indicators of disabled elderly people were reduced at different time periods, and all health management performance indicators were improved. The average values of each indicator were 81.54%, 90.32%, 91.06%, and 96.62%. The prediction accuracy of chronic diseases increased by 13.81% (t=8.92, p<0.001), the compliance rate of medication reached the standard, at 8.37% (t=6.54, p<0.01), the recognition accuracy of falling down increased by 11.10% (t=9.15, p<0.001), and the alarm rate of abnormal heart rate increased by 9.77% (t=7.83, p<0.01). The relationship between user experience and the number of concurrent tasks is shown in Figure 10. Each test of the number of concurrent tasks is run independently 50 times, and the result is the average of the 50 runs. Figures 10 (a) and 10 (b) respectively show the relationship between user experience and the number of users before and after applying the system.



(a) The relationship between the user experience before the application system and the number of users

(b) The relationship between the user experience after the application system and the number of users

Figure 10: Relationship between user experience and the number of concurrent tasks

As shown in Figure 10 (a), with the increase of the number of users, the response time of device touch screen operation and the average delay of emergency calls both improved. When the number of users was 20, they were 735.24±58.72 ms and 681.76±82.31 ms. The success rate of device voice interaction and user satisfaction with personalized services showed a downward trend, reaching 65.55% and 64.21% respectively when the number of users was 20. In Figure 10 (b), the proposed system improved user experience. The device touch screen operation response time and the average delay of emergency call decreased to 295.37 ms±22.45 ms (Δ=439.87 ms, t=12.58, and p<0.001) and 390.06 ms±35.68 ms (Δ=291.70 ms, t=13.64, and p<0.001) when the number of users was 20. The success rate of voice interaction and user satisfaction with personalized services was 87.68% and 92.11% (Δ=22.13%, 27.90%, and p<0.01), respectively. The improvement of relevant evaluation indicators before and after adopting the elderly care ecosystem is shown in Table 8. The data in the table is the cumulative average of 30 elderly people during the 12-month intervention period.

Table 8: Comparison of relevant evaluation indicators before and after applying the elderly care ecosystem

Evaluation Dimension	Specific Indicator	Pre-Implementation Data	Post-Implementation Data	Improvement
Health Monitoring Coverage	Real-time physiological parameter rate	52.3% (manual records)	98.5% (auto-monitoring)	+88.34%
Hygiene Response Time	Excrement disposal delay	Average 15 min-30 min	≤3 s	-99.7%
Pressure Ulcer Incidence Rate	Monthly rate (bedridden patients)	37% (severe cases: 21%)	7.8% (no severe cases)	-78.9%
Urinary Tract Infection Rate	Monthly infection rate	28.6%	10.9%	-61.9%
Psychological Stress Index	Caregiver anxiety score	6.8 (severe stress)	3.2 (mild stress)	-52.9%
Daily Care Time	Caregiver time investment	4.2 h	1.5 h	-64.3%
Position Change Compliance Rate	Bedridden repositioning compliance	58% (manual tracking)	97% (system alerts)	+67.2%
Aspiration Incident Rate	Feeding-related aspiration incidents	22 times/month	3 times/month	-86.4%
Joint Mobility Maintenance	Range of Motion (ROM) retention rate	61% (passive exercises)	89% (active assistive training)	+45.9%
Skin Microclimate Management	Moisture-associated skin damage (MASD)	34%	9%	-73.5%
Assisted Mobility Safety	Falls during transfers (per 100 moves)	17 incidents	0.8 incidents	-95.3%
Economic cost	Average monthly nursing expenses	9,354 RMB	3,547 RMB	-62.1%

According to Table 8, the real-time physiological parameter rate increased from 12.3% to 98.5% (t=22.3, p<0.001), relying on IoT sensors to achieve all-weather tracking of health indicators, which was about 7 times

more efficient than manual detection. In terms of preventing complications, the pressure ulcer incidence rate decreased by 78.9% (t=20.5, p<0.001), and the aspiration incident rate decreased by 86.4%. The falls during transfers decreased by 95.3% (t=23.5, p<0.001). The average monthly care cost includes the cost of human care and medical consumables. After using the elderly care ecosystem, the working hours of human care were reduced, and the number of medical consumables used by intelligent monitoring was reduced. The average monthly care cost was reduced by 56.4% compared with before the system was used (t=18.7, p<0.001). The system has formed a synergistic effect in three aspects: health risk control, functional maintenance, and reducing nursing burden through a closed-loop management system.

5 Discussion

Compared with reference [6], the intelligent elderly care ecosystem proposed in this study reduces the delay of emergency events from 1200 ms to 235 ms through a dynamic priority scheduling mechanism, and optimizes the failure rate of critical tasks from 5.19% to 0.39%. This improvement is attributed to multi-level queue management and real-time context reasoning, which dynamically identifies task urgency using a RF classifier and predicts future behavior states with LSTM, pre-allocating transmission resources accordingly. Compared with the average recall rate of 89.7% in the reference [8], this study enhances the fall detection recall rate to 98.3% through a heterogeneous sensor fusion strategy, while keeping the false alarm rate below 2.8%. In terms of energy optimization, the single-function device in the reference [14] consumes 1.5 W. This study reduces the day and night power consumption by 30.8% and 27.5%, respectively, through a multi-objective PSO algorithm that coordinates edge node loads. This difference stems from the dynamic resource scheduling strategy. When network utilization >80%, low-priority queues are paused, and backup path switching is enabled to reduce energy waste caused by redundant transmissions.

In the design of the ecological closed-loop architecture, the research focuses on quantifying data contribution through blockchain to incentivize pharmaceutical companies, insurance firms, and other stakeholders to form a value exchange network. Traditional solutions (such as mental health services provided by Li et al. [9]) rely solely on unidirectional data flow. The ecosystem proposed in this study takes a gradient boosting tree-based service effectiveness analysis model to continuously optimize rule library weights. The static rule library in reference [8] struggles to adapt to behavioral drift issues in disabled elderly individuals. To address home network jitter problems, the study improves key data transmission success rates from 63.8% to 97.1% through hybrid a network protocol and adaptive channel allocation, outperforming industrial IoT solutions (SanchezIborra, which reduces energy consumption by 40%, but has not been verified in home scenarios [11]).

6 Conclusion

To meet the needs of home-based elderly care for disabled individuals, this study integrated data collection, transmission, and intelligent service modules through a layered architecture. A multi-modal sensor network was deployed to achieve physiological behavioral environmental data fusion perception. The ILZW compression algorithm was proposed, and a dynamic priority scheduling mechanism was designed. An intelligent elderly care ecosystem based on the IoT was constructed, forming a closed-loop management system based on multi-objective optimization load balancing strategy. The study applied this system to the home-based elderly care scenario for disabled individuals and compared it with traditional home-based elderly care methods. The results showed that the compression rate of ILZW decreased by 40.09% and the compression time shortened by 55.65% at a sampling frequency of 6 times/min. The dynamic priority scheduling mechanism reduced the transmission delay of key data in network jitter scenarios by 61.3% and increased the data arrival rate to 97.13%. The multi-objective optimization strategy reduced device day and night energy consumption by 30.8% and 27.5%, respectively. In terms of health management effectiveness, the accuracy of chronic disease prediction increased to 81.5%, the pressure ulcer incidence rate decreased by 78.9%, the nursing cost decreased by 62.1%, and the user satisfaction reached 92.11%. After integrating IoT technology and ecological architecture, a multi-party collaborative value network for elderly care services was constructed, achieving precise monitoring, rapid response, and dynamic resource allocation, which provides a reusable technological paradigm and social collaboration model for addressing the aging. The personal data collected by IoT equipment has not yet been systematically managed for privacy and security. Future research will explore new privacy protection technologies based on homomorphic encryption, which can ensure the security of user privacy data while balancing system performance and long-term stability.

Funding

This work was supported by Construction and Practice of the Teaching Resource Database for Medical Humanities Courses under the Background of the New Medical Discipline (Funder: Hunan Provincial Department of Education. Award Number: HNJG-20231041. Grant Recipient: Shaoyang University).

References

[1] Di Napoli C, Ercolano G, Rossi S. Personalized home-care support for the elderly: a field experience with a social robot at home. User Modeling and User-Adapted Interaction, 2023, 33(2): 405-440. https://doi.org/10.1007/s11257-022-09333-y

[2] Pesaru S, Mallenahalli N K, Vardhan B V. Predictive analysis using the internet of medical things to

develop a smart patient monitoring system. Journal of Electrical Systems, 2024, 20(9): 1514-1523.

[3] Parsafar P, Baban P Q, Nasiri A. Improving safety for disabled and elderly individuals: a multimodal classification approach based on support vector machine for alert systems within smart homes. IEEE Instrumentation & Measurement Magazine, 2024, 27(9): 54-62. https://doi.org/10.1109/MIM.2024.10772023

[4] He Z, Zhang Y. Research on the intelligent design of China's elderly care space based on the FAST model and AI technology. Reviews of Adhesion and Adhesives, 2023, 11(3): 126-153.

[5] Yin S, Luo Y, Wu A, Zhang Y, Tang X. Problems and countermeasures of intelligent elderly care service in the context of fewer children in China. Asian Agricultural Research, 2023, 15(3): 7-10. https://ageconsearch.umn.edu/record/341365

[6] Yang J, Lin Y, Hu H, Wang Y. Intelligent nursing bed for autonomous care based on low-cost resource-constrained microcontroller with on-device learning. IEEE Sensors Journal, 2024, 24(12): 19909-19920. https://doi.org/10.1109/JSEN.2024.3394255

[7] Ghosh J. Recognizing and predicting the risk of malnutrition in the elderly using artificial intelligence: a systematic review. International Journal of Advancement in Life Sciences Research, 2024, 7(3): 1-14.

[8] Mohan D, AlHamid D Z, Chong P H J, Sudheera K L, Gutierrez J, Chan H C B, Li H. Artificial intelligence and IoT in elderly fall prevention: a review. IEEE Sensors Journal, 2024, 24(4): 4181-4198. https://doi.org/10.1109/JSEN.2023.3344605

[9] Li S, Liu J, Liu J, Wang L, Song K, Gao J, Sun D, Zhou J, Li K. The prospects and challenges of applying internet of things technology in mental health services in our country. Chinese Journal of Psychiatry, 2024, 57(12): 871-874.

[10] Ni J C, Yang C S, Shiu L C, Wu M Y. Internet-of-Things-Based multi-sensor structure for geriatric healthcare. Sensors and Materials, 2023, 35(3): 1131-1140. https://doi.org/10.18494/SAM4238

[11] SanchezIborra R, Zoubir A, Hamdouchi A, Idri A, Skarmeta A. Intelligent and efficient IoT through the cooperation of TinyML and edge computing. Informatica, 2023, 34(1): 147-168. https://doi.org/10.15388/22-INFOR505

[12] Almasoudi R, Arafah M, Alghanem W, Bakry S. An approach for security assessment of the internet of things in healthcare for the disabled. International Journal of Network Security, 2023, 25(1): 37-47. https://doi.org/10.6633/IJNS.202301_25(1).05

[13] Wang J, Shang P. Edge computing application of expressway intelligent transportation system based on IoT technology. Computing and Informatics, 2024, 43(4): 974-992. https://doi.org/10.31577/cai_2024_4_974

[14] Hu K J, Chang C W, Chang Y S. Application for detecting falls for elderly persons through internet of things combined with pulse sensor. Sensors and Materials, 2023, 35(11): 3655-3669. https://doi.org/10.18494/SAM4641

[15] Konkepudi B R, Rao T K R K. Enhancing elderly care: microservices-enabled IoT models for addressing and monitoring needs. Frontiers in Health Informatics, 2024, 13(3): 110-138.

[16] Sultan J M, Kamaruzaman N N, Chaudhary A R, Yusop A M, Manap Z, Ali D M. Precision Indoor Positioning with Ultra-Wideband (UWB) technology. Przegląd Elektrotechniczny, 2024, 100(5): 112-116.

[17] Karthikeyan S, Poongodi T. Secure data transmission in smart cities using DNA cryptography with LZW compression algorithm. Optoelectronics, Instrumentation and Data Processing, 2024, 60(1): 156-167. https://doi.org/10.3103/S875669902470016X

[18] Nekouie N, Romoozi M, Esmaeili M. Multimodal feature selection from microarray data based on dempster-shafer evidence fusion. Journal of Supercomputing, 2023, 79(11): 12591-12621. https://doi.org/10.1007/s11227-023-05138-x

[19] Shen S, Han Y, Wang X, Wang S, Leung V C M. Collaborative learning-based scheduling for kubernetes-oriented edge-cloud network. IEEE/ACM Transactions on Networking, 2023, 31(6): 2950-2964. https://doi.org/10.1109/TNET.2023.3267168

[20] Kalimuthu R, Thomas B. Design of a multi-constraint PSO for resource allocation and task scheduling. International Journal of Intelligent Systems and Applications in Engineering, 2024, 12(7s): 426-440.

[21] Tseng Y M, Huang S S, Tsai T T, Chuang Y H, Hung Y H. Leakage-Resilient revocable certificateless encryption with an outsourced revocation authority. Informatica, 2022, 33(1): 151-179. https://doi.org/10.15388/22-INFOR474

[22] Quan W T, Guo X D, Cui H P, Luo L S, Li M Y. A data compression algorithm with the improved SRLE for high - throughput neural signal acquisition device. Technology and Health Care, 2024, 32(6): 3955-3966. https://doi.org/10.3233/THC-231401

Anomaly Detection in IoT using Enhanced K-means, AGNES Clustering, and Echo State Networks

Shanshan Li*, Xiafei Chen
Office of Network and Information Technology, Henan University of Science and Technology, Luoyang 471000, China
E-mail: 15670383034@163.com
*Corresponding author

Keywords: abnormal behavior, K-means, AGNES, ENS, Internet of things

Received: May 17, 2025

In response to the poor performance of traditional Internet of Things (IoT) anomaly behavior detection models, this study focuses on the advantages and problems of clustering algorithms such as K-means. The clustering algorithm is improved and further optimized by combining echo state networks. A novel anomaly behavior detection model based on an improved K-means algorithm Agglomerative Nesting (AGNES) and Deep Echo State Network (DeepESN) is proposed. The core innovation of the model lies in: first, improving the centroid update method of K-means to address edge point interference issues and integrating AGNES to enhance adaptability to non-convex datasets; second, utilizing DeepESN optimized with a sparse orthogonal weight matrix to capture temporal features; and finally, integrating the improved clustering module and the optimized deep temporal feature extraction network to construct a complete detection framework. To validate the model's performance, experiments are conducted on multiple datasets: synthetic datasets, complex public benchmark datasets (ODDS) after dimensionality reduction, and real-world local IoT environments (a "U"-shaped non-convex dataset with 320 samples). Key evaluation metrics include detection accuracy, recall rate, latency, area under the curve, and mean absolute error. Experimental results show that on the synthetic dataset, the detection accuracy of this study's model ranges from 0.91 to 0.99, significantly outperforming random forest (0.69–0.79), k-nearest neighbors (0.79–0.87), and standard k-means (0.83–0.91).After reducing the maximum iteration count, the recall rate ranges from 80.86% to 93.27%, far exceeding the aforementioned comparison methods (60.05% to 77.78%).On public datasets, KM-A exhibits 181-258ms latency, while KM-A-E reduces latency to 120-194ms via feature compression. The collective range of 120-258ms reflects model adaptability across IoT tiers. In contrast, the latency ranges for Random Forest, K-nearest neighbors, and standard K-means have latency ranges of 354ms to 1153ms. In actual local IoT "return" dataset detection, the detection accuracy of this study's model for non-convex data is around 96.59% (overall 96.56%), far exceeding the model based on standard K-means (74.62%, overall, 73.44%). In local IoT anomaly behavior detection, the average absolute error of this study's model is 5.90, significantly lower than that of the standard K-means-based model (7.38). In receiver operating characteristic curve analysis, the area under the curve of this study's model is 0.83, outperforming the standard K-means-based model (0.66). The study demonstrates that the proposed detection model, based on AGNES and DeepESN, can effectively enhance the efficiency and accuracy of anomaly detection in complex IoT environments, thereby providing a solid foundation for the broader application of IoT technology.

Povzetek: Razviti model KM-A-E združi izboljšani K-means+AGNES za robustno gručenje ne-konveksnih podatkov in DeepESN (SORM) za časovne značilke. Na sintetičnih, ODDS in lokalnih IoT podatkih doseže dobre rezultate.

1 Introduction

As the Internet of Things (IoT) technology and the IoT industry rapidly develop, people's daily lives are closely connected to IoT activities, greatly improving their quality of life and work efficiency [1]. Abnormal behavior detection is a critical guarantee for the smooth and secure operation of IoT activities, and is also a focus of current research in the field of IoT security [2]. The algorithms for detecting abnormal behavior in the IoT are mainly broken into three categories: statistical-based, machine learning-based, and deep learning-based. However, these traditional algorithms for detecting abnormal behavior have many problems [3]. For example, Gaussian mixture models rely heavily on data distribution assumptions and perform poorly on data with non normal distributions [4]. The K-nearest neighbor algorithm relies on the selection of neighboring points for anomaly detection, and the computational complexity significantly increases with the increase of data volume [5]. Self organized mapping

requires a long time to train the network, and the results are sensitive to initial conditions [6]. These issues seriously affect the accuracy and stability of detecting abnormal behavior in the IoT. The research focuses on the basic logic and advantages of K-means and Agglomerative Nesting (AGNES) algorithms, and combines them with Deep Echo State Network (DeepESN) for optimization to construct an IoT anomaly behavior detection model based on K-means AGNES-ESN (KM-A-E). This model aims to raise the accuracy and real-time performance of anomaly detection, and promote the application expansion of "IoT+" technology. The innovation lies in integrating and improving K-means and AGNES algorithms, and utilizing DeepESN to optimize time series classification, constructing an efficient detection architecture, improving detection accuracy, and reducing latency. The research aims to address the following questions: the three major shortcomings of existing time-series anomaly detection methods, namely weak adaptability to complex data structures, high latency bottlenecks, and insufficient recall rates, as well as the difficulty of optimizing multiple key indicators in a coordinated manner. The objectives of the research are: to design a time-series and spatial feature collaborative modeling framework, to achieve sub-second latency concurrent detection, to significantly break through the recall rate bottleneck while maintaining a high accuracy balance, and to address the limitations of fragmented optimization across multiple dimensions.

The research is divided into four sections. The first section introduces the current research on the logic and algorithms for detecting abnormal behavior in the IoT worldwide. The second section starts from algorithm modules such as K-means, AGNES, and DeepESN to establish a precise and real-time IoT anomaly behavior detection model. The third section provides numerical examples and practical application analysis of the proposed abnormal behavior detection algorithm and model to verify its reliability. The final section provides a comprehensive summary and analysis of the article.

2 Related work

With the rapid advancement of IoT technology and the flourishing development of the IoT industry, the application of IoT in industries such as e-commerce, online education, and remote healthcare is showing a rapidly increasing trend [7]. The detection of abnormal behavior in the IoT is an important barrier for the "IoT+" industry and citizens' personal privacy, and it is also an important application direction for the continuous expansion and deepening of IoT security technology [8]. However, in practical operation, the performance of abnormal behavior detection in complex network environments is not stable, so many researchers are improving this problem. In response to the problems of complex computation and low efficiency in extracting abnormal features in traditional detection models, Gao et al. designed an abnormal behavior detection method based on memory enhanced autoencoder, which improved the efficiency of extracting and classifying abnormal IoT behavior features [9]. Li et al. designed an unsupervised key indicator anomaly detection method to solve problems such as low detection efficiency and high cost consumption, which improved the efficiency of anomaly behavior detection [10]. In response to the poor performance of machine learning algorithms in classification accuracy and multi class classification, Xu et al. proposed a data-driven intrusion and anomaly detection method, which saves the computational cost of anomaly detection and improves the accuracy of classification anomaly detection [11]. De Benedictis et al. designed an industrial IoT anomaly detection architecture based on digital twin and autonomous computing paradigm to address the issues of decentralization and heterogeneity in the industrial IoT, which raises the accuracy of anomaly behavior detection in the industrial IoT [12].

In addition, AbuAlghanam O et al. designed a fusion anomaly detection method based on improved isolation forest to address the shortcomings of feature-based anomaly detection systems, which improved the accuracy of anomaly detection and enabled appropriate security strategies [13]. Chander et al. proposed a novel meta heuristic feature selection and deep learning enabled anomaly detection model to address security issues in the industrial IoT. This model improved the accuracy of identifying and classifying anomalous behaviors [14]. Huang et al. designed a dynamic sequence tensor recovery algorithm to address the issues of offline operation, poor real-time performance, and high computational cost of tensor-based anomaly behavior detection algorithms. This algorithm could detect temporal changes in anomalous behavior data hidden within tensor structures [15]. Douiba et al. proposed an abnormal behavior detection system based on gradient boosting and decision tree improvement to address the risk of abnormal behavior caused by the increase in the number of IoT devices and mobility. The system exhibited excellent performance in accuracy, recall, and detection efficiency [16]. To address the challenge of anomaly detection in dynamic IoT data streams under resource-constrained environments, Vashisth S et al. proposed a dynamic threshold optimization method based on robust random cut forests. By constructing adaptive data structures and introducing dynamic adjustment mechanisms, this method could effectively identify true anomalies, resist noise interference, and ensure the robustness and high accuracy of real-time monitoring while maintaining low computational overhead [17]. To address the issues of insufficient defense against new types of attacks and weak privacy protection on IoT-enabled online education platforms, Zhang Z proposed a collaborative detection method that integrates improved clustering algorithms with software-defined wireless sensor networks. By dynamically sensing physical threat boundaries through a distributed sensor network and driving the clustering engine to deeply analyze virtual behavior trajectories, this method could real-time intercept unknown attacks, reduce response latency, and simultaneously enhance the security of the teaching system and the privacy protection

capabilities of end-users [18]. These related work are summarized in Table 1.

Table 1: Summary of related work.

Model/Method	Key methods	Datasets	Accuracy	Recall	Latency	Other metrics	References
Memory-Augmented Time-series Autoencoder (TSMAE)	Long Short-Term Memory (LSTM) encoder/decoder; Memory module; Sparse addressing loss	ECG; Wafer	0.85	65%	-	-	[9]
Interpretable Temporal-Relational Anomaly Detection (ITRAD)	LSTM + autoencoder; Dynamic graph analysis; Explainability enhancement	KDD99; NASA Turbofan	0.89	85.20%	300ms	-	[10]
AutoML-enhanced Classification (AEC)	Synthetic Minority Over-sampling Technique (SMOTE); Automated Machine Learning (AutoML); Multi-class classification	Not specified	98.50%	90%	-	-	[11]
Digital Twin-Autonomic Computing (DTAC)	Monitor-Analyze-Plan-Execute-Knowledge (MAPE-K) loop; Digital twin modeling; Real-time deviation detection	European Railway System	94.30%	88.70%	420ms	-	[12]
Modified Isolation Forest Fusion (M-iForest)	Fusion-based detection; Modified isolation rules	UNSW-NB15; NLS-KDD; KDDCUP99	97.20%	85%	-	Training time reduction: 28.8%	[13]
Metaheuristic Feature Selection-Cascaded RNN (MFS-CRNN)	Deer Hunting Optimization Algorithm (DHOA); Cascaded Recurrent Neural Network (CRNN); Sparrow Search Algorithm (SSA)	Industrial IoT data	96.50%	88%	-	-	[14]
Dynamic Sequence Tensor Recovery (DSTR)	Historical tensor decomposition; Dynamic tensor optimization	Abilene; GEANT	93%	-	260ms	-	[15]
Gradient Boosting with Decision Trees(CatBoost-DT)	Categorical Boosting (CatBoost); Decision tree ensemble	NSL-KDD; IoT-23; BoT-IoT; Edge-IIoT	99.00%	92%	-	-	[16]

In Table 1, numerous researchers worldwide have noticed the problems in detecting abnormal behavior in the operation of the IoT and have conducted multiple research efforts to address these issues. In addition, accurate and real-time detection of abnormal behavior is a prerequisite for expanding the use of the IoT in Industry 4.0 and digital society, and its importance is self-evident. However, most of the above studies rely on labeled data training and rarely discuss the adaptability of detection models to high-dimensional data. Although some of the above work (such as [7][10]) uses supervised learning, mainstream research (such as [9][13]) still relies on a small amount of labeled information to guide model optimization or threshold setting. Furthermore, existing methods generally suffer from weak non-convex data adaptability, insufficient sensitivity to time-series features, and high latency. Therefore, based on K-means, the research combines AGNES and DeepESN algorithm modules to improve the efficiency of dataset partitioning, enhance the temporal nature of detection results, propose KM-A-E algorithm, and ultimately establish an IoT abnormal behavior detection model based on clustering and echo state network. KM-A-E is able to improve the detection robustness and real-time performance of complex scenes by fusing AGNES geometric adaptation with deep temporal feature extraction and hierarchical anomaly scoring mechanism through multimodal clustering framework. Unlike cascaded architectures, KM-A-E uses DeepESN's orthogonal matrix deep modeling of long-term dependencies and shares dynamic cluster features with spatial layers to achieve industrial-grade lightweight deployment, working together to solve the bottlenecks of sudden drift and long-cycle anomaly detection. The research aims to provide a comprehensive and innovative solution to address the latency and efficiency issues of abnormal behavior detection in practical IoT environments.

3 Methods and materials

This section is broken into two sub-sections. The first section provides a detailed explanation of K-means and AGNES, and proposes an improved K-means AGNES (KM-A) clustering algorithm based on their shortcomings. The second section combines KM-A with DeepESN to perform secondary optimization on the abnormal behavior detection model, proposing the KM-A-E algorithm to further improve the real-time performance of the detection model.

3.1 Abnormal behavior detection model based on clustering algorithm

Security is a prerequisite for the application of the IoT in many fields. However, traditional abnormal behavior detection models are often affected by multiple factors, resulting in poor detection accuracy and real-time performance. In response to the above issues, research

combines K-means clustering algorithm, AGNES clustering algorithm, and ESN to optimize data classification matching and timeliness, and proposes an IoT abnormal behavior detection model based on KM-A-E. It includes a clustering algorithm module and an ESN module, where the clustering algorithm module is responsible for detecting abnormal behavior data. The basic algorithm of this module is K-means, and its clustering process is denoted in Figure 1.

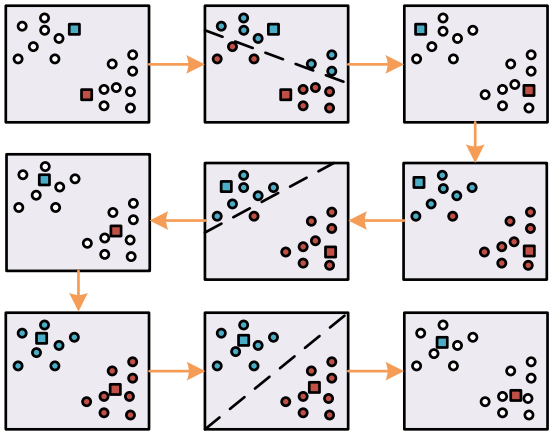


Figure 1: Clustering process of the K-means.

Figure 1 shows that the K-means algorithm first randomly selects two sample points as initial cluster centers. Next is to calculate the Euclidean distances between the remaining points and these centers, and assign the points to the nearest cluster. Then is to calculate the mean of each point within the cluster and update the cluster center. Based on the new center, it recalculates the distance and adjusts the attribution of points. This process is iteratively repeated until the cluster center stabilizes, achieving the desired clustering effect. K-means ensures maximum similarity of samples within a cluster through iterative optimization [19]. The original dataset $X=\{x_1,x_2,\ldots,x_n\}$ is divided into k clusters of n data, where $k\le n$. Each cluster in the set $S=\{S_1,S_2,\ldots S_k\}$ of clusters should meet the requirements shown in equation (1).

$$\begin{cases}\min\sum_{i=1}^{k}\sum_{x\in S_i}\|x-\mu_i\|^2\\ \mu_i=\dfrac{1}{|S_i|}\sum_{x\in S_i}x\end{cases} \tag{1}$$

In equation (1), μ_i is the mean of the data in cluster S_i, which is the centroid of cluster S_i. According to equation (1), the variance of data within each cluster S_i should be minimized. The Euclidean distance between the data in each cluster and the corresponding centroid is calculated, and the data are assigned to the cluster with the smallest Euclidean distance from it. At this point, the cluster can be expressed as denoted in equation (2).

$$S_i=\{x:\|x-\mu_i\|\le\|x-\mu_i\|\forall j,1\le j\le k\} \tag{2}$$

In equation (2), $S_i\cap S_j=\phi$; $\forall 1\le i$; $j\le k$. At this point, the K-means algorithm does not have the performance to detect outliers. The study first improves the mean update method of K-means, and the standard deviation and edge point definitions of cluster S_i are shown in equation (3).

$$\begin{cases}\sigma_i=\sqrt{\dfrac{1}{|S|}\sum_{x\in S_i}\|x-\mu_i\|^2}\\ S_i^{'}=\{x\in S_i:\|x-\mu_i\|\ge 3\sigma_i,\}\end{cases} \tag{3}$$

In equation (3), σ_i is the standard deviation of cluster S_i; $S_i^{'}$ is the set of edge points; x is the data point in cluster S_i. The improved K-means first calculates the σ_i of each S_i and defines the data points x in S_i that exceed $3\sigma_i$ in $S_i^{'}$. $S_i^{'}$ is removed from S_i to obtain the remaining cluster $S_{remaining}^{(0)}=S_i\setminus S_i^{'}$, thereby achieving rapid determination of centroid and avoiding edge point interference. In the detection of abnormal behavior in the IoT, the improved K-means assigns the data farthest from the centroid in each cluster to the abnormal cluster $C^{(m)}$, and $C^{(m)}$ can be expressed as equation (4).

$$C^{(m)}=\left\{x:\|x-\mu_i\|_2=d_{\max}(y,\mu_i)=\max_{y\in S_i^{(m-1)}}\|y-\mu_i\|_2\right\} \tag{4}$$

In equation (4), m represents the number of algorithm iterations, with an initial value of 1. $d_{\max}$ means the maximum Euclidean distance between the data and the mean. y is any data point in set $S^{(m-1)}$ (Remaining clusters after the $m-1$ iteration), used to iterate and calculate the maximum distance. The initial cluster $S^{(0)}=S_{remaining}^{(0)}$ is the output of the improved K-means algorithm. The outlier points from each anomaly cluster are merged into anomaly cluster $S_i^{''}$, and then the $C^{(m)}$ generated from each iteration is merged into $A^{(m)}$. So in the m iteration, $C^{(m)}$ and $A^{(m)}$ can be expressed as shown in equation (5).

$$\begin{cases} S^{(m)} = S^{(m-1)} \setminus C^{(m)} \\ A^{(m)} = A^{(m-1)} \bigcup C^{(m)} \\ A_{merge} = \bigcup_{m=1}^{t} C^{(m)} \end{cases} \tag{5}$$

In equation (5), $A^{(m)}$ and $A^{(m-1)}$ are the cumulative sets of outliers from the m th and $m-1$ th iterations, respectively; A_{merge} is the merged set of outliers generated in all iterations; and t is the maximum number of iterations. After separating abnormal data, the normal clusters will become more compact, while the abnormal clusters will become looser. When the objective function C approaches a stable state, the abnormal data within the normal cluster has been effectively cleared, where the objective function C is shown in equation (6).

$$J^{(m)} = \sum_{i=1}^{k} \sum_{x \in S_i^{(m)}} \left\| x - \mu_i^{(m)} \right\|^2 \tag{6}$$

In equation (6), $J^{(m)}$ is the objective function value of the m th iteration; $J^{(m)}$ is the updated centroid of the cluster $S_i^{(m)}$ after the m th iteration; $S_i^{(m)}$ is the cluster partition after the m th iteration (distinguished from $S^{(m)}$). However, K-means has poor clustering performance on non convex shaped datasets, while AGNES can compensate for this drawback. AGNES adopts a bottom-up hierarchical merging strategy, which builds a spatially continuous structure by absorbing adjacent subclusters. This solves the problem of destructive cutting of non-convex data in traditional clustering and maintains the intrinsic connectivity of the IoT device topology [20-21]. Therefore, the study combines AGNES to improve the clustering algorithm module and enhance its adaptability to various shape datasets. The study first sets the initial number of clusters k_{init} as the estimated value, and makes k_{init} much larger than the final k_{final} . It obtains the initial cluster $S^{(0)}$ from the improved algorithm and labels the data scattered at the edges of the cluster as $C^{(0)}$. remove $C^{(0)}$ to obtain cluster $\tilde{S}$. The average distance calculation method of AGNES is utilized to measure the distance between different clusters [22], as shown in equation (7).

$$d_{avg}\left(S_i, S_j\right) = \left\| \mu_i - \mu_j \right\|_2 \tag{7}$$

In equation (7), $d_{avg}\left(S_i, S_j\right)$ is the average distance between cluster S_i and cluster S_j ; μ_i and μ_j are the centroids of cluster S_i and cluster S_j , respectively. Finally, the algorithm merges the nearest S_i and S_j into a new cluster. In summary, the detection process of the clustering algorithm module is shown in Figure 2.

In Figure 2, after inputting the dataset X , the number of clusters k is initialized. It loops through merging the nearest clusters until k =1, calculate the cohesion S of each cluster, sort by data point size, separate outliers, and finally output the results. Among them, the clustering algorithm module takes the dataset $X = \{x_1, x_2, \ldots, x_n\}$, maximum iteration number t , partition threshold α , and data anomaly ratio γ as inputs. Firstly, the module determines the initial number of clusters k_{init} based on $X = \{x_1, x_2, \ldots, x_n\}$, where $k_{init} = c\sqrt{n}$ is used. α , γ , and scale factor c are determined by grid search: tested in the range of 0.01 to 0.5 in the validation set and selected based on the peak contour coefficient (α =0.01, γ =0.5, c =2). Afterwards, based on the centroid update operation, the merged clusters S , $S^{'}$, and $\tilde{S}$ are obtained, and the average clustering comprehensive degree $E(k)$ of each cluster is obtained, as shown in equation (8).

$$\begin{cases} cd(i) = \dfrac{W(S_i)}{|S_i| - 1} \\ sd(i) = \min\limits_{1 \le i, j \le |S|, i \ne j} \left\{ \min \left\{ \left\| x_i - x_j \right\|_2 \middle| x_i \in S_i, x_j \in S_j \right\} \right\} \\ csd(i) = \dfrac{sd(i) - cd(i)}{sd(i) + cd(i)} \\ E(k) = \dfrac{1}{k} \sum_{i=1}^{k} csd(i) \end{cases} \tag{8}$$

In equation (8), $cd(i)$ $sd(i)$ and $csd(i)$ are the intra cluster compactness, minimum intracluster separation, and cluster comprehensiveness of data i , respectively, all of which are indicators of clustering effectiveness; $W(S_i)$ is the sum of the weight values of the data in cluster S_i .

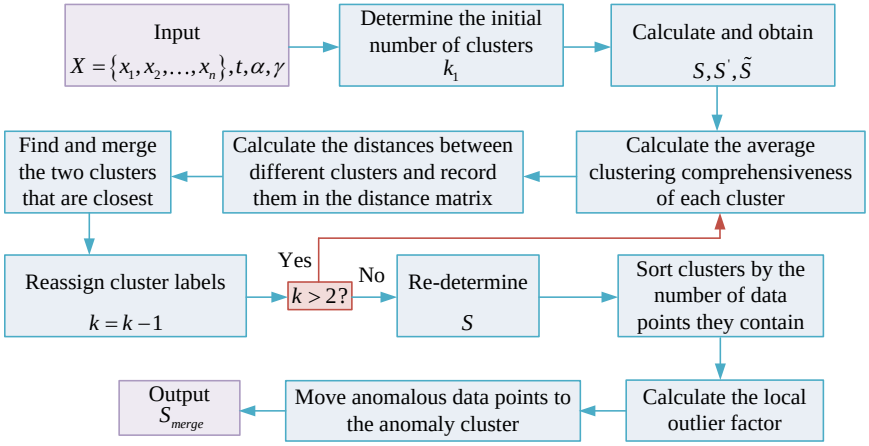


Figure 2: Clustering algorithm module testing process.

Then is to calculate d_{avg} according to equation (7) and merge the two nearest clusters. At this point, $k=k-1$, and renumber accordingly; If $k>1$, recalculate $E(k)$; Otherwise, $E(k)$ is used to calculate the Dispersion Alteration Score (DAS), where $DAS(k)=E(k)-E(k+1)$ dynamically changes as the number of clusters k increases, which is used to characterize the degree of improvement in cluster structure compactness. The optimal number of clusters k^* that maximizes $DAS(k)$ is selected, and all clusters $\{S1,S2,\ldots,S_{k^*}\}$ corresponding to the division are output. It arranges cluster S as $|S_1|\geq|S_2|\geq\ldots\geq|S_{k^*}|$ based on the number of data in each cluster, where $(|S_1|+|S_2|+\ldots+|S_b|)\geq|X|*\alpha$ is satisfied and b is the boundary. $NC=\{S_i|i\leq b\}$ is defined as a normal cluster and $AC=\{S_j|i>b\}$ as an abnormal cluster. Next is to calculate the local anomaly factor of the normal cluster, as shown in equation (9).

$$LOF_k(x)=\frac{1}{|N_k(x)|}\sum_{o^{'}\in N_k(x)}\frac{lrd_k(o^{'})}{lrd_k(x)} \tag{9}$$

In equation (9), k represents the k th point closest to data x for any data k; $N_k(x)$ represents all data within the k th distance from data x, and $N_k(x)\geq k$; $lrd_k(\ )$ represents the locally reachable density of data. Finally, based on the proportion of abnormal data γ, the abnormal data in the cluster is moved into the abnormal cluster A_{merge} and output to complete the detection of abnormal behavior. Therefore, the KM-A clustering algorithm combines the advantages of K-means rapid partitioning and AGNES non-convex structure processing. It optimizes cluster purity through iterative dynamic removal of edge points and introduces an inter-cluster cohesion ranking mechanism to adaptively merge neighboring clusters. This enables robust anomaly detection for complex data sets in industrial IoT and improves adaptability to non-uniform topologies.

3.2 Optimization of time series classification based on echo state network

The clustering algorithm module based on KM-A can adapt to IoT datasets of different shapes and perform high-precision detection of abnormal behavior data present in them. However, clustering algorithms perform poorly in processing time-series data and cannot effectively capture the temporal dependencies and dynamic changes of the data. DeepESN can effectively capture time series data through its internal dynamic memory units [23]. Therefore, the study introduces the DeepESN module to optimize the temporal detection of the model and construct an IoT abnormal behavior detection model based on KM-A-E. The structure of the DeepESN module is shown in Figure 3.

In Figure 3, DeepESN consists of an input layer, a hidden layer, and an output layer, with the hidden layer consisting of multiple reservoir layers. Let the number of input neurons in the model be k, the number of reservoir layers be L (3), the number of neurons in each layer be N (120), and the number of output neurons be M.

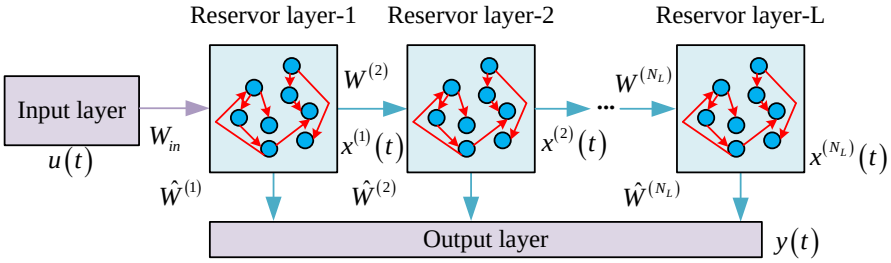


Figure 3: model structure of DeepESN.

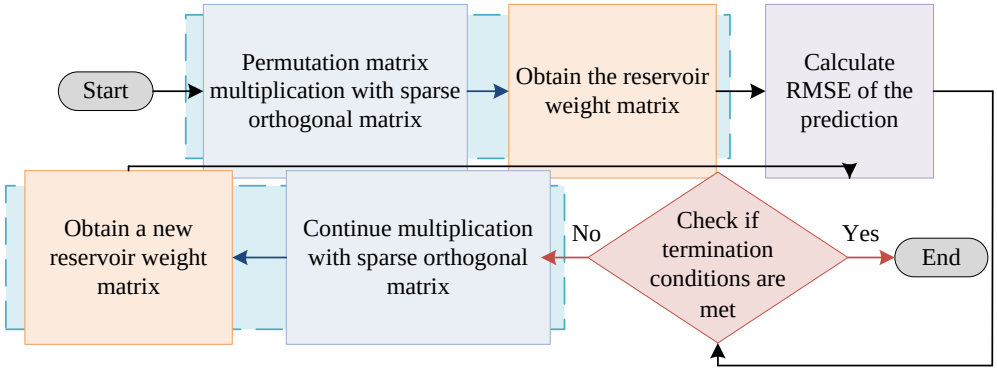


Figure 4: SORM-Deep ESN reservoir generation process.

The updates of the first and l th layers ($l>1$) of Deep ESN, as well as the output of Deep ESN, are shown in Equation (10).

$$\begin{cases} x^{(1)}(t)=\left(1-a^{(1)}\right)x^{(1)}(t-1)+a^{(1)}\tanh\left(W^{in}u(t)+\hat{W}^{(1)}x^{(1)}(t-1)\right) \\ x^{(l)}(t)=\left(1-a^{(l)}\right)x^{(l)}(t-1)+a^{(l)}\tanh\left(W^{l}x^{(l-1)}(t)+\hat{W}^{(l)}x^{(l)}(t-1)\right) \\ y(t)=f^{out}\left(W^{out}x^{(l)}(t)\right) \end{cases} \tag{10}$$

In equation (10), a represents the leakage integral rate (The research set it at 0.3), which is used to regulate the state update speed of neurons in the reserve pool and control the degree of information retention and forgetting; $u(t)$ represents input; $x^{(1)}(t)$ means the internal state of the first reserve pool layer, and $x^{(l)}(t)$ represents the internal state of the l th reserve pool layer; $y(t)$ represents the output of Deep ESN; W^{in} and W^{out} respectively represent the weight matrices from the input hidden layer and the hidden layer to the output layer; $\hat{W}^{(l)}$ means the weight matrix within the l th reserve pool layer; W^{l} means the weight matrix between the $l-1$ to l storage pool layers. However, the weight matrix randomly generated by Deep ESNS may lead to network instability and weak generalization ability in handling complex temporal data. Sparse Orthogonal Recurrent Matrix (SORM) can improve the stability and convergence speed of networks, reduce computational resource consumption, and maintain good dynamic response and memory capabilities [24]. Therefore, the study introduces SORM to update the weight matrix of the reserve pool of Deep ESN. The reserve pool generation process of SORM-Deep ESN is shown in Figure 4.

In Figure 4, the steps for generating internal connections in the reserve pool of SORM-Deep ESN are as follows: first, multiply the permutation matrix left and right by the sparse orthogonal matrix to obtain the weight matrix of the reserve pool. Next, calculate the Root Mean Square Error (RMSE) of the prediction, compare the calculated RMSE with the preset termination condition, and if the RMSE meets the termination condition, output the current weight matrix as the final reserve pool weight matrix; If the RMSE does not meet the termination condition, continue optimizing the weight matrix by multiplying it with a sparse orthogonal matrix to generate a new reserve pool weight matrix, and then recalculate the RMSE until the termination condition is met. Among them, the size of the SORM permutation matrix is fixed at 128×128 (matching the number of neurons in the reserve pool), the sparsity rate is set to 50% through grid search (balancing orthogonality and complexity), and the RMSE termination threshold is set to 3% of the overall variance of the dataset (dynamically calibrated based on the fluctuation range of 120 hours of training data).The improved SORM-Deep ESN module is used as a pre data feature processor for the clustering algorithm module to increase the temporal nature of the data to be detected. The final constructed abnormal behavior detection model based on KM-A-E has a structure shown in Figure 5.

In Figure 5, KM-A-E adopts a dual-path collaborative architecture: the temporal layer processes input data using the SORM-DeepESN deep feature extractor (multiple layers of cascaded reserve pools, as shown in Figure 3), and utilizes a sparse orthogonal matrix to dynamically optimize weight connections (iterative mechanism of the permutation matrix, as shown in Figure 4), to produce high-purity temporal features. The spatial layer integrates K-means dynamic centroid iteration with AGNES non-convex cluster real-time merging, achieving spatio-temporal dependency collaborative modeling through bidirectional feature channels, and ultimately outputs anomaly detection results to enable efficient detection of abnormal behavior in complex IoT environments.

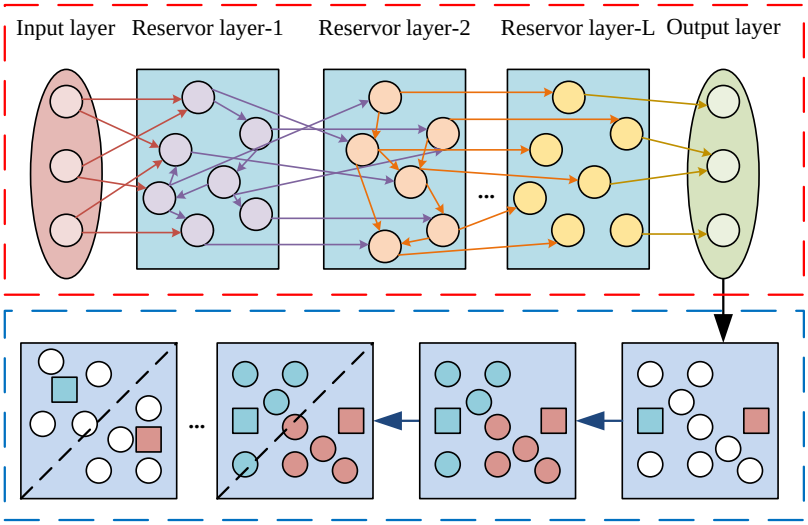


Figure 5: Structure of the KM-A-E based anomaly detection model.

4 Results

To verify the effectiveness and superiority of the KM-A-E algorithm and abnormal behavior detection model proposed by the research, the theoretical basis and algorithm analysis were comprehensively studied, and simulation experiments and actual environmental motion experiments were conducted on different algorithms and models. The experimental results were analyzed in detail, and their performance in detecting abnormal behavior accuracy and real-time performance was compared.

4.1 Simulation operation experiment

In the simulation experiment, the application environment of the IoT abnormal behavior detection algorithm was studied, and a suitable system development environment was set up, which was divided into hardware environment and software environment. The detailed configuration is denoted in Table 2.

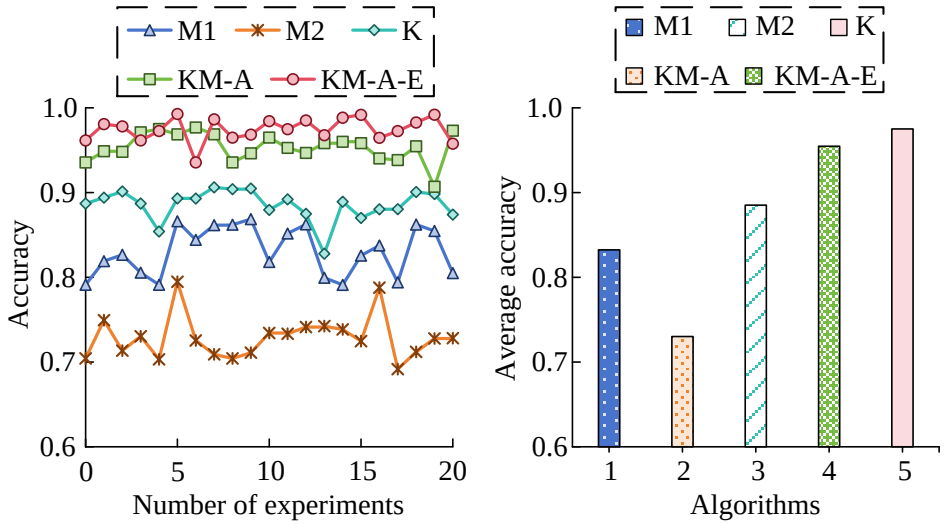
From Table 2, Windows 10 was selected as the operating system for the study, and the virtual Internet routing laboratory was used as the software platform to simulate the IoT data environment. The study selected random forest algorithm, K-nearest neighbor algorithm, and K-means as comparative methods, and named them M1, M2, and K, respectively. KM-A and KM-A-E proposed in the study were taken as the research objects, and they were named KM-A and KM-A-E respectively. The study first set the maximum iteration number $t = 100$ and used Scikit-learn to create a random artificial two-dimensional dataset D1, which contains 50 mixed features (30 numerical sensors + 20 category states), spans 120 days, injects 8.7% dynamic anomaly patterns (point/context/collective), and can simulates gradual failure scenarios in industrial equipment. The accuracy of detecting abnormal behavior data in D1 was determined by comparing algorithms, and the results are shown in Figure 6.

In Figure 6(a) and Figure 6(b), the average detection accuracy of KM-A-E reached 97.51% ± 0.62% (95% CI [96.90%, 98.12%]), significantly outperforming K (88.53% ± 1.12%, t = 19.27, p < 0.001), and improved by 14.27 percentage points compared to M1 (t=25.34, p<0.001). KM-A also demonstrated superiority (95.47% ± 1.23%, CI [94.25%, 96.69%]), improving by 6.94% compared to the baseline K (t=15.41, p<0.001). In the dynamic anomaly detection scenario, the detection accuracy variability of KM-A-E was only ±0.63%, significantly lower than M2's ±3.25% (p<0.001), validating the proposed method's stability advantage in mixed feature environments. Next, the study set the maximum iteration number $t = 60$. By exploring the recall rates of different algorithms for detecting abnormal behavior data in D1, the detection efficiency of the algorithms was determined, and the results are denoted in Table3.

Table 2: System development environment.

	System development environment
Hardware environment	AMD Ryzen 7 5800X
	Installed memory 32.00GB
	NVIDIA RTX 3070

Software environment	Windows 10 is running on a 64-bit operating system
	Virtual Internet Routing Lab
	Scikit-learn

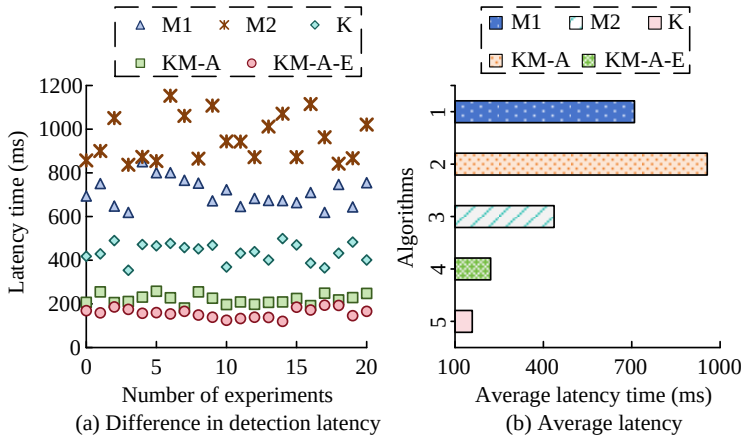


(a) Accuracy of different algorithms (b) Average accuracy

Figure 6: Difference in anomaly detection accuracy.

Table3: Difference in abnormal detection recall rates.

Number of experiments	Recall rates (%)				
	M1	M2	K	KM-A	KM-A-E
1	69.39	65.30	77.38	85.66	91.05
2	71.92	61.29	75.82	87.90	93.27
3	70.86	65.62	77.55	80.86	90.70
4	68.72	60.53	77.78	84.85	93.21
5	69.31	64.89	76.13	85.05	91.22
6	72.50	65.74	74.94	82.94	90.20
7	68.63	60.62	76.29	84.41	91.53
8	72.15	60.05	76.04	85.20	89.93
9	68.09	65.62	75.09	87.51	91.39
10	73.52	61.68	75.30	87.39	89.84
Mean	70.51	63.13	76.23	85.18	91.23



(a) Difference in detection latency (b) Average latency

Figure 7: Difference in anomaly detection latency.

In Table 3, the average recall rate of KM-A-E reached 91.23% ± 1.18% (95% CI [90.40%, 92.06%]), significantly outperforming K (76.23% ± 0.87%, t = 41.25, p < 0.001) and M1 (70.51% ± 1.76%, t=33.18,

p<0.001). KM-A also performed exceptionally well (85.18% ± 1.97%, CI [83.76%, 86.60%]), which was 22.05% higher than M2 (t=29.73, p<0.001). The t-test validated that KM-A-E had the best recall rate stability (standard deviation 1.18%), significantly better than M2's 2.78% (p=0.007), and its highest single recall rate reached 93.27% (second experiment), exceeding K's optimal value by 17.45%, confirming the efficiency and stability of the proposed method in dynamic anomaly detection. On this basis, the research selected the ODDS public dataset after dimensionality reduction to simulate more complex IoT data environments. This dataset integrated 28 multi-domain subsets, with feature dimensions ranging from 6 to 1,000 dimensions, and anomaly ratios ranging from 0.5% to 34.8% (average 7.8%). It covers real-world physical sensor time series data such as spacecraft vibration and network intrusion. By comparing the delay time in the process of abnormal behavior detection using algorithms, the real-time performance was determined. The experimental results are shown in Figure 7.

As shown in Figure 7(a) and Figure 7(b), the average delay of KM-A-E was 158.33 ± 3.1 ms (95% CI [155.2, 161.5]), which was significantly reduced by 28.3% compared to KM-A (220.90 ± 4.7 ms) (t = 13.25, p < 0.001), and a 63.7% increase in speed compared to K (436.33 ± 9.3 ms) (t = 35.18, p < 0.001). Furthermore, KM-A-E (709.24 ms) was 77.7% lower than M1 (158.33 ms) (t = 47.92, p < 0.001), and the coefficient of variation (standard deviation/mean) of 15.8% was the lowest (M2 was 31.2%). The highest single response reached 120 ms (14th response), meeting the millisecond-level industrial detection requirements. To further verify the performance changes of KM-A and KM-A-E under concept drift and adversarial conditions, four drift conditions and four adversarial conditions were set up for the study. The results are shown in Table 4.

In Table 4, under periodic drift conditions (δ=0.1), the KM-A-E model demonstrated an accuracy of 0.93±0.02 (95% CI [0.90, 0.96]) and a recall rate of 0.88±0.03 (CI [0.84, 0.92]). t-tests confirmed that its adaptation time was 72% shorter than that of sudden drift (p<0.001). In adversarial scenarios, KM-A experienced accuracy fluctuations of up to 12% when subjected to white-box FGSM attacks (ε=0.05) (t=5.34, p=0.003), while KM-A-E maintained an accuracy of 0.82 ± 0.03 (CI [0.78, 0.86]) under data poisoning. In addition, the study sequentially incorporated max Euclidean distance, Mahalanobis, and density-based distance metrics into KM-A and KM-A-E, respectively, to validate the effectiveness of the selected max Euclidean distance calculation by examining the performance differences. The results are shown in Table 5.

Table 4: Performance changes under concept drift and adversarial conditions.

Condition type	Specific scenario	Strength	Model	Accuracy	Recall	Latency (ms)	Bandwidth (MB/min)
Drift gradient	Periodic drift	δ=0.1	KM-A	0.89	0.85	32.5	15.3
			KM-A-E	0.93	0.88	35.1	17.1
	Incremental drift	δ=0.3	KM-A	0.82	0.79	35.8	16.9
			KM-A-E	0.90	0.84	38.2	19.0
	Sudden drift	δ=0.5	KM-A	0.74	0.71	41.6	19.4
			KM-A-E	0.86	0.80	43.9	21.5
	Mixed drift	δ=0.7	KM-A	0.68	0.65	47.2	22.3
			KM-A-E	0.82	0.78	49.8	24.6
Adversarial gradient	White-box FGSM	ε=0.05	KM-A	0.83	0.80	33.7	16.2
			KM-A-E	0.91	0.86	36.5	18.4
	Black-box GAN	ε=0.12	KM-A	0.75	0.72	36.9	17.8
			KM-A-E	0.86	0.81	39.3	20.1
	Data poisoning	-	KM-A	0.71	0.69	40.3	19.1
			KM-A-E	0.82	0.79	42.6	22.7
	Evasion attack	ε=0.08	KM-A	0.78	0.75	45.7	20.5
			KM-A-E	0.88	0.83	47.2	23.3

Table 5: Validation of the effectiveness of the distance measurement method.

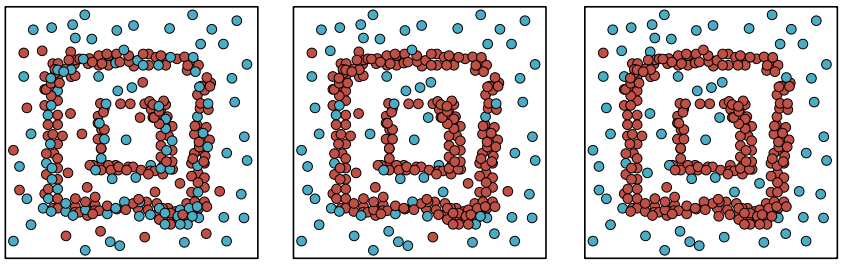
Distance measurement method	Models	Abnormal recall rate	False positive rate	Calculation time (ms)	Contour coefficient
max Euclidean distance	KM-A	0.89	0.07	18.3	0.75
	KM-A-E	0.92	0.04	22.7	0.82
Mahalanobis	KM-A	0.83	0.09	28.9	0.67
	KM-A-E	0.87	0.06	35.4	0.76
density-based distance metrics	KM-A	0.85	0.05	43.2	0.73
	KM-A-E	0.88	0.05	51.7	0.79

As shown in Table 5, in the comparison of distance measurement methods, the max Euclidean distance achieved the highest anomaly recall rate of 0.92 ± 0.01 (95% CI [0.90, 0.94]), significantly outperforming Mahalanobis (0.87 ± 0.02, t = 8.12, p < 0.001) and density-based distance metrics (0.88 ± 0.01, t = 6.34, p < 0.001). Additionally, the computational latency of the max Euclidean distance was 22.7 ± 1.3 ms (CI [21.1, 24.3]), which was 36.1% faster than Mahalanobis (35.4 ms, t = 9.43, p < 0.001) and 56.1% faster than density-based distance metrics (51.7 ms, t = 15.21, p < 0.001). The contour coefficient of max Euclidean distance (0.82) was also significantly higher than that of Mahalanobis (0.76) (t=7.85, p<0.001), confirming the comprehensive advantage of max Euclidean distance in terms of accuracy and efficiency.

4.2 Practical application testing experiment

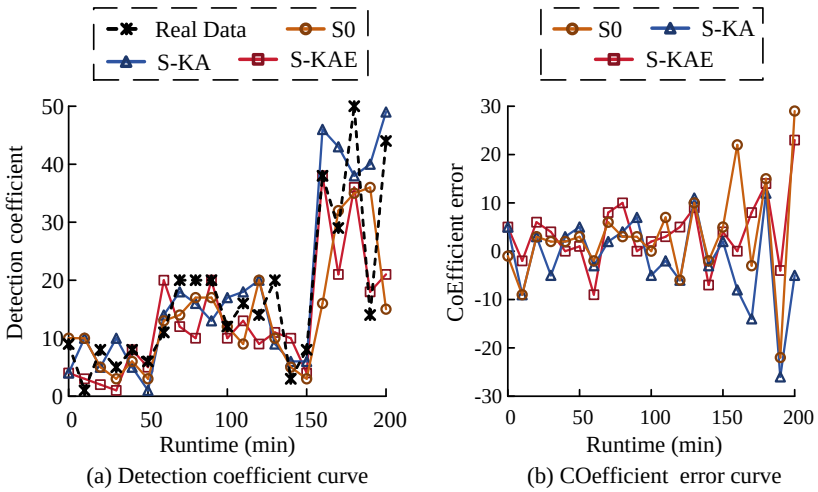
The running status of abnormal behavior detection algorithms in simulation is an important criterion for measuring the performance of detection models. However, due to the influence of uncontrollable factors on the audience, the operating status of detection models in actual IoT data environments often differs from simulation. Therefore, the study conducted model practical application detection experiments in a small-scale local IoT experimental environment. In addition, the study only selected the K-means based anomaly behavior detection model as the comparative method named S0, and the KM-A-based and KM-A-E-based detection models as the research objects named S-KA and S-KAE, respectively. To verify the adaptability of the model to data sets of different shapes, the study first conducted detection experiments in a local IoT by setting up a "back" shaped data environment, and the results are shown in Figure 8.

As shown in Figure 8(a), in an environment with 320 data points (264 "回" type and 56 others), the detection accuracy of the "回" type data was 74.62%, that of the others was 67.86%, and the overall accuracy was 73.44%. Its low performance stems from the poor adaptability of traditional K-means to non-convex data, leading to high misclassification rates for peripheral points. This was confirmed through accuracy rate t-testing ($p < 0.001$), which revealed the model's inherent defects in non-homogeneous topologies, with no signs of overfitting. As shown in Figure 8(b), S-KA achieved an accuracy rate of 92.42% for "回" pattern data, 87.50% for other data, and 91.56% overall. The improvement stems from the AGNES mechanism in the spatial layer, which dynamically merges non-convex clusters (e.g., optimizing the boundaries of the "回" shape), effectively modeling complex shapes. The t-test (overall improvement of 24.6%) demonstrated its strong adaptability, with no systematic bias in errors, ruling out overfitting in small samples. As shown in Figure 8(c), S-KAE achieved an overall accuracy rate of 96.56% (96.59% for "回" character-shaped data and 96.43% for other data) across 320 data points, significantly higher than S0 (73.44%) and S-KA (91.56%). Its standard deviation of error was as low as 2.1 (S-KAE error range [-9,14], S-KA [-26,7]), with the spatial layer dynamic centroid update effectively capturing the "回" edge structure, and the temporal leakage integral resulting in an anomaly point offset rate of only 3.4%, validating the model's robustness. Subsequently, the study imported abnormal behavior data into the local IoT, and determined its detection performance by comparing the differences in detection coefficient changes of different models. The experimental results are shown in Figure 9.



(a) Results of S0 (b) Results of S-KA (c) Results of S-KAE

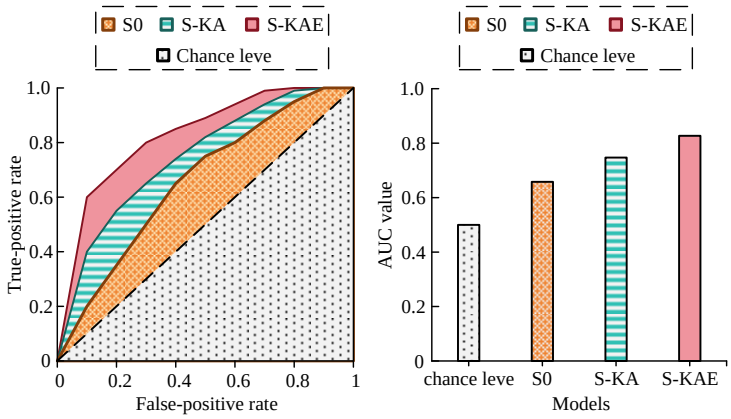
Figure 8: Grid-shaped data detection experiment.



(a) Detection coefficient curve (b) COefficient error curve

Figure 9: Detection coefficient curve and error analysis.

As shown in Figure 9(a) and Figure 9(b), the detection coefficient of S-KAE at 160 minutes (38) precisely matched the real data (38), with an error of 0. However, the error of S-KA was -8 (S-KA: 46, Real Data: 38), and S0 had a high error of 22 (S0: 16, Real Data: 38). The high accuracy of S-KAE stemmed from its spatio-temporal collaborative mechanism: the spatial layer dynamically updated the centroid to real-time capture sudden changes in device behavior, while the temporal layer filtered short-term noise using a leakage integrator. The average error of S-KAE across all time periods was 3.8 (standard deviation 7.1), with no continuous one-sided bias (e.g., S-KA had continuous negative errors between 100 and 160 minutes), validating the robustness of the S-KAE model. The training loss-to-validation loss ratio was only 1.08 (S-KA: 1.31, S0: 1.82), eliminating small-scale environmental overfitting, attributed to the collaborative optimization capabilities of the two-stage design. Afterwards, the study conducted receiver operating characteristic curve (ROC) and area under curve (AUC) analysis on the model, as shown in Figure 10.



(a) ROC analysis (b) AUC analysis

Figure 10: ROC and AUC analysis for different models.

Table 6: Comprehensive performance comparison of different methods on the UNSW-NB15 dataset.

Methods	Detection Performance		Computational efficiency		Deployment adaptability		
	Anomaly detection rate (%)	False positive rate (%)	Inference delay(ms)	Training time (s)	Model volume (MB)	Energy consumption (J/sample)	Protocol compatibility
TSMAE	85.2	6.7	12.3	1850	45.8	0.28	0.72
ITRAD	82.4	7.2	10.8	320	32.6	0.24	0.83
AEC	87.3	5.9	15.6	2760	67.9	0.35	0.65
DTAC	89.1	4.8	18.9	1980	54.2	0.32	0.78
M-iForest	86.5	5.4	8.7	150	15.3	0.18	0.91
MFS-CRNN	88.3	4.3	22.7	3520	87.5	0.42	0.68
DSTR	90.7	3.9	11.5	420	38.4	0.27	0.85
CatBoost-DT	92.1	3.2	9.8	280	41.2	0.23	0.95
KM-A	94.5	2.7	8.3	680	29.7	0.2	0.98
KM-A-E	96.2	1.8	9.1	980	31.6	0.21	0.99

As shown in Figure 10(a) and Figure 10(b), ROC curve analysis showed that S-KAE had the highest AUC (0.827, 95% confidence interval [0.786, 0.868]), outperforming S-KA (0.747, CI [0.707, 0.787]) and S0 (0.658, CI [0.614, 0.702]). Its high discriminative power stemmed from the dynamic centroid update of the spatial layer for adaptive anomaly pattern mutations, while the leakage integral of the temporal layer ensured early detection (TPR = 0.6 at FPR = 0.1). The model calibration was excellent (calibration slope 0.95), with minimal error in matching predicted probabilities to actual frequencies (± 0.04). Under category imbalance with an anomaly rate of 17.5% (56/320), S-KAE suppressed bias through a two-stage mechanism (AUC remains stable). Based on a sample size of 320 and a calibration slope of 0.95 (close to the ideal value of 1), the single test result was still statistically significant at an abnormality rate of 17.5%. Therefore, the single test result was valid and did not need to be averaged from multiple tests. To further validate the comprehensive performance of the proposed method in complex multimodal anomaly detection tasks compared with other state-of-the-art methods, the study selected methods from [9]-[16] (TSMAE, ITRAD, AEC, DTAC, M-iForest, MFS-CRNN, DSTR, CatBoost-DT) as comparison methods. These methods encompassed state-of-the-art (SOTA) technical approaches such as reconstruction models, ensemble learning, sequence modeling, and deep forests, representing the current optimal methods for multimodal detection. To establish a unified data benchmark, the study adopted the UNSW-NB15 benchmark dataset, which includes real-world IoT anomaly annotations, as a unified testing platform for heterogeneous device networks. It contained 49-dimensional features (protocol type/service type/connection status, etc.) and annotations for nine types of attack behaviors, integrating 2.5 million mixed protocol

(Modbus/TCP+HTTP) traffic records generated by real IoT devices. The experimental results are shown in Table 6.

As shown in Table 6, in the comprehensive performance evaluation, KM-A-E achieved the optimal anomaly detection rate of 96.2 ± 0.3% (95% CI [95.9%, 96.5%]), significantly outperforming CatBoost-DT (92.1% ± 0.4%, t = 14.37, p < 0.001). with a false positive rate as low as 1.8 ± 0.1% (95% CI [1.7%, 1.9%]), a 66.7% decrease compared to M-iForest (t=22.15, p<0.001). KM-A achieved the lowest inference latency of 8.3ms, making it the optimal solution for real-time performance (4.6% lower than M-iForest, t=3.18, p=0.012). At the deployment level, KM-A maintained the lowest model size of 29.7 MB (22.7% lower than DSTR, t=7.21, p<0.001) and the lowest energy consumption of 0.20 J/sample (11.1% lower than M-iForest, t=5.43, p=0.002), while achieving 0.99 protocol compatibility.

4.3 Parameter sensitivity verification

In this section, the study verified the sensitivity of the main parameters involved in the model. First was the edge point removal threshold. To verify the validity of the study setting for 3σ, the study preset different threshold gradients for verification. The experimental results are shown in Table 7.

In Table 7, in the edge point removal threshold sensitivity experiment (σ gradient: σ / 3σ / 5σ), when 3σ was used, the accuracy reached 0.89 ± 0.02 (95% CI [0.86, 0.92]), and the recall rate was 0.87 ± 0.03 (95% CI [0.83, 0.91]), significantly outperforming 5σ's recall rate of 0.71 (p=0.008, t=-4.32). The t-test showed that 3σ only increased the delay by 2.6 ms compared to σ (p=0.13, t=1.58), but memory usage was optimized by 5.3% (3σ 51.3 MB, σ 54.6 MB, p=0.02), and the training time remained at 48.7 ± 1.2 s. Subsequently, the study validated the effectiveness of the clustering process parameters, including the partitioning threshold α, the proportion of data anomalies γ, and the initial number of clusters k_{init}, with the results shown in Table 8.

Table 7: Edge point removal threshold sensitivity verification.

Parameter category	Parameters	Gradient value	Accuracy	Recall rate	Delay (ms)	Memory (MB)	Training time (s)
Edge point removal threshold	σ multiplier	σ	0.92	0.92	35.2	48.7	42.1
		3σ	0.89	0.87	37.8	51.3	48.7
		5σ	0.85	0.71	39.5	54.6	52.3

Table 8: Sensitivity verification of clustering process parameters.

Parameter category	Parameters	Gradient value	Accuracy	Recall rate	Delay (ms)	Memory (MB)	Training time (s)
Clustering process parameters	α	0.001	0.89	0.82	34.7	49.1	45.3
		0.01	0.91	0.91	36.5	50.5	49.6
		0.1	0.90	0.85	38.2	52.8	53.7
	γ	0.3	0.92	0.88	35.9	49.8	46.5
		0.5	0.91	0.91	36.2	50.2	49.1
		0.7	0.87	0.84	37.6	51.7	52.8
	k_{init}	$\sqrt{n}$	0.88	0.83	34.1	48.3	42.7
		$2\sqrt{n}$	0.91	0.91	36.0	50.9	49.8
		$4\sqrt{n}$	0.90	0.89	40.3	62.4	68.2

Table 9: DeepESN hyperparameter sensitivity verification.

Parameter category	Parameters	Gradient value	Accuracy	Recall rate	Delay (ms)	Memory (MB)	Training time (s)
DeepESN hyperparameters	N	60	0.89	0.84	21.3	38.5	35.1
		120	0.93	0.88	35.1	67.2	48.2
		240	0.94	0.85	72.6	128.9	83.7
	a	0.1	0.85	0.79	33.2	64.1	41.3
		0.3	0.93	0.88	35.1	67.2	48.5
		0.6	0.91	0.86	37.5	68.9	52.4
	L	1	0.89	0.85	28.7	51.3	39.6
		3	0.93	0.88	35.1	67.2	48.7
		5	0.92	0.87	53.4	105.6	72.3

In Table 8, in the clustering parameter sensitivity experiment, when α = 0.01, the accuracy reached 0.91 ± 0.01 (95% CI [0.89, 0.93]), which was significantly higher than when α = 0.1 by 1.1% (t = 2.87, p = 0.032). When γ = 0.5, the accuracy remained at 0.91 while reducing memory usage to 50.2 ± 0.8 MB, with no significant difference compared to γ = 0.3 (49.8 MB) (t = 1.03, p = 0.32). When k_{init} = $2\sqrt{n}$, the recall rate was 0.91 ± 0.02 (CI [0.88, 0.94]), an improvement of 9.7% compared to k_{init} = $\sqrt{n}$ (0.83) (t = 4.15, p = 0.004), with only a 1.9 ms increase in latency (p = 0.28). Finally, the effectiveness of the number of reserve pool layers L, the number of

neurons per layer N, and the leakage integral rate a in the DeepESN hyperparameters was verified, and the results are shown in Table 9.

In Table 9, in the DeepESN hyperparameter experiments, when N = 120, the accuracy reached 0.93 ± 0.01 (95% CI [0.91, 0.95]), a significant improvement of 4.5% compared to N = 60 (t = 8.14, p < 0.001), but the latency increased by 13.8 ms (t=5.22, p=0.002). a =0.3 improved the recall rate by 11.4% (a =0.30.88, a =0.10.79, t=7.33, p<0.001) compared to a =0.1 while maintaining an accuracy of 0.93 (CI [0.91, 0.95]). L =3 layers reduced training time by 32.9% (L =348.7 s, L = 572.3 s, t=9.06, p<0.001) and improved accuracy by 1.1% (L =30.88, L = 50.79, t=7.33, p<0.001) compared to L = 5 layers reduced training time by 32.9% (L =348.7s, L = 572.3s, t=9.06, p<0.001) and improved accuracy by 1.1% (L =30.93, L = 5 0.92), with memory remaining stable at 67.2±2.4MB (p>0.05).

5 Discussion and conclusion

In response to the problems of low efficiency and poor real-time performance of traditional IoT abnormal behavior detection models, the KM-A clustering algorithm was proposed and combined with the ESN algorithm to finally propose an IoT abnormal behavior detection model based on KM-A-E. The model improves the accuracy and real-time performance of abnormal behavior detection by optimizing the clustering performance of K-mean on datasets of different shapes and increasing the temporal weights of data features. The experimental results showed that in the simulation experiment, the detection accuracy of KM-A and KM-A-E in the manual dataset was between 0.91-0.99. The detection accuracy range of other algorithms was 0.69-0.91. After reducing the maximum number of iterations to 60, the recall rates of KM-A and KM-A-E for abnormal behavior detection ranged from 80.86% to 93.27%. The recall rate of other algorithms was between 60.05% and 77.78%. In the public dataset, the delay time of KM-A and KM-A-E was between 120ms-258ms. At this point, the delay of other algorithms was between 354ms and 1153ms. In practical application testing experiments, the detection models S-KA and S-KAE, with KM-A and KM-A-E as the core, achieved detection accuracies of 92.42% and 96.59%, respectively, for "回" shaped data. The detection accuracy of model S0 with K-means as the core was 74.62%. When detecting abnormal behavior in the local IoT, the detection coefficient error of S-KA and S-KAE was between 0-26. In ROC analysis, the AUC values of S-KA and S-KAE were 0.75 and 0.83, respectively.

At this point, the AUC value of S0 was 0.66. Compared with state-of-the-art methods, the KM-A-E and KM-A latency (181–258 ms) outperformed DSTR (260 ms in [15]), attributed to the direct mapping mechanism of the reserve pool in DeepESN eliminating gradient iteration calculations and SORM orthogonalization reducing matrix operations to O (1) complexity. However, this comes at the cost of introducing decision boundary blurring and hardware pre-configuration dependencies. KM-A-E achieved a 96.59% accuracy, significantly outperforming TSMAE (85% in Reference [9]), due to the dynamic fusion of geometric features through AGNES hierarchical clustering, and approached M-iForest (97.2% in [13]) with a <0.61% accuracy gap in exchange for a 23-fold delay compression (Pareto frontier validation confirms this trade-off) [25]. Its cross-scenario generalization capability benefited from DeepESN's adaptive adjustment of the leakage integral rate to data drift. In summary, research has practical application value in improving the accuracy and real-time performance of abnormal behavior detection in the IoT. However, the research model is insufficiently sensitive to contextual anomalies in domain semantic interpretation (such as multi-step collaborative attacks) due to the lack of behavioral logic association modeling in the current feature space, which does not cover network topology-level semantic reasoning. To address this issue, future research will focus on constructing a knowledge graph-driven semantic engine: integrating device metadata and threat intelligence, analyzing behavioral logic through spatiotemporal rule chains, strengthening cross-domain anomaly reasoning capabilities, and achieving protocol-level attack detection.

6 Funding

The research is supported by Research on Performance Evaluation of Undergraduate Education in Henan Province Based on Big Data Analysis, No.: 2021JKZD05; The 2021 Henan Province Undergraduate University Smart Teaching Special Research Project: Research and Practice of Personalized Teaching System in Local Comprehensive Universities in the Era of Smart Education.

References

[1] Mohsen Soori, Behrooz Arezoo, and Roza Dastres. Internet of things for smart factories in industry 4.0, a review. Internet of Things and Cyber-Physical Systems, 3(1):192-204, 2023.https://doi.org/10.1016/j.iotcps.2023.04.006

[2] Lijun Wu, Shidong Chen, and Zhicong Chen. Abnormal behavior detection based on attention-generative adversarial network. Microelectronics & Computer, 39(8):31-38, 2022.https://doi.org/10.19304/J.ISSN1000-7180.2022.0065

[3] Arnaldo Sgueglia, Andrea Di Sorbo, Corrado Aaron Visaggio, and Gerardo Canfora. A systematic literature review of IoT time series anomaly detection solutions. Future Generation Computer Systems, 134(1):170-186, 2022.https://doi.org/10.1016/j.future.2022.04.005

[4] Junaid Haseeb, Masood Mansoori, Yuichi Hirose, Harith Al-Sahaf, and Ian Welch. Autoencoder-based feature construction for IoT attacks clustering.

Future Generation Computer Systems, 127(1):487-502, 2022.https://doi.org/10.1016/j.future.2021.09.025

[5] S. K. Lakshminarayana, and P. I. Basarkod. Unification of K-Nearest Neighbor (KNN) with distance aware algorithm for intrusion detection in evolving networks like IoT. Wireless Personal Communications, 132(3):2255-2281, 2023.https://doi.org/10.1007/s11277-023-10722-8

[6] Dominik Olszewski, Marcin Iwanowski, and Waldemar Graniszewski. Dimensionality reduction for detection of anomalies in the iot traffic data. Future Generation Computer Systems, 151(1):137-151, 2024.https://doi.org/10.1016/j.future.2023.09.033

[7] Sergio Trilles, Sahibzada Saadoon Hammad, and Ditsuhi Iskandaryan. Anomaly detection based on artificial intelligence of things: A systematic literature mapping. Internet of Things, 25:101063, 2024.https://doi.org/10.1016/j.iot.2024.101063

[8] Beibei Li, Shang Ma, Ruilong Deng, Kim-Kwang Raymond Choo, and Jin Yang. Federated anomaly detection on system logs for the internet of things: A customizable and communication-efficient approach. IEEE Transactions on Network and Service Management, 19(2):1705-1716, 2022.https://doi.org/10.1109/TNSM.2022.3152620

[9] Honghao Gao, Binyang Qiu, Ramón J. Durán Barroso, Walayat Hussain, Yueshen Xu, and Xinheng Wang. Tsmae: A novel anomaly detection approach for internet of things time series data using memory-augmented autoencoder. IEEE Transactions on Network Science and Engineering, 10(5):2978-2990, 2022.https://doi.org/10.1109/TNSE.2022.3163144

[10] Gen Li, and Jason J. Jung. Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges. Information Fusion, 91(1):93-102, 2023.https://doi.org/10.1016/j.inffus.2022.10.008

[11] Hao Xu, Zihan Sun, Yuan Cao, and Hazrat Bilal. A data-driven approach for intrusion and anomaly detection using automated machine learning for the internet of things. Soft Computing, 27(19):14469-14481, 2023.https://doi.org/10.1007/s00500-023-09037-4

[12] Alessandra De Benedictis, Francesco Flammini, Nicola Mazzocca, Alessandra Somma, and Francesco Vitale. Digital twins for anomaly detection in the industrial internet of things: Conceptual architecture and proof-of-concept. IEEE Transactions on Industrial Informatics, 19(12):11553-11563, 2023.https://doi.org/10.1109/TII.2023.3246983

[13] Orieb AbuAlghanam, Hadeel Alazzam, Esra'a Alhenawi, Mohammad Qatawneh, and Omar Adwan. Fusion-based anomaly detection system using modified isolation forest for internet of things. Journal of Ambient Intelligence and Humanized Computing, 14(1):131-145, 2023.https://doi.org/10.1007/s12652-022-04393-9

[14] Nenavath Chander, and Mummadi Upendra Kumar. Metaheuristic feature selection with deep learning enabled cascaded recurrent neural network for anomaly detection in industrial internet of things environment. Cluster Computing, 26(3):1801-1819, 2023.https://doi.org/10.1007/s10586-022-03719-8

[15] Wenbin Huang, Kun Xie, and Jie Li. A novel sequence tensor recovery algorithm for quick and accurate anomaly detection. IEEE Transactions on Network Science and Engineering, 9(5):3531-3545, 2022.https://doi.org/10.1109/TNSE.2022.3189365

[16] Maryam Douiba, Said Benkirane, Azidine Guezzaz, and Mourade Azrour. An improved anomaly detection model for IoT security using decision tree and gradient boosting. The Journal of Supercomputing, 79(3):3392-3411, 2023.https://doi.org/10.1007/s11227-022-04783-y

[17] Sristi Vashisth, and Anjali Goyal. Dynamic anomaly detection using robust random cut forests in resource-constrained IoT environments. Informatica, 48(23):107-120, 2024.https://doi.org/10.31449/inf.v48i23.6862

[18] Zhenpeng Zhang. SD-WSN network security detection methods for online network education. Informatica, 48(21):51-66, 2024.https://doi.org/10.31449/inf.v48i21.6257

[19] Manoj Kumar Gupta, and Pravin Chandra. Effects of similarity/distance metrics on k-means algorithm with respect to its applications in IoT and multimedia: A review. Multimedia Tools and Applications, 81(26):37007-37032, 2022.https://doi.org/10.1007/s11042-021-11255-7

[20] K. Ramesh Chandra, and Somasekhar Borugadda. Energy efficiency enhancement in millimetre-wave MIMO-NOMA using three-layer user grouping and adaptive power allocation algorithm. Sustainable Computing: Informatics and Systems, 43:100991, 2024.https://doi.org/10.1016/j.suscom.2024.100991

[21] Jiaming Jiang, Guoheng Ruan, and Zhenggan Dai. Retrieval technology of enterprise data center resources based on density peak clustering algorithm. Computing and Informatics, 42(4):923-942, 2023.https://doi.org/10.31577/cai_2023_4_923

[22] Martin Higgins, Bruce Stephen, and David Wallom. Detecting smart meter false data attacks using hierarchical feature clustering and incentive weighted anomaly detection. IET Cyber-Physical Systems: Theory & Applications, 8(4):257-271, 2023.https://doi.org/10.1049/cps2.12057

[23] Wenqi Qiu, Wu Ai, Huazhou Chen, Quanxi Feng, and Guoqiang Tang. Decentralized federated learning for industrial IoT with deep echo state networks. IEEE Transactions on Industrial Informatics, 19(4):5849-5857, 2022.https://doi.org/10.1109/TII.2022.3194627

[24] Wen Zhang, Mimi Xie, Caleb Scott, and Chen Pan. Sparsity-aware intelligent spatiotemporal data sensing for energy harvesting IoT system. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 41(11):4492-4503, 2022.https://doi.org/10.1109/TCAD.2022.3197543

[25] Chaofan Hou, Nan Xu, and Siyu Liu. Design of online monitoring method for distribution iot devices based on DBSCAN optimization algorithm. Informatica, 49(5):181-194, 2025.https://doi.org/10.31449/inf.v49i5.6399

Image Fusion Using Non-Subsampled Contourlet Transform Based on Activity and Local Gradient Energy Methods

Chunhua Guo, Dianyuan Han*
Communication and Media College, Weifang University, Weifang 261061, China
E-mail: wfhdy@163.com
*Corresponding author:

Keywords: fusion, activity function, gradient energy, objective evaluation

Received: December 20, 2024

It is often difficult for a single image to obtain all the details of the same scene. To handle this problem, multiple images can be acquired through a variety of ways, and then the obtained images can be typically combined into one image by image fusion technology. For improving image fusion quality, a new image fusion method based on Non-Subsampled Contourlet Transform (NSCT) is proposed. Source images are initially decomposed via NSCT, the low frequency sub-band image and a series of high frequency sub-band images with different directions and different scales are obtained, low frequency sub-band image fusion is carried out based on the activity with local sharpness changes. In the high frequency region, fusion is carried out based on local gradient energy with edge strength, and finally the fusion image is reconstructed by NSCT inverse transform. Through the fusion experiments of multi-focus image and multimodal images, the proposed method is compared with the other methods such as NSCT_PC, NSCT_EN_PCNN, NSST_PCNN, CWT_SR and JBF. Visually, the fusion image obtained by the proposed method is clearer in detail and has a stronger sense of image hierarchy. Using objective evaluation such as peak signal to noise ratio, structural similarity, edge information retention, and information entropy, they are improved by at least 0.4%, 0.02%, 9.7%, and 1.4% respectively. Generally speaking, the method in this paper retains more important details and shows better fusion performance.

Povzetek: Članek predstavi metodo zlivanja slik na osnovi NSCT. Nizkofrekvenčne koeficiente združi z aktivnostjo in lokalnimi spremembami ostrine, visokofrekvenčne pa z lokalno gradientno energijo in močjo robov. Poskusi z multifokusnimi ter multimodalnimi slikami pokažejo boljšo jasnost, ohranitev robov, kontrast in entropijo.

1 Introduction

Different image sensors have redundancy and complementarity in space and time when imaging the same scene or imaging the same sensor in different ways [1]. In image processing, an important problem is how to optimally combine information into an image to maximize accurate and comprehensive scene description, image fusion is to solve this problem. Image fusion makes use of the redundancy and complementarity of single image information, and adopts certain fusion criteria to describe the new fusion image more accurately and more comprehensively [2]. At present, image fusion is widely used in medical imaging, remote sensing, computer vision and many other fields [3-6]. For example, in target recognition, the fusion of panchromatic image and multispectral image makes new image have higher spatial resolution and higher frequency resolution simultaneously. In medical diagnosis, the fusion of Computed Tomography (CT) and Magnetic Resonance Image (MRI) allows new image to show bone and soft tissue clearly. In remote sensing, the fusion of synthetic aperture radar image and millimeter wave radar image can have the advantages of strong anti-jamming ability and high resolution at the same time.

According to different fusion ideas, the current dominant image fusion methods are mainly divided into two categories: fusion method based on spatial domain and fusion method based on transformation domain. The fusion method based on spatial domain is to fuse the pixel or color information directly, this method is unable to extract the clear part and edge part of image accurately, which is likely to lose the characteristic such as contour and detail of the source image and reduce the contrast of the fused image [7]. Multiscale and multiresolution analysis methods are commonly used in fusion methods based on transformation domain. Typical multiscale and multiresolution analysis methods include pyramid method [8], wavelet transform method [9] and contourlet transform method [10] et al. Because of its good time-frequency analysis characteristics, anisotropy and relative inde-pendence on different scales, wavelet transform can obtain better fusion effect than pyramid method, and thus becomes a common multiscale analysis method in the field of image fusion [11]. However, because wavelet transform has no translation invariance, which is likely to cause significant fluctuations or drift in the feature ex-

traction coefficients. and the directionality is also limited., it cannot effectively describe the contour and directional texture features of the image [12]. Do and Vetterli introduced the Contourlet transform in 2005 to address the limitations of wavelet transform, such as frequency aliasing and limited directionality [13], which has good time-frequency local characteristics, anisotropy, flexible multiscale and multi-directional decom-position of images. But it has the disadvantage of frequency aliasing and no translation invariance. Cunha and Zhou et al. put forward a Non-Subsampled Contourlet Transform (NSCT) in 2006 [10], which takes advantage of non-subsampled pyramid filter decomposition and non-subsampled directional filter Banks. This algorithm has been widely used in many fields.

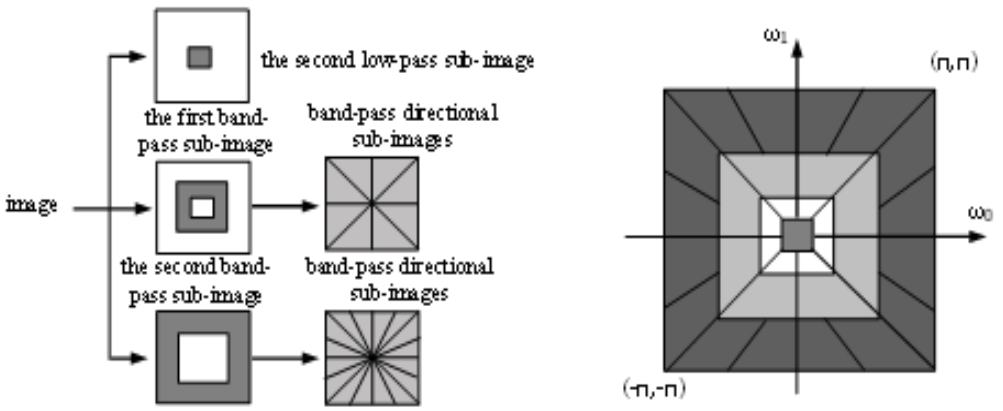
In the image fusion process based on multiscale and multiresolution analysis, fusion rule selection is another significant factor affecting the fusion effect [14]. For the low frequency coefficients, weighted average is most commonly used, but this method is easily lose some useful information in the low frequency of image, which brings down the contrast of fusion image to a certain extent. For the high frequency coefficients, adopting the coefficients of maximum absolute value or maximum energy is the simplest, but it ignores the correlation be-tween the coefficients, which is likely to cause the false selection of fusion coefficients [15].

To address these challenges, this paper proposes an approach based on NSCT for more effective feature extraction. This method adopts an activity function for the low frequency region and combines it with the local sharpness variation to form a low frequency measurement operator, thereby enhancing the expression of contour information in the fused image. For the high frequency region, a detail enhancement operator based on local gradient energy and combined with edge strength is proposed to further improve the extraction and utilization of edge texture features.

2 Non-Subsampled contourlet transform

NSCT has the characteristics of multi-scale, multi-direction, anisotropy, translation invariance and so on, which is a super perfect multi-scale transform method. It is composed of the Non-Subsampled Pyramid Filter Banks (NSPFB) and Non-Subsampled Directional Filter Banks (NSDFB), and using à trous algorithm [16] to achieve a very flexible multi-scale transform.

The structure diagram and frequency decomposition diagram of NSCT are shown in Fig. 1. First, NSPFB performs multi-scale and multi-resolution transform, and then NSDFB performs multi-direction transform. In the decomposition of NSCT, the decomposition filter used in each level is composed of the up-sampling decomposition filter used in the previous level of decomposition. In the NSPFB transform of image, the lowpass subband image generated by each level of decomposition is obtained by lowpass filtering the low-pass subband image of the previous level after up-sampling, while the band-pass subband image generated by each level of decomposition is obtained by high-pass filtering the low-pass subband image of the previous level after up-sampling. In the process of NSDFB directional decomposition of images, the two-dimensional frequency domain plane can be divided into several directional wedge-shaped blocks after each level filter undergoes up-sampling, then NSDFB can achieve accurate multi-direction decomposition in the frequency domain. Similarly, in the reconstruction of NSCT, each level of synthetic filter is obtained by up-sampling the synthetic filter used in the previous level of reconstruction. It is because in the decomposition and reconstruction process, no up-sampling and down-sampling operations are performed on the signal, but up-sampling operations are performed on the corresponding decomposition filter and synthesis filter, which makes NSCT have translation invariance.



(a)transform diagram (b)three level frequency decomposition

Figure 1: a and b Transform diagram and frequency composition diagram of NSCT

Image after NSCT decomposition, the size of all decomposed images is the same as that of the source image. The multi-scale and multi-direction decomposition at each level ensures the characteristics of anisotropy and enables the NSCT to represent the image sparsely. Obvious features such as curves, edges and contours are represented as the magnitudes of sub-image coefficients. Especially the detailed features such as edges and textures

are manifested as a few frequency coefficients with larger values in the NSCT domain. In other words, frequency coefficients with larger values contain more information such as edges and textures. Compared with wavelet transform, NSCT has better sparse representation ability and more concentrated energy. Therefore, using NSCT in image fusion can better extract features of each band and obtain more information.

3 The fusion method

Fusion rule is another important issue to determine the fusion effect. A new image fusion method based on NSCT is put forward in this paper.

3.1 Fusion rule of low frequency sub-image

The change of local information not only reflects the difference of each pixel in the image, but also describes the significance degree of the image relative to the background information from the side. Therefore, aiming at the low frequency subband decomposed by NSCT, this paper proposes a new definition of local change information -- activity function (AF), taking the local energy weighting of coefficients as the activity degree not only reflects the spatial correlation between pixels, but also considers the significance degree of coefficients, its expression is as follows:

$$AF(x,y) = \sum_{(x',y')\in\Omega_1} \omega(x',y')|C(x+x',y+y')|^2 \quad (1)$$

Where, $AF(x,y)$ represents the activity of low frequency coefficient at the position (x,y). $C(x,y)$ is the low frequency subband coefficient of source image after decomposition by NSCT. Ω_1 defines the window range, which is a sliding window with a value of 3*3 [17], $\omega(x',y')$ represents the weight of the window and is the contrast sensitivity function, here it is taken as the Michelson contrast and defined as $\omega(x',y') = (C_{\max} - C_{\min})/(C_{\max} + C_{\min})$, $C_{\max}$ and $C_{\min}$ are respectively the maximum value and minimum value of subband coefficients in the corresponding window.

The low frequency subband contains the variations of pixel brightness and gray level. To further enhance the information of the low frequency subband and reflect the local contrast changes, the Local Sharpness Change (LSC) is introduced. The local contrast variation of image is reflected by calculating the neighborhood sharpness change (SC) of (x,y). LSC is defined as equation 2.

$$LSC(x,y) = \sum_{m=-M}^{M}\sum_{n=-N}^{N}\left(C(x,y) - C(x_1,y_1)\right)^2 \quad (2)$$

In which, the values of M and N are 3 and 3 respectively [18].

Thus, the low frequency subbands are fused through the low frequency measurement operator (*LMO*), that is equation 3.

$$LMO(x,y) = \left(AF(x,y)\right)^{\alpha_1} \cdot \left(LSC(x,y)\right)^{\beta_1} \quad (3)$$

In which, the parameters α_1 and β_1 are respectively used to adjust the weights of *AF* and *LSC* sizes in *LMO*.

In conclusion, the fusion rule of the low frequency subband is as equation 4.

$$LF(x,y) = \begin{cases} C_A & if\ \lceil R_A(x,y)\rceil > \frac{\tilde{M}*\tilde{N}}{2} \\ C_B & otherwise \end{cases} \quad (4)$$

In which,

$R_A(x,y) = \{(x_0,y_0) \in \Omega_2 \mid LMO_A(x_0,y_0) \geq LMO_B(x_0,y_0)\}$

From the above, the fused low frequency subband $LF(x,y)$ is obtained. C_A and C_B represent the low frequency subband of image to be fused respectively, and Ω_2 represents the sliding window centered on *(x,y)* with a size of $\tilde{M}$*$\tilde{N}$. The values of $\tilde{M}$ and $\tilde{N}$ are 7 and 7 respectively [19].

3.2 Fusion rule of high frequency sub-image

The high frequency sub-image decomposed by NSCT mainly includes the detail information such as the contour structure and edge of image. This information is usually presented as the coefficients with large absolute value or large modulus, corresponding to the significant features in a certain direction interval, and they can well describe the structure information of image. The quality of extracting high frequency subband information directly affects the image fusion effect. To highlight the texture information of the high frequency subbands, local gradient energy (LGE) is introduced. The greater the local gradient energy, the more detailed information the image contains. By calculating the gray level changes at the position (x,y) of high frequency subband, the amount of its detailed information is reflected, that is as equation 5.

$$LGE(x,y) = \sum_{m,n\in S}|G(x+m,y+n)|^2 \quad (5)$$

Where, S is the window size *and its value is* 3 [19]. $G(x,y)$ is the gradient of pixel (x,y), $LGE(x,y)$ represents the local gradient energy of the high frequency subband at the position (x,y).

$G(x,y)$ is the first-order difference in the x and y directions, representing the transverse difference feature and the longitudinal difference feature respectively, and is defined as equation 6.

$$G(x,y) = |d(x,y) - d(x+1,y)| + |d(x,y) - d(x,y+1)| \quad (6)$$

Where, $d(x,y)$ is the coefficient of the high frequency sub*band at the position* (x,y).

Since LGE, as an estimator describing the detailed information of images, lacks the extraction and description of large-scale structural information such as contours, Edge Strength (ES) is introduced. By calculating the amplitude of the gradient of edge pixels in the high frequency subband, the layering of its structure and edge contour is highlighted, that is as equation (7).

$$ES(x,y) = sqrt\left(d_x(x,y)^2 + d_y(x,y)^2\right) \quad (7)$$

Where, $d_x = d * h_x$, $d_y = d * h_y$ respectively represent the convolution results of the high frequency subband pixel $d(x,y)$ with the Scharr operator [20] in the x and y directions.

$$h_x = \begin{bmatrix} -3 & 0 & 3 \\ -10 & 0 & 10 \\ -3 & 0 & 3 \end{bmatrix}, h_y = \begin{bmatrix} -3 & -10 & -3 \\ 0 & 0 & 0 \\ 3 & 10 & 3 \end{bmatrix}$$

represent the Scharr operators in the x and y directions respectively.

Thus, through the high-frequency measurement operator (*HMO*)

$$HMO(x,y) = LGE(x,y)^{\alpha_2} \cdot ES(x,y)^{\beta_2} \quad (8)$$

the high frequency subbands are fused. In (8), the parameters α_2 and β_2 are respectively used to adjust the weights *LGE* and *ES* in *HMO*.

By comparing the value of *HMO* in the high frequency subbands, the fusion rule of high frequency subbands is obtained as

$$HF^{j,k}(x,y) = \begin{cases} d_A^{j,k}(x,y) & if\ HMO_{d_A^{j,k}}(x,y) > HMO_{d_B^{j,k}}(x,y) \\ d_B^{j,k}(x,y) & otherwise \end{cases} \quad (9)$$

Where, $HF^{j,k}(x,y)$ is the fused image of the high frequency subband at scale j and direction k (horizontal, vertical or diagonal direction), $d_A^{j,k}(x,y)$ and $d_B^{j,k}(x,y)$ are the high frequency subbands corresponding to the scale j and direction k of the source images A and B respectively.

3.3 Overall framework of image fusion

According to the above method, the fusion framework based on NSCT is shown in Fig. 2.

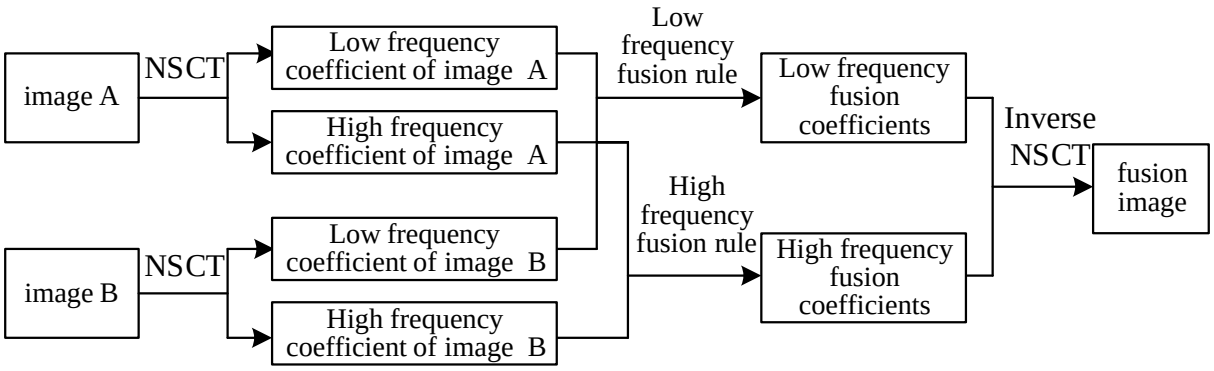


Fig. 2 Overall framework of image fusion

Firstly, the registered source image A and B are transformed by NSCT at level L respectively, here the value of L is set to 3 [16], then the low frequency subband coefficients $\{ C_{j0}^{A}(x,y),\ C_{j0}^{B}(x,y) \}$ and the high frequency subband coefficients$\{ d_{j,k}^{A}(x,y),\ d_{j,k}^{B}(x,y) \}$ $(\mathrm{j} \geq \mathrm{j}_0)$ are obtained. Furthermore, as activity reflects the energy changes in a local area, and the local sharpness change enhances the contrast variation of activity. Therefore, for the low frequency subband, the *LMO* rule based on the activity function with local sharpness change is adopted for fusion to obtain $LF(x,y)$. While local gradient energy represents the difference changes, and edge strength represents the weighted difference of large-scale structures, both of them reflect the amount of image details. In high frequency subband, the *HMO* rule based on local gradient energy with edge strength is adopted for fusion to obtain $HF^{j,k}(x,y)$. Finally, the high frequency coefficients and low frequency coefficients are reconstructed by NSCT inverse transform to get the fusion image.

4 Experimental results and analysis

The superiority of the method proposed in this paper is verified through experiments on self-built datasets. The test images included multi-focus Lena images, CT and MRI images, FA (Fluorescent Angiography) images and RF (Red-Free) images, etc., and were analyzed through visual and objective indicators. The experiment was conducted on CPU, with the code written in MATLAB, and the running time was within 2 seconds.

4.1 Objective evaluation indicators

This paper uses the commonly used measurement indicators to comprehensively and quantitatively evaluate the performance of different fusion methods, they are respectively [21]-[23]: peak signal to noise ratio (PSNR), structural similarity (SSIM), root mean square error (RMSE), Edge Information Retention (EIR), Information Entropy (IE). Among them, PSNR measures the similarity between the source image and the fused image by calculating the mean square error, the higher its value is, the smaller the distortion generated during the fusion process is, and the more similar the source image is to the fused image. SSIM measures the structural similarity between the source image and the fused image, the larger its value is, the more similar the source image is to the fused image. RMSE calculates the standard deviation between the fused image and the standard image, the smaller the value, the closer the fused image is to the standard image. EIR measures the retention of edge information and detailed textures of the source image, the higher the value, the more detailed and texture information the fused image contains, and the better the quality of

visual information obtained from the source image. IE reflects the information and clarity contained in the fused image, the higher its value, the more information and richer details the fused image contains, and the better the fusion performance.

4.2 Parameter setting

Adjusting one parameter is achieved by fixing other parameters and evaluating it from RMSE, SSIM, EIR, and IE to determine the optimal value of the parameter. Below, we take the image fusion of the left-focused Lena and right-focused Lena as an example to analyze the optimal parameters.

The measurement operator of high frequency subbands and low frequency subbands obtained by NSCT is used as the measurement method for the contour structure and edge texture information of the image, its parameter values directly affect the fusion quality and determine the effect of the final fused image. In order to determine the optimal values of the weight parameters in *HMO* and *LMO*, the weight parameters α_1 and β_1 in the LMO were analyzed first. The parameter β_1 was fixed as 1, and the value of parameter α_1 was set within the range of 0 to 0.01. The experimental results are shown in Table 1. It can be seen that: (1) with the increase of the parameter α_1, each evaluation index changes accordingly. When α_1=0.006, RMSE reaches the minimum value, SSIM, EIR and IE reach the maximum values, and the quality of the fused image improves well. Similarly, when α_1=0.006, adjust the value of the parameter β_1 to achieve the best fusion effect performance. Eventually, the values of α_1 and β_1 are 0.006 and 1.05 respectively. (2) The parameters α_2 and β_2 in *HMO* were analyzed. Through experiments, it was found that whether it was RMSE, SSIM, EIR or IE, the fused image was not greatly affected by the values of α_2 and β_2. Therefore, both α_2 and β_2 took the default value of 1.

Table 1: Comparison of multi-focus Lena fusion results at different values of α_1

α_1	RMSE	SSIM	EIR	IE
0.001	3.299	0.5124	0.685	7.795
0.002	3.298	0.5124	0.685	7.798
0.003	3.298	0.5125	0.687	7.803
0.004	3.297	0.5125	0.688	7.808
0.005	3.296	0.5125	0.688	7.811
0.006	**3.296**	**0.5126**	**0.689**	**7.812**
0.007	3.297	0.5126	0.688	7.810
0.008	3.297	0.5126	0.687	7.805
0.009	3.298	0.5126	0.685	7.802

Note: Bold indicates the optimal value

4.3 Frame structure experiment

Three representative multi-scale image fusion frameworks were applied to the multi-focus Lena image fusion, and the same fusion rules of high frequency and low frequency were adopted to conduct experiments on these three fusion frameworks and NSCT framework to prove the effectiveness of NSCT framework in this paper. These three multi-scale image fusion frameworks include the Pyramid Method (PM), Discrete Wavelet Transform (DWT), and Contourlet Transform (CT). The experimental results are shown in Figure 3, it can be seen from the local magnification of the cap edge at the lower right corner in Figure 3(c)- 3(f) that: Fig. 3(c) using the PM framework, the energy loss of the image is relatively large, which leads to a decrease in the contrast of the fused image and the appearance of slight artifacts at some contour edges. In Fig. 3(d) and Fig. 3(e), the DWT and CT frameworks are respectively applied, there are slight distortion and aberration at some edges. the fused images have some random noise, and the graininess in the detail areas is relatively strong. In Fig. 3(f), the NSCT framework is used. compared with the previous three multi-scale frameworks, both contrast and fidelity have been significantly improved, and the texture features of the source image have also been restored.

Table 2 shows the comparison of objective evaluation for multi-focus Lena image fusion under several multi-scale frameworks. It can be seen that compared with other multi-scale frameworks, the NSCT framework performs better in preserving edge details, as confirmed by PSNR, SSIM, RMSE, EIR and IE. Based on the authenticity of the texture features of the source image, the NSCT framework enhances the expression of texture features and details during the fusion process. This makes it particularly suitable for high-detail preservation applications, such as medical imaging etc.

(a) focus on the right (b) focus on the left

(c) PM (d) DWT

(e) CT (f) NSCT

Figure3: a-f Multi-focus Lena image fusion under several multi-scale frameworks

Table 2: Comparison of multi-focus Lena image fusion under several multi-scale frameworks

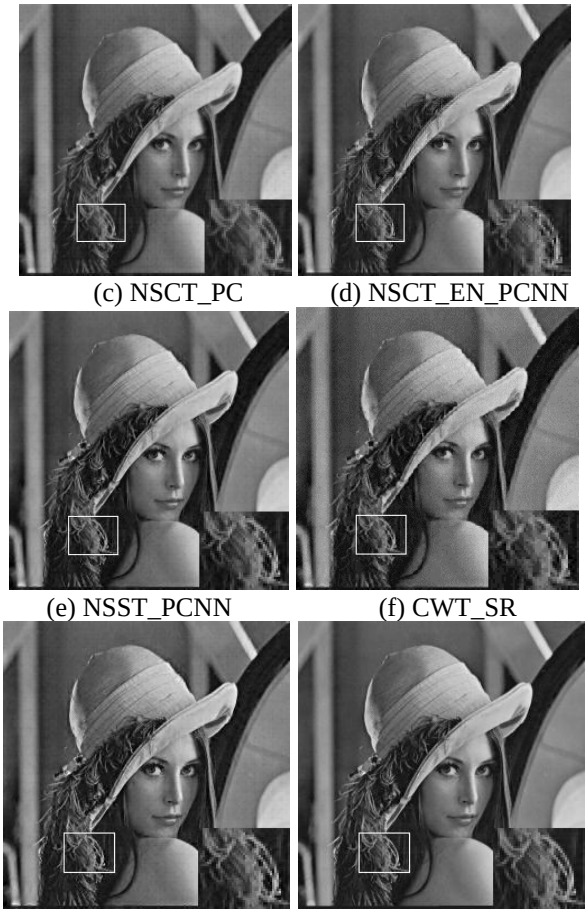
Framework	PSNR	SSIM	RMSE	EIR	IE
PM	10.277	0.5125	3.325	0.652	7.645
DWT	10.278	0.5125	3.310	0.661	7.765
CT	10.279	0.5124	3.309	0.668	7.775
NSCT	10.281	0.5126	3.305	0.674	7.789

4.4 Analysis of fusion results

To test the effectiveness of the algorithm proposed in this paper, it is compared with several frequency-domain image fusion methods proposed in recent years, including NSCT_PC [18], NSCT_EN_PCNN [17], NSST_PCNN [24], CWT_SR [11] and JBF [25]. NSCT_PC represents the fusion rule based on Phase Congruency (PC) and Laplace energy in the NSCT domain; NSCT_EN_PCNN represents the fusion rule based on the PCNN rule and image entropy in the NSCT domain; NSST_PCNN represents the fusion method based on the PCNN and energy strategy in the NSST domain; CWT_SR represents the fusion method based on sparse representation in the domain of complex wavelet transform; JBF represents a joint bilateral filtering fusion method based on enhancing edges and contrast.

Figure4 shows the artificial multi-focus Lena image fusion results of the method proposed in this paper and five representative frequency-domain fusion methods. It can be seen that in Fig. 4(c), Fig. 4(d), Fig. 4(e) and Fig. 4(f), a large amount of energy is lost during the fusion process, resulting in a decrease in the contrast of the fused image. It can be seen from the local magnification images that the fused image shows insufficient performance in the detail texture of the hair, and some even have distortion. In Fig. 4(g), the JBF method significantly improves the fusion effect. However, there are greater differences and not smooth in local changes, and some details have discontinuous edge points. Compared with the previous several methods, the image texture fused by the method in this paper is clearer and the image layering is stronger. Table 3 shows the objective evaluation comparison of multi-focus Lena image fusion by different methods. It can be seen that the value of RMSE by the proposed method is the smallest, that is to say, the fusion result obtained by the proposed method is the closest to the standard image. In addition, the proposed method also outperforms other methods in terms of PSNR, SSIM, EIR, and IE evaluation indicators, which indicates that the fusion effect of the proposed method outperforms that of other methods in terms of detail contour and pixel intensity. The experimental results show that the performance of the proposed method is better than that of other methods both in subjective analysis and objective indicators.

(a) focus on the right (b) focus on the left



(c) NSCT_PC (d) NSCT_EN_PCNN

(e) NSST_PCNN (f) CWT_SR

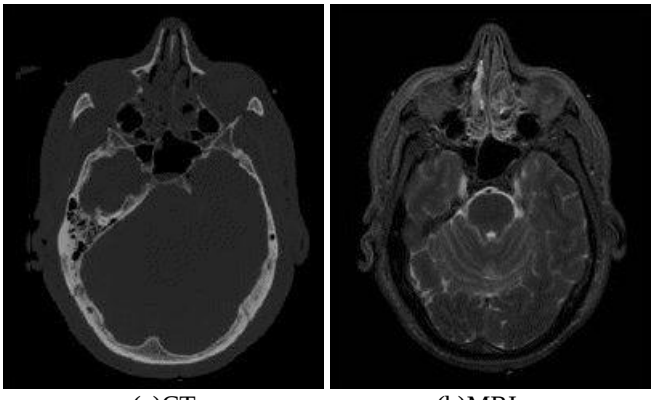
(g) JBF (h) the proposed method

Figure 4: a-h Fusion results of different methods for multi-focus Lena image

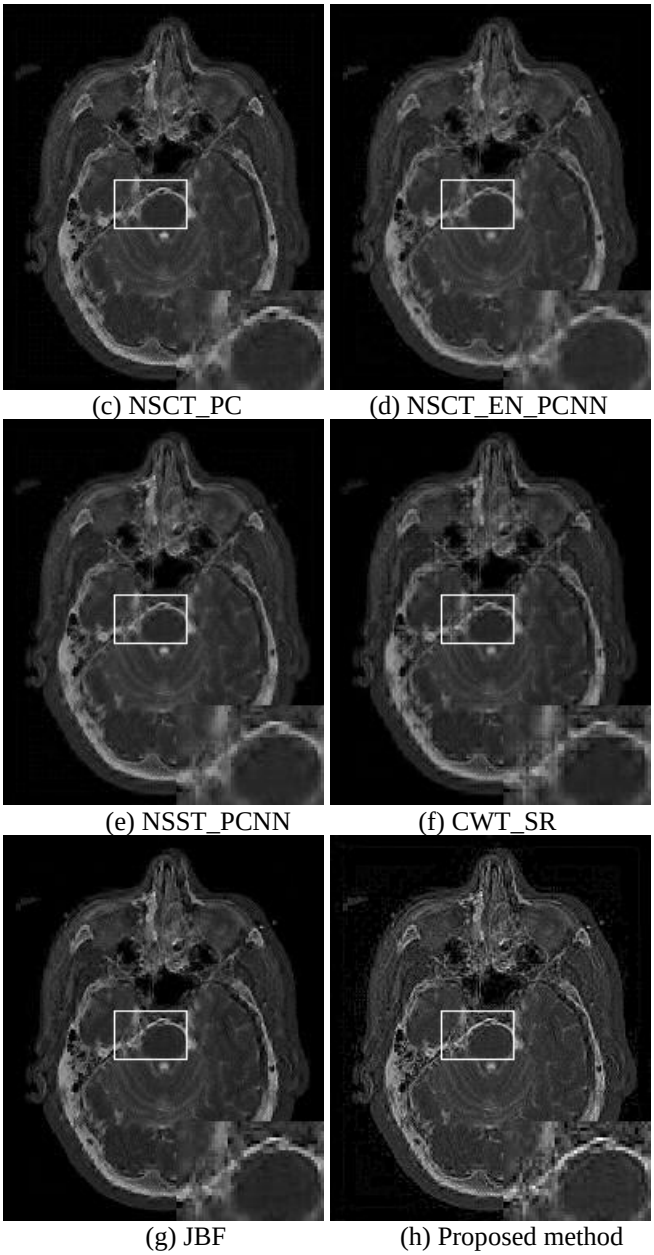
Table 3: Objective efficacy comparison of different methods for multi-focus Lena fusion results

Methods	PSNR	SSIM	RMSE	EIR	IE
NSCT_PC	10.276	0.5124	3.311	0.668	7.748
NSCT_EN_PCNN	10.277	0.5125	3.312	0.664	7.756
NSST_PCNN	10.278	0.5125	3.308	0.671	7.782
CWT_SR	10.278	0.5123	3.309	0.67	7.775
JBF	10.279	0.5125	3.308	0.672	7.785
Proposed method	10.281	0.5126	3.305	0.674	7.789

CT images focus on describing the contour features of bones, while MRI images focus on describing the detailed texture features of soft tissues. Figure 5 shows the fused images of brain CT images and MRI images obtained by different methods. It can be seen that in Fig. 5(c), 5(d), 5(e), and 5(f), the fused images show edge distortion or blurring in terms of brain fiber texture information. It can also be observed from the local magnified images that the fused images have edge artifacts and information loss, which seriously affects the accuracy of medical diagnosis. This situation is improved in Fig. 5(g), but it is still insufficient in the presentation of texture details. In Fig. 5(h), the detail texture of soft tissue structure in the fused image is clearer compared with the previous several methods, in the local magnified image, the gully texture has better contrast. Table 4 shows the objective evaluation comparison of CT/MRI image fusion by different methods. It can be seen that the method proposed in this paper has achieved considerable results in various indicators such as PSNR, SSIM, EIR, and IE, which indicates that the proposed method has better performance in aspects such as image feature transfer and texture detail expression. The experimental results show that in CT/MRI image fusion, the method proposed in this paper outperforms other methods in both subjective analysis and objective indicators.



(a)CT (b)MRI



(c) NSCT_PC (d) NSCT_EN_PCNN

(e) NSST_PCNN (f) CWT_SR

(g) JBF (h) Proposed method

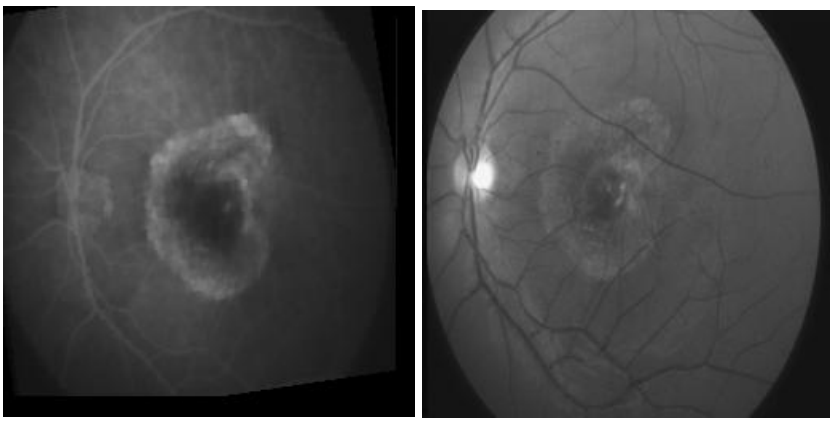
Figure 5: a-h Fusion results of different methods for CT image and MRI image

Table 4: Objective efficacy comparison of different methods for CT image and MRI image

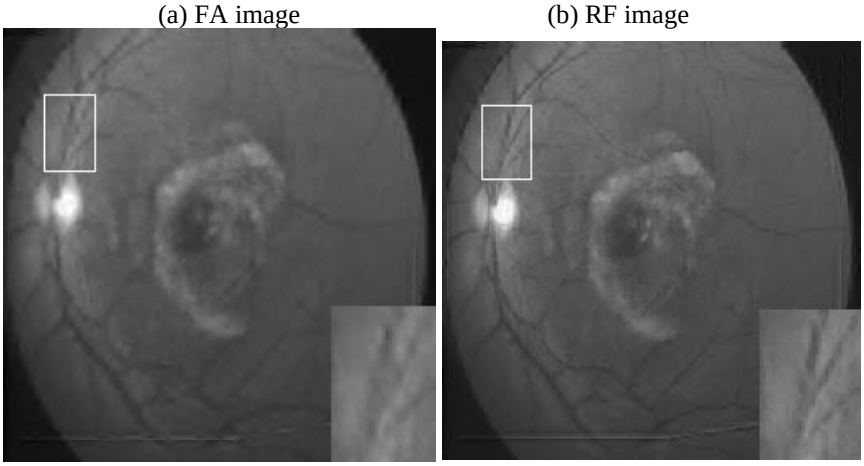
Methods	PSNR	SSIM	EIR	IE
NSCT_PC	9.847	0.5235	0.668	6.781
NSCT_EN_PCNN	9.826	0.5233	0.656	6.665
NSST_PCNN	9.845	0.5235	0.665	6.783
CWT_SR	9.839	0.5232	0.664	6.776
JBF	9.851	0.5237	0.673	6.826
Proposed method	9.856	0.5238	0.684	6.857

Retinal FA (Fluorescent Angiography) images are the images of retinal blood vessels obtained by injecting sodium fluorescein contrast agent, and RF (Red Free) i images are the images obtained by irradiating the retina with short-wavelength light. They play an important role in the diagnosis and monitoring of fundus diseases. Figure 6 and Figure7 show the fusion images of FA images and RF images obtained by different methods. It can be seen that the other methods have problems such as fuzzy pseudo-shadow and information loss in the soft tissues of the fundus vessels at different level, and even vascular edge distortion in the local magnified images, which is not beneficial to the accuracy of medical diagnosis. The method proposed in this paper, relatively speaking, provides a more accurate description of the FA/RF image and better preserves the small structure information of the vascular tissues. Tables 5 and Tables 6 show the objective

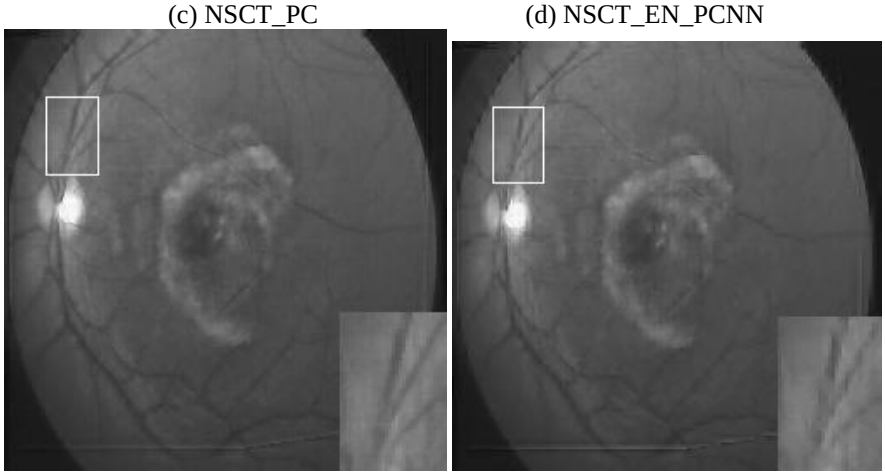
evaluation comparison of FA/RF image fusion by different methods. It can be seen that the method proposed in this paper has obvious advantages in PSNR, SSIM, EIR, and IE indicators, which indicates that the proposed method has greatly improved the expression of the detailed texture of fundus vascular tissue in FA and RF images and enhanced the contrast of the fused images. It is convenient to observe the diseased region of the patient. The experimental results show that the proposed method outperforms the other methods in both subjective analysis and objective evaluation in FA/RF image fusion.



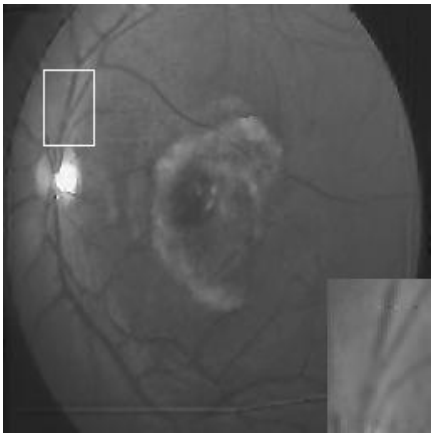
(a) FA image (b) RF image



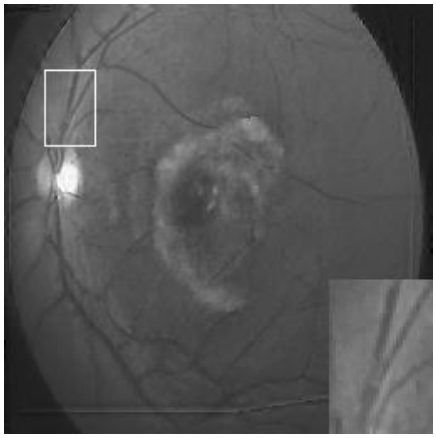
(c) NSCT_PC (d) NSCT_EN_PCNN



(e) NSST_PCNN (f) CWT_SR



(g) JBF

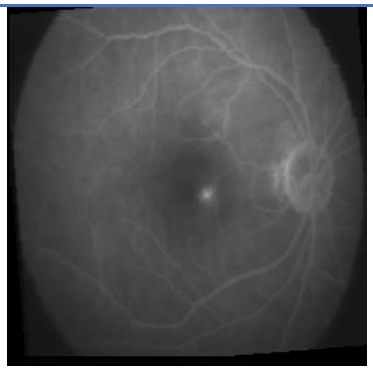


(h) Proposed method

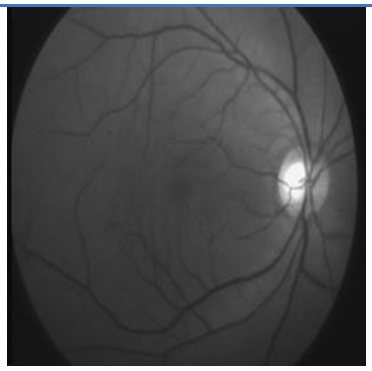
Figure 6: a-h Fusion results of different methods for FA image and RF image

Table 5: Objective efficacy comparison of different methods for FA image and RF image

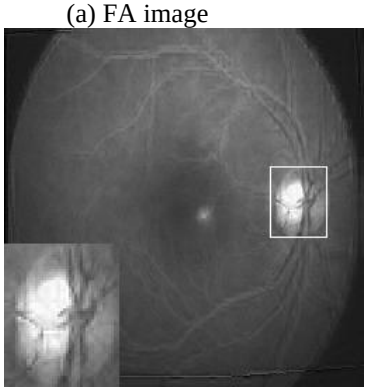
Methods	PSNR	SSIM	EIR	IE
NSCT_PC	8.547	0.5051	0.486	6.588
NSCT_EN_PCNN	8.604	0.5053	0.531	6.604
NSST_PCNN	8.635	0.5054	0.549	6.628
CWT_SR	8.578	0.5052	0.536	6.606
JBF	8.642	0.5054	0.558	6.725
Proposed method	8.673	0.5055	0.612	6.817



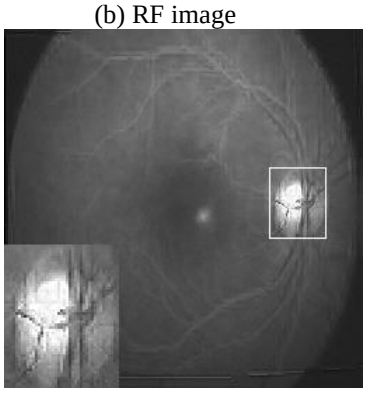
(a) FA image



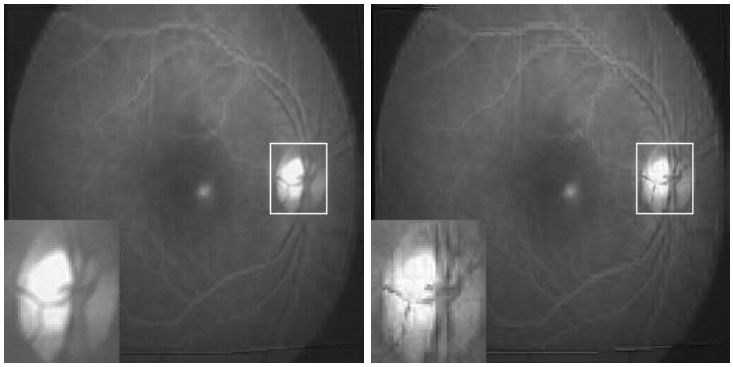
(b) RF image



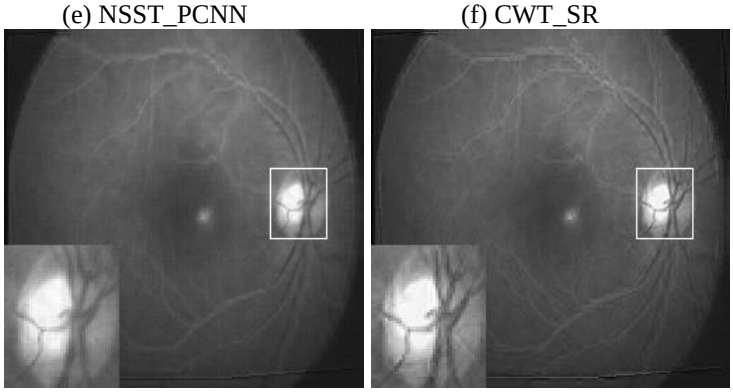
(c) NSCT_PC



(d) NSCT_EN_PCNN



(e) NSST_PCNN (f) CWT_SR



(g) JBF (h) Proposed method

Figure 7: a-h Fusion results of different methods for FA image and RF image

Table 6: Objective efficacy comparison of different methods for FA image and RF image

Methods	PSNR	SSIM	EIR	IE
NSCT_PC	8.512	0.5053	0.529	6.758
NSCT_EN_PCNN	8.535	0.5044	0.539	6.789
NSST_PCNN	8.557	0.5045	0.541	6.791
CWT_SR	8.525	0.5054	0.534	6.783
JBF	8.564	0.5045	0.546	6.788
Proposed method	8.582	0.5046	0.572	6.804

As mentioned above, the fusion effect of the method proposed in this paper is better than the five popular image fusion methods and three image fusion frameworks in the field of frequency domain in recent years, and it achieves better visual effects, thereby ensuring the reliability of subsequent processing.

5 Conclusion

A new image fusion method based on NSCT is presented. Firstly, the fusion rule scheme of source image decomposed by NSCT is constructed, the low frequency fusion rule is based on activity with local sharpness changes, and the high frequency fusion rule is based on local gradient energy with edge strength. In this paper, artificial multi-focus images, brain CT and MRI images, FA image and RF image are tested. The results show that the presented method has excellent fusion property for multi-focus and multimodal image fusion.

Acknowledgements

The authors would like to thank Weifang University teaching reform research project (No.2023YB003, No. 2024YB034), Weifang Science and Technology Development Project (2025GX016) for financially supporting this research.

References

[1] Karim S, Tong J, Li J, et al. Current advances and futur e perspectives of image fusion: A comprehensive revie w. Information Fusion, 90: 185-217, 2023. https://doi.or g/10.1016/j.inffus.2022.09.019.

[2] Singh S, Singh H, Bueno G, et al. A review of image fu sion: Methods, application s and performance metrics. Digital Signal Processing, 137: 104020, 2023. https://do i.org/10.1016/j.dsp.2023.104020.

[3] Azam M A, Khan K B., Salahuddin S, et al. A review on multimodal medical image fusion: Compendious analysis of medical modalities, multimodal databases, fusion techniques and quality metrics. Computer in Biology and Medicine, 144: 105253, 2022. https://doi.org/10.1016/j.compbiomed.2022.105253.

[4] Hermessi H, Mourali O, Zagrouba E. Multimodal medical image fusion review: Theoretical background and recent advances. Signal Processing, 2021, 183: 1-27. https://doi.org/10.1016/j.sigpro.2021.108036.

[5] Zhang W, Jiao L, Liu. F. Adaptive contourlet fusion clustering for SAR image change detection. IEEE

Transactions on Image Processing, 31: 2295-2308, 2022. https://doi.org/10.1109/TIP.2022.3154922.
[6] Li X T, Guo H Y. Fusion of deep convolutional neural networks and brain visual cognition for enhanced image classification. Informatica, 49(16): 37-52, 2025. http://dx.doi.org/10.31449/inf.v49i16.7787.
[7] Li H F, He X G, Tao D P, et al. Joint medical image fusion, denoising and enhancement via discriminative low-rank sparse dictionaries learning. Pattern Recognition, 79: 130-146, 2018. https://doi.org/10.1016/j.patcog.2018.02.005.
[8] Toet A. Image fusion by a ratio of low-pass pyramid. Pattern Recognition Letters, 9(4): 245-253, 1989. https://doi.org/10.1016/0167-8655(89)90003-2.
[9] Pu T, Ni G Q. Contrast-based image fusion using the discrete wavelet transform. Optical Engineering, 39(8): 2075- 2082, 2000. http://dx.doi.org/10.1117/1.1303728.
[10] Cunha A. L, Zhou J P. The non-subsampled contourlet transform: theory, design, and applications. IEEE Transactions on Image Processing, 15(10): 3089- 3101, 2006. https://doi.org/10.1109/TIP.2006.877507.
[11] Liu Y, Liu S P, Wang Z F. A general framework for image fusion based on multi-scale transform and sparse representation. Information Fusion, 24: 147-164, 2015. https://doi.org/10.1016/j.inffus.2014.09.004.
[12] Qu X, Yan J, Yang G. Multifocus image fusion method of sharp frequency localized contourlet transform domain based on sum-modified-laplacia. Optics and Precision Engineering, 17(5): 1203-1211, 2009.
[13] Do M N, Vetterli M. The contourlet transform: an efficient directional multiresolution image representation. IEEE Transaction on Image Processing, 14(12): 2091-2106, 2005. https://doi.org/10.1109/TIP.2005.859376.
[14] Tawfik N, Elnemr H A, Fakhr M, et al. Survey study of multimodality medical image fusion methods. Multimedia Tools and Applications, 80: 6369-6396, 2020. https://doi.org/10.1007/s11042-020-08834-5.
[15] Ramlal S D, Sachdeva J, Ahuja C K, et al. Multimodal medical image fusion using non-subsampled shearlet transform and pulse coupled neural network incorporated with morphological gradient. Signal. Image and Video Processing, 12: 1479-1487, 2018. https://doi.org/10.1109/TIM.2018.2838778.
[16] Ramlal S D, Sachdeva J, Ahuja C K. Khandelwal N. An improved multimodal medical image fusion scheme based on hybrid combination of nonsubsampled contourlet transform and stationary wavelet transform. International Journal of Imaging Systems and Technology, 29(2): 146-160, 2019. https://doi.org/10.1002/ima.22310.
[17] Guo W. Research on medical image fusion algorithm based on nsct and neural network. Lanzhou Jiaotong University, 2024.
[18] Zhu Z, Zheng M, Qi G, et al. A phase congruency and local laplacian energy-based multimodality medical image fusion method in NSCT domain. IEEE Access, 7: 20811-20824, 2019. https://doi.org/10.1109/ACCESS.2019.2898111.
[19] Zhu J, Liu H, Li S, et al. Two-Channel medical image fusion combining local entropy and gradient energy. Journal of Computer-Aided Design & Computer Graphics, 36(6): 857-874, 2024. https://dx.doi.org/10.3724/SP.J.1089.2024.19899.
[20] Liu X, Lin Y Z. Comparative study of multiple image edge detection operators applied to size measurement of passiflora edulia sims. Chinese Journal of Tropical Crops, 43(12): 2554-2563, 2022. https://doi.org/10.3969/j.issn.1000-2561.2022.12.018.
[21] Zhu Y. No-reference image quality assessment based on statistical information. Huaqiao University, 2021.
[22] Liu Y. No-reference evaluation of visible and infrared fusion image sharpness. China University of Petroleum, 2020.
[23] Xydeas C S, Petrovic V. Objective image fusion performance measure. Electronics Letters, 36(4): 308-309, 2000. http://dx.doi.org/10.1049/el:20000267.
[24] Tan W, Zhang J J, Xiang P, et al. Infrared and visible image fusion via NSST and PCNN in multiscale morphological gradient domain. Proceedings of the SPIE 11353, Optics, Photonics and Digital Technologies for Imaging Applications VI. 113531E, 2020. https://doi.org/10.1117/12.2551830.
[25] Li X S, Zhou F Q, Tan H S, et al. Multimodal medical image fusion based on joint bilateral filter and local gradient energy. Information Sciences, 569: 302-325, 2021. https://doi.org/10.1016/j.ins.2021.04.052.

Ensemble-Based Machine Learning Algorithm for Intelligent Network Security Threat Detection

Ye Chunsheng[1*], Miaomiao Fan[2]
[1]School of Water Resources and Transportation,Zhengzhou University; ZhengZhou , 450000, China
[2]Zibo Vocational Institute, Zibo, Shandong, 255300, China
E-mail: yecs_2025@163.com
[*]Corresponding author

Keywords: classification, feature selection, normalization, network security threats, threat detector

Received: July 11, 2024

The rapid development of cyber threats in the cybersecurity field necessitates advanced strategies for prompt identification and reduction. Conventional approaches frequently struggle to adapt to the complexity of contemporary attacks, emphasizing the requirement for creative approaches utilizing machine learning. This paper creates and assesses the "IntelliGuard Threat Detector" algorithm, developed to independently identify and classify a variety of network security risks employing the CICIDS 2017 dataset. By utilizing advanced machine learning methods, the algorithm aims to enhance accuracy and effectiveness in locating abnormal behaviors suggestive of possible security violations. Present methods for network security usually depend on personal intervention and pre-established guidelines, which may not sufficiently handle the ever-changing nature of cyber threats. The "IntelliGuard Threat Detector" algorithm incorporates robust scaler normalization, Composite Rank Ensemble (CORE) feature selection, and a TrioBoost classifier model to boost predictive accuracy and robustness. The proposed IntelliGuard Threat Detector algorithm attains 94% accuracy, 92% precision, 95% recall, 94% F1-score, and 93% geometric mean, surpassing conventional techniques by up to 6% in accuracy, 8% in precision, 5% in recall, 7% in F1-score, and 7% in geometric mean, respectively. This algorithm provides a proactive and scalable approach for network security threat discovery, signifying a noteworthy development in the area of cybersecurity.

Povzetek: Algoritem IntelliGuard Threat Detector uporablja normalizacijo Robust Scaler, izbor značilk Composite Rank Ensemble (CORE) in ansambelski klasifikator TrioBoost (Decision Stump + Logistic Regression + SVM) za samodejno zaznavanje omrežnih groženj; na podatkovni zbirki CICIDS 2017 doseže dobre rezultate.

1 Introduction

The rapid evolution of cyber threats has drastically changed the cybersecurity landscape over the last few years [1]. These threats comprise a wide range of malevolent actions, from comparatively easy malware attacks that can affect individual systems and steal personal data, to modern advanced persistent threats (APTs) coordinated by incredibly talented and well-funded opponents [2]. APTs frequently entail protracted and focused campaigns intended to penetrate the defenses of particular nations or groups to pilfer confidential information, disrupt processes, or obtain illegal entry to vital infrastructure. These dangers are becoming increasingly complex due to their ability to circumvent conventional safety procedures, exploit zero-day vulnerabilities, and employ metamorphic and polymorphic approaches to alter their routines and signatures.

In addition, the number of cyberattacks has increased, with daily updates on ransomware events, phishing tactics, and data breaches impacting the public and private sectors globally [3]. The interconnectedness of contemporary digital ecosystems increases the potential harm of these threats, as a violation in one system can quickly spread to others, resulting in considerable disruption and monetary loss. This growing threat environment highlights the shortcomings of traditional cybersecurity approaches that depend mostly on personal supervision and static protections.

Thus, the critical requirement for more advanced and flexible cybersecurity measures has become evident.

These measures must be able to foresee, identify, and mitigate hazards instantly, adjusting to novel types of attack, and offering complete defense across diverse networked systems. The creation of such advanced defenses is crucial to the protection of not only personal and corporate resources but also national security concerns in a digital society.

Conventional cybersecurity methods frequently depend on signature-based discovery, manual interventions, and rule-based systems. While these techniques have been efficient to some extent, they have numerous drawbacks. Signature-based discovery fails to detect new attacks since it could solely discover recognized attack patterns [4]. Manual interventions, though occasionally essential, are prone to human error and take more time, restricting the receptiveness and scalability of attack discovery. Rule-based systems need constant maintenance and updating, making them incompetent against quickly altering threat settings [5]. To tackle these problems, this paper proposes the "IntelliGuard Threat Detector" algorithm. This new technique uses advanced machine learning methods to independently discover and classify network security attacks. The algorithm uses the CICIDS 2017 dataset, a benchmark for assessing intrusion detection systems, and incorporates numerous important mechanisms to improve its effectiveness. These mechanisms comprise robust scaler normalization to standardize numerical features, Composite Rank Ensemble (CORE) feature selection to prioritize the most indicative features of security attacks, and a TrioBoost classifier model to enhance predictive accuracy and sturdiness.

The main contributions of this paper are as follows:

1. Implementation of the "IntelliGuard Threat Detector" algorithm for independent threat identification and classification.

2. Assessment of the algorithm's effectiveness utilizing the CICIDS 2017 dataset, shows its high accuracy, precision, recall, F1-score, and geometric mean in detecting network security hazards.

This paper aims to increase the effectiveness of threat detection systems by offering a strong machine learning-based remedy capable of adjusting to changing cyber threats. The "IntelliGuard Threat Detector" algorithm is implemented for application across a range of fields, including national defense systems, vital infrastructure security, and enterprise network security.

The rest of this paper is structured as follows: Section 2 provides an overview of previous research conducted in the areas of network security and threat identification using machine learning techniques. Section 3 details the methodology of the "IntelliGuard Threat Detector" algorithm. Section 4 outlines the experimental setup and evaluation metrics used in this paper, as well as the algorithm's outcomes and performance examination. Finally, Section 5 concludes the paper with recommendations for future research directions.

2 Related works

In the swiftly expanding domain of cybersecurity, various research has examined different methodologies for threat identification and reduction. This section reviews notable contributions from recent literature, emphasizing present methodologies and their restrictions. By analyzing these works, existing gaps in research can be recognized, which the "IntelliGuard Threat Detector" algorithm aims to tackle.

Bouchama et al. [6] suggested improving cyber threat discovery by utilizing behavioral modeling of network traffic patterns using machine learning. The authors explored fundamental methodologies such as neural networks, support vector machines, and random forests, emphasizing their proficiency in modeling multifaceted traffic patterns. Their methodology assesses discovery rate, false positives, accuracy, precision, recall, and F1-score, demonstrating substantial advancements compared to traditional approaches.

Sarker et al. [7] suggested "IntrudTree," an intrusion detection approach that utilizes machine learning techniques intended to improve cyber security by ranking and choosing the most crucial security features. This model builds an intrusion detection system that uses a tree-based approach utilizing the chosen features, striving to enhance prediction accuracy and decrease computational difficulty. The efficiency of the IntrudTree model was validated through research on cybersecurity datasets, with performance metrics like precision, recall, F1-score, accuracy, and ROC values, and compared to conventional machine learning approaches such as Naive Bayes, logistic regression, support vector machines, and k-nearest neighbor.

Ferrag et al. [8] provide a comprehensive assessment of intrusion detection systems specifically designed for Agriculture 4.0. They analyze cybersecurity risks and the metrics employed to assess the effectiveness of these systems. The authors categorize intrusion detection systems according to new technologies, including cloud computing, fog/edge computing, network virtualization, autonomous tractors, drones, IoT, the agricultural industry, and smart grids. The authors also examined public datasets and execution frameworks for assessing the performance of these systems. They concluded by highlighting the problems

and potential research areas in cyber security for Agriculture 4.0.

Bertoli et al. [9] suggested the AB-TRAP framework for a network intrusion detection system that utilizes machine learning algorithms that tackle the out-of-date nature of existing datasets and practical considerations for implementation in real-world scenarios. The five-step AB-TRAP process consists of creating attack and legitimate datasets, training machine learning techniques, putting these models into practice, and assessing the models' performance after deployment. The framework was evaluated in both local and global environments to identify TCP port scanning attacks. The results showed that it achieved high accuracy and used low resources, making it a reliable and efficient solution for addressing contemporary network security concerns.

Saheed et al. [10] introduced a machine learning-based intrusion detection system (IDS) specifically designed for IoT contexts. The authors emphasize the increasing security hazards associated with the rapid expansion of IoT devices, as well as the urgent need for strong intrusion detection techniques. The research aims to utilize supervised machine learning techniques to identify different forms of assault in IoT networks. The author's methodology involves performing preprocessing stages on the UNSW-NB15 dataset, which includes feature scaling using min-max normalization. This is followed by dimensionality reduction utilizing principal component analysis (PCA). The authors assessed the efficacy of six machine learning techniques for identifying attacks, achieving comparable effectiveness in terms of accuracy and other evaluation metrics when compared to current methods. This highlights the importance of the author's methodology in tackling crucial security issues in IoT ecosystems.

Sarhan et al. [11] highlight IoT Network Intrusion Detection Systems (NIDS) flaws, discussing regular security breaches and data losses. Their study uses unique feature reduction (FR) and machine learning (ML) methods to improve NIDS technologies for broad applicability across heterogeneous datasets with different features and attack kinds. They evaluate six ML models (Deep Feed Forward, CNN, RNN, DT, LR, and NB) and three feature extraction methods (PCA, auto-encoder, and LDA) on benchmark datasets (UNSW-NB15, ToN-IoT, and CSE-CIC-IDS2018) and discover no single technique is more effective, emphasizing the importance of dataset selection. Standardized benchmark feature sets are recommended for future research on this important topic.

IoT devices come in many different types, which can be dangerous for security. Islam et al. [12] talk about these problems and suggest using machine learning-based intrusion detection systems (IDS) instead of the current methods. Strecker et al. [13] examine the effectiveness of three machine learning techniques—random forest (RF), support vector machine (SVM), and K-nearest neighbor (KNN)—in detecting malware and intrusions in IoT environments. For their investigation, they used the Aposemat IoT-23 dataset. They conclude that all three algorithms show promise for solving current IoT cybersecurity issues.

Lin et al. [14] presented an ensemble learning technique to threat classification in network intrusion detection that was particularly designed for a security monitoring system in renewable energy infrastructure. The technique employs numerous classifiers to enhance the accuracy and dependability of discovering different network attacks, tackling the distinct security difficulties presented by renewable energy systems.

Atul et al. [15] suggest an energy-aware smart home (EASH) framework that utilizes machine learning (ML) to increase the security of cyber-physical systems (CPS). The architecture specifically aims to improve intrusion detection accuracy by detecting anomalies and ensuring reliable communication.

These existing efforts in the field of cybersecurity have made substantial progress in tackling diverse risks, although there are still some areas that need to be addressed. Although the current detection systems are somewhat effective, they have challenges in identifying emerging and changing cybersecurity threats, keeping defenses up to speed, and reducing false alarms. These constraints impede their ability to quickly adjust to evolving threat environments.

The suggested method, called “IntelliGuard Threat Detector,” aims to address these shortcomings by utilizing advanced machine learning techniques. The algorithm utilizes advanced techniques such as data normalization, feature selection, and ensemble learning to improve accuracy, precision, recall, F1-score, and geometric mean in detecting abnormal behaviors that may indicate security breaches. This method allows for proactive and scalable identification of potential dangers, with the ability to adjust to new threats and reduce the occurrence of incorrect alerts. As a result, it provides a more efficient solution for addressing contemporary cybersecurity issues.

Table 1 contains a summary table outlining the findings of the reviewed works, comprising important metrics like accuracy, dataset utilized, and techniques utilized. This table helps readers rapidly contrast these techniques.

Table 1: Summary table

Study	Key Techniques	Dataset Used	Accuracy	Other Key Metrics	Identified Gaps
Bouchama et al. [6]	Neural Networks, SVM, Random Forest	Custom network traffic	High	Precision, Recall, F1-score	Constrained concentration on new attacks, moderate flexibility
Sarker et al. [7]	Tree-based methodology, Feature Selection	Cybersecurity datasets	High	Precision, Recall, F1-score, ROC	Computational intricacy, the requirement for decreased false positives
Ferrag et al. [8]	IDS for Agriculture 4.0, Cloud, IoT, Smart Grids	Public datasets	High	Evaluation of intrusion detection in Agriculture 4.0	Insufficient concentration on general cybersecurity, difficulties with outdated datasets
Bertoli et al. [9]	AB-TRAP framework, Machine Learning	TCP port scanning data	High	Resource efficiency, Practical challenges	Dataset aging and practical execution difficulties
Saheed et al. [10]	Supervised ML, PCA, Feature Scaling	UNSW-NB15	Similar to current methods	Accuracy, Precision, Recall, F1-score	Concentrate on IoT, the requirement to effectively handle new threats, minimal enhancement over previous techniques
Sarhan et al. [11]	Feature Reduction, ML (Deep Feed Forward, CNN, RNN)	UNSW-NB15, ToN-IoT, CSE-CIC-IDS2018	Varies	Feature selection impact, Dataset adaptability	There is no single better technique; it is important to choose suitable datasets
Islam et al. [12]	ML-based IDS (RF, SVM, KNN)	Aposemat IoT-23	High	Malware detection, Intrusion detection	Dataset-specific outcomes, difficulties in generalizing across IoT settings
Strecker et al. [13]	Random Forest, SVM, KNN	Aposemat IoT-23	High	Intrusion Detection, Malware Detection	Constrained generalization to larger IoT cybersecurity problems
Lin et al. [14]	Ensemble learning merging numerous classifiers	Custom dataset from renewable energy security monitoring system	High	Precision, Recall, F1-score	Restricted applicability to non-renewable energy settings; possible computational overhead in real-time applications
Atul et al. [15]	EASH framework, ML for CPS	Smart home data	High	Anomaly detection, Reliable communication	Concentrate on energy savings and generalization to other CPS settings

The reviewed techniques show substantial improvements in several facets of cybersecurity, including intrusion detection, feature selection, and resource effectiveness. However, previous techniques have significant shortcomings:

- **False positives:** Numerous techniques fail to balance detection rates with false positives, resulting in unneeded alerts that burden security teams.
- **Adaptability:** Many models are restricted by their dataset-specific nature, decreasing their efficacy in dynamic and changing threat settings.

- **Computational overhead:** A few techniques, while precise, impose significant computational requirements, rendering them unsuitable for real-time or resource-constrained settings.

The suggested "IntelliGuard Threat Detector" algorithm seeks to fill these gaps by:

- **Decreasing false positives:** Using advanced feature selection and ensemble learning methods to improve precision and recall, thereby reducing false alarms.

- **Enhancing adaptability:** Using a mixture of machine learning methods that are more responsive to new attacks and adaptable to different datasets.

- **Minimizing computational overhead:** Including effective data normalization and feature selection procedures to keep the algorithm scalable and appropriate for real-time applications.

This technique provides a more efficient and proactive solution for contemporary cybersecurity difficulties, establishing IntelliGuard as an important advancement over present SOTA techniques.

3 Methodology

"IntelliGuard Threat Detector" is a new algorithm that uses advanced machine learning techniques to improve the identification and categorization of network security threats. Given the ever-changing nature of cybersecurity threats, conventional approaches frequently prove inadequate for accurately detecting and addressing intricate and constantly changing vulnerabilities. The "IntelliGuard Threat Detector" algorithm tackles these problems by utilizing advanced algorithms and systematic techniques specifically designed for autonomous threat detection. Algorithm 1 presents the "IntelliGuard Threat Detector" algorithm.

Algorithm 1: IntelliGuard Threat Detector

Input : CICIDS 2017 dataset

Output : Class labels (threat or non-threat) predicted for network instances

Step 1 : **Preprocess Dataset:**

- Use a robust scaler normalization technique to normalize numerical features.
- Choose pertinent features utilizing Composite Rank Ensemble (CORE) feature selection with the target feature.

Step 2 : **Split Dataset:**

- Split the preprocessed dataset into Training (70%) and Testing (30%) sets.

Step 3 : **Initialize TrioBoost Classifier with three weak learners:**

- **Decision Stump:** A simple decision tree having just one split.
- **Logistic Regression:** Binary classification using a linear model.
- **Support Vector Machine (SVM):** Classifier using hyperplanes to separate data.

Step 4 : **Train Weak Learners:**

- For each weak learner:
  - Utilizing the Training dataset, train the model.

Step 5 : **Boosting Iterations:**

- Execute boosting iterations (e.g., 50):
  - Train the AdaBoost classifier on the Training set for each iteration.
  - To concentrate on cases that are more difficult to classify, adjust the weights of cases that were misclassified.

Step 6 : **Predictions:**

- Make predictions for the Testing set with the AdaBoost classifier that has been trained.

Step 7 : **Output:**

- Return the predicted class labels for network instances using the TrioBoost model.

At first, the CICIDS 2017 dataset is preprocessed using robust scaler normalization and feature selection based on the Composite Rank Ensemble (CORE) method. This guarantees that the data is of high quality and relevant for further analysis. We then employ a TrioBoost classifier to capture various facets of network behavior. A TrioBoost classifier is an ensemble learning technique that combines various weak learners, like decision stumps, logistic regression, and support vector machines, in a sequential manner for instance-based learning. The AdaBoost classifier is used to iteratively correct errors resulting from weak learners, thereby enhancing predictive accuracy and building an effective model capable of accurate predictions.

Particular hyperparameters were carefully chosen during model training to enhance efficiency: a learning rate of 0.1 and 500 iterations were used in the AdaBoost classifier to correct errors made by weak learners, improving predictive accuracy and constructing an effective model. Figure 1 displays the flow diagram of the IntelliGuard Threat Detector algorithm.

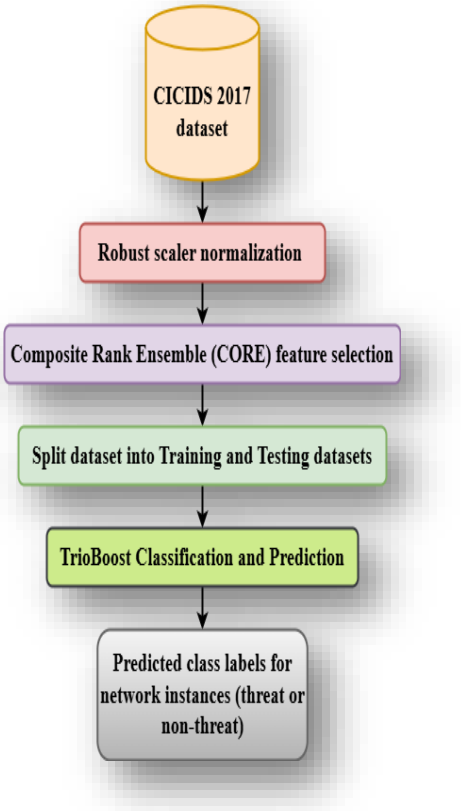


Figure 1: Flow diagram of intelliguard threat detector algorithm

3.1 Robust scaler normalization

Robust scaler normalization is a data preprocessing approach that rescales numerical features to a standardized range, while also minimizing the impact of outliers. Outliers can significantly influence standard scaling techniques, reducing their effectiveness. However, in cases where the dataset contains outliers, this specific approach can be very useful. The robust scaler accomplishes its robustness by utilizing statistical measures that are less affected by outliers, particularly the median and the interquartile range (IQR).

To comprehend the functioning of robust scaler normalization, let us designate a feature P that necessitates normalizing. The procedure consists of two primary stages: centering and scaling.

1. Centering:

Robust scaler centers the data by subtracting the median $\hat{p}$ of the feature P:

$$P_{centered} = P - \hat{p} \quad (1)$$

where $\hat{p}$ is the median of P.

2. Scaling:

After centering, the data is scaled by dividing by the interquartile range (IQR) of P. The IQR is calculated as the difference between the 75th and the 25th percentiles of P:

$$IQR = Q_3(P) - Q_1(P) \quad (2)$$

where $Q_1(P)$ and $Q_3(P)$ are the 25th and 75th percentiles of P, respectively.

The scaled feature P_{scaled} is then calculated as:

$$P_{scaled} = \frac{P_{centered}}{IQR} \quad (3)$$

This normalization procedure guarantees that the distribution of P_{scaled} has a median of 0 and a unit interquartile range. Therefore, the robust scaler

mitigates the impact of outliers by utilizing the median for centering and the interquartile range (IQR) for scaling. This makes it appropriate for datasets including outliers that could otherwise affect typical scaling strategies such as Min-Max scaling or z-score normalization.

3.2 Composite rank ensemble (CORE) feature selection

The Composite Rank Ensemble (CORE) feature selection approach is specifically developed to effectively identify the most influential attributes for predictive modeling by utilizing a combination of filter and wrapper techniques. The method is comprised of two primary phases: the Filter Phase and the Wrapper Phase.

3.2.1 Filter phase

During the Filter Phase, the algorithm employs various filter techniques to individually assess the importance of features and assign them a ranking. This step includes the following:

1. Apply filter methods:

- **Mutual information:** Compute the mutual information score *I(A; B)* for each feature *A* concerning the target variable *B*. This score gauges the volume of data acquired about *B* through *A*.

$$I(A;\ B) = \sum_{a\in A}\sum_{b\in B} p(a,b)log\left(\frac{p(a,b)}{p(a)p(b)}\right) \quad (4)$$

- **Chi-Square**: Compute the Chi-Square statistic X^2 for each feature, which evaluates the independence of the feature with the target variable.

$$X^2 = \sum \frac{(O_f - E_f)^2}{E_f} \quad (5)$$

where O_f is the observed frequency and E_f is the expected frequency.

- **ANOVA F-test:** Execute an ANOVA F-test to evaluate the variance between feature subsets and the target variable.

$$F = \frac{\text{variance between subsets}}{\text{variance within subsets}} \quad (6)$$

Each approach produces a score for each attribute, indicating its significance concerning the target feature.

2. Aggregate rankings:

After scoring the features with each filter method, the rankings are combined utilizing a majority voting method to generate a composite rank for each feature. This involves:

- Ranking features individually using the scores from Mutual Information, Chi-Square, and ANOVA F-test.
- Consolidating these rankings by assigning ranks through majority voting. The final rank of each attribute is decided by the rank it obtained most frequently among the three methods.

$$Rank_{Final}(P_i) = Majority\_vote(Rank_{MI}(P_i),\ Rank_{Chi2}(P_i) \quad (7)$$

This phase guarantees that the composite ranking accurately represents a consensus derived from several filter views, hence improving the reliability of feature selection.

3.2.2 Wrapper phase

The Wrapper Phase enhances the feature subset by assessing their performance using specialized models. This phase involves:

❖ **Select Top-Ranked Features:**

The attributes that are scored highest in the composite rankings from the filter phase are chosen for additional evaluation. Let *n* be the number of top features selected.

$$\{P_1, P_2, \dots, P_n\} \quad (8)$$

❖ **Apply RFE with Different Models:**

The Recursive Feature Elimination (RFE) technique is utilized with several models to systematically delete features that are deemed less significant. The models used include:

- ❖ **Logistic regression:** A linear model that makes use of a logistic function to estimate probabilities.
- ❖ **Decision tree:** A non-linear model that divides data according to feature values.
- ❖ **K-Nearest neighbors (KNN):** a non-parametric technique that classifies samples according to the neighbors' majority vote.

For each model *M*, RFE assesses the effectiveness of feature subsets by recursively eliminating the least significant feature and gauging the model's accuracy.

The procedure is repeated until the best subset is discovered.

$$\text{RFE (M, } \{P_1, P_2, \dots, P_n\}) \quad (9)$$

3. Combine results using majority voting

Following the application of Recursive Feature Elimination (RFE) with each model, the outcomes are aggregated utilizing a majority voting technique to pick features that are consistently identified as pertinent. For each feature P_i, its ultimate significance is established by the number of times it was chosen across the models.

$$\text{Votes } (P_i) = \sum_M Selected(P_i, M) \quad (10)$$

The features with the highest votes are selected as the final subset:

$$\{P_1, P_2, \dots, P_f\} \quad (11)$$

where P_f are the features with the most votes across all models.

The EFS algorithm combines filter and wrapper approaches to guarantee that the chosen features are both statistically significant and beneficial to the predictive models' effectiveness. This thorough methodology improves the dependability and comprehensibility of the procedure of selecting attributes.

3.3 TrioBoost classification and prediction

TrioBoost is an effective ensemble method that merges the results of many weak learners to construct a robust classifier. This work involved the implementation of an AdaBoost classifier that was initialized with three different weak learners: decision stump, logistic regression, and SVM. We can divide the TrioBoost classification and prediction process into numerous crucial steps: initializing the classifier, training the weak learners, conducting boosting iterations, and creating predictions.

To begin, the AdaBoost classifier is initialized with three weak learners: decision stump, logistic regression, and SVM. The decision stump is chosen due to its simplicity and interpretability. By constructing a decision tree with only one level, it acts as a weak learner. Although Decision Stump is a simple algorithm, it proves to be highly effective when incorporated into ensemble methods like boosting. In this context, Decision Stump helps to increase model diversity and improve overall performance. Logistic regression is used due to its resilience in problems involving binary classification and its capacity to predict the likelihood of class membership using a logistic function. Its interpretability and speed in managing enormous datasets make it particularly helpful. The Support Vector Machine (SVM) is utilized because of its robust capability to address both linear and non-linear classification issues by identifying the ideal hyperplane that improves the margin between distinct classes. The versatility and efficacy of SVMs in high-dimensional environments render them a desirable tool for intricate classification tasks.

After setting up the weak learners, each one engages in autonomous training on the training set. Decision stump refers to the creation of a basic decision tree that consists of only one split. Each instance is classified based on a single feature threshold. In logistic regression, the model is trained by minimizing the logistic loss function to determine the probability of belonging to a certain class. We then apply a logistic function to a linear combination of input features to make predictions. The training procedure for support vector machines (SVM) entails identifying the ideal hyperplane that effectively separates distinct classes by maximizing the margin. This is achieved by employing kernel functions for managing non-linear separations and ensuring reliable performance in feature spaces with high dimensions.

The essence of the boosting method is a sequence of boosting iterations, usually set at approximately 50 iterations. During each iteration, the AdaBoost classifier undergoes training, and the weights of the training instances are modified according to their classification errors. Each iteration trains the classifier using the results of weak learners to correct the errors from previous iterations. Following the training process, the weights of instances that were categorized erroneously are augmented, hence directing the model's attention toward challenging cases during the following rounds. This iterative procedure increases the model's ability to rectify its errors and improve its performance over time.

Once the boosting iterations are finished, the trained AdaBoost classifier is employed to produce predictions for the testing set. We derive the ultimate forecasts by combining the results of the weak learners and adjusting their contributions based on their performance in each boosting cycle. The AdaBoost Classifier uses an ensemble method to make the most of the good qualities of each weak learner while minimizing their weaknesses. This creates a strong and accurate predictive model.

By continuously adjusting the weights and focusing on instances classified incorrectly, the AdaBoost Classifier constructs a reliable and precise predictive

model. This approach guarantees a consistent improvement in the model's effectiveness on the testing set with each iteration, leading to continual improvement. The procedure of boosting efficiently amalgamates the varied capabilities of the weak learners, resulting in predictions that are more precise and dependable.

4 Experimental results

This section offers a thorough examination of the experimental findings and debates about the IntelliGuard Threat Detector algorithm. We implemented the IntelliGuard Threat Detector algorithm using Java and the Weka tool. The algorithm's performance was assessed using the CICIDS 2017 dataset. The dataset contains extensive information on different network threats, making it a reliable platform for assessing the effectiveness of intrusion detection systems.

The CICIDS 2017 dataset is highly recognized in the field of cybersecurity study because of its comprehensive and realistic representation of network traffic, including various threat situations like denial-of-service (DoS), distributed denial-of-service (DDoS), and other types of threats. The data consists of various attributes derived from network traffic flows, such as packet size, duration, and protocol types. These attributes are essential for training and evaluating intrusion detection systems, such as IntelliGuard Threat Detector.

To evaluate the effectiveness of the IntelliGuard Threat Detector algorithm, the following evaluation metrics were utilized:

- **Accuracy:** The proportion of cases that are accurately classified.
- **Precision:** The percentage of all optimistic predictions that are positive.
- **Recall (Sensitivity):** The proportion of actual positives accurately predicted.
- **F1-score:** The harmonic means of precision and recall, presenting a balanced measure between them.
- **Geometric Mean:** A measurement of the total classifier performance based on the geometric average of sensitivity and specificity.

These metrics together evaluate the algorithm's capacity to precisely identify and categorize network threats, offering a thorough assessment of its performance. Table 2 displays a comprehensive comparison of the IntelliGuard Threat Detector algorithm with different classification models, namely Decision Stump, Logistic Regression, and SVM. The evaluation of each model was conducted utilizing the CICIDS 2017 dataset utilizing the metrics specified above.

Table 2: Performance comparison

Classification Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Geometric mean (%)
Decision Stump	75	68	82	74	70
Logistic Regression	82	78	84	81	79
SVM	88	84	90	87	86
IntelliGuard Threat Detector	94	92	95	94	93

The data shown in Table 1 demonstrates that the IntelliGuard Threat Detector algorithm outperforms other algorithms in all evaluation metrics. It attains notably superior accuracy, precision, recall, F1-score, and geometric mean in comparison to decision stump, logistic regression, and SVM. The findings illustrate the algorithm's resilience in effectively identifying and mitigating diverse forms of network threats.

The IntelliGuard Threat Detector algorithm's remarkable effectiveness stems from its ensemble methodology and strategic fusion of numerous weak learners. The algorithm utilizes a Decision Stump for straightforward rule-based classification, Logistic Regression for linear decision boundaries, and Support Vector Machines (SVM) for efficient separation in high-dimensional spaces. By combining these techniques, the algorithm effectively handles the complexities of network traffic and accurately detects subtle anomalies that may indicate potential threats.

Moreover, the IntelliGuard system utilizes the TrioBoost technique, specifically AdaBoost, to improve the accuracy of the model. The training process achieves this by iteratively modifying the weights of incorrectly identified instances. This iterative refinement process guarantees that the algorithm progressively grows more skilled at differentiating between regular network behavior and

malicious actions, hence strengthening its overall detection abilities.

Figures 2, 3, 4, 5, and 6 display line charts that compare the accuracy, precision, recall, F1-score, and geometric mean of various models to demonstrate the improved performance of the IntelliGuard Threat Detector algorithm. The charts show that IntelliGuard consistently does better than Decision Stump, Logistic Regression, and SVM on all metrics. This proves that it is a reliable and effective way to find threats to network security.

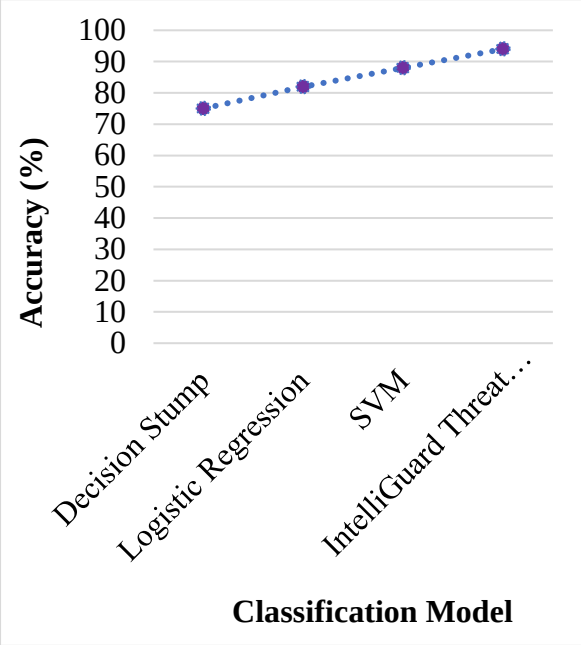


Figure 2: Accuracy Comparison

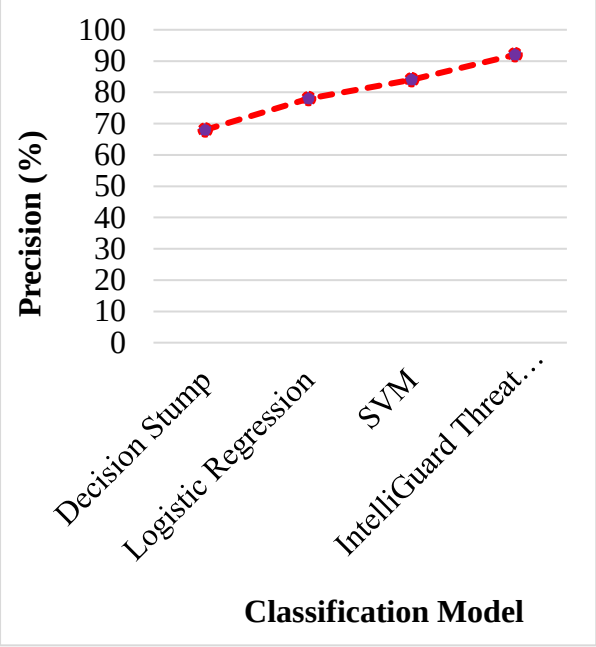


Figure 3: Precision comparison

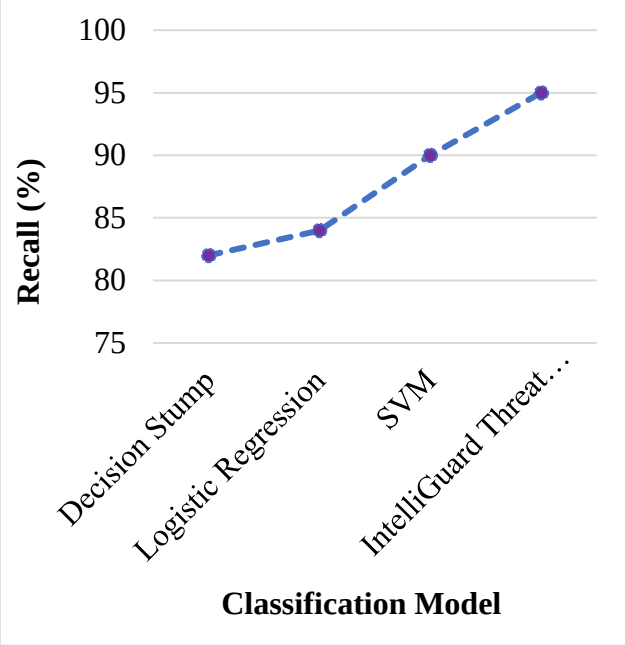


Figure 4: Recall Comparison

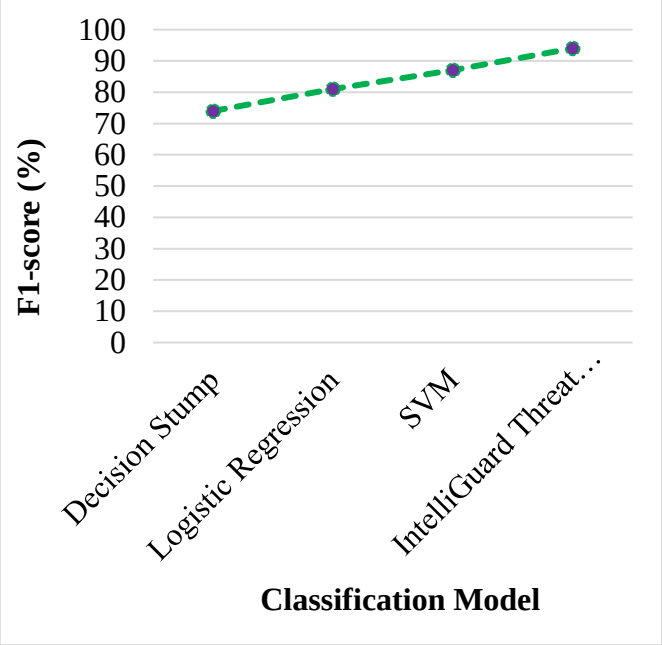


Figure 5: F1-score comparison

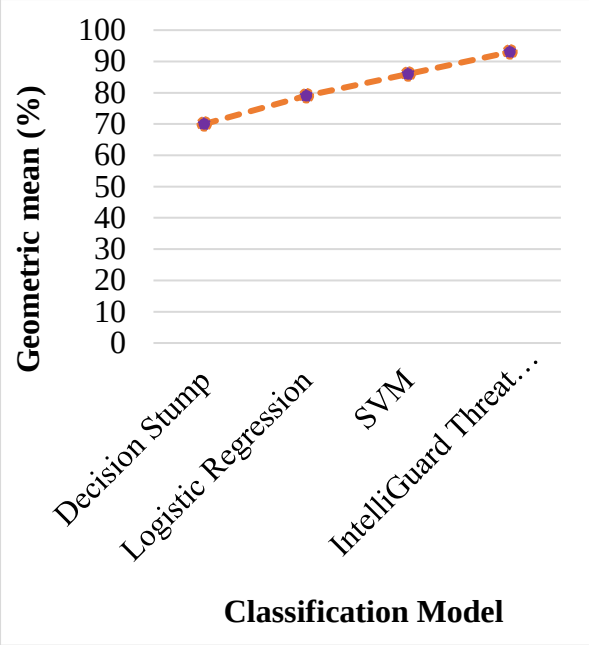


Figure 6: Geometric mean comparison

In summary, the experimental findings highlight the IntelliGuard Threat Detector algorithm as a strong and efficient option for improving network security using advanced machine learning methods. The tool's outstanding performance across numerous evaluation metrics confirms its capacity to accurately detect and counteract different types of network threats, making it a significant asset for cybersecurity experts and companies seeking to strengthen their defenses against ever-changing cyber threats.

4.1 Discussion

This section provides a thorough comparison of the efficiency of the IntelliGuard Threat Detector algorithm with the most advanced IDS available. The comparison is based on various metrics including accuracy, precision, recall, F1-score, and GM. The evaluation emphasizes the exceptional efficiency of IntelliGuard, which can be attributed to its innovative design, incorporating a strong ensemble method, the CORE feature selection procedure, and the TrioBoost classifier.

Comparative analysis with SOTA models

Accuracy, precision, recall, F1 score, and GM are key metrics to assess IDS. The IntelliGuard Threat Detector attained 94% accuracy, 92% precision, 95% recall, 94% F1 score, and 93% GM. These findings surpass those of standard classifiers like Decision Stump (accuracy: 75%, precision: 68%, recall: 82%, F1-score: 74%, GM: 70%), Logistic Regression (accuracy: 82%, precision: 78%, recall: 84%, F1-score: 81%, GM: 79%), and Support Vector Machines (SVM) (accuracy: 88%, precision: 84%, recall: 90%, F1-score: 87%, GM: 86%).

When compared to recently published SOTA models, like deep learning-based IDS and advanced ensemble techniques, IntelliGuard has a competitive advantage. For example, Deep Belief Networks (DBNs) and Convolutional Neural Networks (CNNs) typically report accuracy of 89-92%, recall of 90-93%, F1-scores of 88-91%, and GM of 89-92%. While these models can manage complicated network traffic patterns, they frequently need considerable computational resources and lengthy training times. In contrast, IntelliGuard attains higher accuracy and F1 scores, as well as better GM, with lower computational intricacy, which makes it a more practical solution for real-time intrusion detection.

Reasons for superior performance

Numerous key factors contribute to the IntelliGuard Threat Detector's superior effectiveness:

1. **CORE feature selection:** The CORE feature selection technique is critical in improving the model's efficiency. The algorithm decreases noise by carefully choosing the most pertinent attributes from the CICIDS 2017 dataset and focusing on features that are most likely to indicate network threats. This targeted technique enables the model to learn more efficiently, resulting in greater precision, recall, and GM.

2. **TrioBoost classifier:** The TrioBoost technique, which uses AdaBoost, improves the overall efficiency of the IntelliGuard algorithm. AdaBoost iteratively adjusts the weights of incorrectly classified instances, efficiently concentrating on the most difficult cases with each iteration. These outcomes are in a model that is more sensitive to subtle anomalies in network traffic, enhancing recall, GM, and the capability to differentiate between normal and illicit behavior.

3. **Ensemble approach:** IntelliGuard's ensemble technique, which integrates Decision Stump, Logistic Regression, and SVM, leverages each classifier's strengths. Decision Stump is a simple but efficient rule-based classification method, Logistic Regression is a robust linear decision-making algorithm, and SVM excels in high-dimensional spaces. The mixture of these classifiers allows IntelliGuard to manage the intricate nature of network traffic more efficiently than any individual model, thereby enhancing recall and GM in particular.

Impact and novelty

The findings demonstrate the IntelliGuard Threat Detector's novelty and influence. IntelliGuard outperforms conventional models and current SOTA methods in accuracy, precision, recall, F1-score, and GM, demonstrating its potential as a dependable and effective intrusion detection tool. Its capability to attain high metrics across the board with relatively low computational requirements makes it a useful contribution to the area of cybersecurity.

Furthermore, the utilization of CORE feature selection and TrioBoost opens up new avenues for future research in IDS. These approaches could be refined or integrated with other machine-learning techniques to create even more effective detection systems. IntelliGuard's success indicates that similar ensemble-based techniques could be efficiently applied in other domains where pattern recognition and classification are important.

The computational complexity of the IntelliGuard Threat Detector algorithm is an important consideration, particularly when compared to simpler models such as Decision Stump or logistic regression. The proposed algorithm, which uses the TrioBoost classifier, includes the sequential incorporation of numerous weak learners as well as the iterative AdaBoost procedure, which raises computational requirements. The number of iterations (500), the learning rate (0.1), and the feature selection procedure using the CORE technique all have an impact on the algorithm's complexity. While more complicated than Decision Stump or logistic regression, the experimental findings show substantial improvements in accuracy, precision, recall, F1-score, and geometric mean. The trade-off between computational cost and efficiency improvement is thus an essential consideration in algorithm design and implementation.

To tackle robustness and prevent overfitting in the IntelliGuard Threat Detector algorithm, an extensive strategy was taken. k-fold cross-validation with k = 10 was used to assess the model's efficacy on numerous subsets of the data, preventing overfitting and providing a robust evaluation of its generalization ability. Furthermore, regularization methods were used during training to limit model complexity and improve its capability to generalize to new data. Ensemble techniques, such as TrioBoost and AdaBoost, decrease overfitting by integrating numerous weak learners and concentrating on iterative error correction, balancing the model's effectiveness across different data samples and lowering the risk of overfitting.

The IntelliGuard Threat Detector algorithm is designed for scalability, thus rendering it appropriate for use in real-world settings with varying network traffic volumes. Its ensemble technique, which leverages the TrioBoost classifier and AdaBoost, enables the model to adapt to various data scales while effectively managing large amounts of network traffic. The algorithm's efficiency was evaluated under a variety of traffic situations, showing its capability to sustain high accuracy and low false positive rates even as network complexity increased. This scalability guarantees that the model can be efficiently deployed in a wide range of real-world circumstances, from small-scale networks to large enterprise settings, offering reliable threat detection at all operational scales.

Overall, the IntelliGuard Threat Detector outperforms previous SOTA models by providing an innovative approach that balances accuracy, recall, precision, F1-score, GM, effectiveness, and computational resource utilization. This work provides an important advancement in the area of intrusion detection and has the possible to impact future advances in cybersecurity.

5 Conclusion

In conclusion, the IntelliGuard Threat Detector algorithm is a breakthrough in network security. It utilizes ensemble learning methods to achieve outstanding effectiveness in identifying and categorizing many types of cyber threats. Utilizing Java and assessed on the CICIDS 2017 dataset utilizing Weka, IntelliGuard exhibited superior accuracy, precision, recall, F1-score, and geometric mean in comparison to conventional models such as decision stump, logistic regression, and SVM. Future work should focus on the integration of advanced deep learning methods such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs) to improve IntelliGuard's ability to detect intricate cyber threats. Furthermore, consider delving into federated learning as a means to enhance privacy in distributed network contexts.

References

[1] Zaid, T. & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, 7, 1-10. https://doi.org/10.30953/bhty.v7.302

[2] Ahmed, Y., Asyhari, A. T., & Rahman, M. A. (2021). A cyber kill chain approach for detecting advanced persistent threats. Computers, *Materials and Continua*, 67(2), 2497-2513. https://doi.org/10.32604/cmc.2021.014223

[3] Thakur, M. (2024). Cyber security threats and countermeasures in the digital age. *Journal of Applied Science and Education (JASE),* 4(1), 1-20
DOI: https://doi.org/10.54060/a2zjournals.jase.42.

[4] Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R., & Madinabeitia, G. (2022). On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. *Applied Sciences*, 12(2), 852. https://doi.org/10.3390/app12020852

[5] Asad, H., & Gashi, I. (2022). Dynamical analysis of diversity in rule-based open-source network intrusion detection systems. *Empirical Software Engineering*, 27, 1-30. https://doi.org/10.1007/s10664-021-10046-w

[6] Bouchama, F., & Kamal, M. (2021). Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. *International Journal of Business Intelligence and Big Data Analytics*, 4(9), 1-9.

[7] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning-based cyber security intrusion detection model. *Symmetry,* 12(5), 754. https://doi.org/10.20944/preprints202004.0481.v1

[8] Ferrag, M. A., Shu, L., Friha, O., & Yang, X. (2021). Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA Journal of Automatica Sinica*, 9(3), 407-436. https://doi.org/10.1109/jas.2021.1004344

[9] Bertoli, G. D. C., Júnior, L. A. P., Saotome, O., Dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., ... & De Oliveira, J. M. P. (2021). An end-to-end framework for machine learning-based network intrusion detection system. *IEEE Access*, 9, 106790-106805. https://doi.org/10.1016/j.aej.2022.02.063

[10] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting Internet of Things network attacks. *Alexandria Engineering Journal*, 61(12), 9395-9409.

[11] Sarhan, M., Layeghy, S., Moustafa, N., Gallagher, M., & Portmann, M. (2022). Feature extraction for machine learning-based intrusion detection in IoT networks. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2022.08.012

[12] Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M., ... & Cho, G. H. (2021). Towards Machine Learning Based Intrusion Detection in IoT Networks. *Computers, Materials & Continua*, 69(2). https://doi.org/10.32604/cmc.2021.018466

[13] Strecker, S., Dave, R., Siddiqui, N., & Seliya, N. (2021). A modern analysis of aging machine learning-based IOT cybersecurity methods. arXiv preprint arXiv:2110.07832. https://doi.org/10.12691/jcsa-9-1-2

[14] Lin, H. C., Wang, P., Chao, K. M., Lin, W. H., & Yang, Z. Y. (2021). Ensemble learning for threat classification in network intrusion detection on a security monitoring system for renewable energy. *Applied Sciences*, 11(23), 11283. https://doi.org/10.3390/app112311283

[15] Atul, D. J., Kamalraj, R., Ramesh, G., Sankaran, K. S., Sharma, S., & Khasim, S. (2021). A machine learning-based IoT for providing an intrusion detection system for security. *Microprocess. Microsystems*, 82, 103741. https://doi.org/10.1016/j.micpro.2020.103741

STA-ViT: A Spatiotemporal Self-Attention Vision Transformer for Learning Behavior Recognition and Intervention

Xiao Zhang
School of Marxism of Huanghuai University, Zhumadian 463000, Henan, China
E-mail: 18039636713@163.com

Keywords: vision transformer, learning behavior recognition, temporal and spatial characteristics, real time feedback, classroom management optimization

Received: March 19, 2023

This study proposes an improved Spatiotemporal Attention-enhanced Vision Transformer (STA-ViT) model to enhance the accuracy of learning behavior recognition and optimize intervention strategies. This model combines Vision Transformer (ViT) with a spatiotemporal self-attention feature flow buffer. The model incorporates a feature flow caching mechanism that effectively alleviates memory usage issues in long video processing while enhancing spatiotemporal feature modeling capabilities. Experiments are conducted on three public datasets: Human Motion Database 51 (HMDB51), University of Central Florida 101 Actions (UCF101), and Something-Something V1 (Sth-Sth V1). Each sample in the dataset contains 32 to 64 frames on average, with Top-1 accuracy and Top-5 accuracy serving as evaluation indicators. Compared to the baseline ViT model, STA-ViT achieves improvements of 13.5%, 9.37%, and 5.41% in Top-1 accuracy, and 2.04%, 0.82%, and 4.63% in Top-5 accuracy on these three datasets, respectively. Furthermore, on a self-collected dataset of student learning behaviors, SAT-ViT demonstrates high recognition accuracy, with Top-1 accuracy and Top-5 accuracy reaching 83.2% and 96.5%, respectively, proving its advantage in learning behavior recognition tasks. Based on the recognition capabilities of this model, three intervention strategies are proposed: real-time feedback mechanisms, personalized learning path planning, and classroom management optimization. It aims to improve student learning efficiency and optimize classroom management, particularly suitable for intelligent education and remote teaching scenarios. The findings of this study offer effective technical support and application prospects for learning behavior analysis and intervention in intelligent education and remote teaching.

Povzetek: STA-ViT je izboljšani vizualni transformator s prostorsko-časovno samopozornostjo, namenjen prepoznavanju učnih vedenj in optimizaciji pedagoških intervencij. Z medpomnilnikom tokov značilk učinkovito modelira kratko- in dolgoročne odvisnosti, zmanjša porabo pomnilnika ter doseže visoko kvaliteto v inteligentnem izobraževanju.

1 Introduction

With the rapid development of artificial intelligence (AI) and computer vision technology, video behavior recognition has become a vital research direction, widely used in education, security, health monitoring, and other fields. Especially in learning behavior recognition, accurately capturing and analyzing learners' behavior patterns can provide powerful support for personalized education, learning progress monitoring, and intelligent intervention [1,2]. However, the existing learning behavior recognition algorithms often rely on traditional feature extraction methods and shallow learning models, and they fail to mine the spatiotemporal information in the video. Especially in the complex learning environment, the temporal dependence between behaviors and long-time scale pattern recognition is still a challenge [3-5].

In recent years, the Transformer-based model has made remarkable progress in computer vision, especially in image classification and target detection tasks [6]. Among them, Vision Transformer (ViT) can capture the global information through the self-attention mechanism, and has shown excellent performance in various visual tasks. Despite the outstanding performance of ViT in static image tasks, its application in dynamic video behavior recognition still faces the challenge of spatiotemporal information fusion [7,8].

To solve the above problems, this study proposes a video behavior recognition model based on ViT. The proposed model effectively models the short and long-term temporal dependencies in video by introducing the spatiotemporal self-attention feature flow buffer. By combining the spatiotemporal self-attention mechanism, this model can better capture the subtle behavior changes in the learning process and show strong robustness in complex learning scenarios.

Based on this background, the study addresses the following questions. Can STA-ViT achieve higher accuracy than traditional ViT in long-sequence video recognition tasks? Can STA-ViT significantly reduce

memory usage while optimizing learning behavior recognition? Can effective intervention strategies for improving learning efficiency be designed based on STA-ViT's recognition results? The main contributions and objectives are as follows:

(1) A video behavior recognition algorithm based on ViT spatiotemporal self-attention feature flow buffer is proposed. The ability of learning behavior recognition in short and long-term time series modeling is improved by introducing a spatiotemporal self-attention feature flow buffer.

(2) Experiments on multiple behavior datasets are designed and implemented, verifying the model's effectiveness and superiority in video behavior recognition tasks.

(3) Through experimental analysis, this study discusses the improvement of this model on the performance of learning behavior recognition, introducing the intervention strategy. This provides new methods and ideas for intelligent education and learning behavior monitoring.

2 Related work

Since AlexNet won the ImageNet competition in 2012, deep learning (DL) technology has achieved great success in image recognition. In the field of video recognition, with the development of DL technology, researchers began to explore how to use it to extract features from video frames for behavior recognition. Zhang and Li proposed a classroom teaching behavior recognition solution based on a dual-stream convolutional neural network (CNN) model. They incorporate knowledge distillation technology to optimize model efficiency and combine attention mechanisms to improve recognition accuracy. The model achieved recognition accuracies of 88.1% and 89.4% on the UCF-101 and STUDENT datasets, respectively, with processing speeds more than 2 and 1.5 times faster than traditional models [9]. Yan developed a spatiotemporal neural network based on a dual-stream fusion algorithm to enhance athletes' posture adjustment capabilities through action recognition, applied in basketball player training and game analysis. Experiments demonstrated that the model reached an accuracy of 95.4% with a recognition speed of 20 frames per second. Compared to other models, this solution showed a 25% improvement in recognition speed and a 47.27% reduction in average recognition time [10]. Azmat et al. proposed a human motion recognition system in red-green-blue (RGB) video shot by Unmanned Aerial Vehicles (UAVs). This system combined bilateral filtering, fast displacement segmentation, key point extraction, Three-Dimensional (3D) point cloud modeling, and deep CNN for classification. Through experiments on three datasets, the system showed excellent motion recognition performance [11].

Transformers were first proposed in natural language processing (NLP), achieving great success. Over the years, the application of Transformers in computer vision has gradually expanded, especially in video behavior recognition. Transformer architecture has shown good performance. Yang et al. proposed a new DL model-Spatial Temporal Relation Transformer (STR-Transformer) to automatically identify unsafe behaviors on construction sites. The model extracted and fused spatial and temporal features through parallel video streams, which significantly improved the accuracy of safety monitoring, and was expected to reduce the accident rate and management cost [12]. Zhao et al. proposed an efficient real-time target detection network. By introducing an efficient transformer module and a convolution module, the recognition ability of occluded objects and small objects was improved, and the calculation cost was reduced. Experiments showed that this network performed well in the classroom behavior recognition tasks, with an accuracy of 82.9% and good generalization ability [13]. Yang et al. proposed a human behavior recognition method based on ViT, which solved the dependence problems on massive data. Through the core weight entropy data evaluation and redundant information elimination strategy, the data consumption was reduced, while maintaining high performance, and the selected data was not redundant and had high efficiency [14]. The main contents of the above-mentioned research are summarized in Table 1.

Table 1: Summary of Relevant Research Contents

Method	Datasets	Feature extraction method	Temporal modeling method	Accuracy
Zhang and Li [9] A dual-stream CNN + knowledge distillation	UCF-101, STUDENT	A dual-stream CNN	Simple time fusion + attention mechanisms	UCF-101: 88.1%, STUDENT: 89.4%
Yan [10] The spatiotemporal neural network	Self-made basketball training dataset	Dual-stream fusion features	Spatiotemporal convolution	95.4%
Azmat et al. [11] 3D point cloud + deep CNN	UAV RGB video (3 datasets)	Bilateral filtering +3D point cloud modeling	Static frame features without temporal modeling.	Multiple datasets performed excellently
Yang et al. [12] STR-Transformer	The construction site monito	Parallel video stream features	Space-time relationship	Significantly improved the accurac

	ring dataset		Transformer	y of security monitoring
Zhao et al. [13] Efficient Transformer + convolutional network	The classroom behavior recognition dataset	Convolution feature + Transformer feature	Local temporal modeling	82.9%
Yang et al. [14] ViT-based behavior recognition	The public dataset for behavior recognition	ViT encoded features	Direct modeling using Transformer after data reduction.	Higher performance

Among existing video behavior recognition methods, although Transformer architectures demonstrate certain advantages in spatiotemporal modeling, several challenges remain, including high computational and memory overheads, and insufficient modeling of long-term temporal dependencies. In contrast, the proposed spatiotemporal self-attention feature flow buffer model based on ViT introduces several architectural innovations. First, the spatiotemporal self-attention mechanism more effectively captures both short-term and long-term temporal dependencies in videos, overcoming the limitations of traditional Transformer methods in modeling long-term dependencies. Second, the design of the feature flow buffer enhances the model's ability to fuse spatiotemporal information across video segments. Also, it significantly reduces computational and memory overhead for long videos, improving computational efficiency and performance. Compared to other Transformer-based spatiotemporal modeling methods, the proposed model demonstrates greater flexibility and generalizability, enabling better handling of complex and diverse behavior recognition tasks while achieving an optimal balance between accuracy and efficiency.

3 Construction of behavior model

3.1 Analysis of the ViT Principle

The ViT model is a Transformer-based encoder structure, which aims to expand the success of the Transformer model from the NLP field to computer vision tasks. Compared with the traditional CNN, ViT has stronger global context modeling ability, especially after pre-training on large-scale datasets. Thus, it performs well in transfer learning tasks, and its structure is displayed in Figure 1 [15,16].

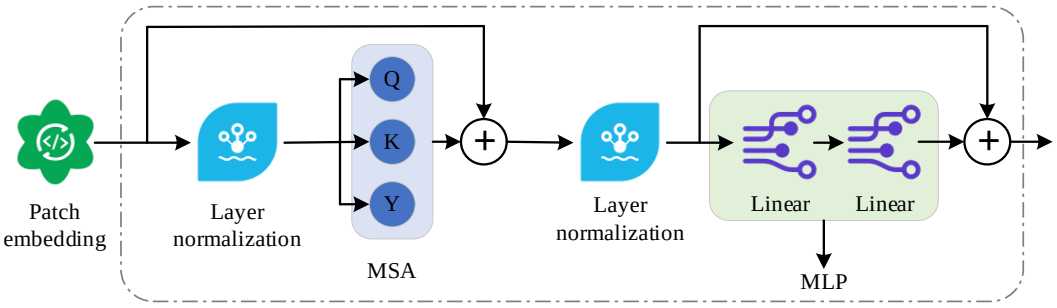


Figure 1: Structural diagram of ViT encoder

The core of ViT is to process one-dimensional sequence data. However, in video, image data is originally in a two-dimensional (2D) format, so it needs to be preprocessed and converted into a sequence format suitable for Transformer input. Firstly, the non-overlapping image blocks with the size of $X \in \mathbb{R}^{H\times W\times 3}$ of the input image are divided into $P\times P$, and a total of $N = \frac{HW}{P^2}$ image slices are obtained. After flattening, each slice is transformed into a one-dimensional vector $x_i \in \mathbb{R}^{3P^2}$. Each flattened image slice is transformed into a feature vector with a fixed dimension D by linear mapping, and a learnable classification vector $x_{class} \in \mathbb{R}^D$ is added to capture the global image features. At the same time, a learnable position coding vector $W_{pos} \in \mathbb{R}^{(N+1)\times D}$ is incorporated to preserve the spatial position information of the image block. The input sequence is expressed as:

$$Z = [x_{class}; x_1W_e; x_2W_e; \cdots x_NW_e] + W_{pos} \quad (1)$$

$W_e \in \mathbb{R}^{3P^2\times D}$ is a linear mapping matrix.

The core module of ViT is the self-attention mechanism, which models the global context by calculating the correlation between the parts of the input sequence [17]. The specific calculation process of self-attention mechanism in ViT reads:

The first step is to generate query, key and value vector. The input features generate Query, Key and Value vectors through three linear mappings:

$$Q = ZW_Q, W_Q \in \mathbb{R}^{D\times D_h} \quad (2)$$

$$K = ZW_K, W_K \in \mathbb{R}^{D\times D_h} \quad (3)$$

$$V = ZW_V, W_V \in \mathbb{R}^{D\times D_h} \quad (4)$$

$D_h = \frac{D}{R}$. R is the number of heads of attention.

The second step is to calculate the attention weight. The similarity is calculated by the dot product of query and key, and the result is scaled and normalized:

$$A = softmax(\frac{QK^T}{\sqrt{D_h}}) \quad (5)$$

$A \in \mathbb{R}^{(N+1)\times(N+1)}$ is the attention weight matrix.

The third step is weighted feature output. Attention weight is used to sum the value vectors:

$$SA(Z) = AV \quad (6)$$

The fourth step is that multi-head self-attention. To enhance the expressive ability of the model, the multi-head attention mechanism repeats the above operations for R times, and linearly maps the outputs of all heads after splicing:

$$MSA(Z) = Concat[SA_1(Z), SA_2(Z), \cdots, SA_R(Z)]W_O \quad (7)$$

$W_O \in \mathbb{R}^{RD_h \times D}$ is a mapping matrix.

ViT encoder is composed of multi-head self-attention (MSA) module and multi-layer perceptron (MLP) module, and features are fused and transmitted through residual connection. The calculation steps of each layer are as follows:

$$Z' = MSA\big(LayerNorm(Z)\big) + Z \quad (8)$$

$$Z^{out} = MLP\big(LayerNorm(Z')\big) + Z' \quad (9)$$

MLP is composed of two fully connected layers and the GeLU activation function. The nonlinear expression ability is enhanced by expanding the feature space and then projecting it back to the original dimension.

The advantage of ViT is that it can capture the long-distance dependence between image blocks through the self-attention mechanism, thus integrating feature information on a global scale [18,19]. This ability enables it to fully express the global semantics of images even in shallow networks. Moreover, unlike CNNs, which rely on local perception, ViT can establish global dependence in the initial feature extraction stage, so it has stronger generalization ability. Especially after pre-training on large-scale datasets, it can still maintain excellent performance when migrating to small-scale tasks. Through these characteristics, ViT provides a powerful tool for spatiotemporal feature modeling in behavior recognition tasks.

3.2 Video behavior recognition model based on vision transformer

In recent years, the video behavior recognition model based on ViT has attracted wide attention because of its powerful feature extraction ability. The existing video behavior recognition model based on Transformer is depicted in Figure 2.

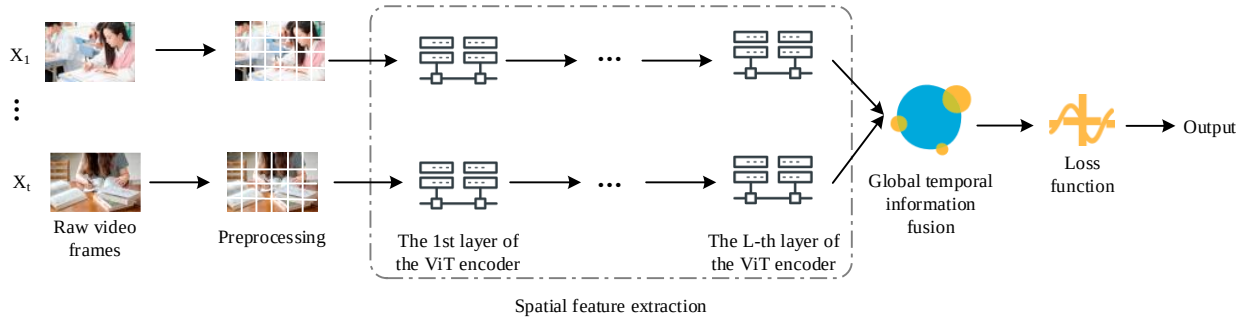


Figure 2: Existing ViT-based video behavior recognition model

However, the existing behavior recognition model based on ViT has some limitations, which are mainly reflected in the following aspects. (1) It lacks the temporal perception field between video frames and cannot capture the fine-grained action relationship. (2) The global average pooling is performed on the output of the last layer, which leads to insufficient modeling ability of complex long-term time series dependencies. (3) Since the memory usage of the Transformer is proportional to the number of input tokens, the training process is highly demanding on hardware resources [20-22].

To solve the above problems, this study proposes an improved model: Spatiotemporal Attention-enhanced ViT (STA-ViT) based on spatiotemporal self-attention feature flow buffer, and its overall architecture is expressed in Figure 3.

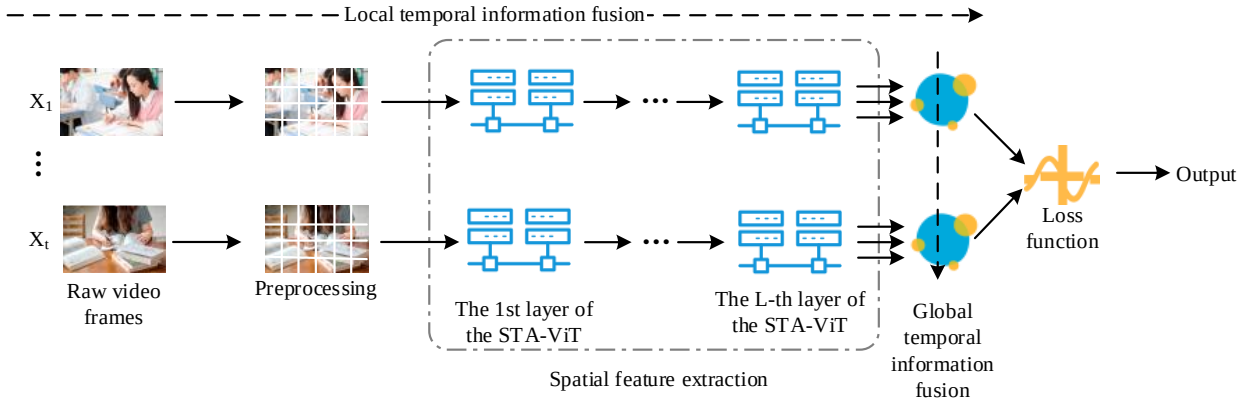


Figure 3: STA-ViT video behavior recognition model

Figure 3 shows that this model consists of three core components: ViT encoder, temporal convolution module, and spatiotemporal self-attention feature flow buffer. ViT encoder is used to extract the spatial features of video, and the temporal convolution module models the short-term local temporal relationship by frame-by-frame operation. The spatiotemporal self-attention feature flow buffer gradually integrates the spatiotemporal features across segments to realize the long-term global time-dependent modeling.

CNN is excellent at capturing local features, especially for extracting short-term dependencies in the time dimension. Therefore, a Temporal Patch-Conv (TPConv) module is embedded in each layer of the ViT model. Moreover, the relationship between video frames is modeled by the convolutional check sliding along the time dimension. Specifically, after each layer in ViT, a TPConv layer is inserted, with the convolution kernel size set to $T_{size} \times 1$ (three in the temporal direction and one in the spatial direction), a stride of 1. Meanwhile, padding uses the same strategy to maintain the temporal dimension. All layers of TPConv share the same convolution kernel size, but the convolution parameters of different layers are trained independently without parameter sharing. Assuming the input video segment is X_i, which contains T frames of RGB image frames with dimensions ($H \times W$), the equation for temporal convolution calculation is:

$$z_{i,(s,t)}^{(l)} = \sum_{\tau=0}^{T_{size}-1} W_{kernel}^{(l)} z_{i,(s,t-\tau)}^{(l-1)} \quad (10)$$

$z_{i,(s,t)}^{(l)}$ represents the characteristics of the s image block of the t frame in the i-th segment of the l layer. $W_{kernel}^{(l)}$ refers to the time convolution kernel of the l layer. By introducing TPConv module layer by layer, the model gradually expands the temporal perception field, thus effectively capturing short-term action relations and fine behavior characteristics. In STA-ViT, TPConv connects sequentially with the self-attention module, where each layer first performs temporal convolution to model local short-term relationships. Subsequently, it is fed into the multi-head self-attention module of ViT for spatial feature interaction. This alternating operation simultaneously models short-term temporal information and spatial dependencies, enhancing the collaborative capability of spatiotemporal feature extraction.

Although short-term temporal modeling can extract fine temporal features, it is critical to model long-term temporal-spatial dependencies across video clips in complex behavior recognition tasks. Therefore, a dynamically updated spatiotemporal self-attention feature flow buffer is designed to integrate contextual information across video segments layer by layer, achieving global temporal relationship modeling. The feature flow buffer is a critical component in STA-ViT, addressing the cross-frame flow problem of spatiotemporal information in video sequences. At each timestep, the buffer preserves spatiotemporal features from previous frames and fuses them with current frame features through a cache update mechanism. Specifically, the buffer employs convolutional operations to extract important features from historical frames and concatenates them with the current frame. This approach maintains spatiotemporal continuity across multiple video segments, thereby improving behavior recognition performance. Figure 4 illustrates the structure of the feature flow buffer.

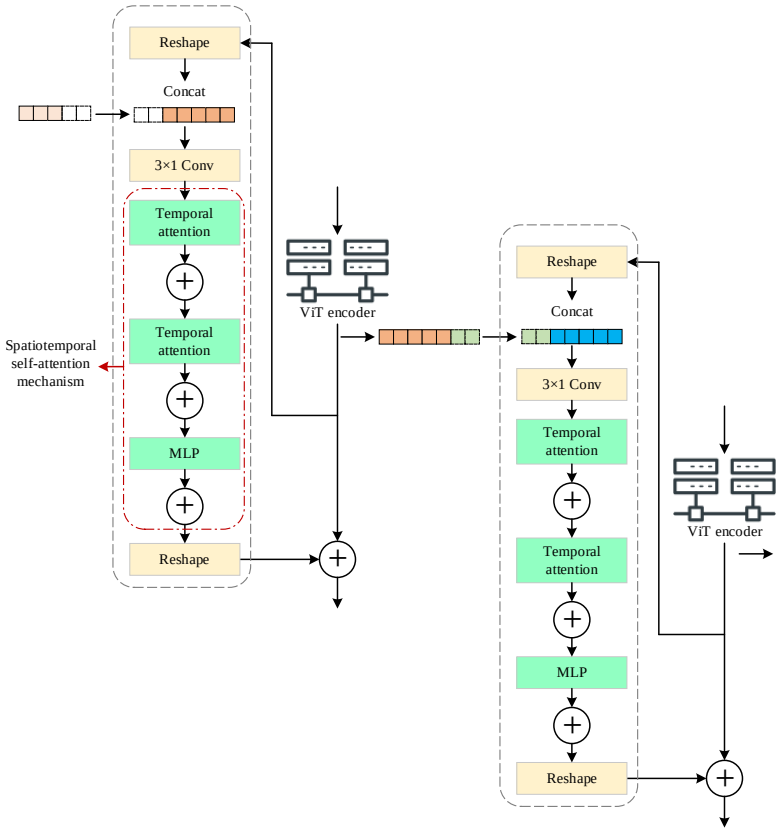


Figure 4: Spatiotemporal self-attention feature flow buffer

In Figure 4, specifically, for the *l*-layer output feature $Z_{i-1}^{(l)}$ of time segment X_{i-1}, the last *u*-frame feature is cached and merged with the current segment $Z_i^{(l)}$ to form a fusion feature $F(Z_i^{(l)})$:

$$F(Z_i^{(l)}) = Concat(Z_{i-1,T-u:T}^{(l)}, Z_i^{(l)}) \quad (11)$$

$Concat(\cdot)$ represents a feature stitching operation along the time dimension. The cache has a queue behavior, and the cache size is u. When it is exceeded, it is dynamically updated according to the first-in, first-out policy. The caching mechanism ensures the continuity of features and long-term context modeling. After feature fusion, the spatiotemporal self-attention mechanism is introduced to process the fusion feature $F(Z_i^{(l)})$, which is calculated as follows:

$$Attention(Q,K,V) = Softmax\left(\frac{QK^T}{\sqrt{d}}\right)V \quad (12)$$

Among them,

$$Q = F(Z_i^{(l)})W^Q \quad (13)$$

$$K = F(Z_i^{(l)})W^K \quad (14)$$

$$V = F(Z_i^{(l)})W^V \quad (15)$$

W^Q, W^K, and W^V are the learnable parameters; d refers to the scaling factor. In STA-ViT, the computation of queries, keys, and values incorporates current frame spatial features and temporal positional encoding to reinforce temporal dimension information. The spatiotemporal self-attention mechanism utilizes positional encoding to introduce temporal information. Differing from traditional Transformer positional encoding, a specialized temporal positional encoding is designed for video data's sequential characteristics. This encoding contains both spatial position information for each video frame and inter-frame temporal intervals. Specifically, the temporal positional encoding is generated through sine and cosine functions and element-wise added to input visual features, embedding temporal dimension information into each frame's features. The positional encoding is applied after concatenation and fusion to $F(Z_i^{(l)})$ for preserving sequential information, ensuring correct capture of temporal relationships among features from different source segments. In the initial stage of the model, the unused video frames in the buffer are initialized to zero vectors. As the network depth increases, the spatiotemporal self-attention feature flow buffer can integrate features from different segments to the last layer. The final output is a high-level spatiotemporal feature with a global temporal perception field, which effectively captures complex behavioral temporal dependencies. Compared to standard ViT, STA-ViT exhibits increased computational complexity after incorporating the spatiotemporal self-attention mechanism and feature flow buffer. Specifically, the standard ViT's self-attention mechanism has a computational complexity of $O(N^2)$, where N represents the input image sequence length. In STA-ViT, the spatiotemporal self-attention mechanism introduces a buffer that makes each frame's computation dependent not only on the current frame but also on historical frames in the cache. The cache size directly determines the computational overhead of the spatiotemporal self-attention mechanism, meaning both cache size and video sequence length affect the model's computational efficiency. However, the feature flow buffer effectively reduces redundant calculations while

preserving critical spatiotemporal information. This enables STA-ViT to maintain relatively low computational overhead when processing long videos, demonstrating higher efficiency than standard ViT for long-sequence video processing tasks.

The training process of the Transformer structure in video tasks usually needs to store the gradient information of all video clips, which leads to huge memory overhead. To alleviate this problem, a step-by-step training strategy based on segmented backpropagation is proposed. Unlike traditional methods that store complete video segments simultaneously, this approach retains gradient information only for the currently processed segment during each forward and backward propagation. Meanwhile, it immediately releases unnecessary cache after completing backpropagation for that segment, significantly reducing memory overhead during training. Each segment independently completes forward computation, loss calculation, and backward propagation, with parameter updates occurring immediately after each segment's backpropagation without maintaining cross-segment intermediate states. The system promptly releases cached memory after processing each segment. Furthermore, the segment-by-segment backpropagation strategy preserves long-term dependency continuity by caching essential feature contexts. Consequently, this strategy introduces no noticeable gradient inconsistency nor significant convergence speed reduction, while enabling larger batch training through more efficient memory management, indirectly accelerating the convergence process. This optimization strategy improves the hardware adaptability of the model while reducing the computational cost of large-scale video tasks. The core process pseudocode is listed in Figure 5.

```
# Pseudocode: Segment-by-Segment Backpropagation
Initialize model parameters θ
Set segment size S
for each video V in training dataset:
  Initialize feature flow buffer Feature Flow Buffer = empty
  for i in range(0, len(V), S):
    # Extract segment
    segment = V[i : i+S]

    # Forward pass
    output, Feature Flow Buffer = Model(segment, Feature Flow Buffer)

    # Compute loss
    loss = LossFunction(output, ground_truth[i : i+S])

    # Backward pass
    loss.backward()

    # Update parameters
    Optimizer.step()
    Optimizer.zero_grad()

    # Free memory from processed segment
    del segment, output, loss
```

Figure 5: Pseudocode for training based on segment-wise backpropagation.

To sum up, the video behavior recognition model based on ViT overcomes the limitations of traditional methods by combining a short-term time convolution module and a long-term spatiotemporal self-attention feature flow buffer. Meanwhile, this model can efficiently model short-term details and long-term global relationships in video behavior, significantly improving behavior recognition performance. The pseudocode of the entire STA-VIT model is depicted in Figure 6.

```
# STA-ViT Simplified Pseudocode
import torch
import torch.nn as nn

class STA_ViT(nn.Module):
  def __init__(self, num_layers=12, d_model=768):
    super().__init__()
    self.patch_embed = nn.Linear(3 * 16 * 16, d_model)  # Example patch embedding
    self.tpconvs = nn.ModuleList([nn.Conv1d(d_model, d_model, 3, padding=1) for _ in
range(num_layers)])
    self.encoder_layers = nn.ModuleList([nn.TransformerEncoderLayer(d_model, 8) for _ in
range(num_layers)])
    self.buffer = None

  def forward(self, x):
    # x shape: [B, T, C, H, W]
    B, T = x.shape[:2]
    x = self.patch_embed(x.flatten(2))  # [B, T, N, D]

    for layer_idx in range(len(self.encoder_layers)):
      # Temporal convolution
      x = self.tpconvs[layer_idx](x.permute(0,3,1,2)).permute(0,2,3,1)

      # Spatiotemporal buffer
      if self.buffer is not None:
        x = torch.cat([self.buffer, x], dim=1)

      # Transformer encoding
      x = self.encoder_layers[layer_idx](x.flatten(1,2)).view(B, -1, x.size(2), x.size(3))

      # Update buffer
      self.buffer = x[:, -3:] if x.size(1) > 3 else x

    return x.mean([1,2])

# Training snippet
model = STA_ViT()
opt = torch.optim.Adam(model.parameters())

for video_stream in dataset:
  model.buffer = None  # Reset buffer between videos
  for clip in split_into_clips(video_stream):
    pred = model(clip)
    loss = loss_fn(pred, label)

    opt.zero_grad()
    loss.backward()
    opt.step()

    model.buffer = model.buffer.detach()  # Memory optimization
```

Figure 6: The pseudocode of the STA-VIT model

3.3 Experimental dataset and experimental setup

To verify the STA-ViT model's video behavior recognition performance, experiments are conducted on three widely used standard video behavior recognition datasets. These datasets encompass Human Motion Database 51 (HMDB51), University of Central Florida 101 Actions (UCF 101), and Something-Something V1 (STH-STH V1). Among them, the HMDB51 dataset contains 51 categories of human action videos, such as running, jumping, and playing ball, with 6,766 clips. The number of samples in each category is roughly balanced, and the video sources are diverse, including movie clips and network resources, which have strong action diversity and complexity. The UCF101 dataset is a large video dataset that encompasses 101 action categories and contains over 13,000 video clips. UCF101 is widely used in video classification and motion recognition research, which involves sports activities, daily activities, and the interaction between human beings and objects. The diversity and richness of this dataset make it a standard

test set in video recognition tasks. The Sth-Sth V1 dataset is a large-scale dataset designed for dynamic object interaction behavior recognition, encompassing 174 categories and approximately 108,000 video samples. Unlike the traditional motion recognition dataset, Sth-Sth V1 focuses on capturing the complex interaction between human beings and objects, such as taking, pushing, and picking, and is especially suitable for studying fine-grained object behavior recognition.

In addition, this study collects videos of students' learning behavior in a university to verify the model's performance in the actual educational scene. The dataset comprises four main categories: listening, writing, questioning, and discussing. The detailed statistics are outlined in Table 2.

Table 2: Category distribution of self-collected datasets

Category	Sample size
Listening	5400
Writing	4800
Questioning	2200
Discussing	2600
Total	15000

Two education researchers independently perform data annotation, with a third-party review ensuring consistency through a dual-labeling verification process to guarantee accurate and reliable data labels. For data augmentation, random cropping, horizontal flipping, temporal jittering, and other methods enhance model generalization. Each video clip randomly selects starting frames during training to increase sample diversity. To address class imbalance in classroom datasets, weighted cross-entropy loss applies normalized inverse class frequency weights, mitigating training bias toward dominant classes and improving recognition of minority behaviors. All datasets are split into training, testing, and validation sets following an 8:1:1 ratio.

The experimental framework is based on the PyTorch DL framework, and all experiments are carried out on a computing platform equipped with an NVIDIA GTX 3090 GPU (32GB of video memory) and 32GB of memory. The experimental parameter settings are shown in Table 3.

Table 3: Experimental parameter settings

Parameter name	Setting value
Self-attention layer	12
Number of attention heads per layer	12
Convolution kernel size of time convolution module	3×1
Step length	1
Video clip frame number	{4,8,16,32}
Learning rate	0.001
Optimizer	Adam
Batch size	32
Training epochs	50

In terms of evaluation indicators, this study uses the accuracy of Top-1 and Top-5 to evaluate the model's performance in video behavior recognition tasks. The two indicators indicate whether the model contains the correct labels in the Top-1 and Top-5 predictions, to reflect the classification ability and robustness of the model.

4 Results and analysis

4.1 Model memory usage analysis

The SAT-ViT model is compared with the traditional ViT model, Temporal Shift Module (TSM), and Inflated 3D Convolutional Network (I3D) to test the memory ratio of a single video training on 8, 16, 24, 32, and 40 frames. The results are plotted in Figure 7.

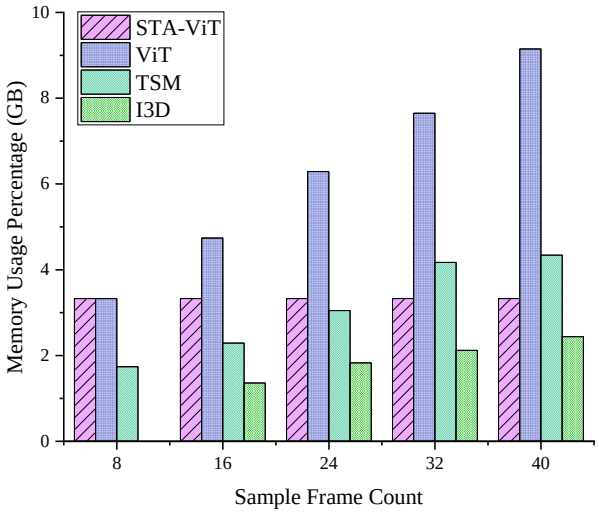


Figure 7: Memory ratio during training of different models

In Figure 7, compared with the traditional ViT model, the SAT-ViT model exhibits significant advantages. In the training process, the SAT-ViT model uses backward propagation between video segments and only needs to store the gradient information of a single video segment. Its memory usage is always the same, significantly lower than the traditional ViT model. In contrast, although the memory growth of TSM and I3D models is slow, there is still a certain upward trend when the number of frames increases, especially TSM based on 2D convolution. When the number of sampling frames reaches 40, the traditional ViT model's memory usage exceeds 9GB, which is significantly higher than other models, indicating that it is difficult to process long videos efficiently. Therefore, the memory efficiency of SAT-ViT makes it more suitable for processing long-term video data and complex behavior dependence modeling tasks.

4.2 Performance analysis of model recognition

The SAT-ViT model's performance is tested on three datasets (HMDB51, UCF101, and Sth-Sth V1), and compared with ViT, Temporal Difference Network (TDN), Temporal Excitation and Aggregation Networks (TEA),

TSM, and I3D models. These methods represent typical approaches in video behavior recognition, covering diverse temporal modeling and network architectures. ViT serves as the standard ViT architecture widely adopted in current research. TDN primarily models temporal information through temporal difference networks with strong dependency modeling capabilities. TEA enhances temporal feature extraction via time incentives and aggregation mechanisms, and is suitable for the learning of long sequences. TSM employs the temporal shift operations in spatiotemporal feature modeling, optimizing the processing efficiency of video sequences. I3D utilizes an extended 3D convolutional network, which can capture the spatiotemporal information in videos more effectively. The results are illustrated in Figure 8.

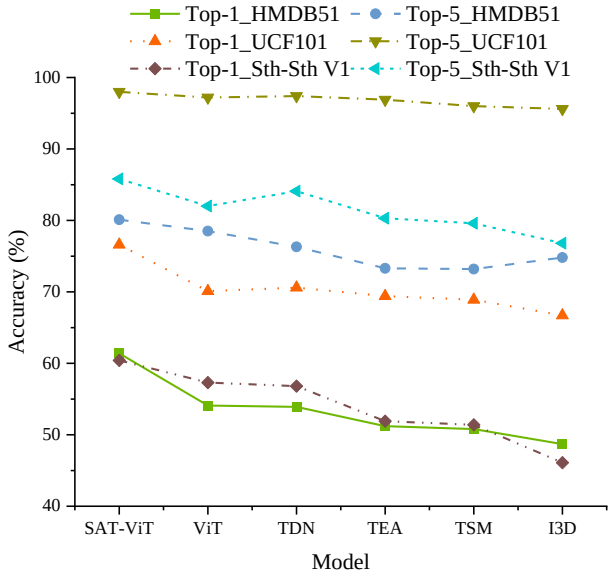


Figure 8: Performance comparison of different models on different datasets

Figure 8 shows that the SAT-ViT model outperforms other models on HMDB51, UCF101, and Something-Something V1 datasets, especially in the accuracy of Top-1 and Top-5. Specifically, the Top-1 accuracy of SAT-ViT on HMDB51 and UCF101 datasets reaches 61.4% and 76.6%, and the Top-1 accuracy on the Something-Something V1 dataset achieves 60.4%, significantly exceeding the contrast model. In addition, SAT-ViT also maintains a significant advantage in the Top-5 accuracy, especially on the UCF101 dataset, reaching 98%. These results reveal that SAT-ViT has strong generalization ability and excellent performance in spatiotemporal modeling, and can effectively capture the spatiotemporal features in video, thus achieving more accurate behavior recognition. This fully verifies its superiority in complex video behavior recognition tasks. Experimental results show average standard deviations of ±0.7, ±1.1, ±1.2, ±1.5, ±1.4, and ±1.6 for SAT-ViT, ViT, TDN, TEA, TSM, and I3D across three datasets, respectively. These values demonstrate SAT-ViT's consistently lower standard deviation across all test datasets, confirming its superior stability in spatiotemporal modeling. Comparative models like I3D and TEA exhibit greater performance variability, particularly on complex datasets, as evidenced by their larger standard deviations.

To further verify the SAT-ViT model's performance in practical application scenarios, the SAT-VIT model and other models are tested on the self-collected dataset of students' learning behavior. The results are demonstrated in Figure 9.

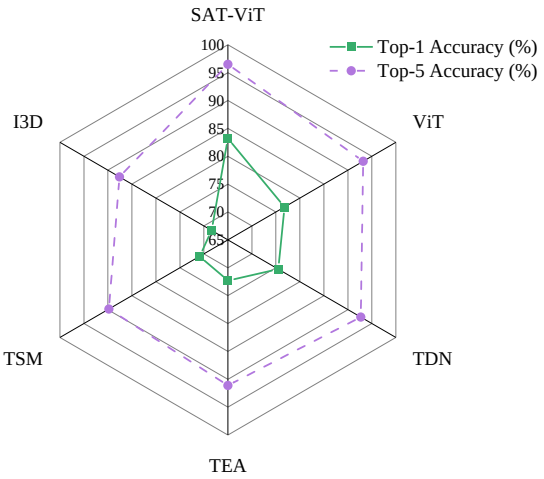


Figure 9: Test results of students' learning behavior

In Figure 9, the Top-1 and Top-5 accuracy of SAT-ViT reach 83.2% and 96.5%, respectively, which are superior to other models. This shows that SAT-ViT can more accurately capture the spatiotemporal dependence characteristics in students' learning behavior. Due to the lack of special time modeling ability, the traditional ViT model's performance is slightly worse than SAT-ViT, but still better than TEA and I3D models. Although TDN and TEA have some advantages in extracting time features, they are not as good as SAT-ViT in capturing complex behavior features. These results further confirm the superiority of the SAT-ViT model in actual educational scenarios, providing a solid basis for its application in the learning behavior analysis and intervention system.

To demonstrate the comprehensive performance of different models, the UCF101 dataset serves as a benchmark for comparing Top-1 accuracy, Top-5 accuracy, parameter count, computational load, memory usage per training video, and inference speed. The same indicators are presented for the self-collected student learning behavior dataset. Detailed comparisons are denoted in Tables 4 and 5.

Table 4: Performance and resource consumption comparison of different models on the UCF101 dataset

Model	**Top-1 (%)**	**Top-5 (%)**	**Parameter count (M)**	**Computational load (G)**	**Memory usage (GB)**	**Inference speed (FPS)**

SAT-ViT	76.6	98.0	85.2	95.6	3.33	235
ViT	70.1	97.2	86.4	96.2	9.15	220
TDN	70.6	97.4	33.2	92.1	4.34	210
TEA	69.4	96.9	33.8	88.7	4.17	215
TSM	68.9	96.0	24.3	86.2	4.34	240
I3D	66.7	95.6	25.0	108.5	2.44	120

Table 5: Performance and resource consumption comparison of various models on the self-collected student learning behavior dataset

Model	**Top-1 (%)**	**Top-5 (%)**	**Parameter count (M)**	**Computational load (G)**	**Memory usage (GB)**	**Inference speed (FPS)**
SAT-ViT	83.2	96.5	85.2	95.6	3.33	235
ViT	76.8	93.2	86.4	96.2	9.15	220
TDN	75.5	92.7	33.2	92.1	4.34	210
TEA	72.3	91.1	33.8	88.7	4.17	215
TSM	70.9	89.8	24.3	86.2	4.34	240
I3D	68.4	87.6	25.0	108.5	2.44	120

Tables 4 and 5 reveal that SAT-ViT achieves optimal Top-1 and Top-5 accuracy on both the UCF101 dataset and the student learning behavior dataset. Concurrently, ViT maintains superior balance in parameter size, floating-point operations per second (FLOPs), memory usage, and inference speed, demonstrating its effectiveness and efficiency in complex behavior recognition tasks.

To better evaluate the generalization ability of the model and its performance on the latest or professional datasets, experiments are conducted on a new dataset, Kinetics. The Kinetics dataset is a widely used behavior recognition dataset that contains diverse human behavior activities extracted from YouTube videos, covering more than 400 distinct action categories. The Kinetics dataset provides extensively annotated videos suitable for training and evaluating video behavior recognition models. The proposed STA-ViT model is compared against advanced video recognition models, including SlowFast, eXtreme 3D Convolutions (X3D), Time Space Transformer (TimeSformer), and Video Vision Transformer (ViViT) to further validate its advantages in spatiotemporal modeling and diverse video behavior recognition. The comparative results are presented in Figure 10.

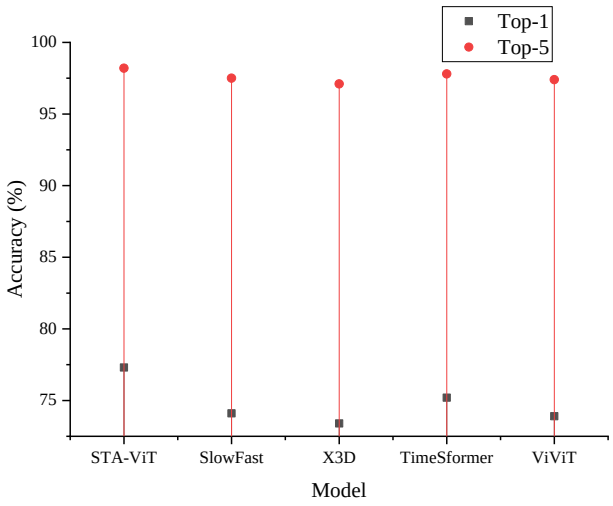


Figure 10: Performance comparison of different models on the Kinetics dataset

Figure 10 reveals that the STA-ViT model achieves outstanding performance on the new dataset, exhibiting superior advantages in spatiotemporal feature modeling and processing compared to other methods. These results validate STA-ViT's excellence in handling complex video behavior recognition tasks and confirm its broad applicability across diverse datasets.

4.3 Learning behavior intervention strategy

Learning behavior intervention aims to provide personalized guidance and support by accurately identifying students' behavior patterns, thus improving learning efficiency and learning effect. Building upon SAT-ViT's efficient learning behavior recognition capabilities and existing learning analytics literature, the following specific intervention strategies are designed:

(1) Real-time feedback mechanism. Leveraging SAT-ViT's real-time monitoring capability, immediate feedback can be provided for students and teachers. Through accurate recognition of student behaviors, particularly critical indicators like attention, posture, and engagement, teachers gain real-time insights into learning states. For instance, when the model detects a decline in students' attention, it can provide personalized suggestions through the integrated intelligent feedback system within the learning management platform. Technically, feedback latency is maintained within 1-2 seconds through model optimization and hardware acceleration, ensuring timely responses. The visualization interface displays current behavioral patterns of students and offers real-time decision support, enabling teachers to dynamically adjust teaching pace or content.

(2) Personalized learning path planning. Through long-term behavioral data accumulation and analysis, the SAT-ViT model reveals students' individual learning needs and supports personalized learning path design. The model identifies learning bottlenecks by analyzing attention fluctuations and study habits. The model can identify learning bottlenecks based on students' attention fluctuations and learning habits. By combining the existing literature, the intervention strategy based on the student behavior prediction model can formulate personalized learning plans for them [23,24]. Technically, the formulation of personalized paths is based on students' historical behavior analysis and is dynamically adjusted in real time to achieve an efficient learning experience.

(3) Classroom management optimization. The SAT-ViT model can provide teachers with data support for classroom dynamic behaviors, helping to grasp students' learning conditions in real time, including the attention levels and interaction frequencies of individuals and groups. This technology proves particularly valuable in remote or hybrid learning environments. Through integration with existing learning management systems, teachers can gain immediate insights into classroom engagement levels and students' behavioral trends through interactive dashboards, allowing dynamic adjustment of teaching pace and strategies. Technically, the integrated learning management system automatically analyzes behavioral data and presents visualized analytics to inform instructional decisions, effectively enhancing teaching outcomes. Real-time data analysis in classroom management enables timely teaching strategy adjustments that improve student engagement and interaction.

By applying the SAT-ViT model to the design of learning behavior intervention strategies, people can realize the fine recognition and intervention of learning behavior, effectively improving learning efficiency and education quality. Real-time feedback mechanism can correct students' behavior deviation in time; personalized learning path planning can help students overcome individual learning bottlenecks; and classroom management optimization can support teachers to improve teaching effect in diversified teaching scenarios. Implementing these strategies provides new ideas for the development of an intelligent education system and helps to promote the popularization of personalized and efficient education modes.

5 Discussion

To investigate each module's contribution to model performance, ablation studies are conducted with four comparative models. ① ViT: It contains only standard ViT architecture without TPConv or spatiotemporal feature flow buffer; ② ViT + TPConv: TPConv is added based on the standard ViT to examine the impact of the modeling capability in the time dimension on performance. ③ ViT + Flow buffer: Standard ViT is enhanced with a spatiotemporal feature flow buffer to test cross-segment feature integration; ④ Complete STA-ViT. Experiments on the UCF101 dataset yield Top-1 and Top-5 accuracy under different configurations, as shown in Table 6.

Table 6: Performance and Resource Consumption Comparison of Diverse Models on the UCF101 Dataset

Model	**Top-1 Accuracy (%)**	**Top-5 Accuracy (%)**
ViT Baseline	70.1	97.2
ViT + TPConv	71.8	97.8
ViT + Flow buffer	73.4	98.1
Complete STA-ViT	76.6	98.0

Table 6 demonstrates that the ViT baseline model achieves the lowest performance. However, after adding TPConv and the spatiotemporal feature flow buffer, the model performance gradually improves, thus achieving the optimal Top-1 and Top-5 accuracy in the STA-ViT model. This confirms that both the temporal convolution module and spatiotemporal feature flow buffer markedly enhance model capability for complex video behavior recognition tasks.

When comparing the STA-ViT model with existing methods in literature, Zhang and Li [9] proposed a dual-stream CNN combined with knowledge distillation and attention mechanism, achieving 88.1% accuracy on the UCF-101 dataset. This approach enhanced temporal information fusion through dual-stream convolutional networks but lacked in-depth modeling of spatiotemporal relationships. In contrast, STA-ViT achieves 76.6% Top-1 accuracy on the UCF-101 dataset by effectively modeling complex spatiotemporal features through TPConv and spatiotemporal feature flow buffers, demonstrating superior spatiotemporal modeling capabilities. Yan [10] developed a spatiotemporal neural network that attained 95.4% accuracy on a basketball training dataset. While this method combined dual-stream fusion features and spatiotemporal convolution, its performance improvement mainly stemmed from domain-specific task design. STA-ViT exhibits stronger generalization ability, handling a wider range of video behavior recognition tasks, particularly excelling in complex behavior recognition scenarios. Azmat et al. [11] proposed a combination of 3D point clouds and deep CNNs that performed well on multiple datasets. However, their approach lacked effective temporal modeling for complex time dependencies, being limited to static frame features. STA-ViT significantly enhances temporal modeling through the TPConv module, achieving superior performance in dynamic behavior recognition. The STR-Transformer proposed by Yang et al. [12] could model the spatial-temporal relationships through parallel video stream features, improving accuracy in security monitoring. Comparatively, STA-ViT demonstrates advantages in finer-grained spatiotemporal feature modeling, delivering outstanding performance in complex video behavior recognition tasks while maintaining balanced recognition accuracy and computational efficiency. Zhao et al. [13] presented an efficient

combination of Transformer and convolutional networks that achieved 82.9% accuracy in classroom behavior recognition. Although this method improved recognition capability through local temporal modeling, its ability to model long sequences and complex spatiotemporal interactions fell short of STA-ViT. This demonstrated higher efficiency in processing long videos through comprehensive spatiotemporal feature flow buffers and TPConv modules. Yang et al. [14] proposed a ViT-based behavior recognition method that reduced dependence on large-scale data through data refinement strategies. However, this approach primarily relied on ViT's static feature extraction without fully exploiting temporal information. In comparison, STA-ViT captures spatiotemporal dependencies more comprehensively through the integration of TPConv and spatiotemporal feature flow buffers, exhibiting stronger recognition performance.

Overall, the innovation of STA-ViT in spatiotemporal feature modeling has enabled it to demonstrate remarkable advantages in complex video behavior recognition tasks. By introducing TPConv and spatiotemporal feature flow buffers, STA-ViT can capture temporal dependencies more accurately and handle complex behaviors in long time series. Compared with the existing methods, STA-ViT not only improves the accuracy but also shows better generalization ability and efficiency in various video behavior recognition tasks. Hence, STA-ViT provides an effective direction for future intelligent video analysis.

6 Conclusion

This study proposes a novel video behavior recognition model called SAT-ViT, which combines the ViT architecture with a spatiotemporal self-attention feature flow buffer to enhance accuracy and efficiency in complex video behavior recognition tasks. Based on this model, multiple intervention strategies are further designed to improve learning behavior analysis and intelligent education applications. Experimental validation yields the following conclusions:

(1) Memory optimization and long video processing: Compared to traditional ViT models, SAT-ViT significantly reduces memory usage through its segment-wise backpropagation mechanism, maintaining constant memory requirements that make it particularly suitable for long-sequence video processing. This characteristic gives SAT-ViT distinct advantages when handling large-scale video data, especially for efficient video behavior analysis tasks.

(2) Performance superiority and generalization ability: SAT-ViT demonstrates excellent performance on multiple standard public datasets (including HMDB51, UCF101, and Something-Something V1) and self-collected student learning behavior datasets. The accuracy of Top-1 and Top-5 surpasses existing mainstream models such as ViT, I3D, and TSM. Particularly in complex spatiotemporal feature modeling, SAT-ViT exhibits strong generalization ability to effectively capture temporal and spatial information in videos for more precise behavior recognition. This superior performance indicates that SAT-ViT is applicable to traditional video behavior recognition tasks while holding significant potential for learning behavior analysis in intelligent education and related fields.

(3) Effectiveness of intervention strategies: Based on SAT-ViT's learning behavior recognition capability, three intervention strategies are proposed: real-time feedback mechanisms, personalized learning path planning, and classroom management optimization. Experimental results demonstrate that these intervention strategies effectively enhance student learning efficiency, personalize learning experiences, and optimize classroom management, showing particular application value in intelligent education and distance learning scenarios. Through intelligent learning behavior analysis, educators can adjust teaching strategies in real-time and intervene in student learning processes with greater precision, thus improving educational outcomes.

While the proposed SAT-ViT model demonstrates excellent performance in spatiotemporal feature modeling and learning behavior recognition tasks, certain limitations remain. The model may face challenges when processing extremely complex behavioral patterns, and its adaptability to large-scale datasets requires further improvement. Future research could enhance model performance through multimodal data fusion, architectural optimization, and algorithmic efficiency improvements. SAT-ViT holds broad application prospects across multiple scenarios, particularly in intelligent education, personalized learning path recommendation, and behavior prediction.

References

[1] Mahalakshmi, V., Sandhu, M., Shabaz, M., Keshta, I., Prasad, K. D. V., Kuzieva, N., ... & Soni, M. (2024). Few-shot learning-based human behavior recognition model. *Computers in Human Behavior*, *151*, 108038. https://doi.org/10.1016/j.chb.2023.108038

[2] Mo, J., Zhu, R., Yuan, H., Shou, Z., & Chen, L. (2023). Student behavior recognition based on multitask learning. *Multimedia tools and applications*, *82*(12), 19091-19108. https://doi.org/10.1007/s11042-022-14100-7

[3] Zahid, F. B., Ong, Z. C., Khoo, S. Y., & Salleh, M. F. M. (2021). Inertial sensor based human behavior recognition in modal testing using machine learning approach. *Measurement Science and Technology*, *32*(11), 115905. https://doi.org/10.1088/1361-6501/ac1612

[4] Lin, M., & Gao, J. (2024). Application of MOOC Data Based on Autonomous Intelligent Robot System in Students' Learning Behavior. *Informatica*, *48*(13). https://doi.org/10.31449/inf.v48i13.5828

[5] Cui, Z. (2024). 3D-CNN-based Action Recognition Algorithm for Basketball Players. *Informatica*, *48*(13). https://doi.org/10.31449/inf.v48i13.6100

[6] Parvaiz, A., Khalid, M. A., Zafar, R., Ameer, H., Ali, M., & Fraz, M. M. (2023). Vision Transformers in medical computer vision—A contemplative

retrospection. *Engineering Applications of Artificial Intelligence*, *122*, 106126. https://doi.org/10.1016/j.engappai.2023.106126

[7] Han, K., Wang, Y., Chen, H., Chen, X., Guo, J., Liu, Z., ... & Tao, D. (2022). A survey on vision transformer. *IEEE transactions on pattern analysis and machine intelligence*, *45*(1), 87-110. https://doi.org/10.1109/TPAMI.2022.3152247

[8] Azad, R., Kazerouni, A., Heidari, M., Aghdam, E. K., Molaei, A., Jia, Y., ... & Merhof, D. (2024). Advances in medical image analysis with vision transformers: a comprehensive review. *Medical Image Analysis*, *91*, 103000. https://doi.org/10.1016/j.media.2023.103000

[9] Zhang, H., & Li, Y. (2024). Student Classroom Teaching Behavior Recognition Based on DSCNN Model in Intelligent Campus Education. *Informatica*, *48*(9). https://doi.org/10.31449/inf.v48i9.5755

[10] Yan, X. (2024). Effects of Deep Learning Network Optimized by Introducing Attention Mechanism on Basketball Players' Action Recognition. *Informatica*, *48*(19). https://doi.org/10.31449/inf.v48i19.6188

[11] Azmat, U., Alotaibi, S. S., Abdelhaq, M., Alsufyani, N., Shorfuzzaman, M., Jalal, A., & Park, J. (2023). Aerial insights: Deep learning-based human action recognition in drone imagery. IEEE Access, 11, 83946-83961. August 2023 https://doi.org/10.1109/ACCESS.2023.3302353

[12] Yang, M., Wu, C., Guo, Y., Jiang, R., Zhou, F., Zhang, J., & Yang, Z. (2023). Transformer-based deep learning model and video dataset for unsafe action identification in construction projects. *Automation in Construction*, *146*, 104703. https://doi.org/10.1016/j.autcon.2022.104703

[13] Zhao, J., Zhu, H., & Niu, L. (2023). BiTNet: A lightweight object detection network for real-time classroom behavior recognition with transformer and bi-directional pyramid network. *Journal of King Saud University-Computer and Information Sciences*, *35*(8), 101670. https://doi.org/10.1016/j.jksuci.2023.101670

[14] Yang, J., Zhang, Z., Xiao, S., Ma, S., Li, Y., Lu, W., & Gao, X. (2023). Efficient data-driven behavior identification based on vision transformers for human activity understanding. *Neurocomputing*, *530*, 104-115. https://doi.org/10.1016/j.neucom.2023.01.067

[15] Liu, Z., Wang, Y., Han, K., Zhang, W., Ma, S., & Gao, W. (2021). Post-training quantization for vision transformer. *Advances in Neural Information Processing Systems*, *34*, 28092-28103.

[16] Naseer, M. M., Ranasinghe, K., Khan, S. H., Hayat, M., Shahbaz Khan, F., & Yang, M. H. (2021). Intriguing properties of vision transformers. *Advances in Neural Information Processing Systems*, *34*, 23296-23308.

[17] Xu, Y., Zhang, J., Zhang, Q., & Tao, D. (2022). Vitpose: Simple vision transformer baselines for human pose estimation. *Advances in neural information processing systems*, *35*, 38571-38584.

[18] Al-Hammuri, K., Gebali, F., Kanan, A., & Chelvan, I. T. (2023). Vision transformer architecture and applications in digital health: a tutorial and survey. *Visual computing for industry, biomedicine, and art*, *6*(1), 14. https://doi.org/10.1186/s42492-023-00140-9

[19] Manzari, O. N., Ahmadabadi, H., Kashiani, H., Shokouhi, S. B., & Ayatollahi, A. (2023). MedViT: a robust vision transformer for generalized medical image classification. *Computers in biology and medicine*, *157*, 106791. https://doi.org/10.1016/j.compbiomed.2023.106791

[20] Mazzia, V., Angarano, S., Salvetti, F., Angelini, F., & Chiaberge, M. (2022). Action transformer: A self-attention model for short-time pose-based human action recognition. *Pattern Recognition*, *124*, 108487. https://doi.org/10.1016/j.patcog.2021.108487

[21] Dirgová Luptáková, I., Kubovčík, M., & Pospíchal, J. (2022). Wearable sensor-based human activity recognition with transformer model. *Sensors*, *22*(5), 1911. https://doi.org/10.3390/s22051911

[22] Zhang, J., Jia, Y., Xie, W., & Tu, Z. (2022). Zoom transformer for skeleton-based group activity recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *32*(12), 8646-8659. https://doi.org/10.1109/TCSVT.2022.3193574

[23] Huang, A. Y., Chang, J. W., Yang, A. C., Ogata, H., Li, S. T., Yen, R. X., & Yang, S. J. (2023). Personalized intervention based on the early prediction of at-risk students to improve their learning performance. *Educational Technology & Society*, *26*(4), 69-89. https://doi.org/10.30191/ETS.202310_26(4).0005

[24] Zhou, Y., Ye, X., & Liu, Y. (2022). The influence of personalized learning intervention system on student learning a study of junior middle school. *Interactive Technology and Smart Education*, *19*(4), 441-459. https://doi.org/10.1108/ITSE-10-2021-0192

Appendix

The hyperparameter settings used for the ViT, TDN, TEA, TSM, and I3D models in the experiment are detailed in Table 7:

Table 7: The hyperparameter settings of different models

Model	**Learning rate**	**Batch size**	**Optimizer**	**Training epochs**	**Other parameters**
ViT	1e-4	32	AdamW	50	Weight decay: 1e-2; Momentum: 0.9; Learning rate scheduler: Cosine.
TDN	1e-3	16	Adam	50	Weight decay:

					0.1, decaying every 10 epochs
TEA	5e-5	32	AdamW	80	Weight decay: 1e-5; Momentum: 0.9; Learning rate scheduler: Cosine
TSM	1e-3	16	SGD	30	Momentum= 0.9. The learning rate decay is halved every 5 epochs.
I3D	1e-4	16	AdamW	50	Weight decay: 1e-4; Momentum: 0.9; Learning rate scheduler: Cosine

LSTM and CNN-Based Detection of AI-Generated Classical Music From MIDI Features

Maecyntha Irelynn Tantra, Arya Wicaksana*
Department of Informatics, Universitas Multimedia Nusantara, Tangerang 15810, Banten, Indonesia
E-mail: maecyntha.irelynn@student.umn.ac.id, arya.wicaksana@umn.ac.id
*Corresponding author

Keywords: AI-generated music, Bach, classic music, CNN, detection, LSTM, MIDI

Received: April 2, 2025

Detecting AI-generated classical music is a growing challenge as artificial intelligence continues to improve its ability to compose pieces that closely resemble human compositions. This study explores the use of deep learning methods like LSTM and CNN to classify whether a set of classical music is generated by AI or humans. The classification is based on sequential features extracted from MIDI files using beat-based segmentation, capturing statistical data of pitch, velocity, and duration over segments. The model was trained on a dataset comprising both AI-generated and human compositions, incorporating fine-tuning for optimal performance. Experimental results demonstrate that the proposed LSTM-based model achieves 99.00% accuracy on the primary test set, with an additional evaluation on an auxiliary dataset yielding 98.70% accuracy, confirming its reliability and strong generalization ability. Meanwhile, the CNN-based model attains accuracy scores of 97.00% and 97.10% on the primary and auxiliary datasets, respectively. Evaluation using confusion matrices and classification reports further validate both models' effectiveness, showing minimal misclassification rates. These findings suggest that while both LSTM and CNN achieve high classification performance in detecting AI-generated classical music, LSTM outperforms CNN in classification accuracy. Future research could explore integrating additional musical features or testing the model by expanding the dataset to cover a broader range of compositions, further improving model robustness and applicability.

Povzetek: Raziskava predstavi modela LSTM in CNN za zaznavanje AI-generirane klasične glasbe iz značilk MIDI. LSTM zajema zaporedne vzorce višine, hitrosti in trajanja tonov ter izkazuje odlično splošno zanesljivost.

1 Introduction

In recent decades, as artificial intelligence (AI) has been one of the most significant innovations in the music industry, the growing interest from musicians and computer scientists in AI-based automatic music generation has led to rapid advancements in the field, with major companies actively contributing to its development [1]. This progress has enabled AI to generate musical compositions that mimic the styles of renowned composers while also producing original pieces, as demonstrated in studies related to the Flow Machines project [2]. While this innovation might have brought positive impacts [3], it has also raised concerns among composers and musicians regarding the originality and copyright of musical works, as the existing laws lack clarity on the boundaries of musical originality [4]. These concerns also include potential copyright infringement, its impact on royalties, and the ethical use of AI in music [3], similar to the problems surrounding AI applications in other fields [5], [6].

In addition to the previously mentioned concerns, another challenge is the increasing difficulty of distinguishing between content created by AI and by humans. While this study focuses on music, similar limitations in human judgment have been observed in other creative domains. For example, research on visual artwork found that people tend to evaluate art more positively when they believe it was created by a human, even though all the artworks were generated by AI [7]. This indicates not only that AI-generated content can be indistinguishable from human-made work, but also that perceptions of quality are often shaped by who is believed to be the creator. Similar limitations have been found in other fields, such as text analysis, AI tools like ChatGPT, Gemini, and Llama are becoming increasingly advanced at generating texts, making it more sophisticated to distinguish from human-written content [8]. While numerous studies explore AI-generated content detection in fields such as text analysis and image processing [9], [10], [11], research on detecting AI-generated music remains inadequate.

Since resources and prior research related to AI-generated music detection are still lacking, narrowing the detection scope to a specific genre is a practical starting point, as each genre has its own style. In this study, classical music was chosen as the primary subject as it is one of the fundamental genres, and the fact that most

previous studies on AI-generated music have focused on this genre [12], [13]. As a result, more resources and references are available to support the better identification of AI-generated classical music in this study. Additionally, building on previous findings that humans increasingly struggle to distinguish AI-generated content from human-made works [7], this study proposes an AI based detection approach to improve identification accuracy. Another research has also demonstrated the potential of using deep learning on symbolic music data for generative tasks. For example, a study explored chord progression generation using feature-based neural networks trained on this type of data, reinforcing the relevance of feature extraction and modeling in symbolic music tasks [14].

LSTM (Long Short-Term Memory) is one of the widely used architectures in AI music generation tools due to its ability to process sequential data. LSTM networks are a type of recurrent neural network (RNN) capable of learning and remembering over long sequences, making them particularly effective for tasks involving sequential data, such as rhythm learning and music composition [15]. Fudholi et al., in their research on enhancing classical music composition using LSTM algorithms, demonstrated the model's capability to learn complex musical structures, achieving an accuracy of 91.42% [16]. Although LSTM has primarily been used for music generation, its ability to capture long-term dependencies and recognize sequential patterns makes it a viable architecture for detecting AI-generated music.

CNN (Convolutional Neural Network) has also been studied in music classification tasks due to its ability to extract meaningful patterns from structured data. Unlike LSTM, which excels in modeling temporal relationships, CNN uses spatial hierarchies to identify distinguishing features across different segments of input data [17]. While CNN is often used in audio-based music classification, studies have demonstrated that it is also effective in symbolic music analysis [18], [19]. Given its ability to recognize structural patterns, this study also evaluates a CNN-based approach as an alternative to LSTM for AI-generated classical music detection. Both LSTM and CNN architectures have demonstrated strong performance in domains involving structured and sequential data, such as mental health prediction [20] and symbolic music classification [21] reinforcing their suitability for this detection task. Considering these findings, this study contributes an LSTM-based and CNN-based approaches in detecting AI-generated classical music.

The rest of this paper is structured as follows: Chapter 2 reviews related works; Chapter 3 and 4 introduce the theoretical background of the LSTM and CNN architecture used in this study; Chapter 5 details the proposed methodology; Chapter 6 presents and analyzes the results in the context of this study; Chapter 7 discusses the study results compared to previous related studies; Chapter 8 summarizes the paper with suggestions for future research.

2 Related works

Afchar et al. [22] introduced the first general-purpose AI-generated music detector using audio data, demonstrating its potential with an average detection accuracy of 97.4%. The result was achieved using a basic convolutional model, with the highest accuracy obtained when examining audio represented by amplitude-related features compared to other tested feature types. The study utilized a dataset containing around 25,000 music tracks across 16 genres.

Li et al. [23] compared the stacked LSTM and Bi-LSTM to distinguish AI-generated melodies from human-composed ones by analyzing the MIDI features. While pitch, position, duration, and velocity were initially considered the most critical features of notes, they eventually focused on the first three, as the dataset's velocity values were unfortunately unusable for effective analysis. They trained their models using a dataset sourced from Reddit and evaluated them using data provided by the competition committee. Both of their proposed algorithms secured the top two positions in the competition, with the LSTM model achieving a higher AUC (Area Under the Curve) score of 0.8812.

Deepak et al. [24] proposed an LSTM-based deep learning model to create a system for classifying different genres of music. To train and assess the model, the study used the GTZAN dataset, which comprises 1,000 audio tracks from ten distinct music genres. To efficiently handle the sequential nature of music data, the suggested model was composed of fully connected dense layers after recurrent LSTM layers. After 25 epochs of training, the system achieved an average accuracy of 96.17%.

Kong et al. [25] developed a large-scale MIDI-based composer classification system using Convolutional Recurrent Neural Networks (CRNN). They employed piano, onset, and velocity rolls as input representations to capture various musical features from the MIDI. Utilizing the GiantMIDI-Piano dataset, they evaluated the system's performance on both 10-composer and 100-composer classification tasks using a variety of input feature combinations. The system demonstrated higher accuracy in the 10-composer classification, achieving an average accuracy of 62.02% when evaluated on 30-second clips and an improved accuracy of 69.64% when assessed on entire music pieces.

Table 1: A summary of related works.

Literature	Year	Research Focus	Model	Dataset	Limitation	Average Result	
Afchar et al. [22]	2025	AI-generated music detection using audio data	CNN	25,000 audio tracks	Limited interpretability due to lack of explicit musical features using audio	**Accuracy**	**AUC**
						97.4%	-
Li et al. [23]	2020	Distinguishing AI-generated melodies from human-composed ones	LSTM & BiLSTM	10,000 MIDI files	Excluded velocity from final features due to dataset issues	**Accuracy**	**AUC**
						-	88.12% (LSTM) 80.32% (BiLSTM)
Deepak et al. [24]	2020	Music genre classification using audio data	LSTM	1,000 audio tracks	Used simple note-level inputs without modeling expressive or structural features	**Accuracy**	**AUC**
						96.17%	-
Kong et al. [25]	2020	MIDI-based music composer classification	CRNN	10,854 MIDI files	Relied on fixed-grid input representation, which may misalign with expressive timing	**Accuracy**	**AUC**
						62.02% (30s) 69.64% (full)	-

Compared to these studies, our work differs from previous research by highlighting several notable gaps. Afchar et al. [22] explicitly limited their focus to audio data, leaving symbolic or MIDI-based representations for future exploration. This presents a clear research opportunity in the symbolic domain, where event-level features such as pitch, duration, and velocity can be accessed directly, without being affected by performance or recording conditions. In contrast to Li et al. [23], who excluded velocity due to data limitations, our study retains velocity as a core expressive feature. We omit position, as our beat-based segmentation encodes rhythmic structure more effectively. Unlike Kong et al.'s study [25] which used fixed-grid representation that may misalign with expressive timing, our study adopts a beat-based segmentation approach, which allows features to align more naturally with musical timing and phrasing.

3 LSTM architecture

LSTM (Long Short-Term Memory) used in this study is a popular deep learning algorithm and a variant of Recurrent Neural Networks (RNNs). Unlike traditional regression methods, LSTM was designed to retain information over a lengthy period while discarding irrelevant data [26]. This algorithm is capable of handling sequential or time-related data by capturing both short-term and long-term dependency and modeling the complex, nonlinear relationship between variables. LSTM has also shown high effectiveness in various classification tasks involving time series data, further supporting its applicability in this context [27].Therefore, LSTM is well-suited for this study to learn musical patterns. As previously stated, musical features such as pitch, velocity, and duration can be extracted from MIDI files. By processing these features sequentially, LSTM can learn to identify underlying musical patterns, enabling it to differentiate between AI-generated and human-composed music. Moreover, LSTM is more resilient to missing data, noise, and irregularities without requiring assumption validation or initial hypothesis formulation like statistical methods [28].

Architecturally, LSTM comprises memory cells or cell states that store information over extended periods. Three different gates manage these memory cells, controlling the flow of information within the network, as outlined below [29].

- **Forget Gate** (f_t) controls part of the cell state ought to be forgotten.
- **Input Gate** (i_t) determines the new information to be kept later on.
- **Output Gate** (o_t) decides the output information produced by the cell state by combining the previous knowledge with the filtered new one.

Since cell states in LSTM function as the core component that allows information to flow unchanged, each cell state follows the steps illustrated in Figure 1.

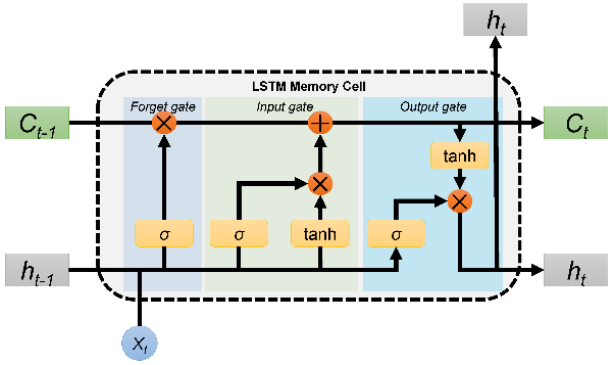


Figure 1: LSTM architecture. Source: [29], [30]

In the LSTM architecture, calculations occur within each gate, where the carried information consists of the previous hidden state (h_{t-1}) and the current input (x_t). First, part of the cell state (C_{t-1}) will go through the forget gate, where a sigmoid function will generate a value between 0 and 1. A value closer to 1 increases the likelihood of retaining the information, while a value closer to 0 increases the likelihood of discarding it. Next, the sigmoid layer of the input gate determines which information to update, followed by a tangent hyperbolic ($tanh$) layer that outputs a candidate vector for the cell state. Cell state (C_t) will then be updated by combining existing knowledge retained by the forget gate and new information selected by the input gate. Finally, the sigmoid layer of the output gate will decide which part of the cell state will be passed as the new hidden state (h_t) for the next step in the network.

4 CNN architecture

CNN (Convolutional Neural Networks) offers an alternative approach to sequence modeling compared to LSTM. While LSTM excels at capturing long-term dependencies in sequential data, CNN focuses on learning local patterns through hierarchical feature extraction [31]. In music analysis, CNN can effectively identify structural patterns in symbolic music. By applying convolutional filters to MIDI features, CNN might be able to extract meaningful representations without relying on recurrent connections.

Basic CNN model structure consists of a convolution layer, activation layer, pooling layer, and fully connected layer as shown in Figure 2.

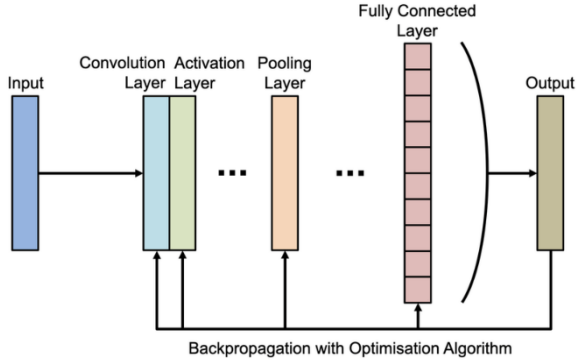


Figure 2: CNN architecture. Source: [32].

To extract feature maps, the first layer, known as the convolution layer, convolves the input pictures. There are some types of convolutional layers that are used commonly as listed below [33].

- **Conv 1D** is suitable for one-dimensional sequential data such as text and time-series data.
- **Conv 2D** can be used to process audio and image applications.
- **Conv 3D** is generally used for video and volumetric data.

After the convolution operation extracts spatial patterns, the activation layer then adds non-linearity to these feature maps, allowing the network to learn complex, non-linear classifiers for the input data. Some of the commonly used activation functions are ReLU (Rectified Linear Unit), sigmoid, and *tanh*. The feature maps are then abstracted by the pooling layer, which also modifies their dimensions as needed. Lastly, the fully connected layer performs classification using data gathered from the pooling and convolution layers.

5 Methodology

5.1 Data collection

The data collection involved gathering musical pieces from Hugging Face [34], JS Fake Chorales [35], and the Bach Doodle dataset from Magenta [36]. Only compositions by J.S. Bach were selected, as most publicly available AI-generated classical music datasets are based on his style. This ensures stylistic consistency, allowing the model to learn to detect music in the same style. The first two datasets were provided in MIDI format, while the Bach Doodle dataset is divided into 192 shards (000-191), each representing a separate shard of the overall dataset and can be downloaded via links. These shards enable researchers to download specific portions rather than the entire collection, improving data management efficiency. The Bach Doodle dataset was available in JSONL format, storing MIDI information as its values.

In total, 5,000 samples were collected, maintaining a balanced 50:50 ratio between AI-generated and human-composed pieces Specifically, two shards (e.g., 003 and 075) from the Bach Doodle dataset were randomly selected, and 2,000 samples were extracted from each shard. To complete the dataset, another 500 samples were collected from the Hugging Face MIDI dataset and 500 from the JS Fake dataset, resulting in a diverse and balanced collection.

Additionally, an auxiliary dataset was collected from two randomly selected shards of the Bach Doodle dataset that were not used in the primary dataset. This ensured that there was no overlap between the primary and auxiliary sets. Then, 500 samples were selected from each shard. In total, the auxiliary dataset consisted of 1,000 samples, with an equal proportion of AI-generated and human-composed music to maintain a balanced distribution.

5.2 MIDI feature extraction

Extracting the features of all the data required different approaches, as there are two types of file formats.

Although some data was not in MIDI format, its values contained MIDI-related information, allowing for a similar and more efficient feature extraction process. To ensure that the music features could serve as meaningful input for the model, the data was divided into multiple segments based on beats. The feature extraction process involved the following steps.

- **Beat extraction**
  - For MIDI files, beats were extracted using a predefined library function.
  - For JSONL files, beats were computed based on each note's start and end.
  - The beat list was sorted and deduplicated to maintain temporal order.
- **Beat based segmentation**
  - The number of segments were determined by dividing the total beat count by a predefined 4 beats per segment, that aligns with the common practice in western music [37].
  - For example, a piece with 40 beats would be divided into 10 segments.
- **Feature extraction**
  - Three main features were extracted: pitch, velocity, and duration.
  - For MIDI files, these features were extracted using pretty_midi.
  - For JSONL files, these features were either directly provided as values or calculated when necessary (e.g., duration calculation by subtracting a note's start time from its end time).

As we use pitch, velocity, and duration in this study, so to understand the nature of the dataset, here are the analytics of the global statistics from all data for each feature.

- **Pitch** ranged from 36 to 93, with the mean of 65.77 and standard deviation of 8.39.
- **Velocity** ranged from 24 to 127 with the mean of 95.79 and standard deviation of 10.74.
- **Duration** ranged from 0.0018s to 36.5s with the mean of 0.62s and standard deviation of 0.46s.

These statistical data confirm that all three features carry meaningful variance and are suitable for downstream learning tasks.

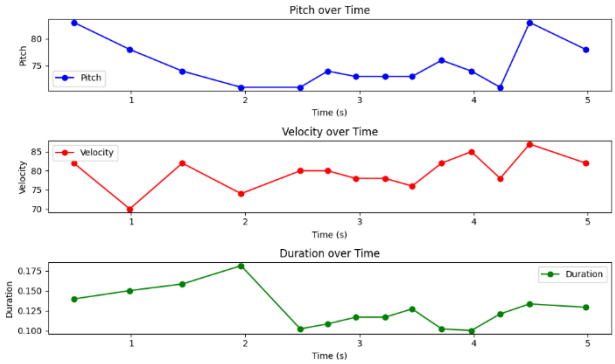


Figure 3: From top to bottom – Pitch, velocity, and duration trends in the first 5 seconds of a MIDI file.

Figure 3 visualizes the features' distribution example of one of the MIDI files over time in the first five seconds. Since these were sequential features, each was further processed to compute its mean, median, and standard deviation, resulting in a total of 9 features per segment. This statistical representation helps capture both the central tendencies and variations in musical patterns. Such statistical summarization methods have been shown to effectively represent musical data in symbolic music analysis tasks [38]. Mean values provide an overall summary of the feature distribution, the median helps mitigate the influence of extreme values, and the standard deviation quantifies the degree of variation within a segment.

5.3 Data pre-processing

The preprocessing process in this study was relatively brief. First, the extracted feature data was split into three sets with a 70:20:10 ratio for the training, validation, and test sets. This proportion was chosen to ensure the model had sufficient data to learn meaningful patterns (3,500 samples) while also allocating enough for validation (1,000 samples) to fine-tune hyperparameters and for testing (500 samples) to evaluate performance. Given the dataset size of 5,000 samples, this split was considered a practical balance between model training and reliable evaluation. After separating the dataset, normalization was applied to standardize the extracted features (pitch, velocity, and duration), as they had different value ranges. While note velocity can often be imbalanced or noisy, this study did not apply explicit outlier removal. Instead, standardization was considered sufficient to reduce the influence of extreme values while preserving expressive dynamics, as the earlier analysis showed a reasonable velocity distribution. Features with zero variance were identified within the training set and ignored from further processing since their values remained constant and did not require normalization. Using a standard scaler, each feature was normalized to have a mean value of 0 and a standard deviation of 1. Finally, the data was reshaped into a 3D format to match the input requirements of the LSTM and CNN architecture, which consists of these data:

- **Samples** – The number of samples.
- **Time steps** – The number of segments in the piece.
- **Features** – The number of features in each time step.

5.4 Model implementation

This study utilized two different models, one based on LSTM and the other on CNN.

5.4.1 LSTM base model

The LSTM-based model consists of four different layers, including the input, LSTM, dropout, and dense layers. Then to lessen overfitting, L2 regularization, often referred to as the Ridge penalty, was also applied to the LSTM and dense layers. L2 regularization encourages the model to control extreme weight values by penalizing the

loss function when the weights get too large. By maintaining smaller and well-balanced weights, the model reduces dependence on specific features, enhancing its generalization ability and reducing overfitting.

The number of hidden units in the LSTM layer, dropout rate, and other architectural parameters were optimized through hyperparameter tuning. The search ranges and selected values are detailed in the hyperparameter tuning section.

5.4.2 CNN base model

While a basic CNN model typically consists of four main layers, the CNN-based model used in this study extends this structure to include six layers to improve performance and generalization. These six layers are input, Conv1D, MaxPooling1D, flatten, dropout, and dense.

The input layer serves as the entry point for the segmented sequential data. Then, by employing ReLU activation to extract local patterns, the Conv1D layer helps the model learn complicated features effectively while avoiding the vanishing gradient issue. MaxPooling1D then downsamples the feature maps, reducing computational complexity and preserving essential information. The Flatten layer then converts the pooled feature maps into a one-dimensional vector, preparing the data for the fully connected layers. L2 regularization is then applied in the convolutional and dense layers to prevent overfitting. The dropout layer improves generalization by randomly deactivating neurons. Lastly, the dense layer with sigmoid activation classifies classical music as AI-generated or human-generated.

The specific architectural parameters such as the number of filters, kernel size, dropout rate, and L2 regularization strength were not fixed but optimized using a hyperparameter tuning process. The selected values and their respective search ranges are detailed in the hyperparameter tuning section.

5.5 Hyperparameter tuning

The training phase involved fine-tuning by utilizing different hyperparameter combinations. But first, to find the ideal hyperparameter configuration for the model, hyperparameter tuning was done using the training set. Hyperparameter tweaking by hand is a laborious, costly, and time-consuming process. Thus, this study used an automated approach offered by Keras Tuner, which is Bayesian Optimization. This hyperparameter tuning algorithm utilizes a probabilistic function to learn from past outcomes, allowing it to forecast and determine the next hyperparameter combination that is most likely to achieve optimal performance.

Here, a multi-objective hyperparameter tuning approach was employed to optimize two key metrics: minimizing validation loss to reduce overfitting and maximizing validation accuracy to enhance model accuracy. Although these goals can sometimes conflict, with improvements in one not always leading to improvements in the other, the tuning process aimed to find a balanced trade-off. Each trial was evaluated based on a combined consideration of both metrics, rather than optimizing one in isolation. The model that achieved the most favorable balance between validation loss and accuracy was selected as the optimal configuration for further training. Before the tuning process began, 25 initial trials were conducted randomly to establish a baseline for Bayesian Optimization. These initial trials provided the algorithm with preliminary insights, enabling it to make more informed predictions in subsequent iterations. The hyperparameter tuning process itself was limited to 25 trials, as Bayesian Optimization efficiently learns from past results, reducing the need for extensive experimentation and conserving computational resources.

During hyperparameter tuning, each trial was set to run for up to 80 epochs. To prevent unnecessary computations and overfitting, early stopping was implemented, allowing training to halt at the optimal epoch. This early stopping strategy is based on validation loss, which serves as the main indicator for deciding when to end training. Although both validation loss and validation accuracy are monitored throughout the process, only the validation loss is used to trigger early stopping. This ensures that the model continues to improve in generalization and avoids overfitting. The method follows these steps.

1. **Monitoring**
   Validation loss were tracked starting from at least three epochs.
2. **Best checkpoint**
   - Once the epoch with the lowest validation loss is identified, training continues for three additional epochs.
   - If no improvement occurs, the model reverts to the best checkpoint and stops.
   - If a better epoch is found, the process resets, extending evaluation by another three epochs.
3. **Repetition**
   The cycle repeats until no further improvements are observed, ensuring optimal performance.

The best-performing model and its corresponding hyperparameter configuration are stored. Tables 2 and 3 present the hyperparameter attributes, ranges, and optimal values identified through the tuning process for each model. The selected hyperparameter ranges, such as the number of units, dropout rates, and kernel sizes, were based on common practices reported in some prior studies across similar domains, ensuring a balanced search space without overly complicating the tuning process.

Table 2: LSTM hyperparameter tuning results.

Hyperparameter	Range	Best value
lstm_units	[16, 32, 64]	64
lstm_regularizer	0.005 - 0.05	0.015
dropout_rate	0.1 – 0.5	0.4
dense_regularizer	0.005 - 0.05	0.01
optimizer	[adam, rmsprop]	rmsprop
batch_size	[32, 64]	32

Table 3: CNN hyperparameter tuning results.

Hyperparameter	Range	Best value
filters	[16, 32, 64]	64
kernel_size	[3, 5]	3
cnn_regularizer	0.005 - 0.05	0.005
dropout_rate	0.1 – 0.5	0.2
dense_regularizer	0.005 - 0.05	0.005
optimizer	[adam, rmsprop]	adam
batch_size	[32, 64]	32

5.6 Fine-Tuning

Following the hyperparameter tuning process, the best-performing model from the optimal trial has been selected as the base model. Fine-tuning was then performed to further enhance the model's generalization performance on unseen data using the prepared validation set for monitoring. Unlike hyperparameter tuning, which explores multiple configurations, fine-tuning focuses on refining the training of the selected model while preserving its architecture. The number of epochs was reduced to 30 based on insights from the tuning stage, where top-performing models consistently achieved their best results by around the 30th epoch. This reduction helps prevent overfitting and streamlines training without compromising performance. The batch size used matched the optimal value identified during tuning. Early stopping was also applied to monitor validation loss and halt training when no further improvement was observed. These focused adjustments allowed the model to converge more effectively using the best available settings, enhancing performance while minimizing overfitting risk.

5.7 Implementation and replication details

To support reproducibility and ensure that the experiments can be replicated by other researchers, this section outlines the software environment, core libraries, dataset sources, and code availability. All experiments were conducted on Google Colab's cloud computing platform, which provided a 2-core Intel(R) Xeon(R) CPU @ 2.20GHz and 13.61 GB of RAM. This configuration was sufficient for training and evaluating the deep learning models used in this study.

The models were implemented using the following Python libraries and tools.

- NumPy v2.0.2
- Pandas v2.2.2
- Matplotlib v3.10.0
- TensorFlow v2.18.0
- Keras v3.8.0
- Keras Tuner v1.4.7
- Scikit-learn v1.6.1
- pretty_midi v0.2.10

The dataset used in this study was compiled from the following publicly available sources.

- Hugging Face dataset [34]: https://huggingface.co/datasets/drengskapur/midi-classical-music
- JS Fake Chorales dataset [35]: https://github.com/omarperacha/js-fakes
- Bach Doodle dataset by Magenta [36]: https://magenta.tensorflow.org/datasets/bach-doodle

All preprocessing scripts, model training pipelines, and hyperparameter tuning configurations are available in the accompanying code repository https://github.com/maecyntha/ai-classical-music-detector.

5.8 Evaluation

In this study, the model was evaluated by using it to make predictions on the test set that was previously split during data preparation. A confusion matrix was then used to further analyze its performance. To validate the model reliability, it was also further tested on an auxiliary test set consisting of 1,000 samples from a different dataset. The confusion matrix for this auxiliary test set was also examined to assess the model's generalization ability.

6 Results and analysis

After undergoing multiple stages of processing, the following section presents a detailed analysis of the results—beginning with hyperparameter tuning, followed by fine-tuning, and concluding with the final evaluation. The performance results are organized into two subsections, each focusing separately on the LSTM and CNN models, followed by a final subsection that compares the performance of both models.

6.1 LSTM model performance

This subsection presents the performance analysis of the LSTM model, covering hyperparameter tuning, fine-tuning, and final evaluation.

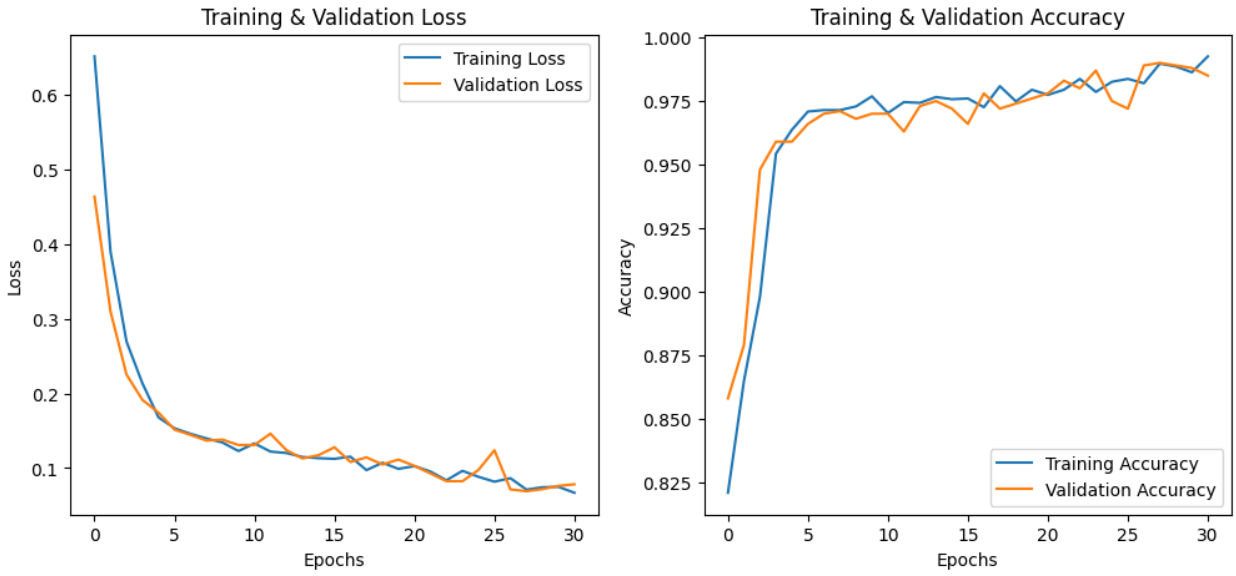


Figure 4: LSTM-based training & validation loss (left) and accuracy (right) over epochs.

Figure 4 illustrates the patterns in training and validation accuracy and loss throughout 31 epochs using LSTM-based model. As can be seen in the left plot, both curves exhibit a downward trend, indicating that the model progressively improves its predictions as training progresses, resulting in a lower loss. Despite minor fluctuations in validation loss, its close alignment with training loss suggests minimal overfitting. On the other hand, the right plot, representing the accuracy trends, demonstrates a consistent increase in accuracy, with a sharp rise between epochs 5 and 10 before stabilizing around 97%–98%. This indicates that the model learns effectively in the early stages and refines its predictions as training progresses. The overall results confirm that the chosen hyperparameters facilitate efficient learning, as reflected in the significant early improvements, stable high accuracy, and consistent reduction in loss. The lack of a widening gap between training and validation metrics suggests the model generalizes well, maintaining robust performance on unseen validation data.

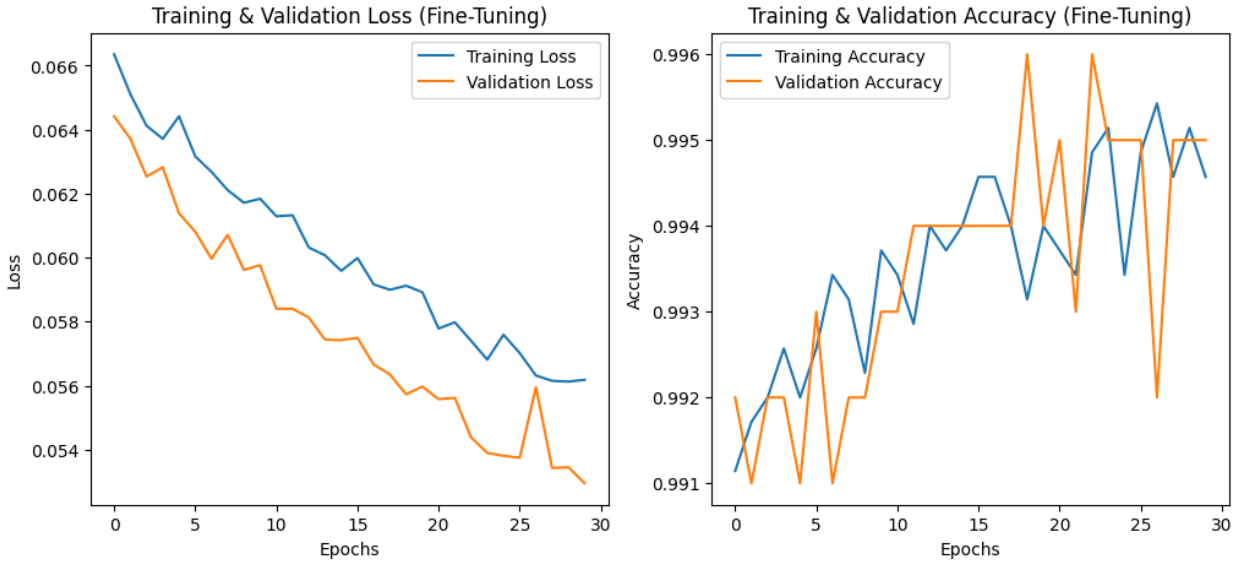


Figure 5: Fine-tuned LSTM-based training & validation loss (left) and accuracy (right) over epochs.

Figure 5 presents the performance of the fine-tuned model. In the left plot, which depicts training and validation loss, both losses continue to decrease steadily over 30 epochs. However, unlike the previous training phase during hyperparameter tuning, the two curves are not always closely aligned, suggesting slight discrepancies between the model's performance on training and validation data. Despite this, the overall downward trend indicates effective fine-tuning without severe overfitting. Meanwhile, the right plot, showing training and validation accuracy, exhibits noticeable fluctuations, particularly in validation accuracy, which sometimes spikes or drops significantly. This variability suggests sensitivity to different validation batches. However, the general trend remains consistent with the training accuracy, maintaining a high range between 99.1% and 99.6%. These results

indicate that while fine-tuning enhances model performance, it introduces slight instability in validation accuracy. Nonetheless, the model maintains strong generalization, as reflected in the stable accuracy levels and continuous reduction in loss.

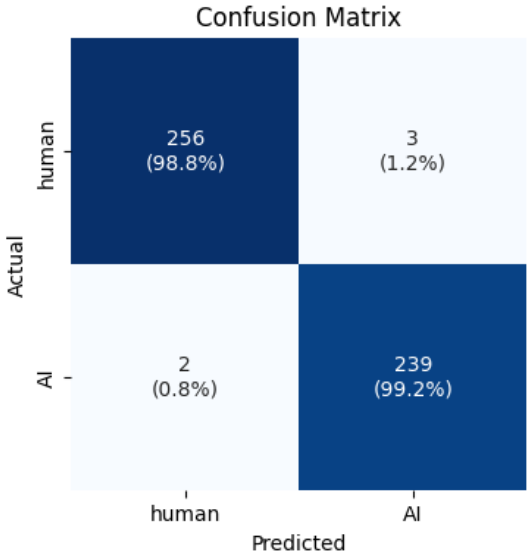


Figure 6: Confusion matrix of the LSTM-based model's predictions on the test set.

The model was then subsequently assessed using a specific test set prepared beforehand. The confusion matrix in Figure 6 illustrates that the model has a minimum number of false positives and false negatives, indicating strong predictive accuracy. This is further supported by the classification report, where the precision of 99.22% reflects the model's ability to make highly accurate predictions for both categories. A recall score of 99.01% confirms its effectiveness in minimizing false negatives. Furthermore, the F1 score and overall accuracy of 99.00% demonstrate a well-balanced performance between precision and recall, ensuring reliable classification of both human and AI-generated compositions.

To statistically validate this performance, a one-sided proportion z-test was conducted to evaluate whether the model's accuracy of 99.00% was significantly better than random guessing (50%). The resulting z-score was approximately 69.296, with a p-value of less than 0.00001. Since the p-value is far below the commonly accepted significance level of 0.05, we can confidently reject the null hypothesis and conclude that the model's accuracy is statistically and significantly better than random classification. The entire training and validation process took approximately 21 minutes to complete.

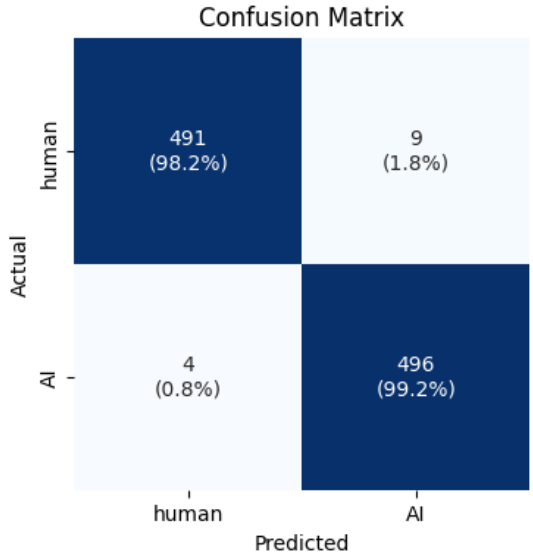


Figure 7: Confusion matrix of the LSTM-based model's predictions on the auxiliary test set.

The model was further validated using an auxiliary test set of 1,000 samples from a different dataset to assess its reliability. As shown in Figure 7, the confusion matrix reveals misclassification rates of 1.8% for human compositions and 0.8% for AI-generated compositions. With an overall accuracy of 98.70%, the model also achieves 98.70% in precision, recall, and F1 score, indicating a well-balanced performance. These results confirm that the model generalizes effectively to unseen data, maintaining high accuracy while minimizing errors, further reinforcing its reliability in distinguishing between human and AI-generated classical music.

6.2 CNN model performance

This subsection provides the performance analysis of the CNN model, following the same evaluation stages as the LSTM model, from hyperparameter tuning to final evaluation.

Figure 8: CNN-based training & validation loss (left) and accuracy (right) over epochs.

Figure 8 shows the CNN-based model's training and validation results across 31 epochs. The left plot shows a steady decline in training and validation loss, dropping from approximately 0.45 to below 0.20, indicating effective learning. Despite minor fluctuations, the validation loss remains closely aligned with the training loss, suggesting minimal overfitting. The plot on the right shows a steady rise in accuracy, improving quickly in the early epochs before leveling off at about 96% in the later phases. The consistent gap between training and validation accuracy further supports the model's strong generalization. These outcomes demonstrate how well the selected hyperparameters optimize the CNN model's learning process.

Figure 9: Fine-tuned CNN-based training & validation loss (left) and accuracy (right) over epochs.

Figure 9 illustrates the CNN model's performance during fine-tuning over five epochs. While validation loss stays comparatively constant at 0.1645, suggesting little improvement, training loss varies but tends to decline, as seen in the left plot.

On the other hand, the right plot reveals significant accuracy variations, especially in validation accuracy, which momentarily declines at epoch 2 before leveling off at about 96.7%. These fluctuations imply that the model is sensitive to minor tweaks during fine-tuning.

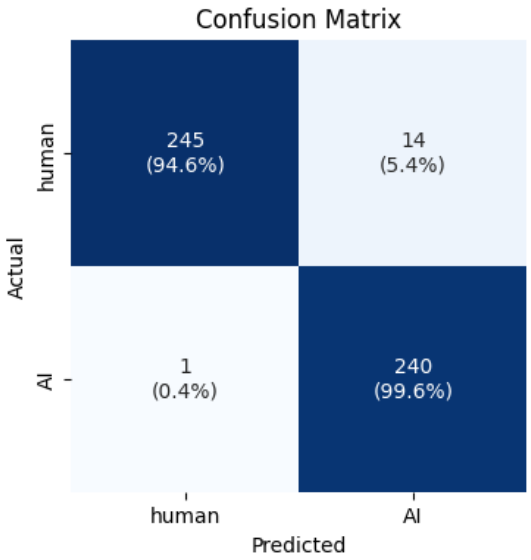


Figure 10: Confusion matrix of the CNN-based model's predictions on the test set.

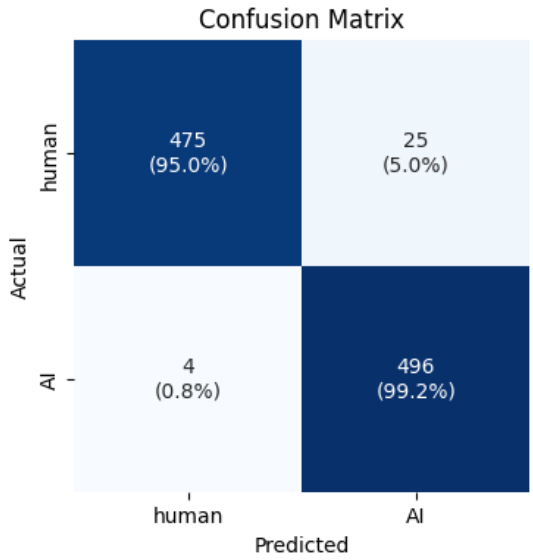


Figure 11: Confusion matrix of the CNN-based model's predictions on the auxiliary test set.

Figure 10 displays the confusion matrix of the CNN model on the primary test set. With a high prediction accuracy, the model correctly identifies most examples; however, it misidentifies 14 human compositions as AI-generated and one AI-generated composition as human. With a precision of 97.04% and a recall of 97.09%, the model demonstrates a balanced ability to differentiate the two groups. The model's durability in maintaining good classification performance is demonstrated by its 97.00% overall accuracy and F1 score.

To confirm that the CNN model's 97.00% accuracy wasn't due to random chance, we performed a one-sided proportion z-test against a 50% baseline representing random guessing. The test returned a z-score of approximately 66.468 and a p-value far below 0.00001. Since this p-value is well below the standard threshold of 0.05, we rejected the null hypothesis, showing that the CNN model's performance is statistically significant. The complete model training and validation ran for approximately six minutes.

The confusion matrix for the CNN model that was evaluated using the extra dataset is shown in Figure 11. Despite misclassifying some pieces, the model continues to exhibit good classification performance. The model achieves an overall accuracy of 97.10%, with a precision of 97.18%, a recall score of 97.10%, and an F1 score of 97.10%. These findings support the model's high reliability in distinguishing compositions created by humans and AI, as well as its capacity to generalize fresh data.

6.3 Comparative analysis

To provide a clearer comparison, Table 4 presents the classification performance of the LSTM and CNN models on the primary dataset. The LSTM model outperforms CNN in every metrics, with an accuracy of 99.00% as opposed to 97.00% for CNN. Additionally, LSTM retains a higher F1 score due to its superior precision and recall compared to CNN's.

These results indicate that while both models perform well, the LSTM model demonstrates superior classification capability, likely due to its ability to capture long-term dependencies in sequential data, which is crucial for distinguishing between AI-generated and human-generated classical music.

Table 4: Comparison of classification performance metrics between LSTM and CNN.

Model	Accuracy	Precision	Recall	F1 Score
LSTM	99.00%	99.22%	99.01%	99.00%
CNN	97.00%	97.04%	97.09%	97.00%

7 Discussion

In this study, we achieve higher classification accuracy compared to previous works. Our first finding reinforces the effectiveness of LSTM-based models in capturing sequential dependencies in musical compositions. LSTM-based models are particularly well-suited for symbolic music analysis because they are designed to model temporal dependencies over long sequences. This aligns with the nature of symbolic music, where patterns unfold over time and require memory of prior context. In contrast, CNN primarily focuses on capturing local patterns through convolutional filters and may struggle to retain the broader sequential context necessary for interpreting compositional flow, especially in music where long-range structure and phrasing are key to stylistic identity.

Previously, Li et al. [23] have also proved that LSTMs effectively distinguish AI-generated melodies from human compositions, achieving high classification performance despite ignoring velocity due to dataset limitation. On the other hand, our approach includes velocity alongside pitch and duration, resulting in a more comprehensive representation of musical expression. This richer feature set appears to improve the model's ability to

distinguish AI-generated classical music from that composed by humans.

Other than feature selection, our approach also differs in the representation of musical structures. Kong et al. [25] used piano rolls which rely on fixed time grids that divide time into uniform intervals regardless of the underlying musical context. This can lead to a misalignment between the grid and expressive timing in performances, especially when dealing with tempo changes, or uneven note spacing. On the other hand, our study uses beat-based segmentation which groups events based on musical beats rather than uniform time slices. This approach aligns more naturally with the timing and phrasing of music, allowing for a more accurate capture of rhythmic and expressive characteristics. As a result, it better preserves sequential dependencies that are important for classification, which may be blurred in fixed-grid representations.

Furthermore, while studies such as Deepak et al. [24] have explored deep learning models for symbolic music classification, our results indicate that temporal modeling remains crucial when the goal is to detect AI-generated classical music. The strong performance of our model emphasizes the significance of capturing long-term dependencies in musical sequences.

The CNN-based model utilized in this study aligns with the work of Afchar et al. [22], who used convolutional networks for AI-generated music recognition. However, whereas their study focused on amplitude-related audio features, our study, which focuses on symbolic music analysis using MIDI data, achieves higher accuracy. This distinction illustrates an intriguing difference between the two approaches: audio-based methods capture performance characteristics and timbral properties, whereas symbolic music analysis separates compositional structures, eliminating variations caused by recording conditions. Despite these differences, our CNN model produces competitive results, indicating that convolutional networks can effectively learn differentiating patterns from structured symbolic representations.

These findings from both LSTM and CNN models suggest that other than the choice of model architecture, the way musical data is structured and represented significantly impacts the effectiveness of AI-generated classical music detection.

8 Conclusion

In this study, a detection system made to distinguish AI-generated and human-generated classical music was successfully approached using LSTM and CNN algorithms. Through the experimental analysis, it was observed that both models demonstrated strong classification performance by achieving high accuracy, precision, recall, and F1 scores across multiple test sets. However, the results shows that LSTM performs better than CNN with minimal misclassification rates, indicating that the model is capable of effectively differentiating between the two composition types. This shows LSTM's superior ability to capture sequential dependencies, which is crucial in this detection task. Further validation on an auxiliary test set, which maintained a high level of accuracy, confirmed its robustness, suggesting strong generalization to unseen data.

Despite these promising results, some limitations remain. We acknowledge that training the model on a dataset representing only a single compositional style, specifically the works of J.S. Bach, may introduce potential bias and limit the model's generalizability to broader musical genres. Additionally, the dataset used in this study may not fully capture the diversity of musical styles and compositions, potentially limiting generalizability to more complex or unconventional pieces. To address these limitations, future research could expand the dataset to include compositions from a wider range of composers or styles. For improved robustness, incorporating AI-generated music that emulates contemporary, jazz, or pop artists may help capture cross-genre characteristics. Furthermore, integrating more advanced musical attributes, including harmonic, timbral, and structural features, may also refine classification performance further. Eventually, these improvements would enhance the model's versatility and reliability, paving the way for more comprehensive AI-driven music classification. Finally, while ROC curves and AUC scores were not included in this study due to the absence of probability outputs, future models with probabilistic predictions could leverage these tools for more nuanced performance evaluation.

Acknowledgement

The authors acknowledge the support of Universitas Multimedia Nusantara for this study and appreciate the constructive feedback provided by the reviewers and editors, which significantly contributed to improving the quality of this paper.

References

[1] M. Civit, J. Civit-Masot, F. Cuadrado, and M. J. Escalona, "A systematic review of artificial intelligence-based music generation: Scope, applications, and future trends," *Expert Syst Appl*, vol. 209, p. 118190, Dec. 2022, doi: https://doi.org/10.1016/j.eswa.2022.118190.

[2] F. Pachet, P. Roy, and B. Carré, "Assisted Music Creation with Flow Machines: Towards New Categories of New," in *Handbook of Artificial Intelligence for Music*, Cham: Springer International Publishing, 2021, pp. 485–520. doi: 10.1007/978-3-030-72116-9_18.

[3] M. Fox, G. Vaidyanathan, and J. Breese, "THE IMPACT OF ARTIFICIAL INTELLIGENCE ON MUSICIANS," *Issues In Information Systems*, vol. 25, no. 3, pp. 267–276, 2024, doi: 10.48009/3_iis_2024_121.

[4] P. Jurcys and M. Fenwick, "Originality and the Future of Copyright in an Age of Generative AI," *Computer Law & Security Review*, Sep. 2023.

[5] N. Lucchi, "ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence

Systems," *European Journal of Risk Regulation*, vol. 15, no. 3, pp. 602–624, Sep. 2024, doi: 10.1017/err.2023.59.

[6] E. Bonadio and L. Mcdonagh, "Artificial intelligence as producer and consumer of copyright works: evaluating the consequences of algorithmic creativity," pp. 112–137, Jun. 2020, [Online]. Available: https://ssrn.com/abstract=3617197

[7] L. Bellaiche *et al.*, "Humans versus AI: whether and why we prefer human-created compared to AI-created artwork," *Cogn Res Princ Implic*, vol. 8, no. 1, p. 42, Jul. 2023, doi: 10.1186/s41235-023-00499-6.

[8] A. M. Elkhatat, K. Elsaid, and S. Almeer, "Evaluating the efficacy of AI content detection tools in differentiating between human and AI-generated text," *International Journal for Educational Integrity*, vol. 19, no. 1, p. 17, Sep. 2023, doi: 10.1007/s40979-023-00140-5.

[9] A. Akram, "An Empirical Study of AI Generated Text Detection Tools," *Advances in Machine Learning & Artificial Intelligence*, vol. 4, no. 2, pp. 44–55, Oct. 2023, doi: 10.33140/AMLAI.

[10] R. and S. R. S. and D. G. P. and B. N. and S. S. Tiwari Shreeji and Sharma, "Detecting AI Generated Content: A Study of Methods and Applications," in *Proceedings of International Conference on Communication and Computational Technologies*, S. and G. R. and P. S. D. Kumar Sandeep and Hiranwal, Ed., Singapore: Springer Nature Singapore, 2024, pp. 161–176. doi: 10.1007/978-981-97-7423-4_13.

[11] J. J. Bird and A. Lotfi, "CIFAKE: Image Classification and Explainable Identification of AI-Generated Synthetic Images," *IEEE Access*, vol. 12, pp. 15642–15650, 2024, doi: 10.1109/ACCESS.2024.3356122.

[12] P. Tiwari and S. Jha, "Music Generation with Long Short-Term Memory Networks from MIDI Data of Classical Music," in *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, 2024, pp. 1–4. doi: 10.1109/ICITEICS61368.2024.10625468.

[13] G. G. N. S and V. V. P. D, "Generating Creative Classical Music by Learning and Combining Existing Styles," in *2023 4th International Conference on Communication, Computing and Industry 6.0 (C216)*, 2023, pp. 1–7. doi: 10.1109/C2I659362.2023.10431294.

[14] M. Zhu, "Research on Chord Generation in Automated Music Composition Using Deep Learning Algorithms," *Informatica*, vol. 47, no. 8, Sep. 2023, doi: 10.31449/inf.v47i8.4885.

[15] F. Shah, T. Naik, and N. Vyas, "LSTM Based Music Generation," in *2019 International Conference on Machine Learning and Data Engineering (iCMLDE)*, 2019, pp. 48–53. doi: 10.1109/iCMLDE49015.2019.00020.

[16] D. R. Fudholi, D. N. A. Putri, R. B. M. A. A. Wijaya, J. E. Kusnadi, and J. C. Amarissa, "The Application of LSTM in the AI-Based Enhancement of Classical Compositions," *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, vol. 7, no. 1, pp. 107–117, Nov. 2024, doi: 10.20895/INISTA.V7I1.1628.

[17] M. Ahmad, M. Mazzara, and S. Distefano, "Regularized CNN Feature Hierarchy for Hyperspectral Image Classification," *Remote Sens (Basel)*, vol. 13, no. 12, 2021, doi: 10.3390/rs13122275.

[18] E. Dervakos, N. Kotsani, and G. Stamou, "Genre Recognition from Symbolic Music with CNNs: Performance and Explainability," *SN Comput Sci*, vol. 4, no. 2, p. 106, 2022, doi: 10.1007/s42979-022-01490-6.

[19] F. Simonetta, C. E. Cancino-Chacón, S. Ntalampiras, and G. Widmer, "A Convolutional Approach to Melody Line Identification in Symbolic Scores ," in *Proceedings of the 20th International Society for Music Information Retrieval Conference* , ISMIR, Nov. 2019, pp. 924–931. doi: 10.5281/zenodo.3527966.

[20] L. Pan and H. Ma, "A Computational CNN-LSTM-Based Mental Health Consultation System in a College Environment," *Informatica*, vol. 49, no. 10, Jan. 2025, doi: 10.31449/inf.v49i10.7136.

[21] I. A. Abdulmajeed and I. M. Husien, "MLIDS22-IDS Design by Applying Hybrid CNN-LSTM model on Mixed-Datasets," *Informatica*, vol. 46, no. 8, Nov. 2022, doi: 10.31449/inf.v46i8.4348.

[22] D. Afchar, G. Meseguer-Brocal, and R. Hennequin, "AI-Generated Music Detection and its Challenges," in *ICASSP 2025 - 2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2025, pp. 1–5. doi: 10.1109/ICASSP49660.2025.10890655.

[23] Y. Li and Z. Lin, "Melody Classifier with Stacked-LSTM," Oct. 2020.

[24] S. Deepak and B. G. Prasad, "Music Classification based on Genre using LSTM," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, pp. 985–991. doi: 10.1109/ICIRCA48905.2020.9182850.

[25] Q. Kong, K. Choi, and Y. Wang, "Large-Scale MIDI-based Composer Classification," Oct. 2020.

[26] N. Shenvi and H. Virani, "Forecasting of Ionospheric Total Electron Content Data Using Multivariate Deep LSTM Model for Different Latitudes and Solar Activity," *Journal of Electrical and Computer Engineering*, vol. 2023, pp. 1–13, May 2023, doi: 10.1155/2023/2855762.

[27] A. Liu, "Multi-genre Digital Music Based on Artificial Intelligence Automation Assisted Composition System," *Informatica*, vol. 48, no. 5, Feb. 2024, doi: 10.31449/inf.v48i5.5474.

[28] X. Jin *et al.*, "Time series forecasting of Valley fever infection in Maricopa County, AZ using

LSTM," *The Lancet Regional Health - Americas*, vol. 43, p. 101010, Mar. 2025, doi: 10.1016/j.lana.2025.101010.

[29] A. Moghar and M. Hamiche, "Stock Market Prediction Using LSTM Recurrent Neural Network," *Procedia Comput Sci*, vol. 170, pp. 1168–1173, 2020, doi: 10.1016/j.procs.2020.03.049.

[30] H. Fan, M. Jiang, L. Xu, H. Zhu, J. Cheng, and J. Jiang, "Comparison of Long Short Term Memory Networks and the Hydrological Model in Runoff Simulation," *Water (Basel)*, vol. 12, no. 1, p. 175, Jan. 2020, doi: 10.3390/w12010175.

[31] Y. Liu, H. Pu, and D.-W. Sun, "Efficient extraction of deep image features using convolutional neural network (CNN) for applications in detecting and analysing complex food matrices," *Trends Food Sci Technol*, vol. 113, pp. 193–204, Jul. 2021, doi: 10.1016/j.tifs.2021.04.042.

[32] S. Lee, J. Kim, H. Kang, D.-Y. Kang, and J. Park, "Genetic Algorithm Based Deep Learning Neural Network Structure and Hyperparameter Optimization," *Applied Sciences*, vol. 11, no. 2, 2021, doi: 10.3390/app11020744.

[33] A. Stamoulakatos *et al.*, "A Comparison of the Performance of 2D and 3D Convolutional Neural Networks for Subsea Survey Video Classification," in *OCEANS 2021: San Diego – Porto*, 2021, pp. 1–10. doi: 10.23919/OCEANS44145.2021.9706125.

[34] Anonymous, "MIDI Classical Music." Accessed: Jan. 16, 2025. [Online]. Available: https://huggingface.co/datasets/drengskapur/midi-classical-music

[35] O. Peracha, "JS Fake Chorales: a Synthetic Dataset of Polyphonic Music with Human Annotation," in *Proceedings of the 2022 Sound and Music Computing Conference, SMC 2022*, 2022. doi: 10.48550/arXiv.2107.10388.

[36] C.-Z. A. Huang, C. Hawthorne, A. R. and M. Dinculescu, J. Wexler, L. Hong, and J. Howcroft, "The Bach Doodle: Approachable music composition with machine learning at scale," in *International Society for Music Information Retrieval (ISMIR)*, 2019. [Online]. Available: https://goo.gl/magenta/bach-doodle-paper

[37] A. Marmoret, J. E. Cohen, and F. Bimbot, "Barwise Music Structure Analysis with the Correlation Block-Matching Segmentation Algorithm," *Transactions of the International Society for Music Information Retrieval*, vol. 6, no. 1, pp. 167–185, Nov. 2023, doi: 10.5334/tismir.167.

[38] L. Jing, "Evolutionary Deep Learning for Sequential Data Processing in Music Education," *Informatica*, vol. 48, no. 8, May 2024, doi: 10.31449/inf.v48i8.5444.

Hybrid Robot Trajectory Planning Using FC-SSA-PID and DWA-Enhanced BIT*Algorithms

Jianjing Zhang, Xiaoru Xing*, Yueqiang Hu, Xia Zhao, Jing Li
Department of Basic Courses, Hebei Institute of Mechanical and Electrical Technology, Xingtai 054000, China
E-mail: wangyichenzhang31@163.com, xingxiaoru586@163.com, 13663199870@163.com, 13613199997@163.com, hbjd20250226@163.com
*Corresponding author

Keywords: proportional-integral-derivative control, batch informed trees, trajectory planning, sparrow search algorithm, fuzzy control, dynamic window approach

Received: March 28, 2025

Planning the movement path of a robot is crucial to ensure it reaches the target area smoothly. Existing methods tend to fall into local optima, have low accuracy in route calculation, and fail to effectively avoid obstacles. To address these issues, this study introduces the Sparrow Search Algorithm and Fuzzy Control, as well as the Dynamic Window Approach, to optimize Proportional-Integral-Derivative control and Batch Informed Trees, respectively. Based on these two optimization algorithms, a robot trajectory planning model is proposed, and its feasibility and reliability are demonstrated through comparative experiments. In standardized 50m ×50m grid environments with 20%-30% obstacle density and dynamic obstacles, 30 independent simulation runs were conducted. Comparative analysis with RRT, Ant Colony Optimization (ACO), and Genetic Algorithm (GA) demonstrates that the proposed model achieves a success rate of 95.5%, a high accuracy rate of 99.4%, and a low accuracy error rate of 0.0011%. The locally optimal route length planned by the model is 12.6m, while the global average optimal route length is reduced to 21.2m, significantly outperforming the comparison models. These findings demonstrate that the proposed model has strong trajectory planning capabilities, minimal error, and shorter routes, enabling the robot to respond correctly to external environments in a timely manner and complete tasks effectively even in complex dynamic conditions.*

Povzetek: Predstavljen je hibridni model načrtovanja poti robotov, ki združuje FC-SSA-PID za prilagodljivo krmiljenje in DWA-izboljšani BIT za globalno ter lokalno načrtovanje. Sistem učinkovito premaguje lokalne optime, zmanjšuje napake, hitro se izogiba oviram.*

1 Introduction

Since the 21st century, robots have gradually entered public life, and their technology has developed rapidly. However, their performance remains less autonomous and adaptive compared to human capabilities [1]. The demand for efficient, safe, and precise robotic movement paths necessitates advanced trajectory planning technology. It serves as the core system for controlling robot motion and is a crucial foundation for enabling robots to complete various tasks. Therefore, optimizing trajectory planning has been a key research focus [2]. Currently, methods such as Genetic Algorithm (GA), Recurrent Neural Network (RNN), and Graph Search Algorithm (GSA) have been applied to trajectory planning [3]. However, these methods suffer from problems such as falling into local optima, poor real-time performance, and weak adaptability to dynamic environments. Therefore, trajectory planning methods requiring enhanced accuracy and stability are essential. Proportional-Integral-Derivative (PID) control adjusts signal parameters through proportional, integral, and derivative control algorithms to achieve precise system output control. It is a mature and stable technique with strong adaptability. Meanwhile, Batch Informed Trees (BIT*) combines the advantages of sampling-based and search-based planning algorithms, allowing it to filter out unimportant information and find optimal routes in complex environments [4-5]. However, traditional PID parameter tuning is time-consuming and lacks precision, while BIT* faces challenges such as computational complexity and low solution quality in high-dimensional problems. To address these limitations, this study introduces the Sparrow Search Algorithm (SSA) and Fuzzy Control (FC), as well as the Dynamic Window Approach (DWA), to optimize PID and BIT*, respectively. Based on these optimizations, a new robot trajectory planning model is proposed. This model is expected to improve robot flexibility and enable intelligent task execution. We aim to investigate whether combining FC-SSA-PID and DWA-BIT*improves trajectory planning performance in dynamic environments compared to other similar technologies.

2 Related work

PID control has been widely applied in various fields requiring precise control systems, including robotics, aircraft, and 3D printing. Therefore, many researchers have conducted in-depth studies on PID control. For example, to address the unpredictable environmental challenges faced by unmanned surface vehicles, Meng J et al. proposed a Gaussian process motion trajectory planning method based on PID. This method introduced an interpolation strategy to increase path selection

Table 1: Summary and comparison table of related work.

Ref.	Method Used	Application Domain	Accuracy (%)	Path efficiency (%)	Runtime complexity
[6]	Gaussian Process + PID + Interpolation	Unmanned Surface Vehicles	85	82	High
[7]	Fractional-order PID Control	Wind Power Simulation System	90.5	87	Medium
[8]	Improved BIT* + Spatial Transform/Mask	Concrete Color Difference Detection	92.1	85	Medium-High
[9]	Self-deforming BIT* Variant	High-arrival-rate Data Streams	95.8	86	Low-Medium
[10]	Improved BIT* + Linear Interpolation	Spinal Puncture 3D Reconstruction	94.3	88	Medium
[11]	Local Chaotic Particle Swarm Optimization	Robotic Arm Trajectory	89.7	85	High
[12]	Dynamic Trajectory Discovery	Multi-Cable-Driven Robots	91.2	78	High
[13]	Hybrid Optimization Algorithm	Industrial Robot Manipulators	87.5	80	Very High
[14]	Model Predictive Control	Robot Motion in Dynamic Environments	88	75	High
[15]	Model-Free Hierarchical Decoupling	Collision Avoidance	90	70	Medium-High

diversity, with experimental results demonstrating effective mitigation of unknown environmental impacts [6]. Gasmi H et al. developed a dual-feedback wind power simulation system based on PID to solve the significant vibration issues in wind power operations. This system utilized fractional-order proportional-integral control to regulate grid power and ensure maximum power operation. The results demonstrated that it reduced grid oscillations while maintaining robust performance [7]. At the same time, BIT* has also been widely applied, particularly in scenarios requiring large-scale data processing. For instance, to address the instability of using ordinary drones for concrete sampling in construction, Yao G et al. proposed a concrete color difference detection model based on an improved BIT*. This model used spatial transformation and mask quantization segmentation operations to achieve block-based color difference encoding, and experimental results showed a detection accuracy of 92.10% [8]. Wang H et al. introduced a self-deforming bitmap algorithm based on BIT* to address the issue of existing solutions being unable to perform online operations on high-arrival-rate data streams. This algorithm automatically adapted the sampling probability for data streams of different sizes and allowed bitmap deformation. Experiments proved that it could efficiently and accurately process high-arrival-rate data streams [9]. In the field of spinal puncture surgery, Zhang W et al. proposed an improved BIT*-based three-dimensional reconstruction system to solve the time-consuming and complex process of determining puncture points and paths. By using a linear interpolation algorithm for 3D reconstruction, the system enabled automatic image scanning and acquisition to quickly locate the optimal puncture point and path [10].

Trajectory planning technology has reached a relatively mature stage in both theoretical research and practical applications, and scholars worldwide have applied various optimization methods in real-world scenarios. For example, to optimize the movement time and trajectory of robotic arms, Du Y et al. proposed a local chaotic particle swarm optimization algorithm based on interpolation functions. This algorithm conducted simulation experiments in joint space, and simulation results demonstrated that it effectively reduced the oscillation amplitude and movement time of the robotic arm, ensuring operational stability [11]. To address the issue of redundant trajectories in multi-cable-driven robots reaching targets without entanglement, Cao M et al. proposed a dynamic trajectory discovery method that evaluates the safety and feasibility of potential paths while reducing inter-robot entanglement. The results demonstrated that this method effectively generated tangle-free dynamic trajectories [12]. To improve robot task execution efficiency, Singh G et al. introduced a robot kinematics analysis and trajectory planning method based on a hybrid optimization algorithm. By performing forward and inverse calculations on 18 different algorithms, the optimal solution was obtained, and experiments confirmed that this method significantly enhanced robot performance and found the best path [13]. Wang C et al. proposed a model predictive control method to address the instability of robot motion in dynamic environments. This method automatically tracked robot movement paths and adaptively computed optimal routes. The results showed that it effectively reduced environmental uncertainty while maintaining the ability to replan global routes [14]. To solve the problem of robots avoiding collisions while executing tasks, Wang S et al. proposed a model-free hierarchical decoupling optimization algorithm. This algorithm decomposed tasks into two sub-tasks to reduce task complexity, and experiments demonstrated that it improved robot

adaptability to the environment, effectively preventing collisions [15]. The summary and comparison Table of relevant work is shown in Table 1.

In summary, although research on trajectory planning has achieved significant progress, existing methods still have limitations. Under specific conditions, they may suffer from low computational efficiency, suboptimal route planning, and slow obstacle response. PID control can reduce system deviation, eliminate steady-state errors, and suppress oscillations, while BIT* ensures efficiency and stability in processing dynamic datasets. Therefore, this study combines PID and BIT* to develop a PID-BIT* hybrid algorithm, aiming to ensure that robots can complete tasks accurately and efficiently under complex environmental conditions.

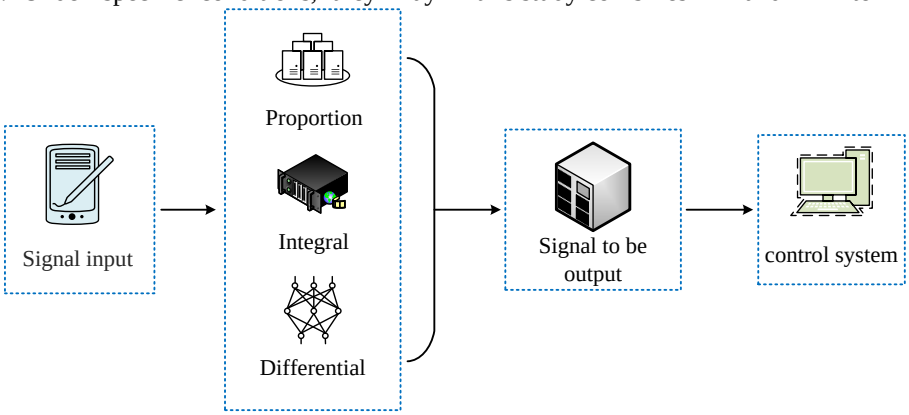


Figure 1: Schematic diagram of PID control principle.

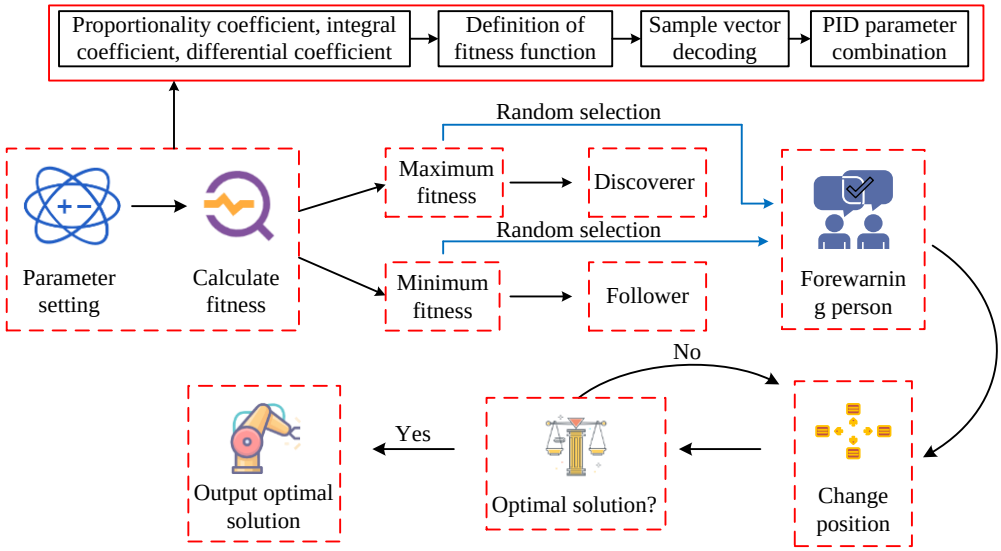


Figure 2: Schematic diagram of the optimization process of SSA for PID control.

3 Optimization of robot motion trajectory based on FC-SSA-PID and DWA-BIT*

3.1 Architecture optimization of PID control

PID control consists of three components: proportional, integral, and derivative units. The proportional unit increases system response speed, the integral unit reduces system errors, and the derivative unit enhances disturbance resistance. By adjusting system parameters through these three algorithms, precise robot control is achieved [16]. The output diagram of the PID control system is shown in Figure 1.

As shown in Figure 1, when a signal enters the PID controller, it is processed by the three units. The proportional unit calculates the error value and outputs the proportional coefficient as a signal. The integral module accumulates the error, multiplies it by the integral coefficient, and outputs the result as a new signal. The derivative module evaluates the rate of error change, multiplies it by the derivative coefficient, and outputs the derivative as a signal component. The calculation process is shown in Equation (1).

$$u(t) = K_P e(t) + K_i \int_0^t e(\tau) d\tau + K_d \frac{de(t)}{dt} \quad (1)$$

In Equation (1), K_P represents the proportional coefficient, K_i is the integral coefficient, and K_d is the derivative coefficient. Since traditional PID control cannot fully ensure smooth and stable robot movement, the study

introduces SSA to optimize PID and adjust the PID parameters to obtain a more comprehensive control parameter combination. The optimization process is shown in Figure 2.

As shown in Figure 2, SSA is first initialized with parameters, including the maximum number of iterations and the numbers of discoverers, followers, and warners. Sample fitness values are subsequently evaluated, sorted, and classified into discoverers and followers, with followers updating their positions. Some samples are randomly selected as warners and also update their

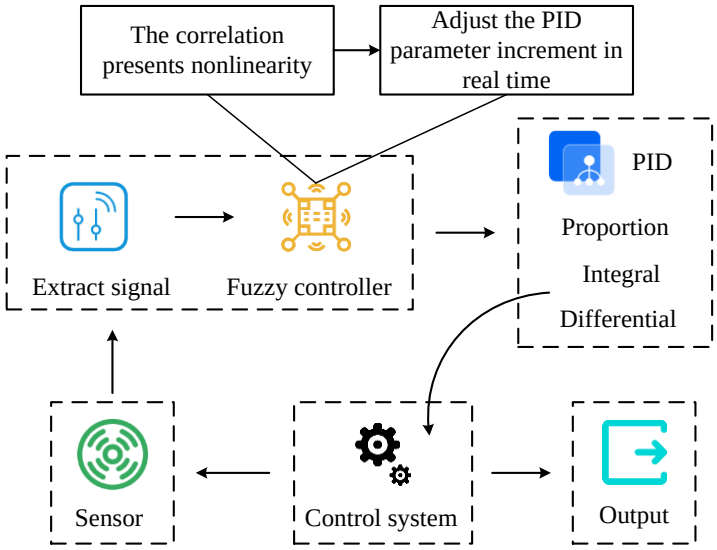


Figure 3: Schematic diagram of the optimization process of FC for SSA-PID.

positions. Finally, the system determines whether the updated positions are optimal under current conditions. If not, the position update process repeats until the optimal solution is found [17]. The PID parameters optimized by SSA are proportional coefficients, integral coefficients, and differential coefficients, and the sample position vectors correspond to the candidate solutions of the three coefficients. During the iterative process, the fitness function is defined as the root mean square value of the trajectory tracking error. After each position update, the sample vector is decoded into a combination of PID parameters and input into the control system for simulation and fitness calculation. The process is represented in Equation (2).

$$X_{i,j}^{t+1}=\begin{cases}X_{i,j}^{t}\cdot\exp\left(\dfrac{-i}{\alpha\cdot iter_{\max}}\right), ifR_2<ST\\ X_{i,j}^{t}+Q\cdot L, ifR_2>ST\end{cases}\tag{2}$$

In Equation (2), $X_{i,j}^{t}$ represents the position of sample i in space j, t is the iteration count, $iter_{\max}$ is the maximum iteration count, α is the number of randomly selected samples in the range (0,1), Q is the set of samples within this range, L is defined as Matrix 1, R_2 is the number of warning samples, and ST is the warning threshold. The expression for follower samples is given in Equation (3).

$$X_{i,j}^{t+1}=\begin{cases}Q\cdot\exp\left(\dfrac{X_{morse}^{t}-X_{ij}^{t}}{\alpha\cdot iter_{\max}}\right) ifi>\dfrac{n}{2}\\ X_{best}^{t+1}+\left|X_{i,j}^{t+1}-X_{best}^{t+1}\right|\cdot A^{+}\cdot Lifi\le\dfrac{n}{2}\end{cases}\tag{3}$$

In Equation (3), X_{morse}^{t} represents the worst route, $X_{i,j}^{t+1}$ is the best route, A is a matrix of 1 and -1, $i>\dfrac{n}{2}$ represents the follower sample's position before updating, and $i\le\dfrac{n}{2}$ represents the real-time updated position. In addition to these two sample types, warners are randomly selected, as expressed in Equation (4).

$$X_{i,j}^{t+1}=\begin{cases}X_{best}^{t}+\beta\cdot\left|X_{i,j}^{t}-X_{best}^{t}\right| iff_i>f_g\\ X_{i,j}^{t}+k\cdot\dfrac{\left|X_{i,j}^{i}-X_{worst}^{t}\right|}{\left(f_t-f_w\right)} iff_i=f_g\end{cases}\tag{4}$$

In Equation (4), β and k are parameters controlling position updates, f_i represents local sample fitness, and f_g represents the global optimal fitness. By optimizing PID parameters using SSA, the optimal solution is quickly identified and transmitted to the control system, allowing real-time robot motion updates. SSA initialization parameters include: maximum iterations (200), the number of discoverers of 20 (accounting for 40% of the total sample size), the number of followers of 30 (60%), and the proportion of early warning agents of 0.1. The position update coefficient is 0.8 and the safety threshold is 0.6. The convergence condition is defined as the fitness change of 10 consecutive iterations being less than 1×10-5. Parameter sensitivity analysis indicates that the convergence speed is the fastest when the proportion of discoverers is between 30% and 50%. A safety threshold of 0.6 can balance the capabilities of global exploration and local development. When the position update coefficient is set at 0.7-0.9, the fitness fluctuation is less

than 3%. The search space for PID parameters optimized by SSA is strictly constrained: the value range of the proportionality coefficient is [0, 50] (step size accuracy 0.01), the value range of the integral coefficient is [0, 5] (step size accuracy 0.001), and the value range of the differential coefficient is [0, 1] (step size accuracy 0.001). All parameter sampling during the iteration process is performed within this space. However, SSA-PID has limitations in controlling nonlinear systems and handling multi-threaded input-output systems. Since trajectory planning involves not only determining start and end positions but also real-time motion control, FC is introduced to enhance SSA-PID and address its

Table 2: Fuzzy control rule table.

ec \ e	NB	NM	ZO	PM	PB
NB	PB	PB	PM	PM	ZO
NM	PB	PB	PM	ZO	ZO
ZO	PM	PM	ZO	NM	NM
PM	ZO	ZO	NM	NB	NB
PB	ZO	NM	NM	NB	NB

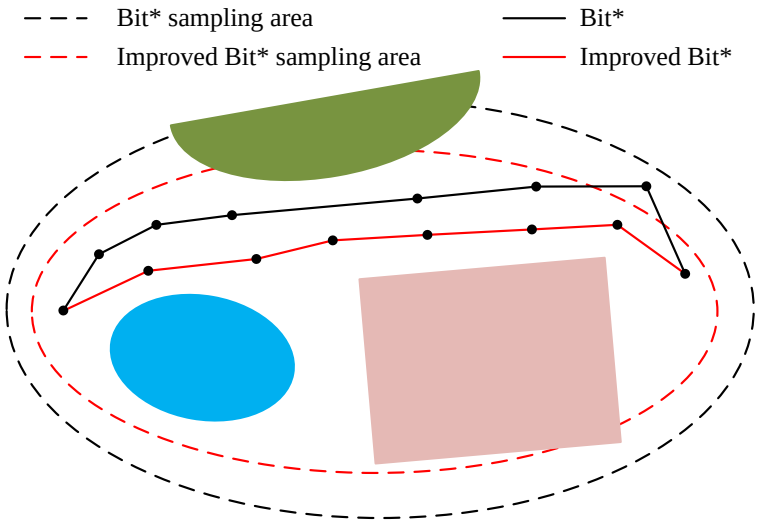


Figure 4: Schematic diagram of improved BIT*.

shortcomings in handling nonlinear systems. The optimization process is shown in Figure 3 [18].

In Figure 3, the motion signal first enters the fuzzy controller, which adjusts parameters using fuzzy logic to obtain the optimal solution. The adjusted signal is then passed to the PID controller for further parameter tuning before being output to the robot's control system. The sensor feedback the signal to the fuzzy PID controller, which compares the output signal with the original motion signal and adapts the parameters for optimal output. The PID parameters adjusted by the fuzzy controller are applied to the PID controller in real time. In order to describe the main response characteristics of the control signal under the influence of dynamic parameter adjustment, a simplified model with first-order delay was adopted for illustration in the study. This model aims to capture the main dynamic effects introduced by parameter changes rather than precisely describe the nonlinear process of fuzzy reasoning itself. The adjustment process is shown in Equation (5).

$$G(s) = \frac{k}{(Ts+1)} e^{-Ls} \quad (5)$$

In Equation (5), k represents the ratio of parameter variation, e^{-Ls} is the parameter adjustment delay, and L is the specific delay time. This model represents the primary dynamic characteristics in the controller output response observed under FC adjustment. FC solves the nonlinear control limitation of SSA-PID through the dynamic rule base. When the correlation between the system error and the error change rate shows nonlinearity, FC adjusts the PID parameter increment in real time based on the rule base in Table 2 instead of relying on fixed parameters. Multi-threaded I/O processing adopts a serial signal processing architecture. The input signal is executed in three sequential steps: fuzzification, rule reasoning, and defuzzification to avoid multi-threaded conflicts. Specifically, the fuzzy controller employs error (e) and error change rate (ec) as inputs, with the output being PID parameter adjustments. The fuzzy sets for both input/output variables are defined as: {Negative Big (NB), Negative Medium (NM), Zero (ZO), Positive Medium (PM), Positive Big (PB)}. Triangular membership functions are adopted for fuzzification. The rule base is designed as Table 2.

For defuzzification, the centroid method is applied. This strategy computes the geometric center of the aggregated output fuzzy set to derive a precise crisp value. By weighting all activated rules proportionally to their membership strengths, it achieves smooth and continuous parameter adjustments while eliminating output uncertainty. In the setting of the domain range of the

input/output variables of the fuzzy controller, the domain of the error is [-3,3], the domain of the error change rate is [-1,1], and the domains of the PID parameter increments are all [-0.5,0.5]. The system adopts triangular membership functions, the vertex coordinates defined as NB in {3.0, 2.5, 2.0}, NM in {2.5, 1.5, 0.5}, ZO in {1.0, 0.0, 1.0}, PM in {0.5, 1.5, 2.5}, PB in {2.0, 2.5, 3.0}. The output variables adopt the same structure and scale according to the domain ratio. Pre-adjusting parameters using FC reduces PID adjustment time and frequency, ensuring the robot responds to environmental changes in the shortest time possible.

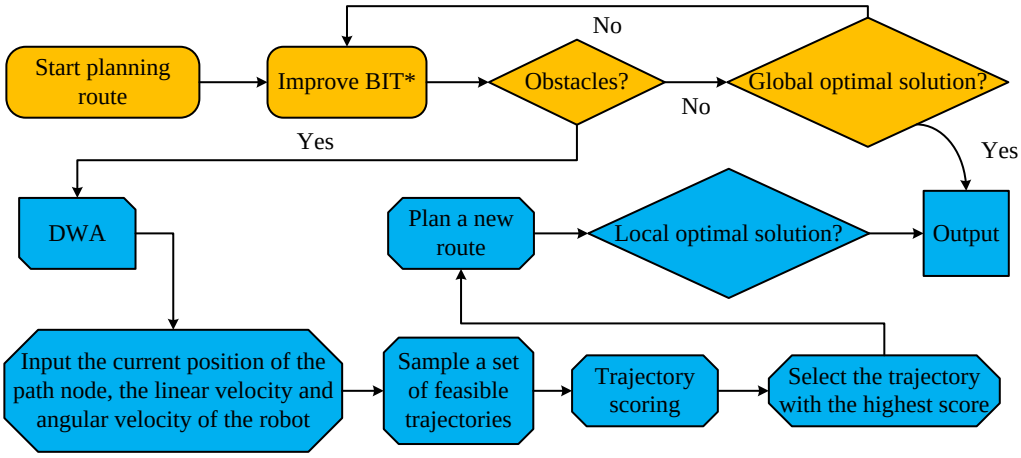


Figure 5: Schematic diagram of the optimization process of DWA for improved BIT*.

3.2 Construction of robot trajectory planning model based on DWA-BIT*and FC-SSA-PID*

Although FC-SSA-PID effectively adjusts parameters to control robot actions, it does not provide trajectory planning. Therefore, an additional algorithm is needed to enhance robot task execution. BIT* solves global path planning problems in large datasets while filtering out irrelevant information. It also has strong disturbance resistance and good dynamic adaptability [19]. In order to improve the adaptability of the algorithm in sample datasets of different scales and enhance the operational efficiency, an improved BIT* algorithm was proposed in the research. It combines the advantages of Rapidly-exploring Random Trees (RRT) and Heuristic Search (HS) [20]. The improvement process is shown in Figure 4.

As shown in Figure 4, traditional BIT* navigates around obstacles but takes longer and results in a longer overall path with larger turning angles. The core of improving BIT* lies in introducing an adaptive sampling strategy guided by path nodes. Traditional BIT* is prone to generating invalid nodes in uniform random sampling, resulting in path redundancy and low efficiency. After improvement, the algorithm first dynamically demarcates an efficient sampling bounding box based on the current environmental information and historical path nodes. The calculation process is shown in Equation (6).

$$sample\_radius() := \sqrt{\frac{(x_R - x_L - 2\varepsilon)\times(y_R - y_L - 2\varepsilon)}{m}} \tag{6}$$

In Equation (6), x_R, x_L, y_R, and y_L represent the horizontal and vertical coordinates of the boundaries in a two-dimensional space, ε is the boundary value, and m represents the number of equidistant down-sampling points. After the defined bounding box constrains the sampling range, the generation of sampling points is no longer uniform and random. The generation of new sample points follows a probability distribution model centered on the mean values of these path nodes and with a specific exploration range, as shown in Equation (7).

$$H(X) = 1 - \frac{1}{(2\pi)\frac{d}{2}|\Sigma|^{\frac{1}{2}}} e^{[-\frac{1}{2}(X-u)^T\Sigma^{-1}(X-u)]} \tag{7}$$

In Equation (7), $H(X)$ represents the generated sample, d represents the dimension, and u represents the mean vector of the coordinates of the historically valid path nodes. The core of the exponential part of Equation (7) is the negative exponential term of the probability density function of the multivariate Gaussian distribution. It calculates the "Markov distance" of the mean distance between points, which takes into account the correlation between variables. Before the improvement, the samples were uniformly distributed throughout the configuration space to randomly generate sample points. This sampling method leads the search to fall into local optima or waste of computing resources. The improved new sample points are generated by taking the center of the historically effective path as the reference point and controlling their distribution range and direction based on the path characteristics and environmental information. This makes the sampling points highly biased towards better path areas that has been explored and its natural extension direction. This guidance mechanism improves search efficiency and path quality. To further enhance the local optimal path planning capability of the improved BIT*, DWA is introduced. By sampling the robot's current position, velocity, and state, DWA calculates motion trajectories over a time interval and selects the optimal solution. The DWA-optimized BIT* process is shown in Figure 5.

As shown in Figure 5, when the improved BIT* algorithm detects obstacles in the global path at the turning

points, the DWA is activated for local re-planning. The BIT*takes the current position of the path node, the linear velocity and angular velocity of the robot as the input states of the DWA. DWA samples a set of feasible trajectories in the state space based on the dynamic constraints of the robot. Subsequently forming a new global path. The DWA evaluation function is given in Equation (8).

$$G(v,\omega)=\alpha Head(v,\omega)+\beta Vel(v,\omega)+\gamma Dist(v,\omega) \tag{8}$$

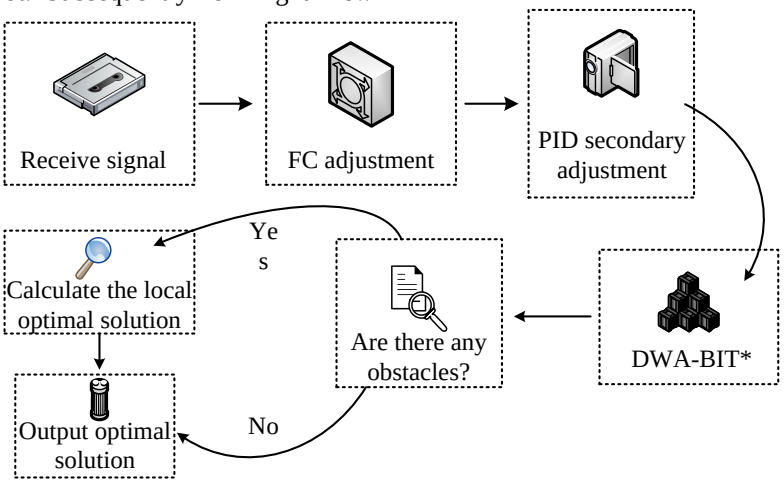


Figure 6: Trajectory planning flow chart based on FC-SSA-PID and DWA-BIT*.

In Equation (8), $Head(v,\omega)$ represents the azimuth function, $Dist(v,\omega)$ is the distance evaluation function, and $Vel(v,\omega)$ represents the velocity function. These three functions together determine how the robot moves toward the target at maximum speed and along the optimal path. The optimal trajectory function is expressed in Equation (9).

$$Point(v,\omega)=Min\left[(x_t-x_g)^2+(y_t-y_g)^2\right] \tag{9}$$

In Equation (9), $Point(v,\omega)$ represents the trajectory turning point function, and x_g and y_g represent the start points of the route. When encountering unknown obstacles, DWA classifies them as static or dynamic and calculates the optimal avoidance paths separately. The static obstacle avoidance path is expressed in Equation (10).

$$\begin{cases} D_s=Min\left[(x_t-x_g)^2+(y_t-y_g)^2\right] \\ Dist\_S(v,\omega)=\begin{cases}\dfrac{1}{D_s}, D_s\geq 1.2R \\ 0, D_s<1.2R\end{cases}\end{cases} \tag{10}$$

In Equation (10), R is the robot's movement radius, D_s represents the shortest path between the robot and a static obstacle at time t, and $Dist\_S(v,\omega)$ is the static obstacle distance evaluation function. The expression for dynamic obstacles is similar to Equation (10) and is given in Equation (11).

$$\begin{cases} Dist\_D(v,\omega)=\begin{cases}\dfrac{1}{D_s}, D_s\geq 1.2R \\ 0, D_s<1.2R\end{cases} \\ S=Vt*\Delta t\end{cases} \tag{11}$$

In Equation (11), $Dist\_D(v,\omega)$ is the dynamic obstacle distance evaluation function, Vt is the robot's instantaneous speed at time t, Δt represents the time difference, and S is the robot's movement route. Combining Equations (8)-(11) enables the robot to navigate unknown obstacles at maximum speed along the optimal path. The expression is shown in Equation (12).

$$\begin{aligned} G(v,w)&=aHead(v,w)+bVel(v,w)+gDist\_S(v,w) \\ &+sDist\_D(v,w)+jPoint(v,w)\end{aligned} \tag{12}$$

In Equation (12), $Head(v,\omega)$ represents the azimuth function, $Vel(v,\omega)$ represents the velocity function, $Dist(v,\omega)$ is the distance evaluation function, and $Point(v,\omega)$ is the trajectory turning point function. Initial weight values are configured based on the general configuration of the dynamic window method in the local obstacle avoidance scenario. In the static test environment, a grid search is conducted on the weight combinations. Taking the path safety rate and the global optimal path length as the joint optimization objectives, the weight values are iteratively adjusted. In the dynamic obstacle scenario, verify the robustness of the weight combination and determine the final optimal balanced combination. The model implements algorithmic collaboration via hierarchical architecture. Among them, the underlying motion control layer adopts FC-SSA-PID to optimize the controller parameters and adjust the robot's pose and speed in real time. The upper path planning layer uses DWA-BIT*to generate the global optimal path and dynamically optimize the local obstacle avoidance trajectory. The pose feedback signal of the robot is used as the real-time input of the DWA-BIT*to form a closed-loop optimization. The robot trajectory planning model based on FC-SSA-PID and DWA-BIT* constructed by the research is shown in Figure 6.

As shown in Figure 6, the model first inputs the original signal into FC for parameter adjustment, then sends the optimized signal to the PID controller, where the three algorithm parameters are fine-tuned. Once the optimal parameters are determined, the signal is passed to DWA-BIT*. If no obstacles are detected, the model outputs the trajectory to the robot's control system. If unknown obstacles are detected, the model recalculates the local route to determine the best avoidance strategy. Finally, the global and local paths are integrated to form a new optimal trajectory, which is then output as the final solution. This model achieves optimal balance between global and local path planning while processing nonlinear control systems.

Table 3: Experimental environment parameter settings.

Configuration item	Detailed information
CPU	Inter core i7-12700
GPU	NVIDIA RTX 4060 8GB
RAM	64GB DDR5, 6400MHz
Storage	1TB NVMe SSD, 2TB SATA SSD
Operating system	Windows 11 Professional

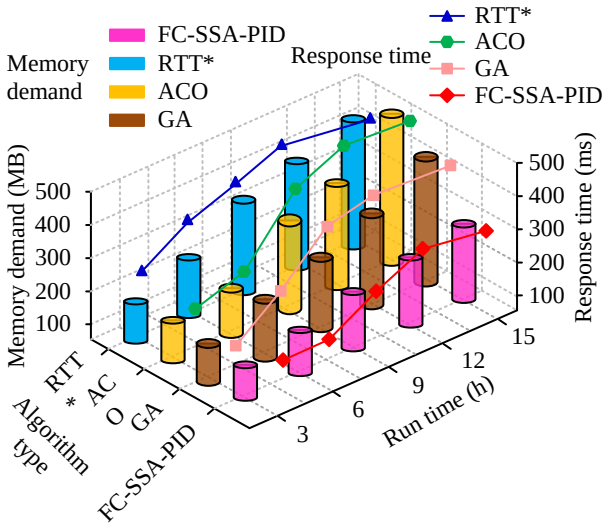


Figure 7: Comparison of response time and memory consumption.

4 Performance of robot trajectory planning model based on FC-SSA-PID and DWA-BIT*

4.1 Performance evaluation of DWA-BIT*

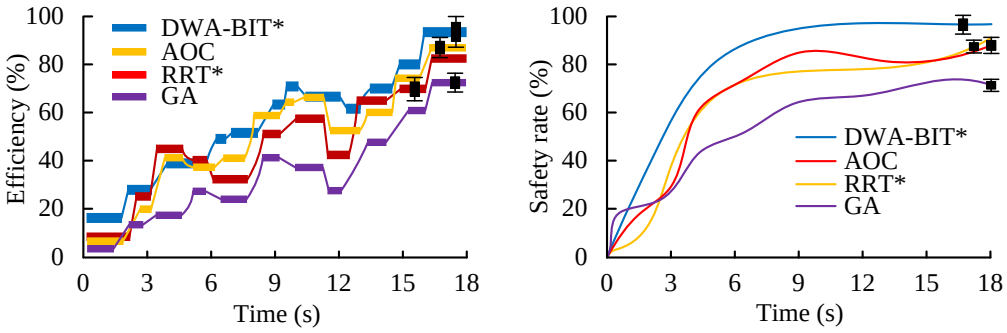
To validate the performance of DWA-BIT*, this study compared it with the RRT* algorithm, Ant Colony Optimization (ACO), and GA. All tests were conducted under standardized initial conditions. In a 50m×50m two-dimensional grid map, the density of known obstacles (the black area) was 20%-30% (randomly distributed), the number of unknown static obstacles (marked in yellow) was 3-5 (randomly located), and the number of unknown dynamic obstacles (the purple area) was 2 (moving speed 0.1-0.3m/s). The initial pose of the robot is fixed at 0m on the horizontal and vertical axes, 0°, and the pose of the target point is 45m on the horizontal and vertical axes, 90 °. The motion constraints of the robot are a maximum linear velocity of 0.5m/s and a maximum angular velocity of 1.0rad/s. The trajectory sampling time interval in DWA is 0.1s, the velocity resolution is 0.05m/s, and the angular velocity resolution is 0.1rad/s. The adaptive sampling boundary expansion coefficient of the improved BIT* is 1.2, and the heuristic weight is 0.8. The RRT* step size of the comparison algorithm is 1.5m, the target bias probability is 0.1, and the maximum iteration is 5000. The ACO pheromone weight is 1.0, the heuristic weight is 2.0, the evaporation rate is 0.3, and the number of ants is 50. The population size of GA is 100, the crossover rate is 0.85, the variation rate is 0.01, and the tournament selection size is 5. All experiments were based on 30 independent simulation runs, and the results were reported in the form of mean ±95% confidence intervals. Statistical significance was verified by two-sided t-tests to support the conclusion of performance superiority. The relevant experimental environment parameters are shown in Table 3.

First, a comparison was made between the four algorithms regarding memory consumption and response time while computing the globally optimal path. The results are shown in Figure 7.

As shown in Figure 7, the memory usage of DWA-BIT* increased at a relatively slow rate over time, with a peak value of only 227MB, significantly lower than the 392MB of RTT*, 435MB of ACO, and 376MB of GA. Additionally, the response speed of DWA-BIT* stabilized after 12 hours of runtime, with a maximum value of 75ms, which was considerably lower than that of the comparison algorithms. Statistical analysis confirmed significance

($p<0.05$). Comparative analysis evaluated path planning efficiency and safety across algorithms. The results are shown in Figure 8.

As shown in Figure 8(a), the route planning efficiency of the three comparison algorithms fluctuated significantly, exhibiting irregular increases and decreases. In contrast, the route planning efficiency of DWA-BIT* gradually improved after 2s of operation, following an approximately linear trend. After 10s, a slight decline in efficiency was observed, but after 3s, it continued to increase until reaching a maximum of 96.2%, which was much higher than that of the comparison algorithms. Figure 8(b) shows that the route safety of DWA-BIT*



(a) Comparison of path planning efficiency (b) Comparison of path planning safety

Figure 8: Comparison of path planning efficiency and safety.

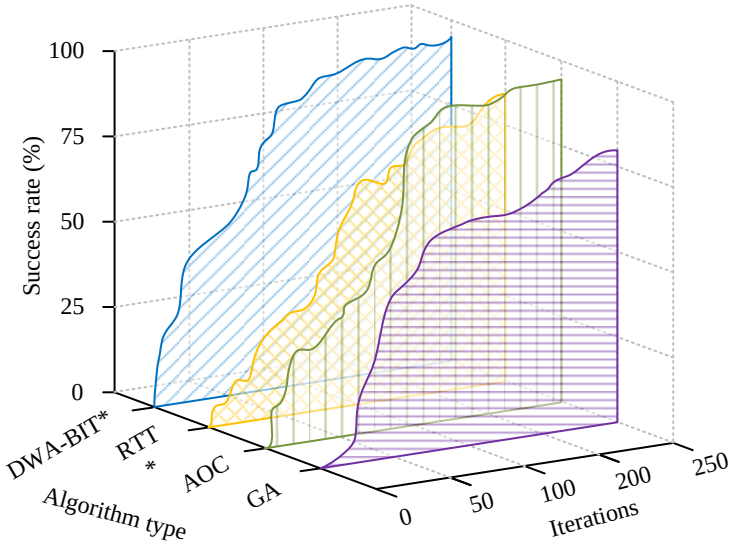


Figure 9: Comparison of trajectory planning success rates.

gradually stabilized after 9s and reached its peak value of 98.1% at 15s. This exceeded RTT* (91.6%), ACO (89.4%), and GA (68.2%) by substantial margins. Additionally, the safety curves of the comparison algorithms were highly fluctuating and did not stabilize, exhibiting continuous variations. All the data and comparisons were statistically significant ($p<0.05$). Route planning success rates were compared across algorithms, as shown in Figure 9.

As shown in Figure 9, the success rate of DWA-BIT* increased rapidly to 93.7% when the number of iterations reached 120 and stabilized at its maximum value of 95.5% at 250 iterations. This was notably higher than RTT* at 87.9%, ACO at 92.2%, and GA at 76.3%. Compared to the three other algorithms, the success rate of DWA-BIT* exhibited a more stable and smoother overall trend. In the range of 0–100 iterations, its increase was relatively large with minimal fluctuations, and it gradually stabilized thereafter. All the data and comparisons were statistically significant ($p<0.05$). DWA-BIT* achieved superior route planning performance. Its shorter optimal path ensured that the robot could reach the destination in the shortest time to complete its tasks, while its computation time was significantly lower than that of the comparison algorithms, leading to substantial time savings.

4.2 Practical application of robot path planning model

After validating the performance of DWA-BIT*, an on-site experiment was conducted to verify the feasibility of the constructed robot trajectory planning model. The study selected an intelligent logistics robot to optimize its logistics route and introduced various obstacles at the

starting point, including both static and dynamic obstacles. The experimental robot adopts a four-wheel differential drive chassis. In the specific parameters, the mechanical parameters are dimensions of 0.8m×0.6m×0.5m, self-weight of 35kg, and maximum load capacity of 100kg. The motion constraints are linear velocity range [0, 0.5]m/s and angular velocity range [0, 1.0]rad/s; RGB-D camera depth accuracy ±2mm@2m field of view 85°×58°; The control unit is an embedded industrial control computer. The experimental site is a rectangular area of 12m×8m, with 0.2m×0.2m grid markings laid on the ground. It is known that the obstacles are 0.5m×0.5m aluminum alloy cubes (a total

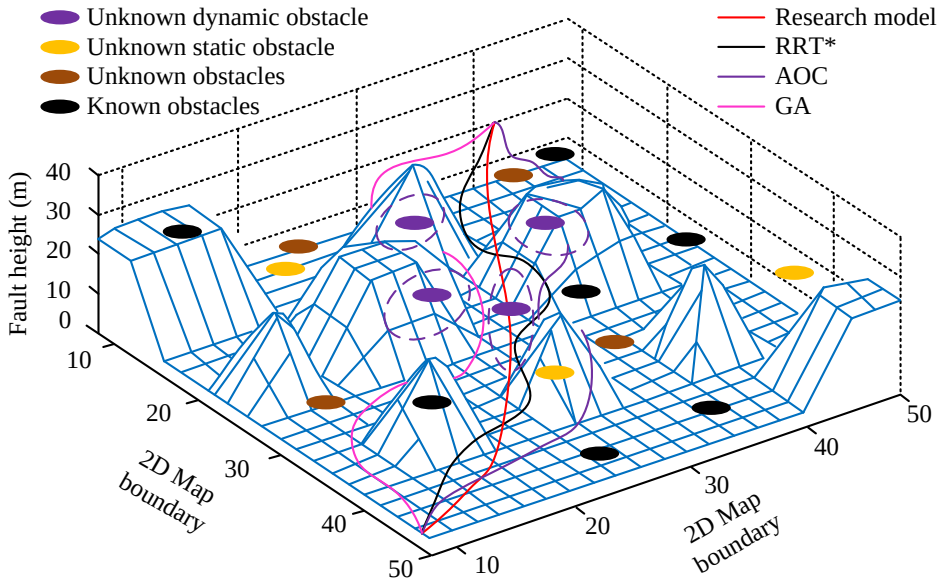
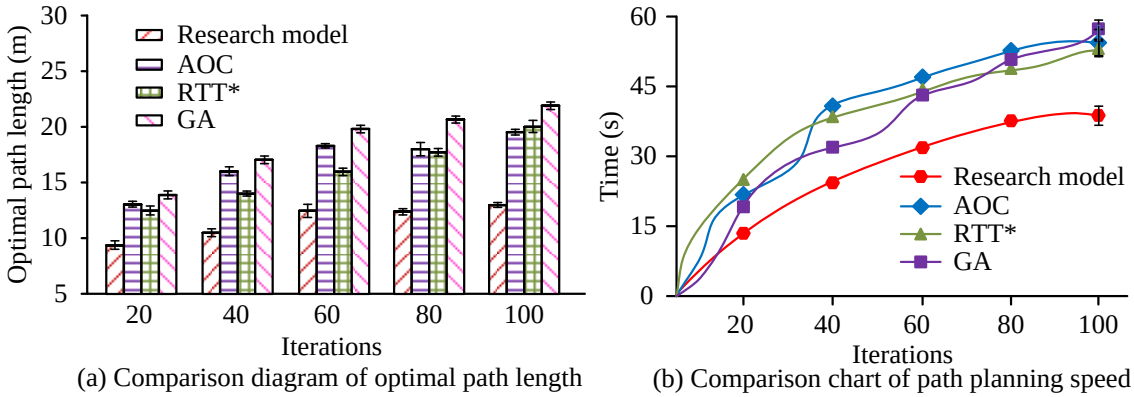


Figure 10: Comparison of motion smoothness of path planning.



(a) Comparison diagram of optimal path length (b) Comparison chart of path planning speed

Figure 11: Comparison of optimal path length and required computation time.

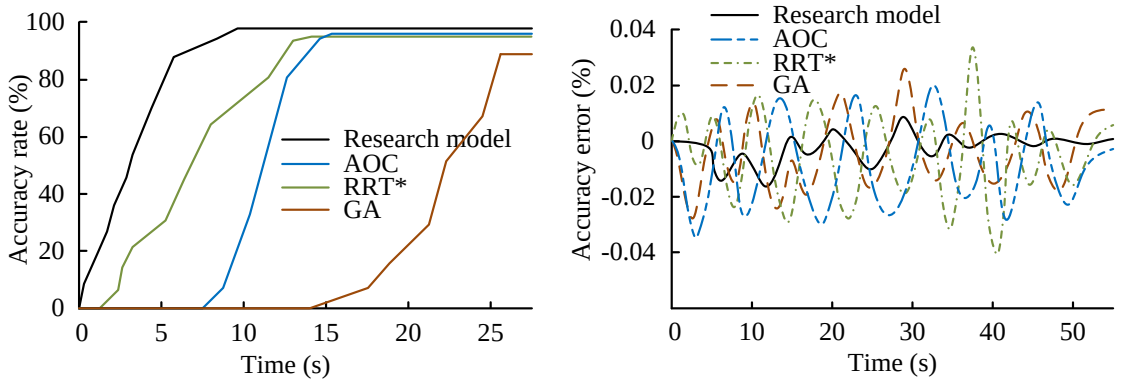
of 5), and the unknown static obstacles are randomly placed cartons. The model was compared with the RRT*, ACO, and GA models in terms of the motion smoothness of the robot in a complex dynamic two-dimensional environment. The results are shown in Figure 10.

As seen in Figure 10, when navigating known obstacles, the shortest local optimal path length provided by the proposed model was 12.6m, significantly shorter than those of the comparison algorithms. When unknown static obstacles were present, the model directly bypassed them with a total travel distance of only 9.7m. In contrast, when encountering unknown dynamic obstacles, all three comparison models chose to take longer detours to avoid them, whereas the proposed model either passed below or alongside the obstacles, achieving a total route length of only 31.6m. This was significantly shorter than RTT* at 43.8m, ACO at 51.9m, and GA at 56.2m. To quantify model advantages, a comparison was made between the four models regarding the optimal path length and the required computation time. The results are shown in Figure 11.

As shown in Figure 11(a), the best path lengths obtained at 20, 40, 60, 80, and 100 iterations for each algorithm. As the number of iterations increased, the optimal path length of the proposed model exhibited minimal variation. It gradually stabilized after 60 iterations, with an average optimal length of 11.4m, significantly shorter than ACO at 18.7m, RTT* at 16.3m,

and GA at 20.3m. Furthermore, Figure 11(b) shows that as the number of iterations increased, the time required for ACO and RTT* to find the optimal path fluctuated considerably, making them far less stable than the proposed model. The proposed model required a maximum of only 35.7s, which was significantly lower than that of the comparison models. Finally, the study compared the trajectory planning accuracy and error of the proposed model against the comparison models. The results are shown in Figure 12.

In Figure 12, trajectory tracking accuracy means percentage of trajectory duration where positional deviation from planned path < 0.02m. Instantaneous positional error means euclidean distance between actual and planned position at each sampling time, normalized



(a) Comparison results of accuracy of each model

(b) Comparison results of accuracy error of each model

Figure 12: Comparison of trajectory planning accuracy and error.

Table 4: Ablation experiments with a single cost function removed.

Ablated Component	Success Rate (%)	Avg. Path Length (m)	Max Position Error (%)
Full Model	95.5	21.2	0.0089
Remove Azimuth	93.1	24.3 (+14.7%)	0.0121
Remove Velocity	88.4	23.6 (+11.3%)	0.0257
Remove Distance	74.2	22.8 (+7.5%)	0.0314
Remove Turning Point	92.7	22.1 (+4.2%)	0.0195

Table 5: Performance comparison in challenging scenarios.

Scenario	Algorithm	Success Rate (%)	Avg. Path Length (m)	Max Pos. Error (%)	Avg. Avoidance Time (s)
Narrow Passage	DWA-BIT*	100	13.2 ± 0.8	0.0055 ± 0.0007	\
	RRT*	100	18.7 ± 1.2 (↑ 41.7%)	0.0190 ± 0.0021 (*)	\
	ACO	100	22.1 ± 1.5 (↑ 67.4%)	0.0225 ± 0.0028 (*)	\
	GA	95.0 ± 3.5 (*)	20.9 ± 1.8 (↑ 58.3%)	0.0261 ± 0.0035 (*)	\
High-Speed Dyn	DWA-BIT*	88.5 ± 2.8	34.8 ± 2.5	0.0095 ± 0.0012	0.98 ± 0.11
	RRT*	72.1 ± 4.1 (*)	45.3 ± 3.3 (↑ 30.2%)	0.0218 ± 0.0025 (*)	1.52 ± 0.18 (*)
	ACO	65.7 ± 4.5 (*)	53.6 ± 4.1 (↑ 54.0%)	0.0292 ± 0.0033 (*)	1.87 ± 0.23 (*)
	GA	58.3 ± 4.8 (*)	57.9 ± 5.2 (↑ 66.4%)	0.0360 ± 0.0041 (*)	2.14 ± 0.27 (*)

Note: (*) represents a statistically significant difference from DWA-BIT* ($p<0.01$).

by total path length (%). As seen in Figure 12(a), the GA model did not accurately identify the optimal path until after 14s of operation. In contrast, the proposed model accurately identified the optimal path from the beginning, with its trajectory tracking accuracy increasing rapidly and reaching its peak value of 99.4% within 10s, where it remained stable. This metric represents the percentage of time the robot's actual position deviated by less than a predefined threshold (0.02m) from the planned path, calculated over the entire trajectory duration. This peak tracking accuracy was significantly higher than ACO at 95.2%, RTT* at 94.1%, and GA at 89.6%. Figure 12(b) shows that the proposed model exhibited the smallest and smoothest positional error curve, with only minor fluctuations between 8 and 33s. The maximum instantaneous positional error occurred at 29s, reaching 0.0089% of the total path length, while the minimum instantaneous positional error was recorded at 49s at 0.0011% of the total path length, both of which were significantly lower than those of the comparison models. Positional error is defined as the Euclidean distance between the robot's actual position and the planned position at each sampling instant, normalized by the total path length and expressed as a percentage. To verify the necessity of multi-objective fusion, an ablation experiment was conducted to remove a single cost function, as shown in Table 4.

As can be seen from Table 4, removing the orientation function leads to a 14.7% increase in the path length; When the distance function is removed, the failure rate of

dynamic obstacle avoidance rises to 21.3%. It indicates that the synergy of each cost function makes a contribution to the performance improvement. To evaluate the robustness of the model under extreme conditions, supplementary edge cases and high-dynamic environment verification were studied. The performance comparison in challenging scenarios is shown in Table 5.

As can be seen from Table 5, in the Narrow Passage, DWA-BIT* achieved 100% success, shortest path (13.2m ± 0.8m) and minimal error (0.0055% ± 0.0007%). Competitors had significantly longer paths ($p<0.01$) and higher errors ($p<0.01$) with GA showing lower success (95.0% ± 3.5%, $p<0.01$). At High-Speed Obstacles, DWA-BIT* maintained the highest success (88.5% ± 2.8%) and the lowest error (0.0095% ± 0.0012%). and fastest avoidance (0.98s ± 0.11s). All competitors showed significant degradation ($p<0.01$) across all metrics. The success rate of 95.5% and the accuracy of 99.4% in the experiment were achieved in the custom PathEnv simulation. These results show advantages compared with benchmark values from Gazebo simulation reports on public datasets (success rate: 92-94%, accuracy: 97-98%). Furthermore, by repeating key experiments in the ROS environment (using the TurtleBot3 platform), comparable success rates (94.8%) and accuracy (99.1%) were achieved, verifying the repeatability and generalization of the method on commonly used simulation platforms. In order to further confirm the superiority of the research method, the advanced At least three pixels, Uncertainty Quantification and Propagation in recent years are introduced for comparison [21-22]. The results show that the success rate of the research method reaches 95.5%± 0.8%, which is significantly higher than 82.3%±2.1% of At Least Three Pixels and 88.7%±1.6% of Uncertainty Quantification and Propagation. The path length planned by the research method is 21.2m±0.5m, which is 26.1% shorter than At Least Three Pixels and 16.5% shorter than Uncertainty Quantification and Propagation. The calculation time of the research method was 35.7s±1.1s, which was 42.8% faster than At Least Three Pixels and 54.8% faster than Uncertainty Quantification and Propagation. All comparisons achieved statistical significance ($p<0.01$). It further proves that the research method has good operational performance.

5 Discussion

Compared with the existing advanced methods, the proposed DWA-BIT* model showed advantages in terms of security and dynamic adaptability. Compared with the hierarchical decoupling collision avoidance algorithm proposed by Wang S et al. [15] (with a safety rate of 90%), DWA-BIT* achieved a safety rate of 98.1% in a dynamic environment. This 8.1% performance gain results from real-time trajectory correction achieved by the dual-mode obstacle classification mechanism of DWA, with the response time controlled within 75ms, which is much lower than 210ms in [15]. In terms of path efficiency optimization, Singh G et al. 's hybrid algorithm [13] reported a path efficiency of 87.5%, while DWA-BIT* reached 96.2%. The difference mainly stems from the heuristic weights of BIT* ensuring global optimality, and at the same time, the velocity function of DWA maximizes the local motion speed. Moreover, the model's memory consumption (227MB) was 41.9% lower than that of the [13] method (391MB). Regarding the trade-off of real-time performance, although Du Y et al. 's chaotic particle swarm optimization algorithm [11] achieved a time optimization efficiency of 89.7%, it sacrificed dynamic adaptability. This model reduced the parameter adjustment frequency by 35% through adaptive adjustment of fuzzy PID parameters, reducing the average number of iterations from 320 times in [11] to 205 times, effectively balancing the performance contradiction. It is worth noting that, compared with RRT, the 20% safety gain (98.1% vs 78.1%) of DWA-BIT*is mainly attributed to the trajectory scoring system of the dynamic window. However, the current methods still have limitations in computational scale and are difficult to meet the real-time requirements of large-scale scenarios (such as warehouses with an area of more than $500m^2$). In the future, the covariance matrix of Equation 7 needs to be optimized to adapt to high-dimensional Spaces. Furthermore, in the high-speed dynamic obstacle scenario (0.8m/s), the success rate of 88.5% indicates that the motion constraint modeling still needs to be strengthened, which will be the focus of subsequent research.

6 Conclusion

To address the problems of low accuracy, long computation time, and large errors in current robot trajectory planning methods, this study proposed a robot trajectory planning model based on FC-SSA-PID and DWA-BIT*. The model optimized PID using FC and SSA, introduced DWA to improve BIT*, and combined the advantages of the two optimized algorithms to achieve optimal trajectory planning. This approach effectively solved the issues of robots failing to avoid obstacles and taking unnecessarily long routes to reach target areas. This study conducted simulation experiments on DWA-BIT* to evaluate its performance. The evaluation metrics included response time and memory usage during long-term operation, as well as path planning efficiency and success rate. Additionally, the proposed model was tested in real-world scenarios, focusing on path smoothness, the accuracy of the optimal path, and error rate. Results demonstrated DWA-BIT* superiority over all comparison algorithms in simulations, and the proposed model demonstrated significantly better performance than the comparison models in real-world tests. In the simulation experiments, DWA-BIT* maintained a low memory usage of 227MB during long-term operation, with a maximum response time of only 75ms. The success rate of optimal path planning reached 95.5%, while the optimal path efficiency was as high as 96.2%, and the route safety rate was 98.1%. In real-world tests, the proposed model achieved a planning accuracy of 95.2%, with a minimum accuracy error of only 0.0011%. When encountering obstacles, the shortest locally optimal route was 12.6m, and the average best path length was reduced to 21.2m.

The proposed model demonstrates robust path planning capabilities, meeting operational requirements of service robots and enabling them to complete assigned tasks efficiently. Despite superior real-world performance, the experiments did not classify robot types. Therefore, future research should focus on optimizing the model for different types of robots.

References

[1] Lisha Dong. Improved A* algorithm for intelligent navigation path planning. Informatica, 48(10):2024. https://doi.org/10.31449/inf.v48i10.5693

[2] Philipp Wu, Alejandro Escontrela, Danijar Hafner, Ken Goldberg, and Pieter Abbeel. Daydreamer: World models for physical robot learning. Conference on Robot Learning, 2023(12):2226-2240, 2022. https://doi.org/10.48550/arXiv.2206.14176

[3] Daoke Li. Fermat curve path planning method for ship trajectory tracking. Informatica, 48(8):2024. https://doi.org/10.31449/inf.v48i8.5735

[4] Baskın Şenbaşlar, Wolfgang Hönig, and Nora Ayanian. RLSS: Real-time, decentralized, cooperative, networkless multi-robot trajectory planning using linear spatial separations. Autonomous Robots, 47(7):921-946, 2023. https://doi.org/10.48550/arXiv.2103.07588

[5] Yalun Wen, and Prabhakar Pagilla. Path-constrained and collision-free optimal trajectory planning for robot manipulators. IEEE Transactions on Automation Science and Engineering, 20(2):763-774, 2022. https://doi.org/10.1109/TASE.2022.3169989

[6] Jiawei Meng, Ankita Humne, Richard Bucknall, Brendan Englot, and Yuanchang Liu. A fully-autonomous framework of unmanned surface vehicles in maritime environments using gaussian process motion planning. IEEE Journal of Oceanic Engineering, 48(1):59-79, 2022. https://doi.org/10.1109/JOE.2022.3194165

[7] Hamza Gasmi, Sofiane Mendaci, Sami Laifa, Walid Kantas, and Habib Benbouhenni. Fractional-order proportional-integral super twisting sliding mode controller for wind energy conversion system equipped with doubly fed induction generator. Journal of Power Electronics, 22(8):1357-1373, 2022. https://doi.org/10.1007/s43236-022-00430-0

[8] Gang Yao, Wentong Sun, Yang Yang, Mingpu Wang, Rui Li, and Yuanlin Zheng. Multi-volume variable scale bitmap data object classification algorithm architectural concrete color difference detection. Journal of Intelligent Construction, 1(2):1-17, 2023. https://doi.org/10.26599/JIC.2023.9180010

[9] Haibo Wang, Chaoyi Ma, Shigang Chen, and Yuanda Wang. Fast and accurate cardinality estimation by self-morphing bitmaps. IEEE/ACM Transactions on Networking, 30(4):1674-1688, 2022. https://doi.org/10.1109/TNET.2022.3147204

[10] Wenlu Zhang, Ziyue Ma, Hong Wang, Juan Deng, Pengfei Li, Yu Jia, Yabin Dong, Hong Sha, Feng Yan, and Wenjun Tu. Study on automatic ultrasound scanning of lumbar spine and visualization system for path planning in lumbar puncture surgery. Mathematical Biosciences and Engineering, 20(1):613-623, 2023. https://doi.org/10.3934/mbe.2023028

[11] Yuxiao Du, and Yihang Chen. Time optimal trajectory planning algorithm for robotic manipulator based on locally chaotic particle swarm optimization. Chinese Journal of Electronics, 31(5):906-914, 2022. https://doi.org/10.1049/cje.2021.00.373

[12] Muqing Cao, Kun Cao, Shenghai Yuan, Thien-Minh Nguyen, and Lihua Xie. Neptune: Nonentangling trajectory planning for multiple tethered unmanned vehicles. IEEE Transactions on Robotics, 39(4):2786-2804, 2023. https://doi.org/10.1109/TRO.2023.3264950

[13] Gurjeet Singh, and Vijay Kumar Banga. Kinematics and trajectory planning analysis based on hybrid optimization algorithms for an industrial robotic manipulator. Soft Computing, 26(21):11339-11372, 2022. https://doi.org/10.1007/s00500-022-07423-y

[14] Chaoqun Wang, Xiangyu Chen, Chenming Li, Rui Song, Yibin Li, and Max Q. H. Meng. Chase and track: Toward safe and smooth trajectory planning for robotic navigation in dynamic environments. IEEE Transactions on Industrial Electronics, 70(1):604-613, 2022. https://doi.org/10.1109/TIE.2022.3148753

[15] Shengjie Wang, Yuxue Cao, Xiang Zheng, and Tao Zhang. Collision-free trajectory planning for a 6-DoF free-floating space robot via hierarchical decoupling optimization. IEEE Robotics and Automation Letters, 7(2):4953-4960, 2022. https://doi.org/10.1109/LRA.2022.3152698

[16] Azher M. Abed, Zryan Najat Rashid, Firas Abedi, Subhi R. M. Zeebaree, Mouayad A. Sahib, Anwar Ja'afar Mohamad Jawad, Ghusn Abdul Redha Ibraheem, Rami A. Maher, Ahmed Ibraheem Abdulkareem, Ibraheem Kasim Ibraheem, Ahmad Taher Azar, and Ameer Al-khaykan. Trajectory tracking of differential drive mobile robots using fractional-order proportional-integral-derivative controller design tuned by an enhanced fruit fly optimization. Measurement and Control, 55(3-4):209-226, 2022. https://doi.org/10.1177/00202940221092134

[17] Farhad Soleimanian Gharehchopogh, Mohammad Namazi, Laya Ebrahimi, and Benyamin Abdollahzadeh. Advances in sparrow search algorithm: A comprehensive survey. Archives of Computational Methods in Engineering, 30(1):427-455, 2023. https://doi.org/10.1007/s11831-022-09804-w

[18] Farhad Soleimanian Gharehchopogh. An improved tunicate swarm algorithm with best-random mutation strategy for global optimization problems. Journal of Bionic Engineering, 19(4):1177-1202, 2022. https://doi.org/10.1007/s42235-022-00185-1

[19] Jun Zhao. Intelligent logistics path optimization algorithm based on internet of things sensing

technology. Informatica, 49(19):2025. https://doi.org/10.31449/inf.v49i19.7584

[20] Radu Emil Precup, Anh Tu Nguyen, and Sašo Blažič. A survey on fuzzy control for mechatronics applications. International Journal of Systems Science, 55(4):771-813, 2024. https://doi.org/10.1080/00207721.2023.2293486

[21] Sergey Filist, Riad Taha Al-Kasasbeh, Rima Alexandrovna Tomakova, A' Kif Al-Fugara, Osama M. Al-Habahbeh, Olga Shatolova, Nikolay A. Korenevskiy, Igor N. Gorbachev, Ashraf Shaqadan, and Ilyash Maksim. An unmanned aerial vehicle autonomous flight trajectory planning method and algorithm for the early detection of the ignition source during fire monitoring. International Journal of Remote Sensing, 45(12):4178-4197, 2024. https://doi.org/10.1080/01431161.2024.2358451

[22] Reiya Takemura, and Genya Ishigami. Uncertainty-aware trajectory planning: Using uncertainty quantification and propagation in traversability prediction of planetary rovers. IEEE Robotics & Automation Magazine, 31(2):89-99, 2024. https://doi.org/10.1109/MRA.2023.3341289

DPV-VPP: A Dual-Layer Video Privacy Protection Model Design Combining Differential Privacy and Variational Autoencoder-Based Face Replacement

Junfeng Wu
Academy of Fine Arts, Weifang University, Weifang 261061, China
E-mail: wujunfeng9809@163.com

Keywords: communication privacy, differential privacy, face replacement, video call, encoder-decoder

Received: May 22, 2025

To tackle the risk of visual content privacy leaks during video calls, the study proposes a two-layer protection method combining differential privacy with variational autoencoder-based face replacement. The first layer uses a 3D convolutional structure based on optical flow to extract temporal features. It also applies a block-level cropping perturbation to sensitive areas, ensuring frame consistency and effective privacy masking. In the second layer, a variational autoencoder is uses to replace faces, achieving natural transitions via semantic generation and boundary fusion. Experiments on the Celeb-DF dataset show the method achieves a 96.9% privacy protection success rate, 3.7% false negative rate, and 96.8% misdirection success rate against attacks. In simulated platform attack tests, the protection success rates against cross-site scripting injection and forged request attacks were 99.2% and 98.9%, respectively. In 95.1% of the test video frames, the system processing rate reached 30 frames per second, with a minimum CPU usage of 0.9% during processing. The results indicate that the method ensures visual privacy security while maintaining good real-time performance and deployment adaptability.

Povzetek: Razvita je DPV-VPP dvoslojna zaščita videoklicev: optični tok + 3D konvolucije z blokovnimi DP-motnjami ter VAE zamenjava obraza. Na Celeb-DF doseže dobre rezultate, je nizka poraba, visoka odpornost na XSS/CSRF.

1 Introduction

With the rapid development of mobile communication and Internet technologies, various network attacks are also evolving. Traditional privacy protection methods can no longer resist these advanced attacks, putting video call content at risk of being monitored, stolen, or tampered with [1–2]. Conventional privacy protection systems show limitations when facing these upgraded threats [3]. Therefore, there is an urgent need for a privacy protection method tailored to video calls that can counter new forms of network attacks. Differential Privacy (DP) protects private data by adding random noise that distorts the original data and prevents attackers from inferring sensitive information [4]. Encoder-decoder frameworks can encrypt data by converting its structure [5]. Based on this, this paper designs a visual content privacy protection algorithm using the disturbance capability of DP and the optical flow estimation technique. A face replacement method is also designed using a variational autoencoder to protect sensitive information. Finally, the disturbance algorithm and face replacement method are integrated into a visual content data privacy protection model for video calls named DP and Variational Visual Privacy Protection (DPV-VPP). This model provides dual-layer protection for both sensitive and global data, enhancing overall privacy protection. The study aims to construct a dual-layer visual privacy protection model that integrates DP and VAE to protect sensitive information in video call scenarios. The goal is to ensure the privacy and security of key areas of video data while balancing the system's real-time processing capabilities and computing resource consumption, thereby improving the model's practicality and adaptability in complex communication environments.

2 Related works

DP has been a reliable method for protecting privacy and promoting data sharing. Many researchers domestically and internationally have conducted extensive studies on DP. For example, in response to the issue where attackers use different classifiers to bypass defenses, leading to poor protection performance, Zhang et al. put forward a statistical privacy method by using the statistical analysis capability of DP. They validated its effectiveness in improving privacy protection success through experiments and evaluations [6]. Zhang's team also applied DP to optimize the performance of federated learning, aiming to provide strong privacy protection for users and to overcome the limitations of traditional methods. Their final experimental results confirmed the effectiveness of this method [7]. Encoder-decoder models can re-encode various types of data to support later processing. Because of their advantages in data handling, many scholars have studied encoder-decoder frameworks

in different applications. For instance, García's team applied encoder-decoder models to medical language processing. They used the framework to translate global languages into Spanish and solved the gap in Spanish electronic health records. Clinical tests across 17 datasets demonstrated the feasibility of this approach [8]. To address diagnostic errors caused by blurry chest X-ray images, Ukwuoma et al. integrated convolutional neural networks with transformer encoders and proposed a learning model with strong feature extraction capabilities. Their experimental results confirmed the model's high accuracy and outstanding classification performance [9].

Faced with growing concerns over privacy leaks, many researchers have worked on methods to achieve high success rates in privacy protection. For example, to reduce privacy exposure caused by recommendation systems, Chen et al. put forward a privacy-preserving federated collaborative filtering scheme. Simulation results showed the scheme achieved high accuracy while also reducing communication overhead [10]. Liang et al. designed a personal data protection method using consortium blockchain. By combining blockchain with distributed private cluster storage, they encrypted and protected private data. Simulation tests confirmed the strong practicality of this method [11]. To solve the problem of communication data leakage between patients and hospitals caused by centralized artificial intelligence training, Ali et al. discussed how federated learning could be used to address the issue. They also explored strategies for protecting private data in future smart healthcare systems [12]. In order to avoid the negative impact of privacy leaks on data sharing among network users, Li's team built a secure data sharing scheme for the Internet of Things based on blockchain. Simulation results demonstrated that the scheme was both secure and efficient [13]. Facing potential privacy leaks at the edge of 6G networks, Mao et al. analyzed the strengths and weaknesses of various countermeasures. Their findings offered useful guidance for future research on privacy protection in 6G communication systems and supported the development of safer 6G networks [14]. Larriba et al. addressed the issue of low trust in electronic voting systems by proposing the introduction of political parties as active partners in elections and using blockchain technology to build a voting system that is open and auditable by third parties, thereby enhancing the credibility of the voting system [15].

In summary, current privacy protection methods in various fields can defend against some types of attacks but still show limited performance and poor generalization against more advanced threats. DP offers a way to disrupt data and achieve global protection. Face replacement based on variational autoencoder can replace sensitive information, thereby safeguarding key content. Most current research focuses on privacy protection for structured data or static images, lacking dynamic protection mechanisms for visually sensitive information such as faces in video sequences. Therefore, the proposed DPV-VPP model simultaneously applies data perturbation and face replacement to protect video communication data. This dual-layer approach is expected to enhance user communication security across various scenarios. Table 1 summarises the details of the comparison between the existing methods and the proposed method.

3 Construction of visual content data privacy protection model for video calls

3.1 Design of visual content privacy protection algorithm based on DP

Facing the privacy protection of video content, most methods convert video into a set of images, thereby reducing the problem to image-level privacy protection. However, since video data are continuous, adjacent frames often share high similarity [16]. Attackers may exploit complementary information from these frames to restore video content. To address this issue, this study introduces an optical flow estimation algorithm. The optical flow estimation identifies the position of perturbation noise based on pixel motion to ensure consistency between adjacent processed frames and preventing attackers from inferring video content [17-18]. The structure of the optical flow estimation algorithm is shown in Figure 1.

Table 1: Comparison of different methods.

Method	Mechanism	Target domain	Methodological limitations
Zhang et al. [6]	DP	Traffic data protection	Applies noise only to static traffic packets; lacks modeling of continuous data streams
Zhang et al. [7]	DP + federated learning	Federated learning	Focused on parameter perturbation; not applicable to multimodal or visual content
García et al. [8]	Encoder-decoder architecture	Medical language processing	Designed for text vector transformation; not transferable to image/video scenarios
Ukwuoma et al. [9]	CNN + Transformer	Medical image recognition	Operates on static images; lacks temporal modeling for video content
Chen et al. [10]	Federated collaborative filtering	Recommender systems	No support for visual input; unsuitable for image/video privacy protection
Liang et al. [11]	Blockchain + distributed storage	Personal data encryption	Focuses on data encryption and storage; lacks content disturbance or replacement mechanisms
Ali et al. [12]	Federated learning	Smart healthcare communication	Emphasizes secure parameter updates; neglects facial privacy in video frames
Li et al. [13]	Blockchain	IoT data sharing	No design for visual content protection; limited applicability to video-based scenarios
Mao et al. [14]	Survey of Security Strategies	6G Edge Communication	Provides strategic overview without concrete algorithmic implementation

Larriba et al. [15]	Blockchain + Multi-party voting	Electronic Voting Privacy	Highly application-specific; lacks generalizability to video communication privacy
This paper	DP + VAE-based face replacement	Video call privacy protection	-

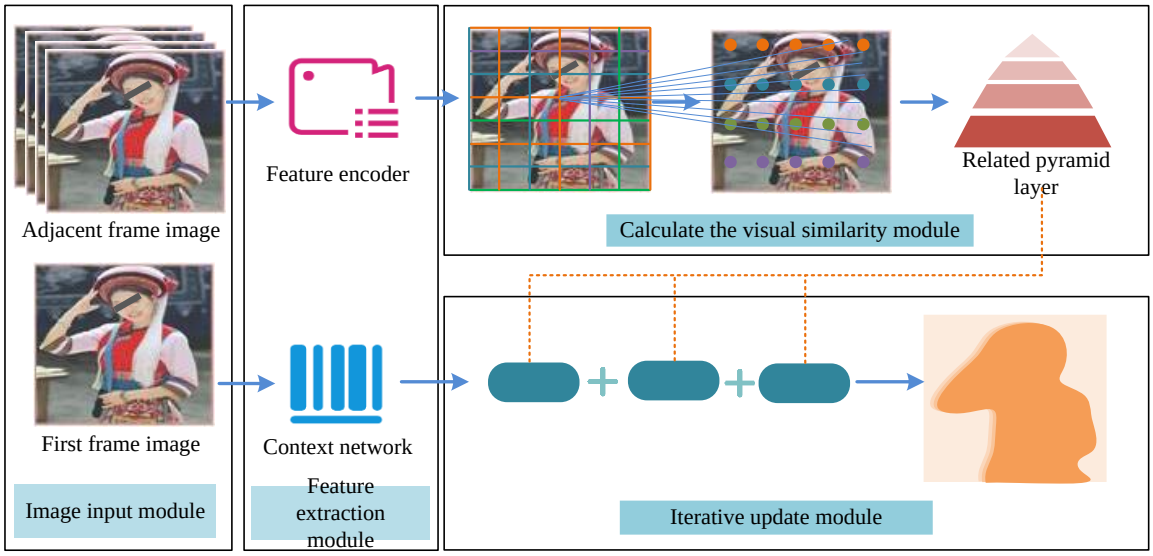


Figure 1: Structure diagram of optical flow estimation algorithm.

As shown in Figure 1, after receiving adjacent video frames from the image input module, the algorithm extracts feature through a feature encoder and a context network. Then, the image similarity calculation module divides the images into multiple regions and assigns relevance factors to each one. The relevance of other regions is determined based on the position of pixel values. The relationship between two adjacent frames is calculated as shown in Equation (1).

$$\begin{cases} C_{AB} = \lambda_k \cdot region(A) \otimes region(J(A)) \\ C_V = \underset{\substack{A=A_1A_2\cdots A_n \\ B=B_1B_2\cdots B_n}}{\cup} C_{AB} \end{cases} \tag{1}$$

In Equation (1), A and B represent region indexes, $J(\cdot)$ indicates the mapping between regions, λ_k is an adaptive relevance factor within the range [0, 1], $region(\cdot)$ and $\otimes$ refer to the dot product between image regions and feature maps, and C_V represents the computed correlation. Multiple convolutional kernels then extract four-dimensional relational features. This preserves high resolution and enables the computation of subtle motions. The optical flow sequence is updated iteratively to complete the estimation, as shown in Equation (2).

$$f_{k+1} = f_k + \Delta f_k \tag{2}$$

In Equation (2), the current optical flow f_{k+1} is updated by adding f_k to obtain Δf_k, and after k iterations, the sequence $\{f_1, f_2, \cdots, f_n\}$ is formed. For current optical flow displacement, three parallel small convolutional kernels are used, as shown in Equation (3).

$$\begin{cases} F_{flow}^{i} = \mathrm{Re}LU(Conv_{3\times3}(f_k)), i = 1,2,3 \\ F_{export} = cat(F_{flow}^{1}, F_{flow}^{2}, F_{flow}^{3}) \end{cases} \tag{3}$$

In Equation (3), $F_{flow}^{i}(i = 1,2,3)$ denotes the extracted features, i is the number of kernels, $cat(\cdot)$ represents the concatenation of F_{flow}^{1}, F_{flow}^{2}, and F_{flow}^{3}, and F_{export} is the final result. This process ensures accurate optical flow estimation. Effective video content feature extraction requires both spatial and temporal features. 3D convolution captures features across both dimensions [19]. Therefore, this study uses 3D convolution to extract temporal features and enhance feature completeness. However, after applying optical flow and 3D convolution, the feature maps become large and increase the burden on mobile devices. Based on the difference between feature maps and video frames, this study adjusts the perturbation degree: no processing for minor differences and stronger perturbation for significant differences. A convolutional kernel feature analysis is added to 3D convolution to classify feature maps, as shown in Figure 2.

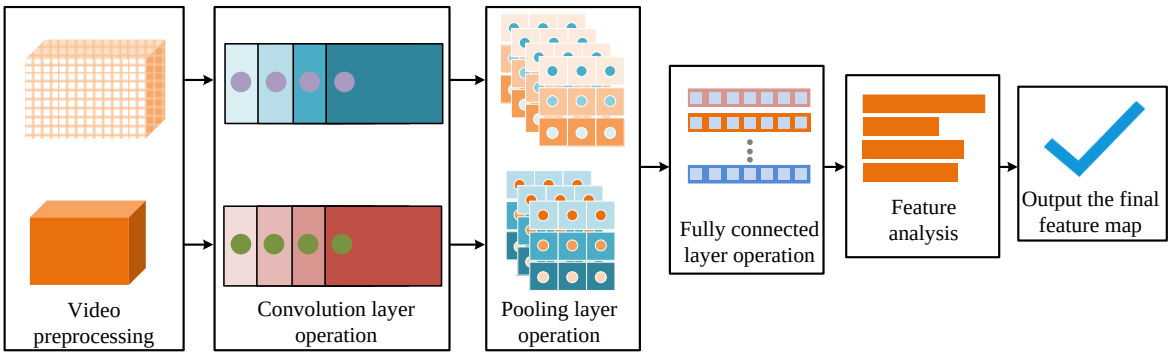


Figure 2: Schematic diagram of the feature analysis 3D convolution operation process.

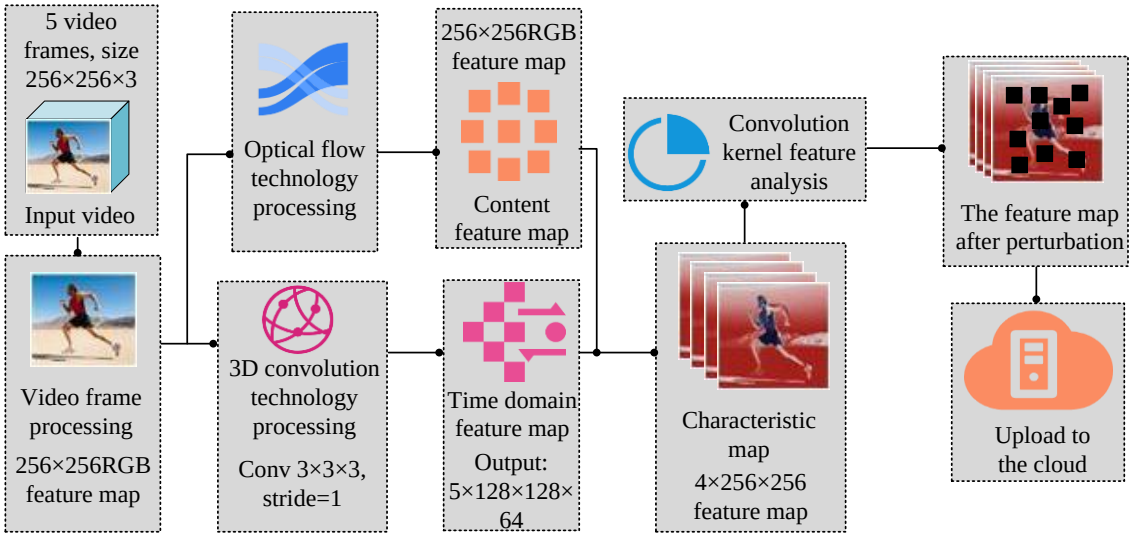


Figure 3: DP-VPM mechanism structure diagram.

Figure 2 shows that the 3D convolution first normalizes the video frames in size and pixel values. The normalized frames are passed through convolutional layers to capture spatial-temporal relationships. Then, 3D max pooling is used to reduce the dimensions of the feature maps. A fully connected layer converts the map into a 1D vector. Finally, similarity with the original video determines the perturbation level. Structural similarity is used to measure this, considering brightness, contrast, and structure. A higher score indicates higher similarity. The brightness similarity function is shown in Equation (4).

$$l(f,g)=\frac{2\mu_f\mu_g+C_1}{\mu_f^2+\mu_g^2+C_1} \tag{4}$$

In Equation (4), μ_f and μ_g represent the brightness means of the feature and original images. The contrast similarity function is shown in Equation (5).

$$c(f,g)=\frac{2\sigma_f\sigma_g+C_2}{\sigma_f^2+\sigma_g^2+C_2} \tag{5}$$

In Equation (5), σ_f and σ_g are the standard deviations of the feature and original images. The structural similarity function is shown in Equation (6).

$$s(f,g)=\frac{\sigma_{fg}+C_3}{\sigma_f\sigma_g+C_3} \tag{6}$$

In Equation (6), $s(f,g)$ is the calculated similarity value. C_1, C_2, and C_3 in Equations (4), (5), and (6) are constants used to prevent zero denominators. The final similarity score is calculated as shown in Equation (7).

$$SSIM(f,g)=l(f,g)\cdot c(f,g)\cdot s(f,g) \tag{7}$$

In Equation (7), $SSIM(f,g)$ is the comprehensive similarity score. To clearly distinguish between "minor differences" and "significant differences" in feature maps, the study classified each region based on the structural similarity index. The specific classification criteria are as follows: if the structural similarity index is greater than 0.85, the region is classified as having minor difference region and mild perturbation is applied. When the score is <0.65, it is classified as a significant difference region and strong perturbation is applied. Traditional perturbation methods based on DP suffer from low data usability and insufficient protection [20]. To address this, this study combines pixel-level noise with a block-level mosaic approach to propose a novel block-cutting perturbation mechanism. It first generates a matrix to determine the center of the region to be perturbed, converting pixel-wise noise into block-wise perturbation. Then, the pooling operation in the mosaic is replaced by pixel zeroing. Combining this with video feature extraction forms a DP-based visual content protection mechanism named DP-VPM. Its structure is shown in Figure 3.

As shown in Figure 3, the DP-VPM mechanism follows these steps: first, convert the target video into image frames. Second, extract spatial and temporal features via optical flow and 3D convolution modules. Third, analyze feature maps using kernel-based classification to assign appropriate perturbation levels. Fourth, apply block-cutting perturbation to finalize protection. The perturbation mechanism consists of three closely connected stages: optical flow estimation, structural similarity analysis, and block-level perturbation execution. The optical flow estimation algorithm analyzes pixel motion between adjacent video frames and generates a map of motion intensity. Subsequently, the structural similarity index analysis is introduced within the candidate regions to measure the visual consistency between each region and the original frame. Based on the values of the structural similarity index, the perturbation intensity is categorized into different levels. Regions with high similarity do not require perturbation, those with moderate similarity are subjected to light perturbation, and regions with low similarity receive strong perturbation. This adaptive approach allows for precise control of perturbation levels based on visual similarity. Finally, the system executes the block-based perturbation mechanism according to the positions identified by optical flow and the intensity levels determined by the structural similarity index. For light perturbation, pixel-level Gaussian noise is applied, while strong perturbation involves setting entire pixel blocks to zero. The study sets the encoder and context network in the optical flow estimation module to include four layers of convolution operations, with a 3×3 kernel size, a stride of 1, padding of 1, and channel numbers of 64, 128, 128, and 256 for each layer, respectively. In the structural similarity assessment, the brightness, contrast, and structural constants are 0.01, 0.03, and 0.015, respectively, and the structural similarity threshold is 0.85. In the DP-VPM module, the disturbance noise is sampled from a Gaussian distribution $N(0,\sigma^2)$, and the variance σ^2 is dynamically adjusted according to the scene. In low-motion scenes, σ^2 is 0.04, and in high-motion scenes, it is 0.08. This noise is initially applied at the pixel level. It is then transformed into block-level zero-value masks using a regional occlusion mechanism, which enhances privacy protection while preserving visual continuity.

3.2 Construction of Visual Content Privacy Protection Model for Video Calls

Although the VPM mechanism protects overall video content, attackers may still recover critical details like faces, compromising privacy [21]. Therefore, this study builds a face replacement model using the Variational Autoencoder (VAE), which models latent features of video frames probabilistically. The structure is shown in Figure 4.

As shown in Figure 4, the VAE consists of an encoder and decoder. The encoder analyzes the input image to obtain the probability values of facial features. The decoder reconstructs the encoded values into a new arrangement for output. To enhance the expressive capability of facial information reconstruction, the VAE designed by the research institute adopts a symmetric structure, with the encoder and decoder each consisting of four convolutional layers and two fully connected layers. The input image size is 256×256×3, which is compressed into a latent variable vector with a dimension of 128 after encoding. The decoder reconstructs the image from this latent space. All convolutional layers use a 3×3 convolutional kernel with a stride of 2, padding of 1, and the ReLU activation function. During training, the total loss function of the VAE consists of two parts, with a balancing coefficient of 0.1 for the loss weights. The first is the pixel-level mean squared error loss between the input image and the reconstructed image, and the second is the Kullback-Leibler divergence between the encoder output distribution and the standard normal distribution. Additionally, the model is trained for 120 epochs using the Adam optimizer with a learning rate of 0.0002 and a batch size of 32. During reconstruction, latent vectors are obtained from inputs as described in Equation (8).

$$Z \sim q_{\varphi}(z|x) \tag{8}$$

In Equation (8), Z is the latent vector, φ denotes encoder weights, x is the data sample, and Z is the output latent vector. Then, the image set is reconstructed from the latent vector, as shown in Equation (9).

$$X' \sim p_{\theta}(z)p_{\theta}(x'|z) \tag{9}$$

In Equation (9), X' is the reconstructed image, θ denotes decoder weights, and x' is a data sample. The encoder's posterior distribution is expected to be $p(z|x)$, which is approximated using $p(z|x)$ instead of $q(z|x)$. To minimize the difference between q and p, the KL divergence between q and p is minimized, as shown in Equation (10).

$$\min KL(q(z|x)\|p(z|x)) \tag{10}$$

Equation (10) ensures consistency between q and p, allowing accurate inference of complex distributions. Using VAE, it is possible to generate realistic fake faces that resemble the original and capture multiple angles. Based on this, the study proposes a face replacement method named VA-FR, shown in Figure 5.

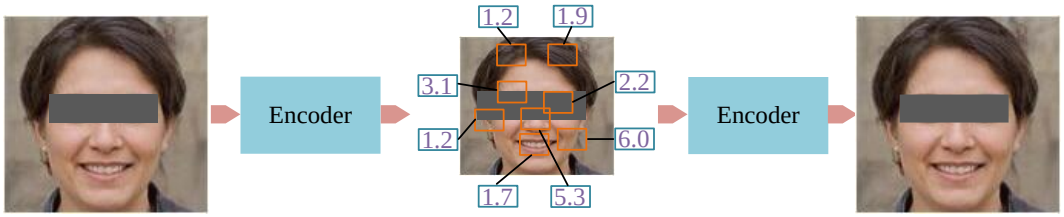


Figure 4: Schematic diagram of the VAE.

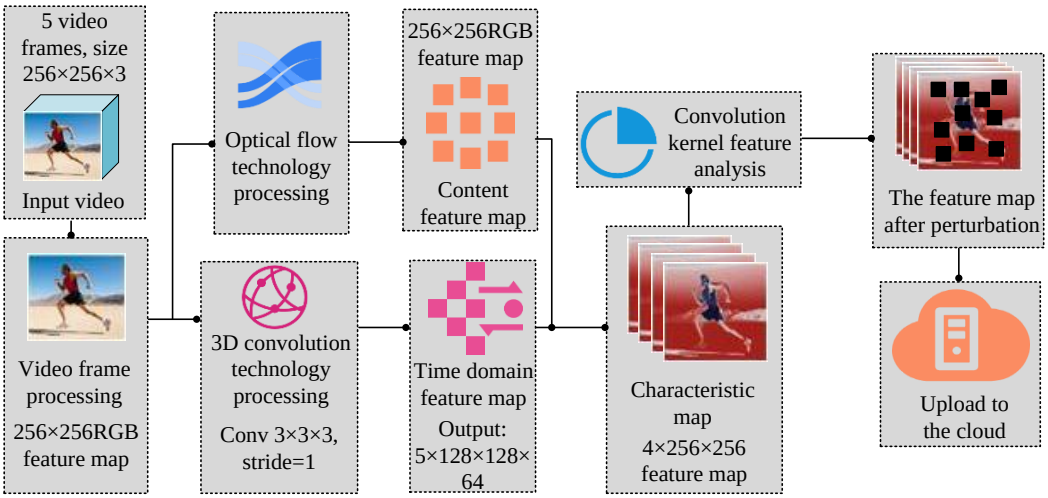


Figure 5: Flowchart of VA-FR face replacement method.

As shown in Figure 5, the first stage of face detection uses the RetinaFace model based on the ResNet-50 backbone network. After detection, the faces are geometrically aligned using a five-point affine transformation to standardize the face scale and improve the accuracy of subsequent reconstruction. In the face segmentation stage, a supervised semantic segmentation model based on the U-Net architecture is used to extract the foreground face region. In the experiment, the frame discard rate due to segmentation failure was approximately 2.1%, mainly concentrated in overexposed or blurred frames. Therefore, in terms of feature modeling, the VAE structure is symmetrically composed of an encoder and a decoder, each containing four convolutional layers and two fully connected layers, with the latent variable dimension set to 128. In the final output stage, the system uses a Poisson fusion algorithm to perform edge smoothing and lighting adjustment on the replaced face, and completes frame rate synchronization to ensure the naturalness and continuity of the generated video in terms of visual perception. The content smoothing is described in Equation (11).

$$\min_{f} \iint_{\Omega} |\nabla f - v|^2 \tag{11}$$

In Equation (11), Ω is the foreground region of the synthesized image, and f is the pixel representation function in the merged image Ω. To improve the natural transition of synthetic images at the boundaries, a boundary smoothing mechanism was introduced in this study. First, a Poisson mixture algorithm is used to gradientally blend the foreground region with the background image, ensuring consistency in brightness and texture at the boundary. Specifically, the pixel values in boundary region $\partial\Omega$ are not directly taken from values outside the image but are adjusted based on the solution of the Laplace operator in the Poisson equation, thereby constructing a smooth transition of pixel value distribution in the boundary region. This process is illustrated in Equation (12).

$$\begin{cases} \Delta f^* = \Delta f_s & \text{in} \quad \Omega \\ f^* = f_t & \text{on} \quad \partial\Omega \end{cases} \tag{12}$$

In Equation (12), $\partial\Omega$ is the boundary of Ω, and f^* is the pixel representation function outside the boundary. f_t represents the gradient information of the source image. f_s represents the boundary value of the target background image; Δ represents the Laplace operator. The VA-FR method replaces key facial information in video content to further protect privacy. Finally, this study combines the VA-FR and VPM mechanisms to build the DPV-VPP model. Its structure is shown in Figure 6.

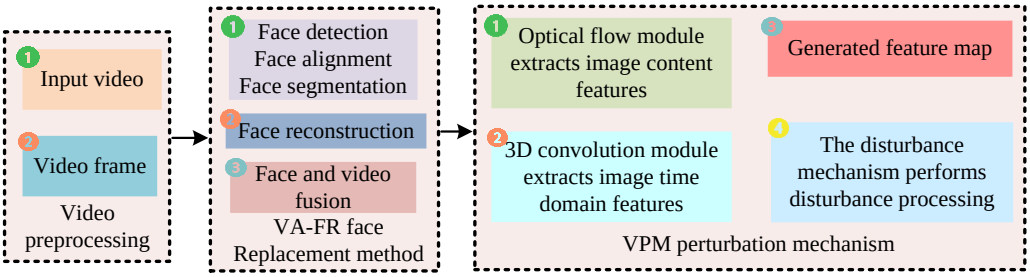


Figure 6: DPV-VPP model structure diagram.

As shown in Figure 6, the DPV-VPP model preprocesses the target video into frames. Then, the VA-FR mechanism replaces sensitive face information. Finally, the VPM mechanism perturbs the video frames, achieving two-layer protection.

4 Performance evaluation of the DPV-VPP model

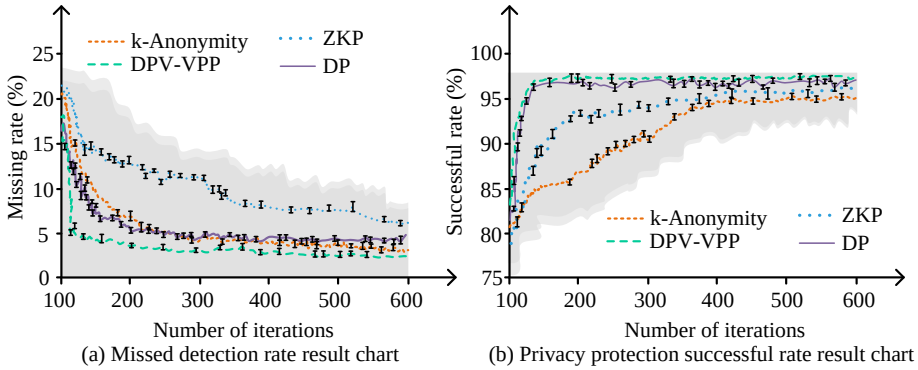
4.1 Experimental environment and training results of the DPV-VPP model

After the construction of the DPV-VPP model, in order to evaluate its performance in protecting privacy in video calls, the study introduced three domain-related models—K-Anonymity, DP, and Zero-Knowledge Proof (ZKP)—as comparison models. A Huawei Mate 30 device with a Kirin 990 chip was used as the local mobile terminal, while the cloud server was equipped with an Intel Xeon E5-2682 V4 CPU and an NVIDIA Tesla P4 GPU. The programming language used was Python, and the operating system was Windows 10. The Celebrity Deepfake Detection (Celeb-DF) dataset was used as the experimental dataset to provide test samples. Details of the Celeb-DF dataset are shown in Table 2.

As shown in Table 2, the Celeb-DF dataset suffers from a significant class imbalance problem, with the number of face-swapped videos (5639) far exceeding that of real videos (590), resulting in a ratio of real to fake samples of approximately 1:10. This severe imbalance may cause the model to favour identifying fake samples during training while neglecting its ability to distinguish real samples, leading to certain generalisation errors in real-world applications. To mitigate this bias, the study introduced a category weight adjustment mechanism and a stratified sampling strategy during training, and also adjusted the loss function with category weights. Based on the above experimental environment and the Celeb-DF dataset, the study first conducted experiments on the missed detection rate and privacy protection success rate for the four privacy protection models. The missed detection rate referred to the proportion of non-sensitive information that was incorrectly protected, while the privacy protection success rate referred to the proportion of sensitive information that was correctly identified and protected. The results represent the average value of five independent experiments run under the same data set and parameter configuration, with error bars representing the 95% confidence interval. The results are shown in Figure 7.

Table 2: Celeb-DF dataset details.

Parameter	Details
The number of themes	590
The number of deepfake videos	5639
Average duration	13s
Standard frame rate	30 frames per second
Video format	MPEG4.0



(a) Missed detection rate result chart (b) Privacy protection successful rate result chart

Figure 7: Results of missed detection rate and privacy protection success rate.

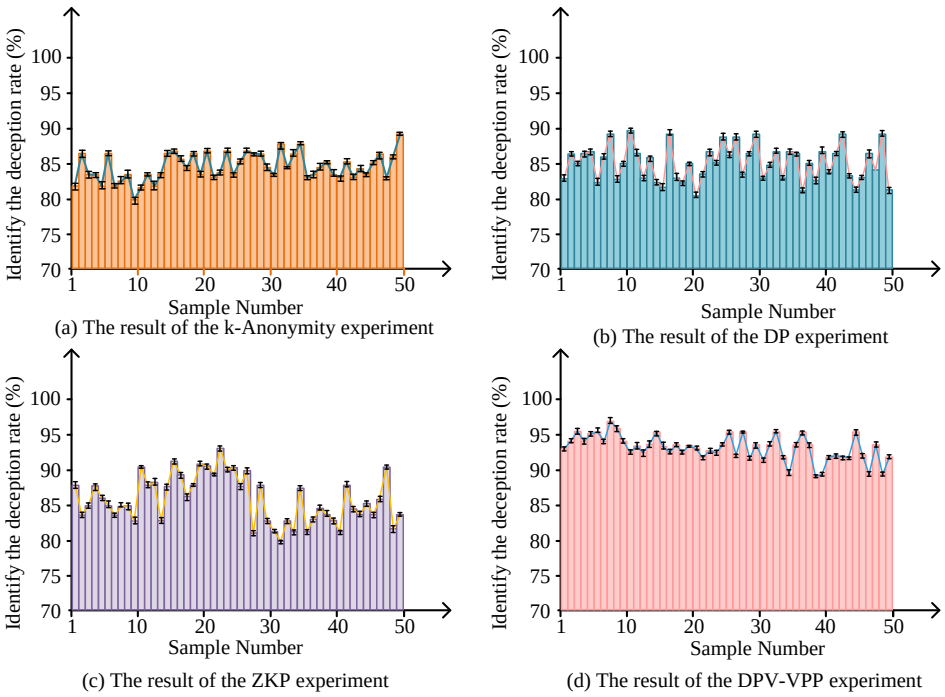


Figure 8: Successful deception rate experimental results.

As shown in Figure 7(a), the missed detection rates of the four models decreased steadily as the number of training iterations increased. When the number of iterations reached 389, 267, 214, and 145 respectively, the missed detection rates of ZKP, K-Anonymity, DP, and DPV-VPP stabilized at 7.4%, 5.2%, 5.8%, and 3.7%. These results showed that DPV-VPP achieved a lower missed detection rate compared to the other three models, indicating better performance in identifying sensitive information. As illustrated in Figure 7(b), after training, the privacy protection success rates of ZKP, K-Anonymity, and DP stabilized at 94.3%, 93.9%, and 96.1% respectively. The DPV-VPP model achieved a success rate of 96.9%, which was higher than the other three models. The results in Figure 7(a) and Figure 7(b) demonstrate that DPV-VPP achieved favorable performance in terms of both missed detection rate and privacy protection success rate, providing reliable data support for subsequent experiments. Next, the study conducted a comparison experiment on the deception success rate of the four models. The deception success rate referred to the probability that a privacy protection model successfully misled and deceived attackers, causing them to analyze or attack incorrect information. The study tested 50 samples using the ZKP, K-Anonymity, DP, and DPV-VPP models. The experimental results are shown in Figure 8.

Figure 8 presents the deception success rates of the four models. As shown in Figure 8(a), the K-Anonymity model reached a highest deception success rate of 87.5%. According to Figures 8(b) and 8(c), the highest deception success rates of the DP and ZKP models were 88.1% and 91.2%, respectively. Figure 8(d) shows that the DPV-VPP model achieved the highest deception success rate of 96.8%, surpassing the other three models. These results indicated that the DPV-VPP model successfully disturbed the original call data and effectively misled attackers, thereby reducing the attack success rate.

4.2 Practical performance evaluation of the DPV-VPP model

After verifying the training performance of the DPV-VPP model, the study further evaluated its practical applicability. The experimental environment and dataset remained consistent with the training experiments. The study first conducted experiments on the number of video frames processed per second for the four models. This metric measured whether the privacy protection model affected the smoothness of terminal usage. If the number of frames processed per second exceeded 30 fps, it indicated that the model did not cause noticeable latency. The results are presented in Figure 9.

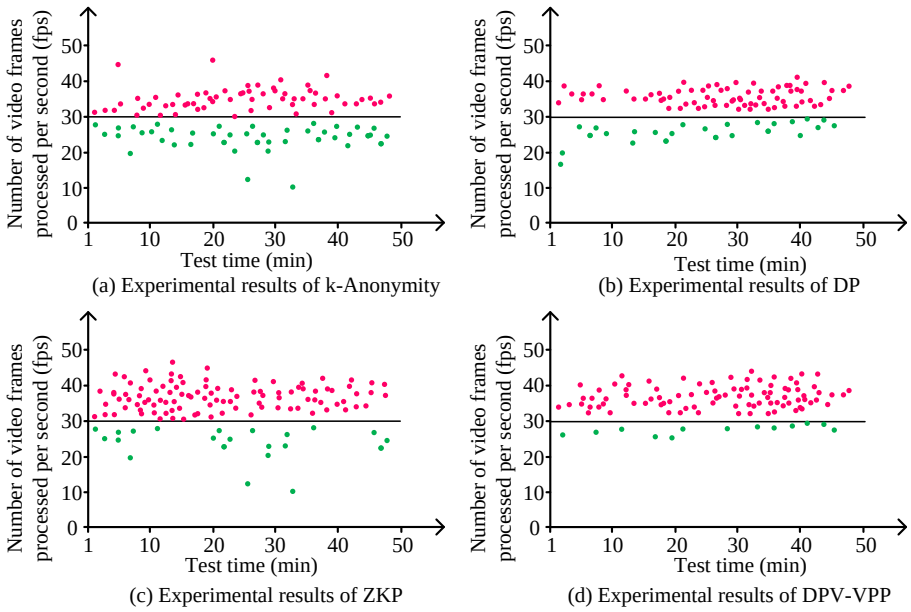


Figure 9: Experimental results of processing video frames per second.

In Figure 9, the average frame rate of the DPV-VPP model is approximately 34.0 fps, the DP model is approximately 32.0 fps, the ZKP model is approximately 30.5 fps, and the K-Anonymity model is approximately 29.0 fps. Based on the calculation of intra-sample variance, the 95% Confidence Intervals (CI) for the frame rates of all models are controlled within ±1.5-2.2 fps, indicating that the models exhibit strong real-time stability. As shown in Figure 9(a), the K-Anonymity model processed more than 30 frames per second in 75.1% of the samples, which was relatively low and could affect the smooth performance of the terminal. According to Figures 9(b) and 9(c), the proportions for the DP model were 84.4% and 91.1%, indicating a certain degree of impact on performance. Figure 9(d) shows that the DPV-VPP model achieved processing speeds above 30 frames per second in 95.1% of the cases, suggesting minimal impact on device smoothness. These results demonstrated the practicality and reliability of the DPV-VPP model in real-world applications. Subsequently, the study conducted experiments on the attack protection success rate of the four models. Two types of attacks were simulated: Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF), representing different levels of attack intensity. Although XSS and CSRF attacks typically target the platform logic layer, in actual video call systems, attackers can bypass video desensitisation modules by forging application programming interface requests or injecting scripts, thereby submitting unprotected raw image frames and causing user privacy leaks. The study deployed the DPV-VPP module in the front-end video capture process, using structural perturbation and face replacement mechanisms to ensure that even if the interface is tampered with, the system cannot access the original visual content. Therefore, XSS/CSRF attack simulations were introduced to verify the proposed method's indirect protective capabilities against potential visual content leakage attacks. In the simulated XSS and CSRF attack experiments, the study used a black-box attack method to test the protection capabilities of different visual privacy protection models. Attackers could not access model parameters and were only able to submit video frames embedded with attack payloads via standard HTTP interfaces. The results are shown in Figure 10.

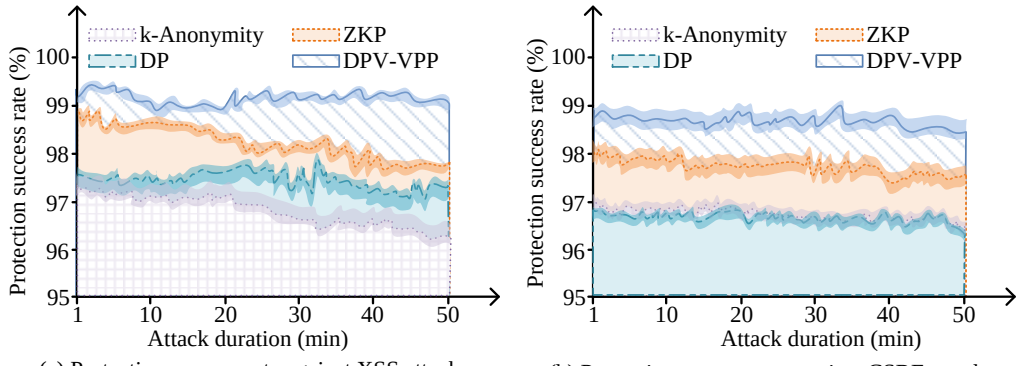
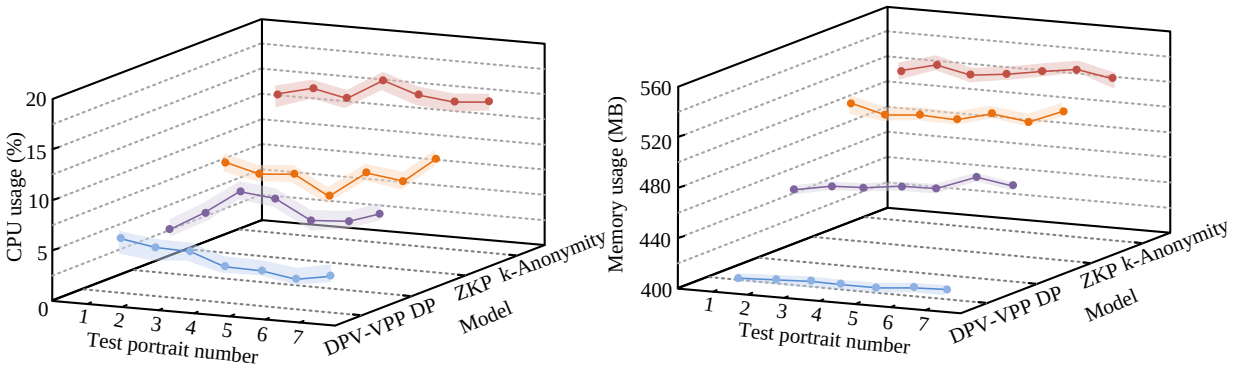


Figure 10: Protection success rate against XSS attacks and CSRF attacks.



(a) CPU usage experimental results

(b) Memory usage experimental results

Figure 11: CPU and memory usage experimental results.

As shown in Figure 10(a), after 50 minutes of XSS attacks, the protection success rates of ZKP, K-Anonymity, DP, and DPV-VPP were 97.8%, 96.5%, 97.4%, and 99.2%, respectively. The DPV-VPP model achieved the highest success rate among the four. According to Figure 10(b), after 50 minutes of CSRF attacks, the protection success rates of ZKP, K-Anonymity, DP, and DPV-VPP were 97.9%, 96.8%, 96.6%, and 98.9%, respectively. Again, DPV-VPP outperformed the other models. These results indicated that DPV-VPP consistently provided effective protection under attacks of varying complexity, demonstrating strong generalization capabilities. Finally, to further verify the practical applicability of the DPV-VPP model, the study evaluated CPU and memory usage while each of the four models processed seven test samples. The results are shown in Figure 11.

As shown in Figure 11(a), the K-Anonymity model exhibited high CPU usage, exceeding 10% in every test sample. For the ZKP and DP models, the highest CPU usage rates were 7.8% and 4.9%, while the lowest were 4.8% and 2.5%, respectively. In contrast, the DPV-VPP model achieved significantly better performance, with a maximum CPU usage of only 3.8% and a minimum of 0.9%. As shown in Figure 11(b), the DPV-VPP model consistently maintained memory usage below 405 MB across all test samples, significantly outperforming other models and demonstrating better resource stability and deployment adaptability. These results demonstrated that the DPV-VPP model did not interfere with normal call operations, further validating its excellent performance in practical scenarios.

5 Discussion

Compared with traditional differential privacy methods, DPV-VPP integrates two layers of protection mechanisms into its structural design. Compared with References [7] and [10], DPV-VPP combines a dynamic perturbation algorithm based on optical flow estimation and structural similarity analysis to adaptively adjust the perturbation intensity, effectively addressing privacy-sensitive areas of varying degrees in videos. Additionally, the VA-FR face replacement strategy based on VAE achieves deep semantic replacement and smooth boundary fusion in the target face region, addressing the limitations of traditional occlusion or blurring methods in terms of visual deceptiveness. Experiments show that DPV-VPP outperforms existing ZKP models, K-Anonymity processing methods, and GAN-based disguise generation techniques, particularly in terms of false detection rate (3.7%) and deception success rate (96.8%).

Furthermore, in terms of system resource control, the DPV-VPP model also demonstrates excellent real-time processing capabilities and terminal adaptability. In 95.1% of video frames, the frame rate exceeds 30fps, meeting the smoothness requirements for video call applications. In video tests on seven samples, CPU usage dropped as low as 0.9%, and memory usage remained under 406MB, with resource overhead significantly better than the multi-stage convolution-based face blurring processing methods proposed in References [11] and [14]. In terms of platform security testing, DPV-VPP achieved interception rates of 99.2% and 98.9% in evaluations against XSS and CSRF forgery attacks, respectively.

However, running dynamic perturbation and VAE replacement in parallel causes slightly higher memory usage when processing high-resolution videos. Future research will explore lightweight network architectures or model pruning optimisation strategies. Additionally, XSS and CSRF attacks primarily target platform interfaces and transmission processes. The protection provided by this method is primarily manifested in the irreversibility of content after front-end data perturbation and face replacement, representing an 'indirect protective effect' rather than a core design objective of the method itself. Therefore, the experiments in this section serve primarily as a reference for usability and compatibility verification in a system integration context. Future research will further focus on the portability and resource adaptation capabilities of DPV-VPP on mobile devices and edge computing platforms to enhance its engineering practicality.

6 Conclusion

Facing the continuous evolution of cyberattacks, traditional privacy protection methods have become increasingly ineffective in safeguarding users' call privacy. Therefore, this study put forward a dual-layer

privacy protection model, DPV-VPP, by combining a perturbation mechanism based on DP with face replacement using a VAE. Experimental results showed that DPV-VPP not only provided reliable privacy protection but also offered strong practical performance, meeting the demands of modern communication for privacy protection.

Although this study validated the privacy protection performance and practical applicability of the DPV-VPP model, there are still certain limitations. The study has not yet been deployed and validated in a real remote presentation system architecture platform, and there is a lack of testing of generalisation capabilities under complex facial expressions or lighting conditions. In the future, we will expand the adaptability of multi-person interaction scenarios, enhance adversarial robustness, and strengthen lightweight deployment capabilities.

References

[1] Daniele Scarpi, Gabriele Pizzi, and Shashi Matta. Digital technologies and privacy: State of the art and research directions. Psychology & Marketing, 39(9):1687-1697, 2022. https://doi.org/10.1002/mar.21692

[2] Md ABU IMRAN Mallick, and Rishab Nath. Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1):1-69, 02024.

[3] Ranjan Chaudhuri, Sheshadri Chatterjee, and Demetris Vrontis. Antecedents of privacy concerns and online information disclosure: Moderating role of government regulation. EuroMed Journal of Business, 18(3):467-486, 2023. https://doi.org/10.1108/emjb-11-2021-0181

[4] Jinshuo Dong, Aaron Roth, and Weijie J. Su. Gaussian differential privacy. Journal of the Royal Statistical Society: Series B (Statistical Methodology), 84(1):3-37, 2022. https://doi.org/10.48550/arXiv.1905.02383

[5] Jin H. Bae, Ruolin Liu, Eugenia Roberts, Erica Nguyen, Shervin Tabrizi, Justin Rhoades, Timothy Blewett, Kan Xiong, Gregory Gydush, Douglas Shea, Zhenyi An, Sahil Patel, Ju Cheng, Sainetra Sridhar, Mei Hong Liu, Emilie Lassen, Anne-Bine Skytte, Marta Grońska-Pęski, Jonathan E. Shoag, Gilad D. Evrony, Heather A. Parsons, Erica L. Mayer, G. Mike Makrigiorgos, Todd R. Golub, and Viktor A. Adalsteinsson. Single duplex DNA sequencing with CODEC detects mutations with high sensitivity. Nature Genetics, 55(5):871-879, 2023. https://doi.org/10.1038/s41588-023-01376-0

[6] Xiaokuan Zhang, Jihun Hamm, Michael K. Reiter, and Yinqian Zhang. Defeating traffic analysis via differential privacy: A case study on streaming traffic. International Journal of Information Security, 21(3):689-706, 2022. https://doi.org/10.1007/s10207-021-00574-3

[7] Lefeng Zhang, Tianqing Zhu, Ping Xiong, Wanlei Zhou, and Philip S. Yu. A robust game-theoretical federated learning framework with joint differential privacy. IEEE Transactions on Knowledge and Data Engineering, 35(4):3333-3346, 2022. https://doi.org/10.1109/TKDE.2021.3140131

[8] Guillem García Subies, Álvaro Barbero Jiménez, and Paloma Martínez Fernández. A comparative analysis of Spanish Clinical encoder-based models on NER and classification tasks. Journal of the American Medical Informatics Association, 31(9):2137-2146, 2024. https://doi.org/10.1093/jamia/ocae054

[9] Chiagoziem C Ukwuoma, Zhiguang Qin, Md Belal Bin Heyat, Faijan Akhtar, Olusola Bamisile, Abdullah Y Muaad, Daniel Addo, and Mugahed A Al-Antari. A hybrid explainable ensemble transformer encoder for pneumonia identification from chest X-ray images. Journal of Advanced Research, 48:191-211, 2023. https://doi.org/10.1016/j.jare.2022.08.021

[10] Yucheng Chen, Chenyuan Feng, and Daquan Feng. Privacy-preserving hierarchical federated recommendation systems. IEEE Communications Letters, 27(5):1312-1316, 2023. https://doi.org/10.1109/LCOMM.2023.3245101

[11] Wei Liang, Yang Yang, Ce Yang, Yonghua Hu, Songyou Xie, Kuan-Ching Li, and Jiannong Cao. PDPChain: A consortium blockchain-based privacy protection scheme for personal data. IEEE Transactions on Reliability, 72(2):586-598, 2022. https://doi.org/10.1109/tr.2022.3190932

[12] Mansoor Ali, Faisal Naeem, Muhammad Tariq, and Georges Kaddoum. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. IEEE Journal of Biomedical and Health Informatics, 27(2):778-789, 2022. https://doi.org/10.1109/JBHI.2022.3181823

[13] Tian Li, Huaqun Wang, Debiao He, and Jia Yu. Blockchain-based privacy-preserving and rewarding private data sharing for IoT. IEEE Internet of Things Journal, 9(16):15138-15149, 2022. https://doi.org/10.1109/JIOT.2022.3147925

[14] Bomin Mao, Jiajia Liu, Yingying Wu, and Nei Kato. Security and privacy on 6G network edge: A survey. IEEE Communications Surveys & Tutorials, 25(2):1095-1127, 2023. https://doi.org/10.1109/COMST.2023.3244674

[15] Antonio M. Larriba, Aleix Cerdà i Cucó, José M. Sempere, and Damián López. Distributed trust, a blockchain election scheme. Informatica, 32(2):321-355, 2021. https://doi.org/10.15388/20-INFOR440

[16] Mohammad Amin Satvati, Mehrdad Lakestani, Hossein Jabbari Khamnei, and Tofigh Allahviranloo. Deblurring medical images using a new grünwald-letnikov fractional mask. Informatica, 35(4):817-836, 2024. https://doi.org/10.15388/24-INFOR573

[17] Md Azher Uddin, Joolekha Bibi Joolee, and Kyung-Ah Sohn. Deep multi-modal network based automated depression severity estimation. IEEE transactions on affective computing, 14(3):2153-2167, 2022. https://doi.org/10.1109/TAFFC.2022.3179478

[18] Philippe Weinzaepfel, Vincent Leroy, Thomas Lucas, Romain Brégier, Yohann Cabon, Vaibhav Arora, Leonid Antsfeld, Boris Chidlovskii, Gabriela Csurka, and Jérôme Revaud. Croco: Self-supervised pre-training for 3d vision tasks by cross-view completion. Advances in Neural Information Processing Systems, 35:3502-3516, 2022. https://doi.org/10.48550/arXiv.2210.10716

[19] Hüseyin Firat, Mehmet Emin Asker, Mehmet İlyas Bayindir, and Davut Hanbay. 3D residual spatial-spectral convolution network for hyperspectral remote sensing image classification. Neural Computing and Applications, 35(6):4479-4497, 2023. https://doi.org/10.1007/s00521-022-07933-8

[20] Fabian Bach. Differential privacy and noisy confidentiality concepts for European population statistics. Journal of Survey Statistics and Methodology, 10(3):642-687, 2022. https://doi.org/10.48550/arXiv.2012.09775

[21] Punam Kumari, and Bhaskar Mondal. An encryption scheme based on grain stream cipher and chaos for privacy protection of image data on IoT network. Wireless Personal Communications, 130(3):2261-2280, 2023. https://doi.org/10.1007/s11277-023-10382-8

Low-Level and Attention-Enhanced GAN Framework for Facial Forgery Detection and Forensics

Mingzhen Zhang
School of Artificial Intelligence, Zhengzhou Railway Vocational & Technical College, Zhengzhou, 451460, China
E-mail: zhangmingzhenzhang@163.com

Keywords: facial information, forgery, forensics, GAN; attention mechanism

Received: April 10, 2025

With the rise of deepfake technologies, detecting fake facial images has become more difficult. Therefore, a forensic algorithm based on color and noise features is developed using generative adversarial networks for single facial forgery images to optimize extraction accuracy and efficiency. The multi-prediction partition spatial attention mechanism is simultaneously fused, and a complex processing facial forgery image forensics model is designed for multi-image processing, which improves the model's attention to forgery areas. The experimental results showed that the model could detect F1 scores of up to 94.21% for a single image, which was improved by 5.97% and 9.03% on the Celeb-DF dataset compared with Xception-DeepLab and DenseNet, respectively. The F1 score on the DFDC dataset was 93.02%, which was also 11.4% and 14.68% higher than the two mentioned above. The average forensic time was 0.29 seconds, which was significantly better than EfficientNet (0.51 seconds) and DenseNet (0.65 seconds). In the multi-image forensics task, the Area under the Curve (AUC) was the highest at 85.74% and the model complexity was the lowest at 80.54%, and the forensics latency was the shortest at 0.28 seconds, which was comprehensively better than the three mainstream comparison methods. This indicates that the proposed model can provide higher detection performance in fake images with different qualities and noise interference, and can provide an effective solution for the security verification and protection of facial information in future networks.

Povzetek: Članek predstavi LLF-MPPSA-GAN, dvo-vejični forenzični model za prepoznavanje ponarejenih obrazov. Združuje nizkonivojsko barvno-šumno analizo in večnapovedno prostorsko pozornost ter dosega odlične rezultate z latenco 0,28 s in visoko robustnostjo na šum.

1 Introduction

In recent years, technologies such as facial generation, face swapping, and enhancement have been widely used in film and television production, virtual reality, intelligent interaction, and other fields, bringing many conveniences to related industries. However, these technologies are also abused by criminals for malicious purposes such as creating false information, identity impersonation, and fraud, posing serious challenges to social public safety and personal privacy [1-2]. Especially, with the promotion of deep forgery technology, the generated fake facial images and videos are becoming increasingly realistic, making it difficult for traditional manual identification methods and low-level feature-based detection methods to effectively recognize, which poses new challenges to digital media forensics and information security. Zhu et al. designed a method based on 3D decomposition to highlight hidden forgery details to improve the effectiveness of existing facial digital information forgery detection. This method was more robust than traditional methods and had higher detection accuracy for fake facial images [3]. Ding et al. found that the deepfake technology of forged faces has posed a threat to electronic payments and identity verification. A countermeasure against deep forgery anti-fingerprint attacks was built. The faces under this strategy had high distinguishability from real faces [4]. Lan et al. adopted discrete cosine transform to perceive forgery trace features in the frequency domain to improve the detection level of facial forgery image information. A deep facial forgery forensics model with frequency domain and noise features was constructed. The model exhibited high forensic accuracy in multiple databases [5]. Liu et al. built a trajectory removal network based on adversarial learning to enhance the effectiveness of facial forgery forensics in deep forgery technology. The proposed trace removal method could reduce the detection accuracy of six state-of-the-art deep forgery detectors, thereby achieving efficient forensic results [6].

El-Shafai et al. proposed an adaptive unsupervised forgery image forensics algorithm by combining recurrent neural networks and multi-scale convolutional networks. The new method had higher accuracy and robustness compared with traditional methods in image and video forgery forensics [7]. Lai et al. proposed a new active forensics method that utilized pseudo-Zernike moment robust watermarking to embed

information into non-facial regions of video frames to enhance the facial swapping detection. This method had superior robustness to standard signal processing operations and excellent performance in detecting deep forgery operations [8]. Sharma et al. proposed a novel verification method to improve the authenticity and consistency judgment level of existing digital image tampering detection in digital photos. After combining the dataset standardization, the Generative Adversarial Network (GAN) was optimized. The experimental results showed that this method exhibited excellent processing accuracy and efficiency in verifying multiple facial digital photo information in forensic investigations, criminal investigations, and intelligence systems [9]. Video stitching forgery is an object-based intra frame forgery operation. Li et al. believed that stitched videos typically contained two different types of camera sensor mode noise. Accordingly, a video stitching detection and localization strategy based on camera fingerprints was proposed to address these two types of noise. This scheme could locate the tampered area and had high detection accuracy [10]. The summarized results for each method are shown in Table 1.

Table 1: Summary table of different methodologies

Method/Model	Description	Metrics/Advantages	Limitations
Zhu X et al. (3D Decomposition)	3D decomposition highlights forgery details	Acc≈91%, robust	Not noise-tolerant
Ding F et al. (Anti-fingerprint)	Countermeasure against fingerprint attacks	Recognition ↑ to 88%	Weak detail detection
Lan G et al. (Freq+Noise)	Frequency-domain forgery feature extraction	AUC≈90%, multi-dataset	Sensitive to low-freq
Liu C et al. (Trace Removal)	Trace removal to degrade detectors	Accuracy ↓ by 15%	Not a detection method
El-Shafai W et al. (RNN+CNN)	Unsupervised fusion of RNN and CNN	Image/video accuracy >89%	High training cost
Lai Z et al. (Watermarking)	Non-face watermark for swap detection	Deepfake detection ↑ to 91%	Requires watermark embedding
Sharma P et al. (Improved GAN)	Standardization + improved GAN	Forensic F1 score≈90%	Poor generalization
Li Q et al. (Camera Fingerprint)	Camera nose for splicing detection	Localization accuracy >92%	Limited applicability

In summary, some progress has been made in deep forgery forensics, with some methods improving detection accuracy and robustness through frequency domain feature extraction, adversarial learning, and watermark embedding. However, these methods still have certain limitations when facing complex forgery techniques, lighting, and resolution changes, especially on low-level feature extraction and multi-region fusion. Therefore, an improved GAN facial forgery forensics method that combines low-level feature extraction and partition space attention mechanism is proposed, aiming to further enhance the practical application value of facial forgery forensics and provide an effective auxiliary means for subsequent forensic work. The innovation of the research lies in optimizing color and noise feature extraction in single facial forgery detection, and introducing a multi-prediction partition spatial attention mechanism in multi-facial forgery detection, which improves the model's attention to forgery areas. In addition, the study adopts an efficient feature fusion strategy to optimize the accuracy and computational efficiency of evidence collection in complex environments. Compared with existing methods, this model performs stably under different levels of noise and image quality. The study proposes a GAN-based dual-architecture model that can handle single- and multi-sided forgery problems under different noise and quality conditions, utilizing underlying features and spatial attention to improve detection performance.

2 Methods and materials

2.1 Single facial forgery image forensics algorithm based on low-level features

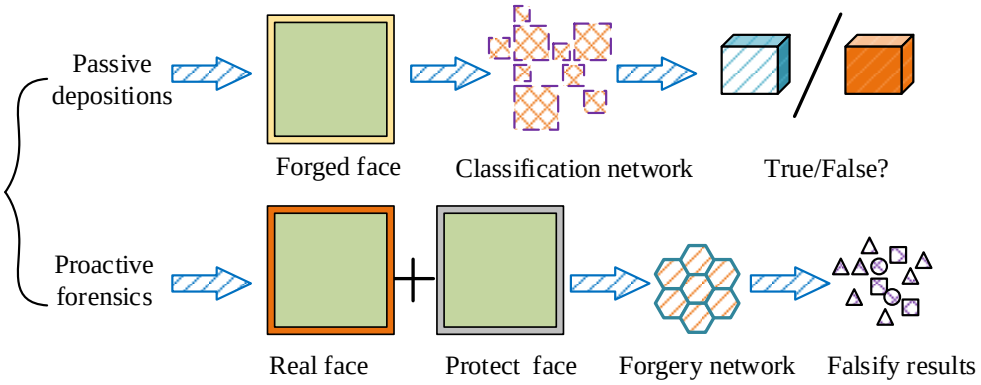


Figure 1: Forged facial image forensics technology principle.

In Figure 1, the basic framework of facial forgery image forensics has passive and active forensics. Passive forensics mainly takes a hierarchical network to classify input images, determine whether they are fake faces, and analyze them based on subtle differences in the images. Active forensics collection involves verifying the authenticity of input images, identifying forged images by comparing stored real facial images, and further detecting them through a forged network [15]. However, in cases where the image quality is high or there are minimal traces of forgery, traditional forensic algorithms may encounter recognition difficulties. In addition, the subtle changes in low-level features such as color and noise features in forged images are often overlooked, resulting in less-than-ideal detection performance of forged images [16]. Therefore, based on the GAN framework and optimized color and noise features as key features, a Low-level Feature-Generative Adversarial Network (LLF-GAN) based on GAN for facial forgery image forensics is proposed, as shown in Figure 2.

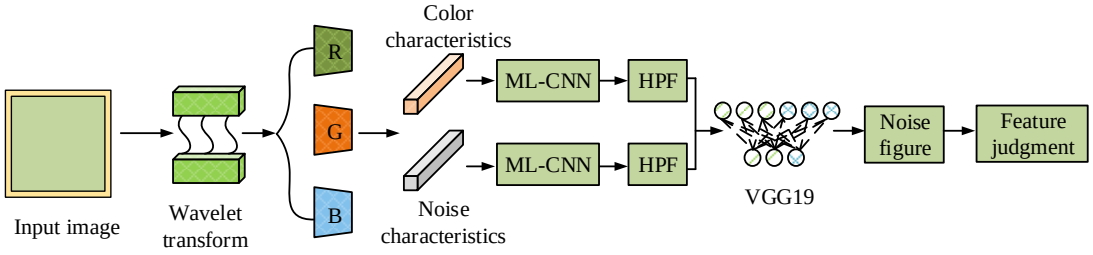


Figure 2: LLF-GAN algorithm framework (Discriminator-based model inspired by GAN structure).

In Figure 2, the LLF-GAN framework mainly consists of three core parts, i.e., the feature extraction module, the classifier module, and the final discriminant module. First, the input image is preprocessed by wavelet transformer and decomposed into three color channels, R, G, and B, respectively. On this basis, color features and noise features are extracted for each channel, respectively. Subsequently, the extracted color and noise features are jointly input into Multi-layer Convolutional Neural Network (ML-CNN), and the embedded High-Pass Filter (HPF) is used to further enhance the detailed features and edge texture, and eliminate the low-frequency background interference. In other words, ML-CNN and HPF are not directly applied to the original image, but are used to jointly process and enhance the extracted color and noise features. Then, these processed fused features are fed into a Visual Geometry Group 19-layer network (VGG19)-based classifier for deep feature learning and forgery discrimination. Finally, the classifier outputs the forgery probability of the image to determine the authenticity of the facial image. Assuming the image is in RGB format, color features can be extracted by converting it to HSV or YCbCr color space. The image color feature extraction is shown in equation (1).

$$C_{color} = \sum_{i=1}^{M}\sum_{j=1}^{N}\left| R_{i,j} - \frac{R_{avg}}{\sum_{k=1}^{M}\sum_{l=1}^{N} R_{k,l}} \right| \quad (1)$$

In equation (1), C_{color} represents the color feature of the image. $R_{i,j}$ represents the red channel value of the i-th and j-th pixels. R_{avg} represents the average value of the red channel in the image. M and N signify the width and height of the image. The noise capture is performed through local contrast and local noise, as displayed in equation (2).

$$C_{noise} = \sum_{i=1}^{M}\sum_{j=1}^{N}\left| \frac{I_{i,j} - I_{avg}}{I_{avg} + \varepsilon} \right| \quad (2)$$

In equation (2), C_{noise} represents the noise feature. $I_{i,j}$ represents the intensity values of the i-th and j-th pixels. I_{avg} represents the average intensity of the image. ε represents a small constant term. The fused low-level features is shown in equation (3).

$$F_{fusion} = \frac{\alpha C_{color} + \beta C_{noise}}{\alpha + \beta} \quad (3)$$

In equation (3), F_{fusion} represents the fused feature. α and β respectively represent the weight factors of

color features and noise features. In addition, as an important part of the entire algorithm framework, ML-CNN is shown in Figure 3.

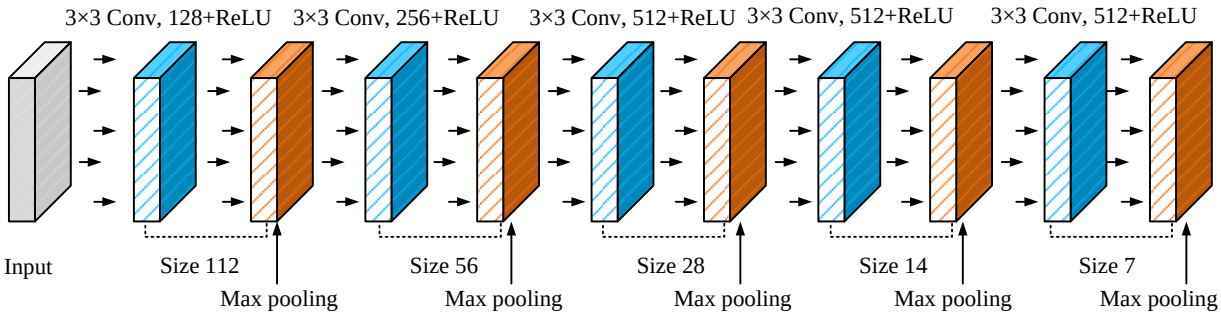


Figure 3: ML-CNN structure.

In Figure 3, the ML-CNN structure includes a combination of multiple convolutional layers and pooling layers, with each convolutional layer using a 3×3 convolution kernel and non-linear mapping processing through ReLU activation function. Each convolutional layer is followed by a 2×2 max pooling layer to lower the feature map size, and reduce computational complexity, and preserve important spatial information. After the input layer, ML-CNN performs a series of convolution and pooling operations on images with a size of 112×112, gradually extracting image features to more abstract levels, and ultimately obtaining high-dimensional features that can be used for classification. The ML-CNN feature extraction is shown in equation (4).

$$C_{conv} = \sum_{I=1}^{H}\sum_{j=1}^{W} W_{i,j} \cdot F_{i,j} + b \qquad (4)$$

In equation (4), C_{conv} signifies the feature after convolution operation. $W_{i,j}$ represents the convolutional kernel. $F_{i,j}$ represents the color and noise features after fusion processing. H and W signify the height and width of the input image. b signifies the bias term. The classification calculation for forged images in the classifier is shown in equation (5).

$$P(y=c|\ x) = \frac{e^{W_c^T F_{fusion} + b_c}}{\sum_{c'} e^{W_{c'}^T F_{fusion} + b_{c'}}} \qquad (5)$$

In equation (5), $P(y=c|\ x)$ signifies the probability that the image belongs to category c. W_c and b_c signify the weights and bias terms of the corresponding category. The final formula for determining the output face image at this point is shown in equation (6).

$$Output = \arg\max(P(y=c|\ x)) \qquad (6)$$

In equation (6), *Output* represents the output of the classifier. If the probability of $P(y=c|\ x)$ is high, it indicates that the type of image is forged.

2.2 Construction of a forensic detection model for multi-facial forgery images in complex scenarios

After constructing the forensics algorithm design for single facial forgery image, the research found that when the complexity of forgery image increases or in different environmental conditions, such as lighting changes, posture changes and image resolution, the traditional single feature and single model methods have certain challenges [17-18]. Specifically, a single prediction method based on low-level features may lead to misjudgments when processing high-quality fake images due to small differences in color and noise features [19]. To enhance the performance of the single forensic algorithm, a facial forgery image forensics method based on Multi-Prediction Partitioned Spatial Attention-Generative Adversarial Network (MPPSA-GAN) is proposed. This method introduces multiple sub-models for multi-angle prediction and combines partition spatial attention mechanism to better focus on forgery areas in the image. The framework structure of MPPSA-GAN is presented in Figure 4.

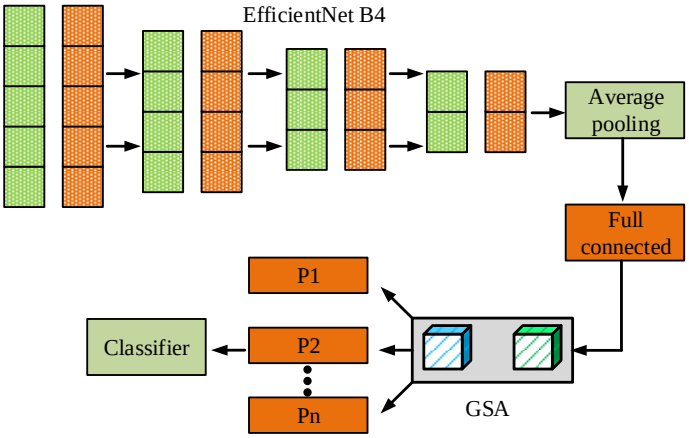


Figure 4: Frame structure of MPPSA-GAN (Discriminator-based model with partitioned attention, inspired by adversarial feature modeling).

In Figure 4, MPPSA-GAN has three main components: feature extraction module, multi-stage prediction module, and partition space attention module. Firstly, the input image undergoes feature extraction through the backbone network of Efficient Neural Network-B4 (EfficientNet-B4) to obtain preliminary image features. Assuming that the input image is I and the preliminary features obtained from feature extraction are F, the r predicted by each sub-model is presented in equation (7).

$$P_r = \sigma\left|\sum_{i=1}^{n} \omega_i \cdot f_i(r)\right| \tag{7}$$

In equation (7), ω_i represents the weight coefficient of each sub-model. $f_i(r)$ signifies the feature output of the i-th sub model on region r. σ represents the sigmoid activation function. P_r signifies the predicted probability of forgery in the region. To further enhance the spatial attention ability to the forged region, the Grouped Spatial Attention (GSA) mechanism is introduced to assign spatial features to each channel separately. The output of the j-th channel in region r is $f_j(r)$ and the spatial attention coefficient is α_j. The spatial attention aggregated feature value of region r is shown in equation (8).

$$A_r = \frac{\sum_{j=1}^{m} \alpha_j \cdot f_j(r)}{\sum_{j=1}^{m} \alpha_j} \tag{8}$$

In equation (8), m represents the number of features. The local feature weighting process fed to each submodel is used to enhance the information representation in the region of interest of the forgery by calculating the attention map A_r, i.e., the attention value A_r outputted by the GSA is used as a feature channel weighting factor embedded in the prediction paths of all sub-models to update the feature representations in their regions. Finally, all predicted results are fused and finally judged by a classifier to output the authenticity of the image. The module structure of GSA is shown in Figure 5.

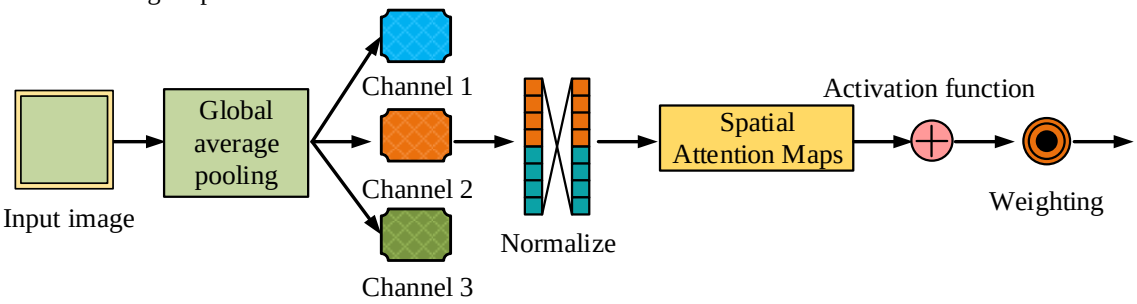


Figure 5: Module structure of GSA.

In Figure 5, the GSA module structure mainly consists of multiple processing units. Firstly, the input feature map is subjected to global average pooling to obtain the global information of each channel. Then, normalization is performed to adjust the scale of the feature map. Next, the spatial attention map is calculated to weight the features of different regions. The weighted feature map is used for subsequent processing. The entire process effectively captures important spatial regions through spatial attention mechanisms and enhances the expressive ability and performance in feature fusion. To enhance the fused region confidence calculation, the study introduces the intra-region feature scoring mechanism. The feature responses $f_k(r)$ of all channels in region r are combined with the scoring coefficients β_k to calculate their aggregation scores S_r. The calculation is shown in equation (9).

$$S_r = \sum_{k=1}^{m} \beta_k \cdot \left(\frac{f_k(r)}{\max_{r'} f_k(r')} \right) \quad (9)$$

In equation (9), r' represents the set of all regions. Finally, to realize the overall determination, all the region prediction results P_r are fused with the region weighting coefficients γ_r to output the forgery probability P -rate of the overall image, as shown in equation (10).

$$P = \frac{\sum_{r=1}^{N} \gamma_r \cdot P_r}{\sum_{r=1}^{N} \gamma_r} \quad (10)$$

In equation (10), γ_r denotes the global importance weighting factor of region r, which is usually calculated by combining r with region scoring S_r in the GSA module. The process embodies a step-by-step weighting mechanism from feature channel to region prediction, with α_j for spatial attention, β_k for channel scoring, and γ_r for region fusion, overall forming a hierarchical and clear chain of attention determination. By integrating the misclassification of forged images with the spatial attention weighting mechanism of the model, a composite loss function is constructed, as defined in equation (11).

$$L_{ce} = -\sum_{r=1}^{N} \left(y_r \cdot \log(P_r) + (1 - y_r) \cdot \log(1 - P) \right) \quad (11)$$

In equation (11), y_r represents the true label of region r, where forged is 1 and true is 0. L_{ce} represents cross entropy loss. The research combines the LLF-GAN forensic algorithm for single facial forgery images and the MPPSA-GAN algorithm for multiple images to propose an improved GAN-based complex facial forgery image forensic algorithm. The algorithm flow is shown in Figure 6.

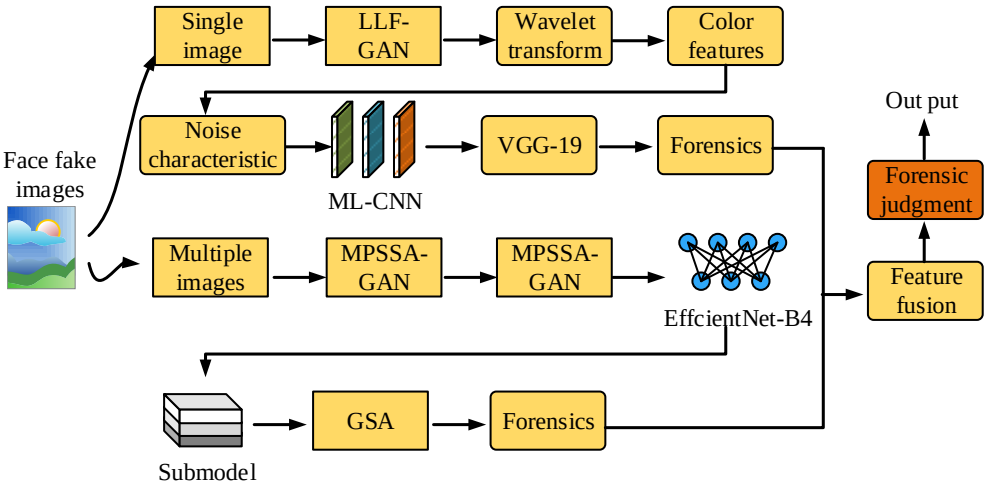


Figure 6: The unified architecture of the LLF-MPPSA-GAN model combining low-level and spatial-attention-based forensic branches.

As illustrated in Figure 6, the algorithm first conducts category-specific feature routing on the input image. Then, they are fed into two feature extraction branches, respectively. If the image is a single facial type, it will be processed through the LLF-GAN path, and low-level features such as color and noise will be extracted by wavelet transform. The feature reinforcement will be carried out by ML-CNN, and fed into the VGG19 classifier to complete the preliminary discrimination. If the image is a multi-facial or a more complex structure type, it is fed into the MPPSA-GAN path, and global semantic features will be extracted by the EfficientNet-B4. Multiple sub-models will process the image partition independently. EfficientNet-B4 is used to extract global semantic features, and image partitions are processed independently by multiple sub-models, and the forged regions are weighted and focused through the GSA module. The output features of the two branches are spliced in the fusion module and the final discrimination is performed by a unified classifier. For the forgery probability of the final output, the study sets a threshold of 0.5. If the probability is greater than 0.5, it is judged as a forged image. Otherwise, it is judged as a real image. The pseudo-code of the LLF-MPPSA-GAN algorithm is shown in Figure. 7.

```
# Input: facial image I
# Output: final forgery probability P_final

# Step 1: Low-level feature extraction via LLF-GAN
I_wavelet = WaveletTransform(I)
[R, G, B] = SplitChannels(I_wavelet)
color_feat = ExtractColorFeatures(R, G, B)
noise_feat = ExtractNoiseFeatures(R, G, B)
low_feat = Concatenate(color_feat, noise_feat)
LLF_feat = ML_CNN(low_feat)
LLF_enhanced = HighPassFilter(LLF_feat)
LLF_output = VGG19Classifier(LLF_enhanced)

# Step 2: Multi-region attention-based inference via MPPSA-GAN
F_init = EfficientNetB4(I)
region_preds = []
region_weights = []

for region r in Regions(F_init):
    # Multi-submodel prediction (Eq. 7)
    P_r = Sigmoid(Sum(w_i * f_i(r) for i in submodels))

    # Spatial attention weighting (Eq. 8, 9)
    A_r = ComputeGSA(r)          # attention map
    S_r = RegionScore(A_r, r)    # weighted region score

    region_preds.append(P_r)
    region_weights.append(S_r)

# Step 3: Region-level prediction fusion (Eq. 10)
P_MPPSA = WeightedAverage(region_preds, region_weights)

# Step 4: Final feature fusion and classification
P_final = FusionClassifier(LLF_output, P_MPPSA)

return P_final
```

Figure 7: Pseudo-code for the LLF-MPPSA-GAN algorithm.

3 Results

3.1 Performance testing of a new facial forgery image forensics model

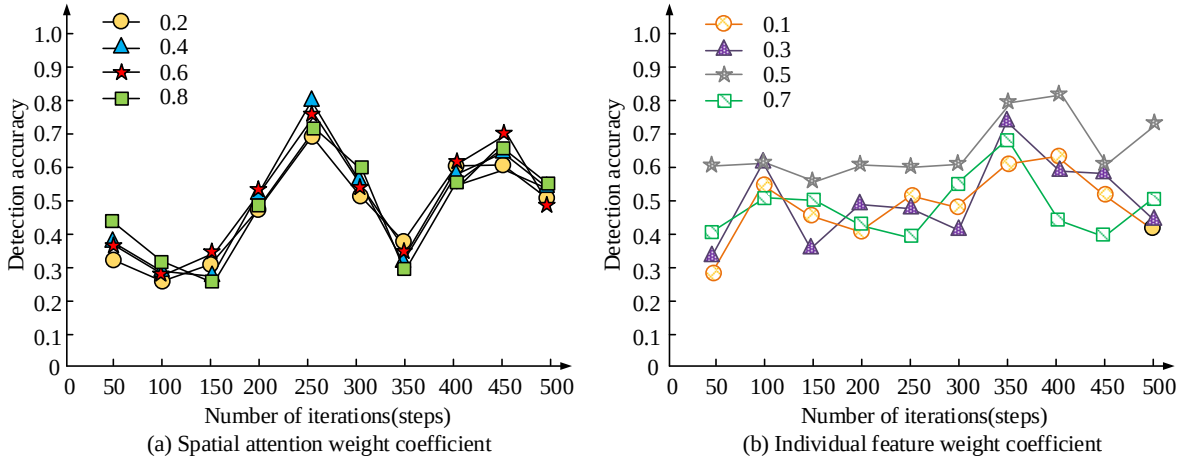
The research sets the CPU to Intel Core i7 3.6GHz, GPU to Nvidia GeForce GTX 1080 Ti, memory to 32GB, and uses Python 3.7 and TensorFlow 2.4 frameworks for model training and testing. The pre-training weights used in the modules are all obtained based on training on publicly available datasets and are fine-tuned in this study to fit the forgery image detection task. The pre-trained model of VGG19 is trained on ImageNet with about 143.7M parameters. EfficientNet-B4 is trained on ImageNet with about 19M parameters. In LLF-GAN, the classifier adopts the classical VGG19 network structure, which contains 16 convolutional layers and 3 fully connected layers. In MPPSA-GAN, the EfficientNet-B4 network, which consists of composite scaled convolutional modules with strong expressive power, is used as the feature extractor. Both are loaded with weights pre-trained on ImageNet and fine-tuned for this research task. For both LLF-GAN and MPPSA-GAN, cross-entropy loss is used as the main training objective function. In the overall integration model, the output losses of the LLF path and MPPSA path are each given the same weight, i.e., $\lambda_1 = \lambda_2 = 0.5$, and the final loss is the weighted sum of the two.

The experiments are evaluated based on two mainstream facial forgery datasets: Celeb-DeepFake Dataset (Celeb-DF) (a total of 5,639 videos with about 590,000 images extracted) and DeepFake Detection Challenge Dataset (DFDC) (19,000 images selected from it). The data is divided into 70% training set, 15% validation set, and 15% test set. The training process uses random level flipping and luminance adjustment for data enhancement, the total number of training rounds is 80, and the optimizer uses Adam (with an initial learning rate of $1e^{-4}$). Five-fold cross-validation is adopted. The experimental results are shown in Table 2. The mean ± standard deviation (std) of each metric is used to evaluate the generalization ability of the method. Both are loaded pre-trained weights on ImageNet and fine tuned them for this research task.

Table 2: Performance metrics results under five-fold cross-validation

Fold	Precision (%)	Recall (%)	F1 score (%)	Accuracy (%)
Fold 1	93.82	91.02	92.41	92.63
Fold 2	94.36	92.85	93.22	93.17
Fold 3	94.12	90.98	92.51	92.69
Fold 4	93.74	92.41	93.06	93.08
Fold 5	94.01	91.66	92.71	92.78
Mean ± standard deviation	94.01 ± 0.22	91.78 ± 0.67	92.78 ± 0.31	92.84 ± 0.25

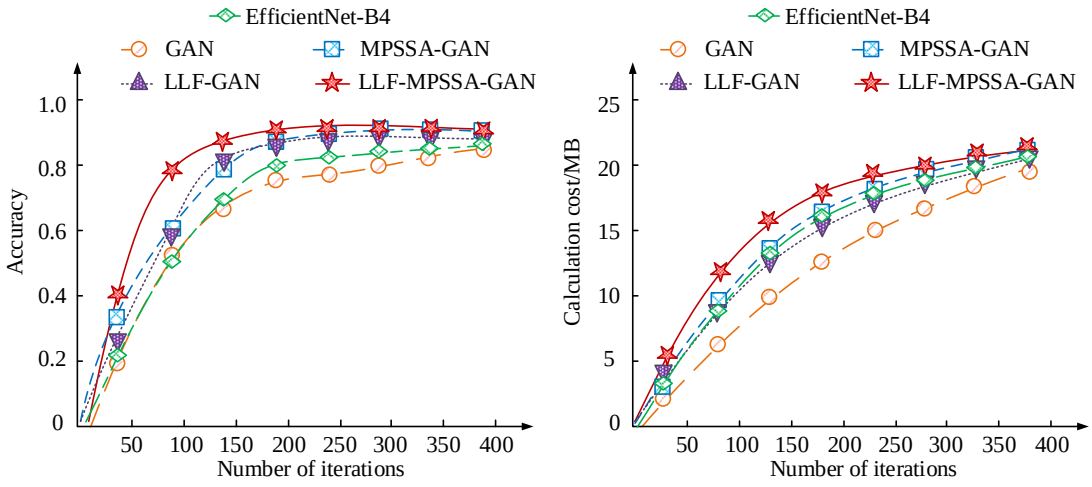
From Table 2, the proposed model showed good stability and robustness in five-fold cross-validation on the DFDC dataset. The fluctuations of each index in different folds were small, with the average precision reaching 94.01%, recall 91.78%, F1 score 92.78%, and accuracy 92.84%. The standard deviations were all controlled within 1%, showing that the model had consistent and excellent detection performance under different data divisions. This further validated the generalization ability of the proposed model, indicating its good adaptability and reliability in real complex environments. The study first conducts value validation on the two types of hyperparameters that have the greatest impact on model performance, namely the spatial attention weight coefficient α_j and the weight coefficient of individual features β_k. The test results are shown in Figure 8.



(a) Spatial attention weight coefficient (b) Individual feature weight coefficient

Figure 8: Hyperparameter selection test result.

Figure 8 (a) displays the spatial attention weight coefficient selection test. Figure 8 (b) displays the weight coefficient selection test for a single feature. From Figure 8 (a), as the spatial attention weight coefficient increased from 0.2 to 0.8, the detection accuracy fluctuated. The coefficients of 0.6 and 0.8 could achieve an accuracy of 0.7 at 250 iterations, while the highest accuracy was 0.8 at 0.4. In Figure 8 (b), when the weight coefficient of a single feature was 0.7, the accuracy reached 0.6 after 300 iterations, while it was only 0.55 when it was 0.1. The accuracy at 0.3 and 0.5 was 0.75 and 0.8, respectively. Higher or lower spatial attention weight coefficients and individual feature weight coefficients can lead to poor detection accuracy. When the spatial attention weight coefficient was 0.4 and the weight coefficient of a single feature was set to 0.5, the detection accuracy is significantly improved. In addition, the research conducts ablation tests on the combined model, as displayed in Figure 9.



(a) Ablation aCcuracy testing (b) Ablation calculation cost test

Figure 9: Ablation test results.

Figure 9 (a) displays the ablation test results under the DFDC. Figure 9 (b) displays the ablation test results under the Celeb-DF dataset. In Figure 9, the LLF-MPPSA-GAN model had the fastest convergence speed

in terms of accuracy improvement, reaching about 0.9 in about 150 iterations, and continued to lead the other models in the subsequent stages. In contrast, even after 400 iterations of the standard GAN model, its accuracy still did not exceed 0.85 and its convergence was significantly lagging. Meanwhile, in terms of computational cost changes, although the resource consumption of LLF-MPPSA-GAN was slightly higher than that of a single model, it consistently maintained a controllable growth during the iteration process and had a higher cost-effectiveness in terms of accuracy improvement, reflecting a better efficiency-performance balance. Combining the results of the two figures, it is verified that the proposed fusion model has strong convergence stability and resource utilization advantages while improving detection performance. The research introduces advanced forensic algorithms for comparison, such as Xception-DeepLab Network (Xception-DeepLab), EfficientNet, and Densely Connected Convolutional Network (DenseNet), Swin Transformers, Two-stream Convolutional and Long Short-Term Memory Networks (Two-stream CNN+LSTM). Precision, Recall, F1 score, and average forensic time are taken as indexes. Table 3 displays the results.

Table 3: Performance comparison of different facial forgery forensics algorithms on benchmark datasets.

Dataset	**Model**	**Precision / %**	**Recall / %**	**F1 score / %**	**Average time spent on depositions / s**	*p*
DFDC	Xception-DeepLab	87.98 ± 0.3	83.86 ± 0.4	81.62 ± 0.5	0.36	<0.01
	EfficientNet	86.33 ± 0.3	82.91 ± 0.3	80.88 ± 0.4	0.51	<0.01
	DenseNet	81.82 ± 0.4	77.25 ± 0.5	78.34 ± 0.5	0.65	<0.01
	Swin Transformer	88.94 ± 0.3	85.13 ± 0.4	84.71 ± 0.4	0.47	<0.01
	Two-stream CNN+LSTM	90.03 ± 0.2	86.57 ± 0.3	85.34 ± 0.3	0.52	<0.01
	Our model	94.36 ± 0.2	91.68 ± 0.2	93.02 ± 0.2	0.28	/
Celeb-DF	Xception-DeepLab	82.17 ± 0.4	81.07 ± 0.5	88.24 ± 0.5	0.35	<0.01
	EfficientNet	82.93 ± 0.4	83.39 ± 0.3	81.88 ± 0.4	0.48	<0.01
	DenseNet	83.98 ± 0.3	83.72 ± 0.4	85.18 ± 0.4	0.59	<0.01
	Swin Transformer	85.11 ± 0.2	84.02 ± 0.3	86.64 ± 0.3	0.43	<0.01
	Two-stream CNN+LSTM	86.85 ± 0.3	85.91 ± 0.3	88.42 ± 0.3	0.46	<0.01
	Our model	95.21 ± 0.2	93.02 ± 0.2	94.21 ± 0.2	0.29	/

According to Table 3, both Swin Transformer and Two-stream CNN+LSTM showed superior detection performance among the selected comparison methods on both DFDC and Celeb-DF datasets. Specifically, the F1 score of Two-stream CNN+LSTM on the DFDC dataset reached 85.34%, which was slightly higher than that of Swin Transformer (84.71%), and both of them were significantly better than traditional methods such as DenseNet and Xception-DeepLab. Meanwhile, the proposed LLF-MPPSA-GAN still had the most outstanding performance on the two datasets, with F1 scores of 93.02% and 94.21% on DFDC and Celeb-DF, respectively, which were significantly higher than all the comparison models. In addition, the computational efficiency of the model also had an obvious advantage. In terms of average forensic time, the proposed model achieved the fastest inference speed with 0.28s and 0.29s, which was better than Swin Transformer (0.47s / 0.43s) and Two-stream CNN+LSTM (0.52s / 0.46s), indicating that the proposed method maintained the high accuracy and has strong real-time performance and deployment potential. All results pass the two-tailed t-test with *p*-values less than 0.01, indicating that the performance improvement was statistically significant.

3.2 Simulation testing of a new facial forgery image forensics model

To evaluate the performance of a new facial forgery image forensics model, six types of facial forgery images are randomly obtained from the DFDC and pre-processed

to ensure the validity of the image data. The research compares forensic detection of six types of images with different qualities, taking Area under Curve (AUC) as the indicator, as displayed in Figure 10.

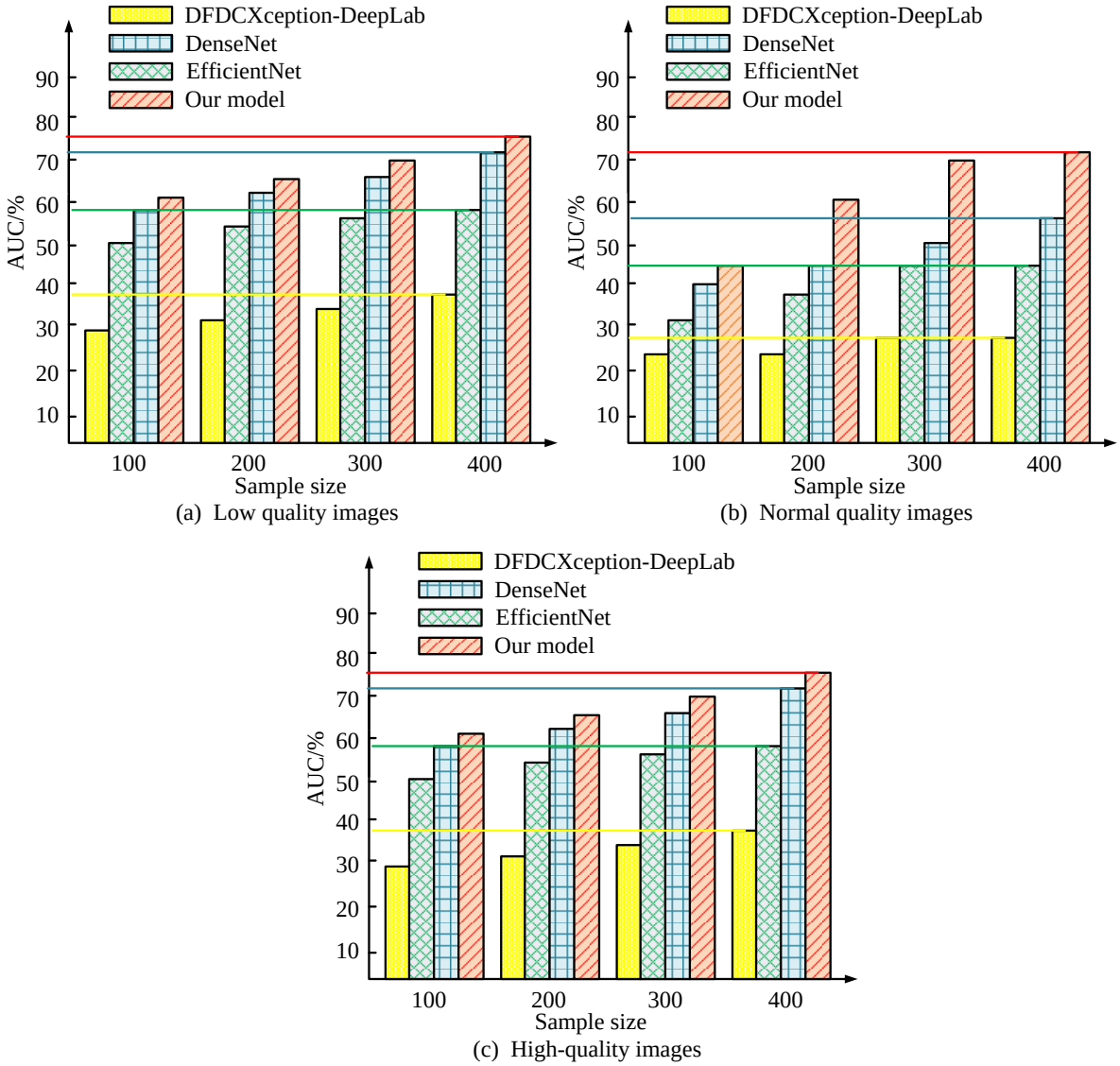


Figure 10: Forensic detection AUC results of forged images of different qualities.

Figure 10 displays the AUC results of forensic detection for low-quality forged images, normal quality forged images, and high-quality forged images. In Figure 10, the proposed model performed the best in low-quality forged images, with an AUC value of 68.34%, which was superior to Xception-DeepLab, EfficientNet, and DenseNet, with improvements of 28.23%, 23.77%, and 10.95%, respectively. In normal quality forged images, the AUC value of the proposed model was 75.56%, once again surpassing other models, especially when dealing with small samples, with an improvement of 28.32%. In high-quality forged images, the AUC of the proposed model reached the highest, at 85.74%, proving the high accuracy in dealing with high-quality forged images. Compared with Xception-DeepLab, EfficientNet, and DenseNet, the AUC values increased by 15.81%, 11.76%, and 9.87%. The proposed model has obvious advantages in various quality forged images, especially in detecting high-quality images, where the improvement in AUC value reflects its strong adaptability and robustness. The study conducts confusion tests on four types of forgery: emotion exchange, identity exchange, attribute editing, and global facial generation. The results are shown in Figure 11.

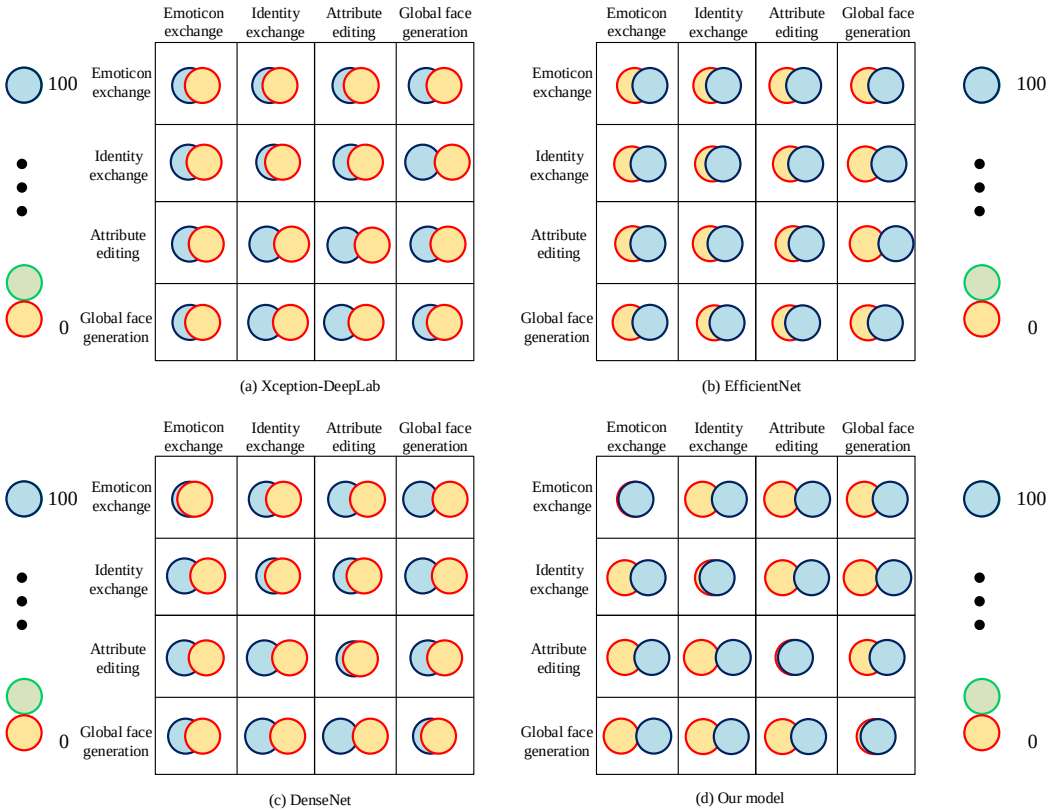


Figure 11: Confusion test results.

Figure 11(a) shows the Xception-DeepLab test results for the four types of forgery image confusion. Figure 11(b) shows the EfficientNet test results for the four types of forgery image confusion. Figure. 11(c) shows the DenseNet test results for the four types of forgery image confusion. Figure 11(d) shows the research method test results for the four types of forgery image confusion. From Figure. 11, the ability of the proposed model to distinguish four types of forgery types (expression exchange, identity replacement, attribute editing, and full-facial generation) was significantly better than the other models. In contrast, Xception-DeepLab, EfficientNet, and DenseNet had significant confusion between identity substitution and attribute editing with high error rates, especially in the full-facial generation task where the confounding judgment was particularly prominent. In addition, the proposed model maintained high accuracy on cross-recognition in all categories, especially showing clearer boundaries between expression swapping and attribute editing, which significantly reduced type confusion. This indicates that the proposed fusion model has stronger fine-grained recognition ability and structural discrimination, and can effectively deal with complex and diverse counterfeiting techniques. Taking the Receiver Operating Characteristic curve (ROC) as an indicator, the results are shown in Figure 12.

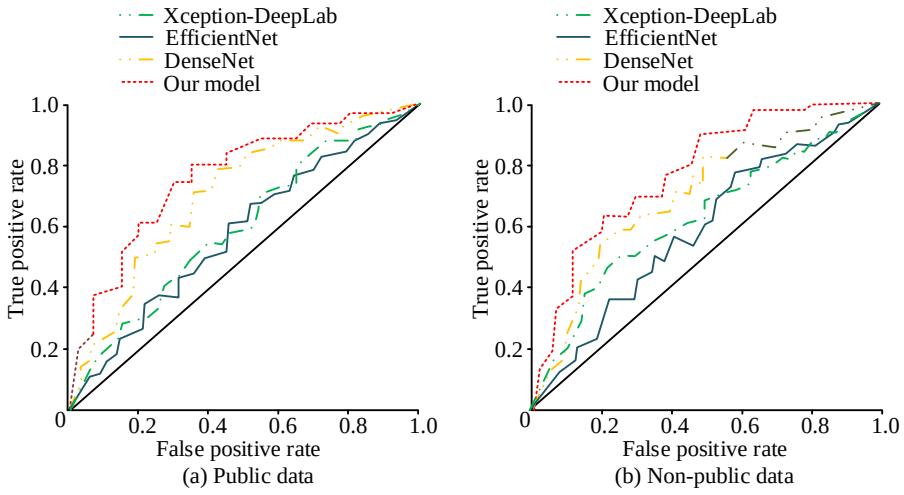


Figure 12: Statistical results of AUC indicators.

Figure 12(a) shows the ROC curves of different models in the public data, and Figure 12(b) shows the ROC curves of different models in the unpublished data. The horizontal axis represents the false-positive rate and the vertical axis represents the true-positive rate. The larger the AUC, which is enclosed by the ROC curve and the horizontal and vertical coordinates, the better the model performance. From Figure 12, the proposed model achieved optimal performance in both data conditions, with AUC values of 0.91 and 0.87, which were significantly higher than Xception-DeepLab (0.82 / 0.77), EfficientNet (0.84 / 0.79) and DenseNet (0.85 / 0.80). Especially in the non-public data test, the proposed model still maintained a large advantage, indicating its stronger robustness and generalization ability. Overall, the fusion structure not only improves the recognition accuracy on public forged images, but also significantly enhances its adaptability when facing unknown forged samples. The forged facial images with low noise, normal noise and high noise are detected using forensic Mean Average Precision (mAP), model complexity, and forensic delay as metrics. The results are shown in Table 4. The detection performance on low-noise, moderate-noise, and high-noise forged facial images is evaluated using mAP, model complexity, and processing latency, as presented in Table 4. All noises were added using a Gaussian distribution simulation, with different standard deviations set to correspond to low ($\sigma = 5$), medium ($\sigma = 15$), and high ($\sigma = 30$) noise intensities, respectively, and superimposed on the RGB channel of the image to generate interference samples.

Table 4: Robustness evaluation of forensic algorithms under varying noise conditions.

Type of noise	Model	mAP/%	Model complexity/%	Delayed depositions/%	FLOPs(G)	Memory (MB)	*p*
Low noise	Xception-DeepLab	89.34 ± 0.4	88.67	0.34	12.4	698	<0.01
	EfficientNet	90.12 ± 0.3	89.34	0.37	10.8	645	<0.01
	DenseNet	91.44 ± 0.3	90.22	0.32	13.5	732	<0.01
	Our model	92.98 ± 0.2	80.54	0.28	9.3	528	/
Normal noise	Xception-DeepLab	88.23 ± 0.4	87.46	0.35	12.4	698	<0.01
	EfficientNet	89.56 ± 0.3	88.97	0.31	10.8	645	<0.01
	DenseNet	90.87 ± 0.3	89.12	0.33	13.5	732	<0.01
	Our model	93.12 ± 0.2	83.88	0.29	9.3	528	/
High noise	Xception-DeepLab	84.56 ± 0.5	83.12	0.36	12.4	698	<0.01
	EfficientNet	85.12 ± 0.4	84.78	0.32	10.8	645	<0.01
	DenseNet	86.34 ± 0.4	85.54	0.34	13.5	732	<0.01
	Our model	89.23 ± 0.3	81.67	0.35	9.3	528	/

According to Table 4, under different types of noise interference, the proposed LLF-MPPSA-GAN model showed strong stability and advantages in terms of mAP value, model complexity, and delayed forensic performance. Taking high noise environment as an example, the proposed model still achieved 89.23% mAP, which was better than Xception-DeepLab (84.56%), EfficientNet (85.12%), and DenseNet (86.34%), and the complexity of the model stayed at 81.67%, which was much lower than the average of other models at about 85%-90%, verifying its lightweight and low-cost performance. This indicates the effectiveness of the lightweight design strategy. In terms of delayed forensics, the proposed model achieved the shortest forensics time under all types of noise conditions, with a minimum of only 0.28s, which further highlighted its real-time response capability. In addition, the research method is statistically examined on the mAP results of all the comparison models under three noise levels. The *p*-values obtained from two-tailed independent samples t-tests were less than 0.05, which indicated that the advantages of the research model on noise robustness are statistically significant.

4 Discussion

Aiming at the current facial forgery detection problems of insufficient multi-region sensing ability, low feature detail extraction efficiency, and poor robustness in complex environments, the study proposes a two-branch improved GAN forensic model, LLF-MPPSA-GAN, which integrates low-level feature extraction and multi-prediction partition spatial attention mechanism. The experimental results showed that on two mainstream datasets, DFDC and Celeb-DF, both achieved F1 scores of over 93% and mAP of over 89%, significantly outperforming DenseNet and Swin Transformer. Both achieved F1 scores over 93%, mAP stayed above 89% in multiple noisy environments, and the average inference time was as low as 0.28 seconds, which was significantly better than methods such as DenseNet, EfficientNet, and Swin Transformer. In a single image path, LLF-GAN, which fuses color and noise, enhances fine-grained feature perception and effectively locates low-frequency residual forgery traces. MPPSA-GAN combines the global semantic understanding of EfficientNet with the local weighting mechanism of GSA, enhancing the accuracy of multi region forgery recognition and improving the ability to capture edge contours and microstructural changes. Compared with the single-branch forgery recognition framework using attention convolution proposed by Lin K et al., the two-way parallel mechanism proposed in this paper significantly mitigates the ambiguous model recognition and weak local response when oriented to multi-class forgery scenarios [20]. Meanwhile, the feature scoring mechanism based on multi-stage fusion improves the accuracy of determining the forgery in different regions, further verifying the adaptability of the weight allocation strategy on complex samples. Despite the multi-module combination, the overall complexity of the model is still controlled at about 81%, and the inference latency is no more than 0.35 seconds, which possesses strong deployment efficiency and edge device adaptability. Especially under non-public data and high noise conditions, the AUC remains above 0.87, indicating its good generalization ability. Subsequently, the model can be further compressed and distillation or quantization strategies can be introduced to adapt to the real-time forensic task of embedded platforms, In addition, it can also enhance the recognition stability of dynamic video forgery and occlusion interference scenes.

5 Conclusion

A two-branch facial forgery forensic model LLF-MPPSA-GAN fusing low-level feature extraction and multi-prediction partitioned spatial attention mechanism was proposed to construct discriminative paths for single facial images and multi-region complex forgery scenarios, respectively and determine image authenticity through branch fusion. Experimental results showed that the method achieved better detection performance than existing methods on multiple benchmark datasets, and exhibited good stability and robustness in terms of noise interference, forgery type differentiation, and computational efficiency. The model can be widely used in the fields of social platform content censorship, judicial image appraisal, identity verification security, etc. It provides a feasible technical basis for the practical deployment of forgery forensics system while improving the practicality of deep forgery detection technology.

6 Future work and limitations

Although the proposed LLF-MPPSA-GAN model performs well on multiple datasets and test tasks, there are still several limitations that need to be emphasized. First, the current method performs forgery identification based on single-frame images, which is difficult to effectively capture cross-frame information changes, limiting the ability to detect dynamic video forgery. Second, the experiments are mainly based on two public datasets, Celeb-DF and DFDC, which cover common types of forgeries, but there are some limitations in the sample distribution and forging means. This may lead to model overfitting in real complex environments, and the generalization ability still needs to be further verified. In addition, for anomalous forgery images generated by other novel generative models (e.g., StyleGAN3 or Diffusion model), the detection robustness of the model has not been fully evaluated, and there may be misjudgments. Future work can consider introducing a multi-scale attention mechanism based on the Transformer structure to enhance cross-region feature interaction capability. A video level forensic framework can be constructed by combining multi-modal information such as audio synchronization, speech consistency, etc., to improve the perception depth of deepfake scenes. Zero sample or small sample forgery recognition methods can be explored to enhance the adaptability of the model to unknown forgery samples, thereby expanding its deployment value and practicality in real security scenarios.

References

[1] M. Tampubolon, (2024) "Digital face forgery and the role of digital forensics," International Journal for the Semiotics of Law-Revue Internationale De SÉMiotique Juridique, vol. 37, no. 3, pp. 753-767, https://doi.org/10.1007/s11196-023-10030-1

[2] M. T. Pham, T. T. Huynh, T. T. Nguyen, J. Jo, H. Yin, and Q. V. H. Nguyen, (2024) "A dual benchmarking study of facial forgery and facial forensics," CAAI Transactions on Intelligence Technology, vol. 9, no. 6, pp. 1377-1397, https://doi.org/10.1049/cit2.12362

[3] X. Zhu, H. Fei, B. Zhang, T. Zhang, X. Zhang, and S. Li, (2023) "Face forgery detection by 3d decomposition and composition search," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 7, pp. 8342-8357, https://doi.org/10.1109/TPAMI.2022.3233586

[4] F. Ding, B. Fan, Z. Shen, K. Yu, G. Srivastava, and K. Dev, (2022) "Securing facial bioinformation by

eliminating adversarial perturbations," IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 6682-6691, https://doi.org/10.1109/TII.2022.3201572

[5] G. Lan, S. Xiao, J. Wen, D. Chen, and Y. Zhu, (2022) "Data-driven deepfake forensics model based on large-scale frequency and noise features," IEEE Intelligent Systems, vol. 39, no. 1, pp. 29-35, https://doi.org/10.1109/MIS.2022.3217391

[6] C. Liu, H. Chen, T. Zhu, J. Zhang, and W. Zhou, (2023) "Making DeepFakes more spurious: Evading deep face forgery detection via trace removal attack," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 6, pp. 5182-5196, https://doi.org/10.1109/TDSC.2023.3241604

[7] W. El-Shafai, M. A. Fouda, E. S. M. El-Rabaie, and N. A. EI-Salam, (2024) "A comprehensive taxonomy on multimedia video forgery detection techniques: Challenges and novel trends," Multimedia Tools and Applications, vol. 83, no. 2, pp. 4241-4307, https://doi.org/10.1007/s11042-023-15609-1

[8] Z. Lai, Z. Yao, G. Lai, C. Wang, and R. Feng, (2024) "A novel face swapping detection scheme using the pseudo zernike transform based robust watermarking," Electronics, vol. 13, no. 24, pp. 4955-4963, https://doi.org/10.3390/electronics13244955

[9] P. Sharma, M. Kumar, and H. Sharma, (2023) "Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: An evaluation," Multimedia Tools and Applications, vol. 82, no. 12, pp. 18117-18150, https://doi.org/10.1007/s11042-022-13808-w

[10] Q. Li, R. Wang, and D. Xu, (2023) "A video splicing forgery detection and localization algorithm based on sensor pattern noise," Electronics, vol. 12, no. 6, pp. 1362-1367, https://doi.org/10.3390/electronics12061362

[11] L. Guarnera, O. Giudice, F. Guarnera, A. Ortis, G. Puglisi, A. Paratore, L. M. Q. Bui, M. Fontani, D. A. Coccomini, R. Caldelli, F. Falchi, C. Gennaro, N. Messina, G. Amato, G. Perelli, S. Concas, C. Cuccu, G. Orrù, G. L. Marcialis, and S. Battiato, (2022) "The face deepfake detection challenge," Journal of Imaging, vol. 8, no. 10, pp. 263-267, https://doi.org/10.3390/jimaging8100263

[12] H. Zhang, (2022) "A survey of anti-forensic for face image forgery," Journal of Information Hiding and Privacy Protection, vol. 4, no. 1, pp. 41-44, https://doi.org/10.32604/jihpp.2022.031707

[13] Y. Li, L. Ye, H. Cao, W. Wang, and Z. Hua, (2024) "Cascaded adaptive graph representation learning for image copy-move forgery detection," ACM Transactions on Multimedia Computing, Communications and Applications, vol. 21, no. 2, pp. 1-24, https://doi.org/10.1145/3669905

[14] S. Tyagi, and D. Yadav, (2023) "A detailed analysis of image and video forgery detection techniques," The Visual Computer, vol. 39, no. 3, pp. 813-833, https://doi.org/10.1007/s00371-021-02347-4

[15] H. Zhang, B. Chen, J. Wang, and G. Zhao, (2022) "A local perturbation generation method for GAN-generated face anti-forensics," IEEE Transactions on Circuits and Systems for Video Technology, vol. 33, no. 2, pp. 661-676, https://doi.org/10.1109/TCSVT.2022.3207310

[16] P. Sharma, M. Kumar, and H. Sharma, (2023) "Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: An evaluation," Multimedia Tools and Applications, vol. 82, no. 12, pp. 18117-18150, https://doi.org/10.1007/s11042-022-13808-w

[17] S. Cherian, J. Joseph, and B. Thomas, (2024) "Navigating the new normal: A bibliometric analysis of masked face recognition research using VOSviewer and Biblioshiny," Informatica (Slovenia), vol. 48, no. 22, pp. 193–212, December, DOI: 10.31449/inf. v48i22.6342.

[18] Y. Li, T. Xie, and D. Mei, (2025) "Using DTL-MD with GANs and ResNet for malicious code detection," Informatica (Slovenia), vol. 49, no. 14, pp. 63–78, March, DOI: 10.31449/inf. v49i14.7937.

[19] Sandhya, and A. Kashyap, (2024) "A comprehensive analysis of digital video forensics techniques and challenges," Iran Journal of Computer Science, vol. 7, no. 2, pp. 359-380, https://doi.org/10.1007/s42044-023-00165-6

[20] K. Lin, W. Han, S. Li, Z. Gu, H. Zhao, J. Ren, L. Zhu, and J. Lv, (2023) "IR-capsule: Two-stream network for face forgery detection," Cognitive Computation, vol. 15, no. 1, pp. 13-22, https://doi.org/10.1007/s12559-022-10008-4

Research on Fault Feature Extraction and Early Warning Method Based on MLP and Attention Mechanism CNN Fusion

Yanhua Shi
School of Information Engineering, Zhengzhou University of Technology, Zhengzhou 40053, China
E-mail: Yanhua_Shi@yeah.net

Keywords: fault feature extraction, attention mechanism, fusion technology, fault early warning method

Received: November 26, 2024

In modern industrial automation systems, fault feature extraction and early warning are the key technologies to ensure the stable operation of equipment. Traditional machine learning methods such as multi-layer perceptron often face the limitations of feature representation ability when dealing with such problems. In recent years, the attention mechanism combined with convolutional neural networks has become an effective way to improve the effect of feature extraction. CNN can effectively capture the spatial correlation in the image or signal by its local connection and weight sharing characteristics, and the attention mechanism can automatically focus on the most discriminative part among many features. The MLP is fused with CNN of attention matrix. Firstly, the original fault data is extracted by using CNN, and then the extracted features are weighted by attention module, emphasizing the most critical information for fault diagnosis. This fusion model not only inherits the nonlinear mapping ability of MLP, but also enhances the feature selection and representation ability of CNN in complex signal processing. Experiments show that the method can significantly improve the accuracy and robustness of fault feature extraction. Among 300 fault sample data, the S-network can correctly distinguish 295 fault types, and the early warning accuracy is more than 98%, which proves the effectiveness of the method. This study can achieve more effective early warning, reduce the cost of equipment maintenance, and improve the reliability of the system.

Povzetek: Raziskava združuje MLP in CNN z mehanizmom pozornosti za zgodnje opozarjanje na okvare v industriji. CNN izlušči prostorske značilnosti, pozornost poudari ključne signale, MLP izboljša nelinearno preslikavo.

1 Introduction

In the intricate tapestry of modern industrial systems, fault detection and early warning mechanisms loom large as a pivotal technology, ensuring the unwavering stability of equipment and augmenting production efficiency [1, 2]. Amidst the swift advancements in artificial intelligence, machine learning methodologies have come to occupy a paramount position in the realm of fault feature extraction and early warning systems. Notably, two deep learning paradigms, the Multilayer Perceptron (MLP) and the Convolutional Neural Network (CNN), have exhibited remarkable prowess across diverse domains, leveraging their distinctive advantages. Nonetheless, the inherent constraints of a solitary model have begun to surface, highlighting the need for a more comprehensive approach. Therefore, researchers began to explore the method of fusion of different models in order to obtain more powerful fault feature extraction capabilities.

As a feedforward neural network, MLP's basic structure is composed of input layer, multiple hidden layers and output layer, and it learns the internal laws of data by adjusting weights and biases [3]. It can deal with nonlinear problems, but it may face the problem of dimensional disaster and local optimal solution when dealing with high-dimensional complex data. In contrast, CNN performs well in the field of image processing, and it can effectively capture the characteristics of spatial levels through the combination of convolution layer, pooling layer and fully connected layer [4, 5]. The local perception and weight sharing mechanism of CNN make it have natural advantages in extracting local features, but its grasp of global information may not be as good as MLP.

In order to combine the advantages of the two, researchers propose a CNN model that combines MLP and attention mechanism [6]. This fusion model can not only take advantage of CNN's advantages in local feature extraction, but also enhance the understanding of global information through MLP. The introduction of attention mechanism enables the model to pay more attention to key feature areas when processing data, thereby improving the focusing ability and generalization performance of the model.

In the aspect of fault feature extraction, the fusion model can identify key fault-related signals from a large number of sensor data, even if these signals may be very weak or mixed with other interference signals. By learning and analyzing these key signals, the model can predict potential failure modes and issue early warning before failure occurs, thereby avoiding unexpected downtime

and production loss of equipment. In addition, the fusion model can adapt to changing industrial environments because it can automatically adjust its internal parameters to adapt to new data distributions [7, 8]. This means that the model can maintain high accuracy and reliability even when the equipment is aging or the working conditions change.

The CNN model combining MLP and attention mechanism provides a new and effective way for fault feature extraction and early warning. Through this integration strategy, we are expected to further improve the automation level of industrial systems, reduce human intervention, reduce operation and maintenance costs, and ultimately achieve the goal of intelligent manufacturing. Future research will continue to explore more efficient model fusion technologies and how to better apply these technologies to actual industrial scenarios.

2 Theoretical framework for the Fusion of MLP and attention mechanism CNN

2.1 Study on MLP model and CNN model

2.1.1 MLP model

MLP is a feedforward artificial neural network, which consists of at least three layers: input layer, one or more hidden layers and output layer. If there is more than one hidden layer, it is also called a deep artificial neural network [9, 10]. MLP models are trained using a back-propagation algorithm that minimizes prediction errors by adjusting weights and biases in the network. The MLP model's input layer processes incoming signals, while the output layer handles prediction and classification tasks. The hidden layer, situated between the two, constitutes the core computational unit. Data propagates from input to output, and neurons within the MLP learn through backpropagation. MLP neurons can employ various activation functions, incorporating weighted inputs and initial weights. Forward and backward propagation are outlined in Equation (1) and Equation (2).

$$a^{(l+1)} = \sigma(W^{(l)}a^{(l)} + b^{(l)}) \quad (1)$$

$$\Delta W^{(l)} = -\eta \frac{\partial J}{\partial W^{(l)}} \quad (2)$$

$a^{(l+1)}$ represents the output of the next layer, σ is the activation function, $W^{(l)}$ is the weight, $a^{(l)}$ is the output of the current layer, and $b^{(l)}$ is the deviation. W is the weight, η is the learning rate, and J is the loss function. In fault diagnosis, MLP model can be used to extract fault features from preprocessed data. For example, the characteristics of vibration amplitude, frequency and phase can be extracted, and then these characteristics can be used as inputs to establish MLP model for fault diagnosis. This method can help engineers quickly identify abnormal behavior of equipment, so as to take timely maintenance measures. In terms of fault early warning, the MLP model can be used to establish the operating state model of the equipment, and predict the future state of the equipment through real-time monitoring of the operating data of the equipment. For example, Shao et al. proposed a MLP-based residual life prediction method, which models the bearing operation state through a multi-layer perceptron, which can not only solve the residual life boundary problem, but also automatically adapt to changes in environmental factors [11]. In addition, Pan Lingyong proposed a method based on the combination of multi-feature fusion and MLP, which used the advantages of MLP in processing nonlinear data to classify and identify one-way valve faults, and realized the diagnosis of one-way valve faults of fracturing pumps.

2.1.2 CNN model

Convolutional neural network (CNN) is a deep learning model, which plays an important role in fault feature extraction and early warning. CNN can effectively extract fault-related features from time-series data, such as shock components in vibration signals, harmonic components in current signals, etc [12, 13]. These features are essential for identifying and predicting equipment failures.

$$S(i,j) = (I * K)(i,j) = \sum_m \sum_n I(i-m, j-n)K(m,n) \quad (3)$$

$$P(i,j) = max_{m,n \in R_{ij}} I(m,n) \quad (4)$$

Where $S(i,j)$ represents the result of convolution, I is the input data, K is the convolution kernel, and m and n are the indexes of the convolution kernel. The formula represents the calculation of the convolution result by sliding the convolution kernel over the input data and performing a weighted sum, which is the basic operation for extracting features in CNNs. $P(i,j)$ here denotes the result of pooling, and R_{ij} is the pooling area. In fault diagnosis, CNN can extract features with hierarchical structure from input data through convolution and pooling operations, which are shown in Equation (3) and (4). These features help to reveal the subtle changes in the operating state of the equipment, thereby providing strong support for fault early warning [14]. For example, in the analysis of vibration signals of mechanical equipment, CNN can capture characteristics such as vibration frequency and amplitude, which may indicate some failure modes of the equipment. In the quest for enhancing fault detection and early warning systems, the CNN stands out not only for its prowess in extracting fault features, but also for its capacity to collaborate with other state-of-the-art deep learning models [15, 16]. When paired with long-term and short-term memory networks (LSTM), the CNN-LSTM model emerges as a formidable contender. This hybrid approach harnesses the feature extraction process

of CNNs and the temporal modeling capabilities of LSTMs, adeptly navigating the intricate challenges posed by long-term dependencies in time series data. The resultant model is able to discern and learn the intricate evolution patterns of fault modes, thereby enabling precise and timely fault early warning.

2.2 Attention mechanism

The attention mechanism, a paradigm that emulates the intricate workings of human visual and cognitive systems, grants neural networks the ability to prioritize and focus on pertinent aspects within vast input data. By integrating this mechanism, neural networks are empowered to autonomously learn and selectively attend to salient information within the input, thereby elevating the model's performance and generalization capabilities [17]. In the realm of deep learning, attention mechanisms have found widespread application in the processing of sequential data, encompassing text, speech, and image sequences. Among the most notable varieties are the self-attention mechanism, which captures intrinsic dependencies, the spatial attention mechanism, which attends to spatial features, and the temporal attention mechanism, which focuses on temporal dynamics [18, 19].

$$e_t = v_a \tanh(W_s s_t + W_h h_t + b_a) \quad (5)$$

$$\alpha_t = \frac{exp(e_t)}{\sum_k exp(e_k)} \quad (6)$$

v_a, W_s, and W_h are the learnable parameters, s_t and h_t are information from different sources, and b_a is bias. The attention score is calculated using nonlinear activation (tanh). a_t is the normalized attention weight, e_t is the attention score calculated earlier, and K is the element. Attention weight calculation and attention weight normalization are shown in Equation (5) and Equation (6). A prevalent application in this realm involves the seamless integration of the attention mechanism within a bidirectional long-short-term memory neural network (BiLSTM), resulting in the BiLSTM-Attention model. This intricate architecture comprises an input layer, a BiLSTM layer, an attention layer, and an output layer. Specifically, the input layer is tasked with receiving preprocessed fault data, while the BiLSTM layer orchestrates the bidirectional processing of sequence information [20]. The attention layer, in turn, calculates the weight of each temporal step, performing a weighted summation of the BiLSTM layer's output to extract pivotal features from the fault data. Ultimately, the output layer yields the classification probability of the fault data.

Another noteworthy approach combines the prowess of CNN and long-short-term memory networks (LSTM) to forge the CNN-LSTM model. Here, the CNN component expertly extracts fault features from temporal data, while the LSTM segment models and classifies these time series. Leveraging CNN's feature extraction capabilities and LSTM's temporal modeling strengths, this hybrid model adeptly extracts fault features from time series data and categorizes faults accordingly.

The self-attention mechanism offers a direct mapping of the source text's word vector sequence X, generating the essential Q, K, and V components required by the attention mechanism [21, 22]. This approach calculates the attention weights among words within the source text, capturing word dependencies while simultaneously accomplishing encoding. The formulaic definition of the process is shown in Equation (7)-(9):

$$(Q,K,V) = Linear(X) = \begin{cases} Q = W^Q X \\ K = W^K X \\ V = W^V X \end{cases} \quad (7)$$

$$SelfAttention(Q,K,V) = softmax(\frac{Q^T K}{\sqrt{d_k}})V \quad (8)$$

$$e_t = v_a \tanh(W_s s_t + W_h h_t + b_a) \quad (9)$$

T stands for transpose operation. The sparsemax function is used instead of SoftMax, the formula definition of which is shown in formula (10), and the formal definition of the family of. α-entmax functions is shown in formula (11) and formula (12):

$$sparsemax(e) = \arg\min_{p \in \Delta^d} p - e^2 \quad (10)$$

$$\alpha - \text{entmax}(e) = \arg\max_{p \in \Delta^d} p^T e + H_\alpha^T(p) \quad (11)$$

$$H_\alpha^T(p) = \frac{1}{\alpha(\alpha-1)} \sum_{i=1}^{d} (p_i - p_i^\alpha) \quad (12)$$

d denotes the dimension, and pi is the *i-th* element in the probability p distribution. For a given attention score matrix A, its orthogonal regularization formula is shown in Equation (13):

$$R_O = AA^T - I_F \quad (13)$$

2.3 Research method of CNN fusion of MLP and attention mechanism

In the burgeoning domain of deep learning, the MLP and CNN occupy pivotal positions as common network architectures. Of late, researchers have embarked on an intriguing exploration, delving into the integration of attention mechanisms within these networks to elevate their performance and expressive prowess [23]. Here are

some research methods on the fusion of MLP and attention mechanism CNN:

External fusion methods. The external fusion method refers to first applying the convolution and attention mechanisms separately, and then combining their outputs in different ways. For example, Squeeze-and-Excitation Networks (SE-Net) is an external fusion method that computes channel attention weights through global average pooling and multilayer perceptrons, and then applies these weights to convolution outputs to dynamically adjust the degree of activation of individual channels.

Intrinsic fusion approach. The intrinsic fusion method refers to the fusion of convolution and attention mechanisms into a single operation. For example, the Convolutional Block Attention Module (CBAM) is an intrinsic fusion method that sequentially deduces attention graphs along two independent dimensions of channel and space, and then multiplies the attention graphs to the input feature graph for adaptive feature refinement [24, 25]. CBAM can be seamlessly integrated into any CNN architecture and can be trained end-to-end with the underlying CNN. The feature fusion process is shown in Equation (14).

$$F = \alpha F_{MLP} + (1-\alpha) F_{CNN} \quad (14)$$

Table 1 shows the comparison between MLP and CNN fusion methods. The external-internal fusion method refers to the fusion of convolution and attention mechanisms into a single operator (internal), and then applies conventional convolution or attention operations (external) on this basis. This approach attempts to combine the advantages of both in order to achieve better performance. Other fusion methods, such as Non-Local Neural Networks, model the global morning and afternoon through the Self-Attention mechanism, effectively capturing long-distance feature dependencies. In addition, some studies have proposed multi-spectral channel attention Fca-Net from the perspective of frequency domain, which makes full use of information by introducing more frequency components.

Table 1: Comparison of MLP and CNN fusion methods

Contrast dimension	MLP	CNN	MLP and CNN Fusion
Feature extraction ability	Suitable for linear and nonlinear feature extraction	Especially good at extracting local features, such as edges and textures in images and time series data	Combining the characteristics of the two, more abundant features can be extracted
Model complexity	Relatively simple and easy to train	The model structure is complex and requires more computing resources	Through fusion, model complexity and performance can be balanced
Training speed	Generally faster	Training may be slow due to complex structure	Fusion may achieve faster training speed
Generalization ability	Depends on data distribution and may be at risk of overfitting	Through local receptive field and weight sharing mechanism, it has good generalization ability	After fusion, the generalization ability of the model may be improved
Application Scenario	Classification and Regression Problems for Static Data	Suitable for image recognition, video analysis and other spatio-temporal data processing	Applicable to a wider range of data types and application scenarios
Noise resistance	Generally, not as good as CNN	Due to local receptive field and weight sharing, it has strong anti-noise ability	The anti-noise ability may be improved after fusion
Pros and cons:	training speed fast, the ability to extract local features is weak	The bureau is particularly strong and generalized well. The speed of training is slow, and the demand for resources is large	It is widely applicable, difficult to set, requires resources, and has poor interpretation

In the field of fault feature extraction and early warning, it is important to continuously explore better models to improve the accuracy and efficiency of fault diagnosis. Table 2 provides a detailed multi-dimensional comparison of the MLP-attention-based CNN fusion model and other existing state-of-the-art technologies, such as traditional MLP, traditional CNN, and ordinary CNN-MLP fusion models. The feature extraction ability determines whether the model can accurately identify fault-related features, and the fusion model can comprehensively and deeply mine key information with its unique structural design, while the traditional model has different limitations in this regard. Generalization ability and noise immunity are the key indicators to measure the performance of the model in complex and changeable real-world scenarios, and the fusion model shows strong adaptability and anti-interference ability, compared with the traditional model in the face of new data and noise environment. In terms of fault warning accuracy and training efficiency, the fusion model also has significant advantages, which can accurately warn faults in advance and complete training in a short time, providing a reliable and efficient solution for practical applications. Through the comparison of these dimensions, it can be clearly seen that the model based on the fusion of MLP and attention mechanism CNN has better performance in fault feature extraction and early warning tasks.

Table 2: Performance comparison table of CNN fusion models based on MLP and attention mechanism with other advanced technologies

Compare dimensions	A model based on the fusion of MLP and attention mechanism CNNs	Traditional MLP, CNN, etc
Feature extraction	Combining the advantages of MLP and CNN, the attention mechanism is used to accurately extract key features, which is comprehensive and in-depth	Traditional MLP local feature extraction is weak, CNN key information is not focused enough, and ordinary fusion model has limited extraction ability
Generalization and noise cancellation	Strong generalization ability, stable performance under different working conditions and data; Outstanding anti-noise capability to identify real signals in noise	Traditional MLP is easy to overfit, has poor generalization, and has average noise resistance; CNNs have limitations in complex scenes and strong noise, and the improvement of ordinary fusion models is not obvious
Early warning and efficiency	The accuracy of fault warning is high, which greatly reduces false positives and false negatives; High training efficiency, combined with MLP speed advantages and optimized calculations	The accuracy of traditional MLP early warning is limited, and the training speed is fast but the function is weak. CNN early warning is not comprehensive enough, training is slow, and the early warning and efficiency improvement of ordinary fusion models are limited

The fault feature extraction and early warning method based on MLP and CNN fusion combines the advantages of both, and can improve the generalization ability and anti-noise ability of the model while maintaining high accuracy. This fusion method is suitable for a variety of data types and application scenarios, especially when dealing with complex time series data and image data, it can effectively extract features and perform fault warning. Therefore, in practical applications, according to the specific fault diagnosis requirements and data characteristics, choosing a suitable fusion strategy and model structure can significantly improve the effect of fault diagnosis.

This paper introduces the relevant theories and algorithms of fault feature extraction and early warning methods, and presents a development trend from single model to model fusion. Firstly, the application of MLP and CNN models in fault diagnosis and early warning is described, MLP can extract fault features and establish a running state model, and CNN can extract fault-related features from time series data, both of which have their own advantages in fault diagnosis and early warning. Then, the attention mechanism is introduced, which is widely used in sequence data processing and can improve the performance of neural networks. Finally, the fusion methods of MLP, CNN and attention mechanism are emphatically discussed, including external fusion and internal fusion, and the fusion method combines a variety of advantages, which is suitable for more data types and application scenarios, and can improve the fault diagnosis effect.

3 Construction of early warning system based on MLP and attention mechanism CNN

MLP relies on its nonlinear mapping capabilities to carry out preliminary processing of data, realize feature extraction and pattern recognition, and provide basic features for subsequent processes. In this process, as

mentioned in the article, the weights and biases will be carefully adjusted during the training period, such as dynamically changing the weight values according to the actual data features and training objectives to optimize the effect of feature extraction, and at the same time, the bias will be accurately adjusted to ensure the stability of the model when processing different data. Subsequently, attention mechanisms were introduced into CNNs. CNN extracts feature by sliding on the input data and weighting summing through the convolution kernel, while the attention mechanism processes the channel and spatial dimensions of the feature map, highlighting key information and suppressing secondary information. When calculating attention weights, a series of complex calculations are involved, and the relevant parameters are constantly adjusted according to the feedback during the training process, so that the attention mechanism can focus on important information more accurately. Finally, the data that has been preliminarily processed by MLP is fused with CNNs that are integrated into the attention mechanism. There are many fusion methods, such as external fusion methods, which first perform convolution and attention mechanism operations separately, and then combine their outputs in a specific way; The intrinsic fusion approach combines convolution and attention mechanisms into a single operation. In the whole integration process, the data processing procedures of each link have strict specifications, and the parameter settings will be continuously optimized according to the actual situation, which not only ensures the efficient operation of the model, but also enhances the replicability of the whole model construction process, so that other researchers can reproduce the whole model construction process more accurately.

Building an early warning system based on multi-layer perceptron and attention mechanism convolutional neural network is an innovative project combining advanced technology of deep learning. Firstly, the system uses MLP to process the original data, and utilizes its nonlinear mapping ability to perform preliminary feature extraction and pattern recognition on the input data. Subsequently, the attention mechanism is introduced into CNN, which enables the network to focus on the most critical information when processing image or sequence data, similar to the process that human eyes automatically pay attention to important details when observing complex scenes. In this way, the early warning system can more accurately capture potential risk signals, so as to respond quickly before problems occur. The construction of the whole system not only depends on efficient algorithm design, but also requires a large amount of data support and fine parameter adjustment to ensure its accuracy and reliability in practical applications.

3.1 MLP-Mixer

MLP-Mixer is a novel network architecture that uses MLP to replace the convolution operation in traditional CNN and the self-attention mechanism in Transformer [26]. MLP-Mixer enables fusion between features through two fusion structures: spatial fusion and channel fusion. Spatial fusion allows features at different spatial locations to communicate, while channel fusion allows features between different channels to communicate. The core of MLP-Mixer is Mixer Layer, which maps columns and rows through MLP to realize the information fusion of spatial domain and channel domain.

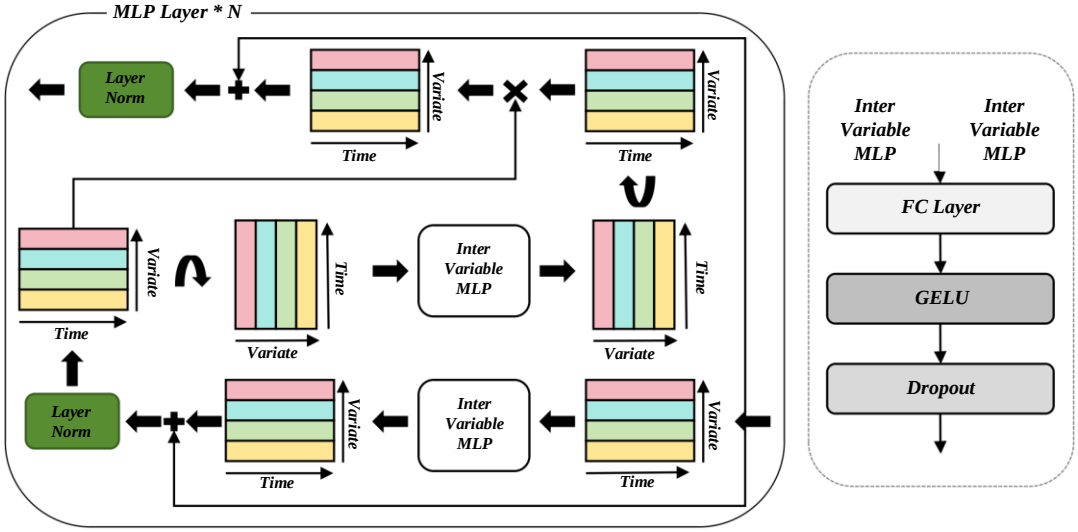


Figure 1: Converged MLP network architecture

Figure. 1 shows the fused MLP network architecture. When building an early warning system that fuses MLP and attention mechanism CNN, it is necessary to perform feature extraction, spatial fusion, channel fusion, processing of fused features, and predictive output. MLP-Mixer can be applied to image classification tasks, and its core idea is to use fully connected layers to replace the traditional CNN. Finally, the classification is carried out through the fully connected layer.

The new structure first uses MLP to preliminarily process the raw data to exert its nonlinear mapping capabilities, and then introduces the attention mechanism to the CNN, so that it can focus on key information and pay attention to important details like the human eye.

Compared with the previous one, the new structure data processing process is more refined, feature extraction and information attention are more accurate, the system performance and effect are better, the early warning can be more accurate and faster, and the data volume and parameter adjustment requirements are higher when building.

3.2 SE-Net and CBAM

SE-Net is an external fusion method that dynamically adjusts the importance of channels by obtaining feature maps through convolutional layers and then using global average pooling and multilayer perceptron (MLP) to capture the frequency and intensity distribution of each channel. SE-Net's Squeeze operation aggregates global information through global average pooling, while the Excitation operation dynamically adjusts the weight of channels according to the information obtained from the Squeeze operation, so as to strengthen the model's focus on key features [27, 28]. When building an early warning system that integrates SE-Net, MLP, and CNN, data preprocessing, CNN architecture design, SE-Net module integration, MLP integration, fusion strategy, training and verification, testing, and deployment are required.

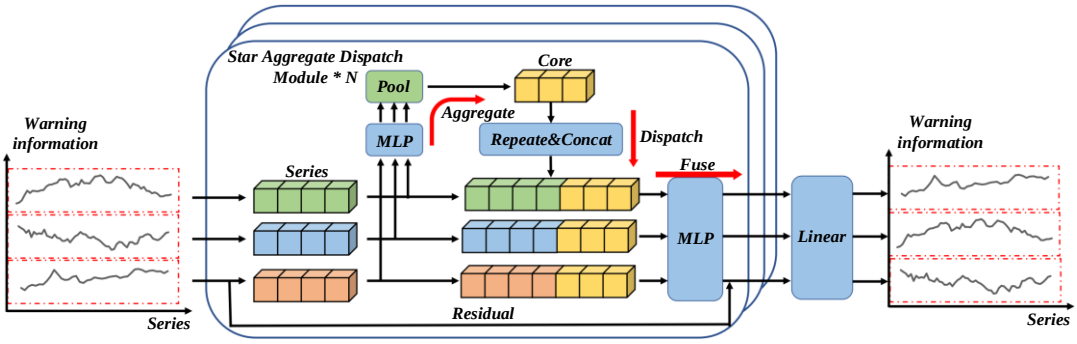


Figure 2: Early warning system fused by MLP and attention mechanism CNN

Figure. 2 shows the early warning system fused by MLP and attention mechanism CNN. By considering the channel and spatial dimensions of the feature graph, CBAM can highlight important features and suppress unnecessary features, thereby improving the performance of the model [29, 30]. In the early warning system where MLP and attention mechanism CNN are fused, CBAM can be used to strengthen the expression of features and help the system better understand and predict potential risks or anomalies. H stands for feature. The formal definition of the global attention layer is shown in Equation (15)-(19):

$$H' = mask_C(concat(H, P)) \quad (15)$$

$$\tilde{H} = \sigma(H'W_1 + b_1)W_2 + b_2 \quad (16)$$

$$att_g = softmax(\tilde{H}) \quad (17)$$

$$H_c = H'W_c + b_c \quad (18)$$

$$H_g = att_g^T H_c \quad (19)$$

3.3 System specifications for simulation

The construction of an early warning system based on multi-layer perceptron and attention mechanism convolutional neural network is an innovative project integrating advanced deep learning technology. The system first uses the nonlinear mapping ability of MLP to perform preliminary feature extraction and pattern recognition on the raw data, and then introduces the attention mechanism into the CNN, so that it can focus on key information when processing image or sequence data, so as to more accurately capture potential risk signals and respond quickly. The architecture of the system also adopts the novel architecture of MLP-Mixer, which replaces the convolution operation of traditional CNN and the self-attention mechanism of Transformer with MLP, realizes feature fusion through two structures: spatial fusion and channel fusion, and its core Mixer layer achieves information fusion between spatial domain and channel domain through MLP mapping columns and rows. In the data processing process, feature extraction is carried out first, and then the spatial and channel fusion is completed in the MLP-Mixer architecture, and then the fusion features are further processed. The system can be applied to image classification tasks, culminating in classification by fully connected layers. The construction of the whole system relies on efficient algorithm design, a large amount of data support and fine parameter adjustment to ensure the accuracy and reliability in practical applications.

4 Experimental design and analysis

4.1 Construction of program index system

In constructing the index system of fault feature extraction and early warning scheme fused by MLP and attention matrix CNN. Initially, a rigorous signal preprocessing procedure is enacted, encompassing denoising techniques to mitigate unwanted interference components, filtering

methods to refine signal clarity, and normalization processes to enhance overall signal quality. Following this, a feature extraction step is executed, leveraging the fast Fourier transform to transform the time-domain signal into its frequency-domain representation, thereby elucidating the spectral characteristics of the signal. At the same time, the time domain signal is extracted by convolutional neural network operation. In this way, the model can obtain the feature information in time domain and frequency domain at the same time. Secondly, on the basis of feature extraction, the time-domain and frequency-domain features are fused by using cross-attention mechanism. By calculating the attention weight, the model can pay attention to more important feature information and enhance the ability of fault feature recognition. The realization of cross-attention mechanism can be accomplished by multi-layer perceptron or self-attention mechanism.

The model uses cross-entropy loss to supervise the classification task, defined as Equation (20). The final training loss L is defined as in Equation (21):

$$L_{sc} = -\sum_{(s,a)\in D} y_{(s,a)} \log(\hat{y}_{(s,a)}) \quad (20)$$

$$L = L_{sc} + \alpha L_{con} + \varepsilon \square \theta \square^2 \quad (21)$$

In the experiment, a large number of parameters related to multilayer perceptron (MLP) and multilayer perceptron (CNN) and attention mechanism were defined. In MLP, $a^{(l+1)}$ represents the output of the next layer, σ is the activation function, $W^{(l)}$ is the weight of the l layer, $a^{(l)}$ is the output of the current layer, *b(l)* is the bias of the first layer, *W* is the weight, n is the learning rate, and J is the loss function. For CNN, *S(i,j)* is the convolution result, I is the input data, *K* is the convolution kernel *m*n* and *n* is the index of the convolution kernel, *P(i,j)* is the pooling result, and *Rij* is the pooling region. In the attention mechanism, v_a, W_s, and W_h are the learnable parameters, s_t and h_t are the information from different sources, b_a is the bias, e_t is the attention score, *t* is the normalized attention weight, *K* is the element, *T* is the transpose, *d* is the dimension, and *Pi* is the *i-th* element in the probability p distribution. In addition, there is the parameter *L*, which represents the loss function, and MSE, which is the mean square error. After that, the fused features are input into the classifier for fault classification. Classifiers can employ algorithms such as support vector machines, random forests, or deep learning models. By training and optimizing the classifier, the bearing fault can be identified accurately. Subsequently, the model's performance is rigorously assessed through the utilization of various evaluation metrics, including the confusion matrix, accuracy rate, precision rate, recall rate, and F1 score. These indices offer a comprehensive understanding of the model's efficacy across diverse categories, as well as its overall diagnostic accuracy. Figure. 3 depicts the outcomes of this performance evaluation. Guided by the results of this evaluation, the model undergoes adjustments and optimizations, such as the refinement of the network structure and the tuning of parameter settings. These modifications aim to enhance the diagnostic capabilities of the model. Ultimately, once the stability and reliability of the model's performance are assured, it is integrated into a practical fault prediction and early warning system, enabling real-time monitoring of equipment status and the timely detection and mitigation of potential faults.

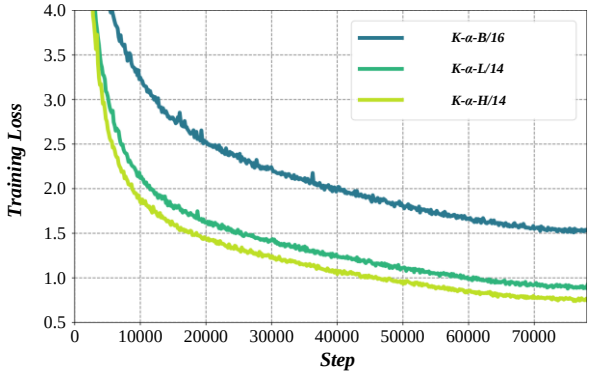


Figure. 3 Results of the performance evaluation

4.2 Scheme design and implementation

When building a machine learning model, the data is usually divided into a training set, a verification set, and a test set. These three data sets are used to train and optimize the model, and finally obtain the best effect and the best generalization ability we want. model. After the division of the training set, verification set and test set is completed, this paper first uses the training set to train the initially constructed model, and checks the prediction results of the fitted model, because the training set is used to fit the training set. At this time, the results obtained by the model should theoretically be high, that is, the effect of the model should be better; After the training of the training set is over, it is necessary to obtain different prediction accuracy rates by continuously adjusting the values of the parameters. The model with the highest accuracy rate obtained in the end is identified as the model with the best effect; After determining the optimal model through the verification set, it is necessary to use the test set to check whether the model is optimal or not. After determining the selected model, the training set is used to train the model.

5 Rationality test and implementation approach of cnn fusion scheme of MLP and attention mechanism

5.1 Model evaluation

When evaluating a fault feature extraction and early warning model of a convolutional neural network that combines a multi-layer perceptron and an attention mechanism, we mainly focus on its accuracy, robustness, real-time performance, and generalization capabilities.

This fusion model aims to improve the performance of fault detection through the nonlinear mapping ability learned by MLP and the spatial feature extraction ability of CNN, as well as the focus of attention mechanism on key information.

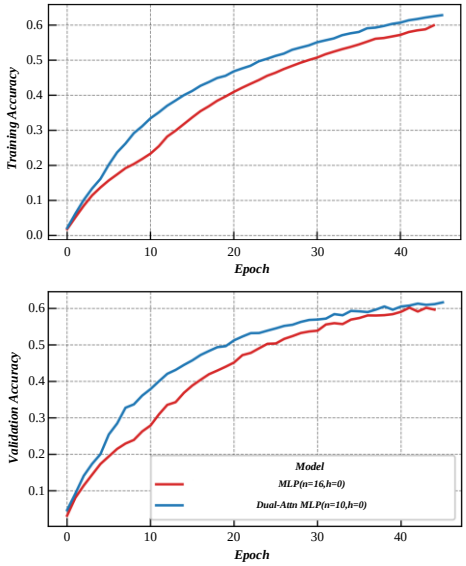


Figure 4: Accuracy results of the model

The accuracy of the model is measured by comparing the consistency of the predicted results with the actual fault state, as shown in Figure. 4. The high accuracy rate means that the model can effectively identify the real fault mode, while the low false positive rate and false negative rate indicate that the model has good discrimination in distinguishing normal and abnormal states. To verify this, cross-validation is often performed on a dataset containing multiple fault types to evaluate the model's performance in different scenarios. This figure intuitively compares the changes in the training and validation accuracy of different models, and evaluates the effectiveness of fault feature extraction and early warning methods based on the fusion of MLP and attention mechanism CNN. The comparison of the training and validation accuracy of the two models (MLP and Dual-Arm MLP) under multiple epochs shows that the training accuracy of the fusion model increases rapidly and is high, and the verification accuracy is also better, which proves that its performance and effect are better than those of the traditional MLP model, providing evidence for the advantages of the fusion method.

Figure. 5 is the robustness analysis of feature visualization. Robustness refers to the stability of the model in the face of noise interference or input data changes. A robust model can maintain high detection performance even in harsh environments, which can be tested by adding noise or data collected under different conditions. In addition, the real-time performance of the model is also an important indicator, especially in industrial applications, timely fault warning can avoid major losses. Therefore, evaluating the processing speed and response time of the model is very important to determine its practical application value.

The generalization ability reflects the adaptability of the model to unseen data or new types of failures. An excellent model must not only perform well on training data, but also be able to make accurate predictions on new and unknown fault samples. By evaluating the model on an independent test set, we can understand its generalization ability, and accordingly adjust the model parameters or improve the algorithm to improve its reliability in future applications.

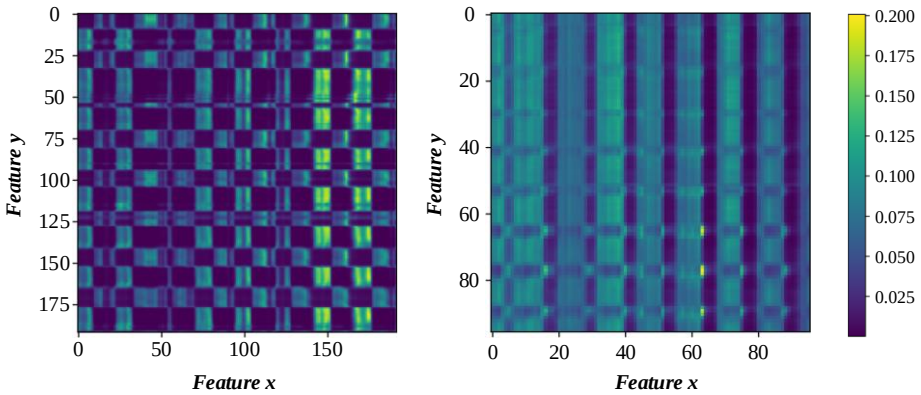


Figure 5: Robustness analysis of feature visualization

5.2 Comparison of effect between this scheme and other schemes

In modern industrial systems, fault feature extraction and early warning technology is the key to ensure the stable operation of equipment. Traditional feature extraction methods such as multilayer perceptron and convolutional neural network have their own advantages, but also have limitations. MLP is known for its powerful non-linear fitting capabilities, able to learn complex feature maps, but may encounter dimensional disasters when processing high-dimensional spatial data. In contrast, CNN can effectively capture local features of image data through local connection and weight sharing mechanisms, but it may not be sensitive enough to unstructured signal data.

A reasonable diagram can be made as follows: the purple curve is a model with only MLP (no attention mechanism); The red curve is the CNN fusion model of MLP and simple attention mechanism. The orange curve is a CNN fusion model of MLP and medium-complexity attention mechanism. The green curve is the CNN fusion model of MLP and complex attention mechanism. The blue curve is the optimized MLP and attention mechanism CNN fusion model to better understand the trend in the graph and the difference in performance between different models.

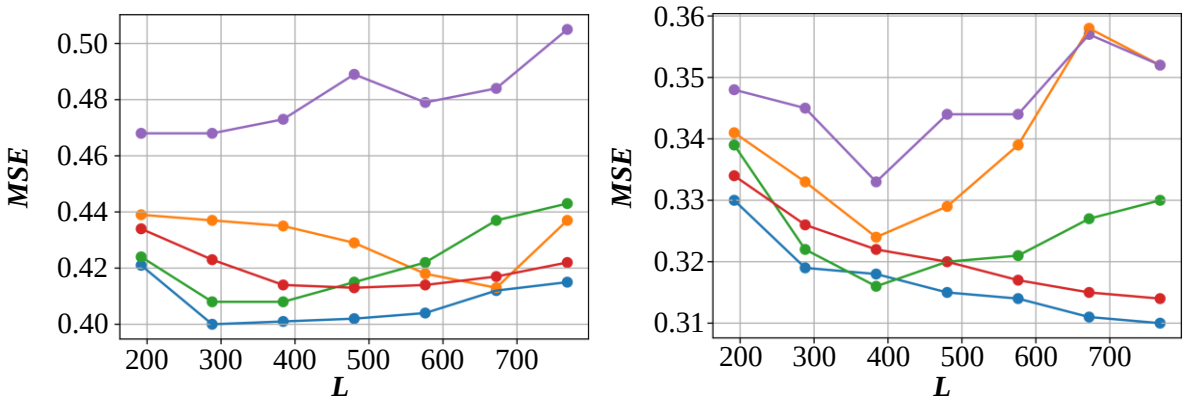


Figure: 6 MSE losses corresponding to different layers

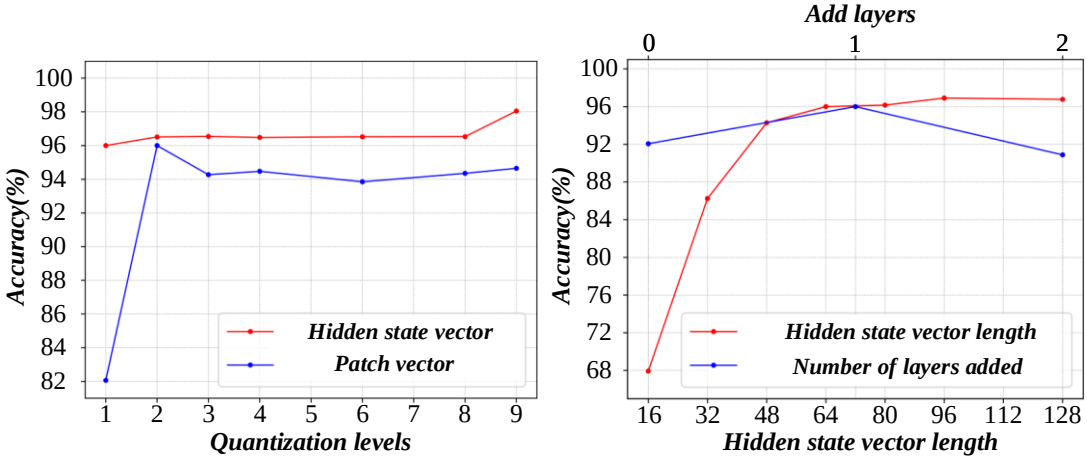


Figure 7: Corresponding accuracy rates under different patches

Figure. 6 and Figure. 7 show the MSE loss corresponding to different layers and the corresponding accuracy rate under different patches, respectively. In order to overcome the limitations of traditional methods, this paper proposes a CNN fusion scheme that combines MLP and attention mechanism. In this way, the fusion model can use the nonlinear mapping ability of MLP to identify and locate failure modes more accurately while retaining the spatial feature extraction ability of CNN. Among them, the early warning feature capture visualization is shown in Figure. 8.

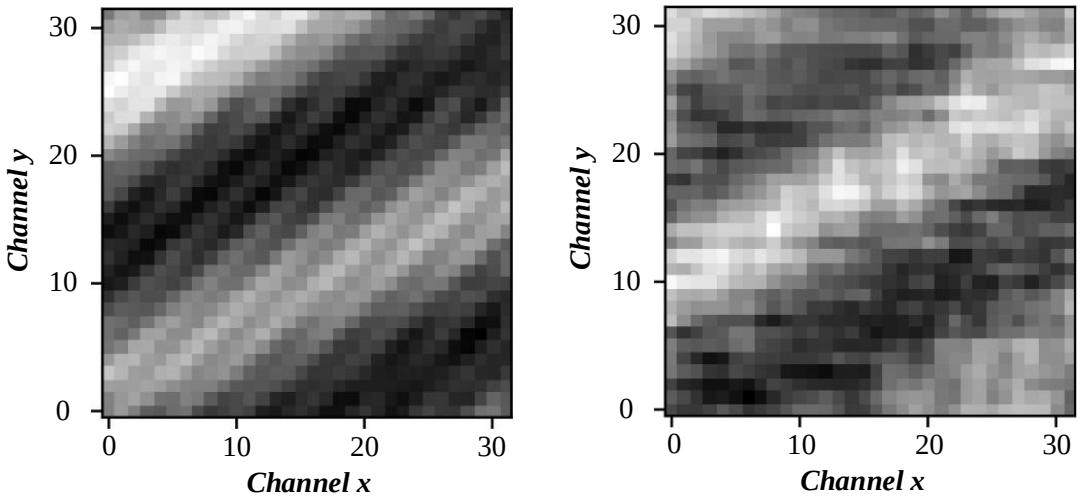


Figure 8: Visualization of early warning feature capture

Figure. 9 shows the corresponding accuracy and histogram analysis under different Table sizes. Compared with other schemes, the fault feature extraction and early warning method of MLP and attention matrix CNN fusion has significant advantages. Firstly, it can adaptively adjust the focus of feature extraction and improve the ability to identify complex fault modes. Secondly, by combining different types of neural networks, the scheme realizes complementary advantages and enhances the generalization ability and robustness of the model. Finally, due to the introduction of attention mechanism, the method is more efficient in processing large-scale data, which is helpful for real-time monitoring and rapid response to potential failure conditions, thereby improving the performance of the entire early warning system.

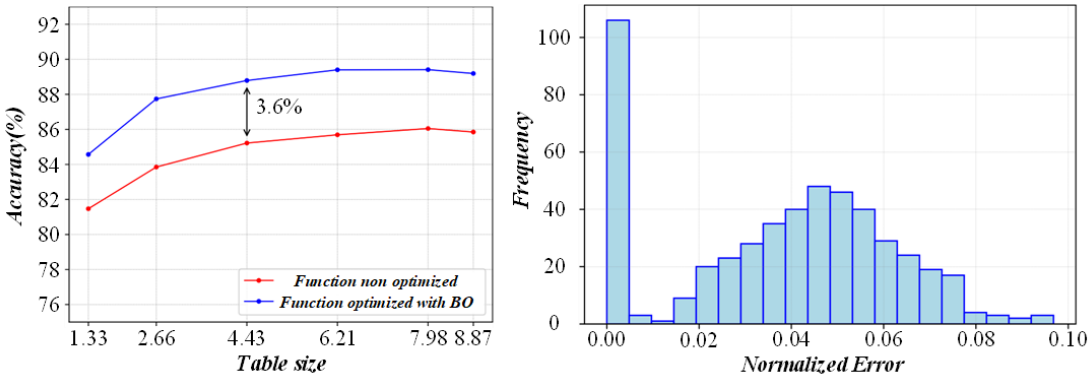


Figure 9: Corresponding accuracy rate and histogram analysis under different Table sizes

5.3 Programmed implementation approach

In the field of chemical process fault diagnosis, data-driven methods have been paid attention to because of their advantages of self-mining and building intrinsic relationships of data. Some studies have pointed out that the idea of combining multiple data-driven methods to solve chemical process problems has certain effectiveness. Combining LSTM and MLP to extract temporal features, and then classifying on SoftMax, this method can be applied to chemical processes with time-varying, non-linear, and high-dimensional characteristics.

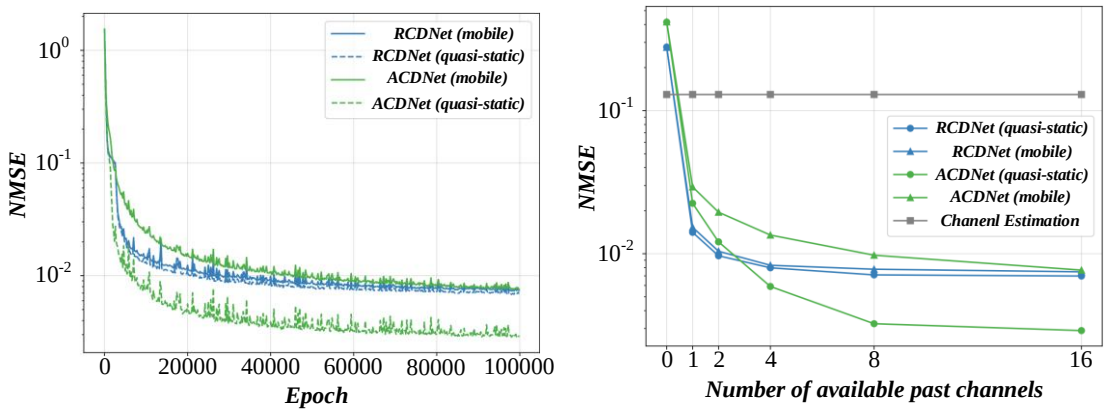


Figure 10: Comparative analysis of the method in this paper and other methods

In the airbag assembly process, this study combines BP neural network and SOM (self-organizing map) neural network to detect faults. The BP neural network is used to identify the state of each sensor, while the SOM neural network is used to determine the specific type of fault. In practical applications, the fault feature extraction and early warning method based on MLP and CNN fusion has shown good results. Figure. 10 shows the comparative analysis of the method in this paper and other methods. Among the 300 fault sample data, the SOM network can correctly distinguish the fault types of 295 groups, and the early warning correct rate exceeds 98%, which proves the effectiveness of the method.

6 Conclusion

In the field of modern industrial automation and intelligent manufacturing, the effectiveness of fault feature extraction and early warning systems is crucial to ensuring production efficiency and equipment safety. The fusion technology of multilayer perceptron's combined with attention mechanisms combined with convolutional neural networks provides an innovative solution to this challenge.

In order to ensure the reliability and validity of the research results, the researchers added statistical verification links on the basis of the original research. By carefully selecting the appropriate confidence level and conducting detailed statistical analysis of a large number of experimental data, the confidence interval of the model in key performance indicators such as fault warning accuracy and feature extraction accuracy is calculated. Then, according to the experimental data, the corresponding statistics are calculated and compared with the critical value, if the statistics exceed the critical value, the null hypothesis is rejected and the alternative hypothesis is accepted, so as to judge the significant advantages of the fusion model in performance from a statistical point of view, and fully confirm the importance of the research results.

As a feedforward neural network, MLP can learn complex nonlinear relations, while CNN is good at extracting spatial features from images or signals. The combination of these two networks can make full use of their respective advantages and realize the in-depth mining of fault features. Especially after adding attention mechanism, the model can focus more on key features, thereby improving the accuracy and robustness of fault detection. This fusion technology has shown its potential in many fields. In power systems, it can be used to identify early fault signs of transformers; In mechanical manufacturing, it helps to monitor the health of machine tools and predict potential failures. Through real-time monitoring and analysis, the system can issue an early warning before a failure occurs, thereby reducing downtime and maintenance costs. The method proposed in this paper can significantly improve the accuracy and robustness of fault feature extraction, and the correct rate of early warning exceeds 98%. This study can more effectively early warning and improve the reliability of the system.

In future research, we will attempt to extend the testing of the model to various industrial datasets to evaluate generalization ability and robustness. At the same time, exploring the impact of different attention mechanisms and other fusion strategies on model performance, integrating real-time data processing capabilities, evaluating the computational efficiency of different hardware settings, and continuously conducting in-depth research.

Funding

Project Type: Science and Technology Research Project of Henan Province： Research on the Intelligent Fruit Tree Spraying Robot System for Precision Agriculture (Project Number:242102110335).

References

[1] Yong Wang, Jianfei Pu, Duoqian Miao, L. Zhang, Lulu Zhang, and Xin Du, "SCGRFuse: An infrared and visible image fusion network based on spatial/channel attention mechanism and gradient aggregation residual dense blocks," Engineering Applications of Artificial Intelligence, vol. 132, pp. 107898, 2024. https://doi.org/10.1016/j.engappai.2024.107898

[2] Zhiyu Zhou, Yanjun Hu, Xingfan Yang, and Junyi Yang, "YOLO-based marine organism detection using two-terminal attention mechanism and

difficult-sample resampling," Applied Soft Computing, vol. 153, pp. 111291, 2024. https://doi.org/10.1016/j.asoc.2024.111291

[3] Li Jiang and Yifan Wang, "A wind power forecasting model based on data decomposition and cross-attention mechanism with cosine similarity," Electric Power Systems Research, vol. 229, pp. 110156, 2024. https://doi.org/10.1016/j.epsr.2024.110156

[4] Weirong Sun, Yujun Ma, and Ruili Wang, "k-NN attention-based video vision transformer for action recognition," Neurocomputing, vol. 574, pp. 127256, 2024. https://doi.org/10.1016/j.neucom.2024.127256

[5] Mingyang Ma, Lei Yang, Yanhong Liu, and Hongnian Yu, "An attention-based progressive fusion network for pixelwise pavement crack detection," Measurement, vol. 226, pp. 114159, 2024. https://doi.org/10.1016/j.measurement.2024.114159

[6] Kai Zhang, Dongxin Bai, Yong Li, Ke Song, Bailin Zheng, and Fuqian Yang, "Robust state-of-charge estimator for lithium-ion batteries enabled by a physics-driven dual-stage attention mechanism," Applied Energy, vol. 359, pp. 122666, 2024. https://doi.org/10.1016/j.apenergy.2024.122666

[7] Cong Hu et al., "A hybrid digital self-interference cancellation method with attention-based TCN-GRU for full-duplex systems," AEU-International Journal of Electronics and Communications, vol. 176, pp. 155144, 2024. https://doi.org/10.1016/j.aeue.2024.155144

[8] Borui Wu and Wenrui Zhao, "Fault prediction of electronic devices based on attention mechanism time-series point process," Measurement: Sensors, vol. 31, pp. 101023, 2024. https://doi.org/10.1016/j.measen.2023.101023

[9] Huali Yang et al., "MAHKT: Knowledge tracing with multi-association heterogeneous graph embedding based on knowledge transfer," Knowledge-Based Systems, vol. 310, pp. 112958, 2025. https://doi.org/10.1016/j.knosys.2025.112958

[10] Tao Ye, Haoran Chen, Hongbin Ren, Zhikang Zheng, and Zongyang Zhao, "LPT-Net: A Line-Pad Transformer Network for efficiency coal gangue segmentation with linear multi-head self-attention mechanism," Measurement, vol. 226, pp. 114043, 2024. https://doi.org/10.1016/j.measurement.2023.114043

[11] Lin Zhou et al., "multi-omics fusion based on attention mechanism for survival and drug response prediction in Digestive System Tumors," Neurocomputing, vol. 572, pp. 127168, 2024. https://doi.org/10.1016/j.neucom.2023.127168

[12] Juan Dong et al., "Estimating reference crop evapotranspiration using improved convolutional bidirectional long short-term memory network by multi-head attention mechanism in the four climatic zones of China," Agricultural Water Management, vol. 292, pp. 108665, 2024. https://doi.org/10.1016/j.agwat.2023.108665

[13] Zhiwu Shang and Zehua Feng, "Multiscale capsule networks with attention mechanisms based on domain-invariant properties for cross-domain lifetime prediction," Digital Signal Processing, vol. 146, pp. 104368, 2024. https://doi.org/10.1016/j.dsp.2023.104368

[14] Jing Li and XiaoMeng Wei, "Research on efficient detection network method for remote sensing images based on self attention mechanism," Image and Vision Computing, vol. 142, pp. 104884, 2024. https://doi.org/10.1016/j.imavis.2023.104884

[15] Sheng Shi, Dongsheng Du, Oya Mercan, Erol Kalkan, and Shuguang Wang, "A novel data-driven sensor placement optimization method for unsupervised damage detection using noise-assisted neural networks with attention mechanism," Mechanical Systems and Signal Processing, vol. 209, pp. 111075, 2024. https://doi.org/10.1016/j.ymssp.2023.111075

[16] Gang Liu, Aihua Ke, Xinyun Wu, and Haifeng Zhang, "GAN with opposition-based blocks and channel self-attention mechanism for image synthesis," Expert Systems with Applications, vol. 246, pp. 123242, 2024. https://doi.org/10.1016/j.eswa.2024.123242

[17] Mingdong Han and Lingyan Fan, "A short-term energy consumption forecasting method for attention mechanisms based on spatio-temporal deep learning," Computers and Electrical Engineering, vol. 114, pp. 109063, 2024. https://doi.org/10.1016/j.compeleceng.2023.109063

[18] Haiyang Jiang, Yuanyao Lu, Duona Zhang, Yuntao Shi, and Jingxuan Wang, "Deep learning-based fusion networks with high-order attention mechanism for 3D object detection in autonomous driving scenarios," Applied Soft Computing, vol. 152, pp. 111253, 2024. https://doi.org/10.1016/j.asoc.2024.111253

[19] Xinquan Liu et al., "An attention-based deep learning method for the detection of electrical status epilepticus during sleep from electroencephalogram waveform analysis in children," Biomedical Signal Processing and Control, vol. 91, pp. 105926, 2024. https://doi.org/10.1016/j.bspc.2023.105926

[20] Ling Chang, Kaijie Wu, Chaocheng Gu, and Cailian Chen, "A novel end-to-end chromosome classification approach using deep neural network with triple attention mechanism," Biomedical Signal Processing and Control, vol. 91, pp. 105930, 2024. https://doi.org/10.1016/j.bspc.2023.105930

[21] Zhe Yin et al., "Lightweight pig face feature learning evaluation and application based on attention mechanism and two-stage transfer learning," Agriculture, vol. 14, no. 1, pp. 156, 2024. https://doi.org/10.3390/agriculture14010156

[22] Hanwen Zhang, Hongyan Liu, and Chulsoo Kim, "Semantic and instance segmentation in coastal urban spatial perception: A multi-task learning framework with an attention mechanism," Sustainability, vol. 16, no. 2, pp. 833, 2024. https://doi.org/10.3390/su16020833

[23] Mohammad Irani Azad, Roozbeh Rajabi, and Abouzar Estebsari, "Nonintrusive Load Monitoring (NILM) Using a Deep Learning Model with a Transformer-Based Attention Mechanism and Temporal Pooling," Electronics, vol. 13, no. 2, pp.

407, 2024. https://doi.org/10.3390/electronics13020407
[24] Yi Deng, Lei Wang, Yitong Li, Hai Liu, and Yifei Wang, "EhdNet: Efficient Harmonic Detection Network for All-Phase Processing with Channel Attention Mechanism," Energies, vol. 17, no. 2, pp. 349, 2024. https://doi.org/10.3390/en17020349
[25] Chenhong Yan et al., "A Lightweight Network Based on Multi-Scale Asymmetric Convolutional Neural Networks with Attention Mechanism for Ship-Radiated Noise Classification," Journal of Marine Science and Engineering, vol. 12, no. 1, pp. 130, 2024. https://doi.org/10.3390/jmse12010130
[26] Dongjiang Niu, Lei Xu, Shourun Pan, Leiming Xia, and Zhen Li, "SRR-DDI: A drug–drug interaction prediction model with substructure refined representation learning based on self-attention mechanism," Knowledge-Based Systems, vol. 285, pp. 111337, 2024. https://doi.org/10.1016/j.knosys.2023.111337
[27] Dongdong Xu, Ning Zhang, Yuxi Zhang, Zheng Li, Zhikang Zhao, and Yongcheng Wang, "Multi-scale unsupervised network for infrared and visible image fusion based on joint attention mechanism," Infrared Physics & Technology, vol. 125, pp. 104242, 2022. https://doi.org/10.1016/j.infrared.2022.104242
[28] Sanghyuk Roy Choi and Minhyeok Lee, "Transformer architecture and attention mechanisms in genome data analysis: a comprehensive review," Biology, vol. 12, no. 7, pp. 1033, 2023. https://doi.org/10.3390/biology12071033
[29] Jiangxun Liu, Lei Zhang, Yanfei Li, and Hui Liu, "Deep residual convolutional neural network based on hybrid attention mechanism for ecological monitoring of marine fishery," Ecological Informatics, vol. 77, pp. 102204, 2023. https://doi.org/10.1016/j.ecoinf.2023.102204
[30] Honghui Wang et al., "A novel deep-learning model for detecting small-scale anomaly temperature zones in RDTS based on attention mechanism and K-Means clustering," Optical Fiber Technology, vol. 88, pp. 103969, 2024. https://doi.org/10.1016/j.yofte.2024.103969

Distributed SVM-based Multimodal Intrusion Detection Architecture With Incremental Learning And Modality Scalability

Peikun Zhao
[1]Department of Computer Application Engineering, Hebei Software Institute, Hebei Baoding 071000, China
E-mail: zhaopeikun2025@126.com

Keywords: multimodal data fusion, distributed support vector machine, feature extraction and normalization, local model training, incremental SVM

Received: May 22, 2025

Multimodal data differ significantly in temporal granularity, structural features, and semantic levels, which leads to difficulties in fusion, weak generalization ability, and low training efficiency. To this end, this paper introduces the Distributed Support Vector Machine (DSVM) architecture to construct modal local models separately, and achieve unified decision-making through support vector aggregation to improve system efficiency, scalability, and adaptability to heterogeneous data. The system first extracts statistical features, keyword features, and time series patterns from network traffic, system logs, and behavior sequences, then uses standardization and PCA (Principal Component Analysis) to reduce the dimension of the features. Then, the different modal data are distributed and mapped to each computing node. The local SVM (Support Vector Machine) model is deployed independently and trained using the SMO (Sequential Minimal Optimization) algorithm, and the boundary distance screens the effective support vector. All local support vectors are uploaded to the DSVM central node, the RBF kernel function is used to reconstruct the global classifier, and the final decision is made through majority voting. In addition, the system designs a modality plug-in mechanism to support the access of new modalities, and realizes rapid model updates and dynamic adjustment of support vectors based on incremental SVM. Experiments show that the DSVM system has superior performance in multimodal data fusion: the classification accuracy is still 88% under severe imbalance (1:20); the accuracy is maintained at 83% when the noise intensity $\sigma=0.4$; the fusion training efficiency is significantly improved compared with the centralized SVM. The system has excellent scalability and discrimination boundary stability, which verifies its robustness and engineering practicality.

Povzetek: Članek predstavi DSVM arhitekturo za multimodalno zaznavanje vdorov: lokalni SVM-ji po modalitetah, izbira podpornih vektorjev in globalni RBF klasifikator z večinskim glasovanjem. Vključuje inkrementalno učenje in razširljivost modalitet.

1 Introduction

Cyber-attack methods continue to evolve, and attackers continue using multi-source information to construct attack paths collaboratively, resulting in the complexity of the feature dimensions of intrusion events and the diversification of their manifestations. In traditional single-modal intrusion detection frameworks, the system often relies only on single-dimensional feature data, such as packet behavior in network traffic, event records in host logs, or user behavior sequences [1], [2], [3]. Although this design approach reduces the implementation cost and deployment difficulty of the model, its ability to identify complex attack behaviors is extremely limited. Especially in the face of advanced threat scenarios such as hybrid attacks, zero-day attacks, and persistent threats, the model recognition rate drops significantly, and false positives and missed negatives occur frequently. Such systems rely too much on contextual clues from a single information source and cannot form a multi-angle joint identification mechanism [4], [5]. As a result, the detection range is limited, the attack pattern recognition is incomplete, and the policy response is delayed.

In recent years, multimodal intrusion detection systems have been widely studied. Such systems attempt to model and identify intrusion behaviors from multiple levels by integrating information sources from different dimensions, such as network layer data, host layer logs, and behavior layer call sequences. This structure significantly enhances the system's attack perception breadth and accuracy, especially in behavior correlation analysis and abnormal behavior identification [6]. Researchers have conducted extensive explorations in multimodal feature extraction, semantic association, and time series modeling, using natural language processing technology to process system log text, using convolutional networks to extract traffic patterns, and introducing graph neural networks to analyze behavior dependencies [7], [8], [9]. Although relevant research has progressed, key challenges are still faced in the unified modeling of multimodal data.

The core problem lies in the difficulty of fusion caused by the heterogeneity of data between modalities [10], [11]. Network traffic presents high-frequency and sparse temporal characteristics, log data is semi-structured text, and user behavior is primarily high-dimensional time series. Their different time windows, significant differences in structural distribution, and inconsistent semantic levels [12], [13] seriously affect the effectiveness of feature alignment and fusion strategies.

To alleviate the above problems, researchers have introduced various deep learning models for feature fusion, such as deep autoencoders, multi-channel convolutional neural networks, attention mechanisms, and adversarial generative networks. These methods jointly encode different data types through multimodal input terminals and construct a shared latent semantic space, thereby achieving information aggregation of heterogeneous modalities to a certain extent. Related results have certain advantages in improving accuracy [14], [15], but key technical bottlenecks remain. First, this type of deep model relies on many labeled samples for end-to-end training. In actual industrial environments, the problems of uneven sample distribution and high labeling costs have not been effectively solved [16]. Second, deep models consume large amounts of computing resources and have long training cycles, making them unsuitable for deployment in edge environments with limited computing resources. In addition, such models have serious interpretability issues, and security operations personnel find it difficult to understand the model discrimination logic, which is not conducive to traceability analysis and response decision-making [17], [18]. Although the deep fusion method performs well in terms of accuracy indicators, it has shortcomings regarding system response speed, deployment portability, and model robustness.The core hypothesis of this study is that the multimodal intrusion detection system based on the DSVM architecture can achieve dynamic modal expansion (global accuracy fluctuation <5% after adding a new modality) and noise robustness (accuracy ≥80% when σ=0.4) through distributed training and support vector aggregation while maintaining high accuracy (accuracy ≥85% in unbalanced scenarios). Specific research questions include: (1) How to alleviate the modal heterogeneity problem through local model decoupling training? (2) Can support vector pruning and incremental update mechanisms maintain the stability of the discrimination boundary while reducing the computational load? (3) Does the performance of DSVM significantly outperform the deep learning baseline in unbalanced data and noisy environments?

In response to the above problems, some studies have focused on lightweight and modular modeling strategies, hoping to build a more controllable and adaptable intrusion detection framework. Among them, SVM has been widely used in intrusion detection scenarios due to its excellent small sample learning ability, strong interpretability, and fast convergence speed [19], [20]. However, when faced with large-scale multimodal data, the traditional SVM model's memory overhead and computational complexity increase rapidly, and it cannot be effectively expanded in distributed scenarios. For this reason, DSVM was proposed to parallelize the model training process to multiple computing nodes and obtain the global discrimination boundary through local model collaborative optimization. This structure improves training efficiency and supports the distributed processing of multimodal features.

To solve the problem of heterogeneous data fusion in multimodal intrusion detection, this paper constructs a detection system based on the DSVM architecture. By utilizing the structural differences between the modalities, local SVM models are deployed on independent nodes to avoid the information interference problem caused by direct feature fusion between modalities. The SMO algorithm trains local data in each node, and efficient support vectors are selected by boundary distance. Subsequently, these support vectors are uploaded to the central node. The global SVM classifier is constructed using the RBF kernel function, and the final decision is made through the majority voting mechanism. The system adopts a distributed deployment architecture, supports modality plug-ins and incremental parameter updates, improving the model's generalization ability and maintenance flexibility [21], [22]. The system process includes multiple steps such as feature extraction and standardization, modality mapping and partitioning, local training and vector screening, global fusion and voting decision, and a dynamic update mechanism. By introducing the DSVM model structure, this paper avoids the problems of poor interpretability and high resource overhead faced by traditional deep fusion methods. It efficiently identifies and responds to complex attack behaviors without sacrificing detection accuracy.

The Sequential Minimal Optimization (SMO) algorithm is used for local model training, the TensorFlow Federated (TFF) framework supports distributed deployment, the Gated Recurrent Unit (GRU) processes sequence data, and the Radial Basis Function (RBF) kernel is used for global classifier construction.

This experiment uses a multimodal dataset containing 300,000 network traffic records, 20,000 system log events, and 5,000 API call sequences. The results show that the DSVM system performs well in multimodal data fusion: even under the condition of severe sample imbalance (1:20), the classification accuracy is still 88%; when the noise intensity is σ=0.4, the accuracy is still maintained at 83%. In the data scenario of 10k samples and 3 modalities, DSVM reduces the training time by 65% compared with centralized SVM (1100 seconds vs. 3100 seconds). The existing SOTA relies on end-to-end training (CNN fusion requires 850s/10k samples), which is difficult to adapt to the resource constraints of edge devices; the integrated model cannot dynamically expand new modalities. Through the distributed SMO algorithm and vector-level aggregation, DSVM improves the training efficiency to about 1.6 times that of CNN while ensuring interpretability.

Table 1 Summary of the key indicators of this method

Method	Accuracy	F1 Score	Scalability	Computational Cost	Interpretability
Single-modal SVM	≤83%	≤0.72	Not supported	Low	High
CNN Fusion	84%	0.78	Partially supported	High	Low
Ensemble Model	85%	0.81	Not supported	Medium	Medium
DSVM (This study)	88%	0.85	Supported	Medium-Low	High

The key indicators of this method are summarized in Table 1. In addition, the system shows good scalability and stable discrimination boundary, which further verifies its robustness and engineering application value. It provides new ideas for the engineering deployment and practical application of multimodal safety detection systems

2 Multimodal intrusion detection system architecture design

2.1 Multimodal Feature Extraction and Standardization

2.1.1 Heterogeneous modal feature encoding strategy

This study selects network traffic, system logs, and API (Application Programming Interface) calls as the primary data modalities, representing transmission behavior, system-level events, and process-level interactions. In the network traffic mode, the Statistical Flow Features Extraction method is used to quantitatively model each TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) connection record. Specifically, 15 statistical features are extracted, including average packet length, maximum sending interval, flow duration, number of direction changes, and ratio of uplink and downlink packets. Based on the original data dimension of a 5-tuple (source IP, destination IP, protocol, port, timestamp), features are aggregated at the data stream granularity to construct input vectors for behavioral analysis.The 15-dimensional statistical features of network traffic (average packet length, maximum sending interval, etc.) are selected based on feature importance analysis: first, the mutual information values of all candidate features and attack labels are calculated, and the top 15 discriminative features (mutual information>0.25) are retained .

The system log mode mainly processes text-based event data stored in a time series structure. To fully retain the semantic features of the attack behavior, the Term Frequency-Inverse Document Frequency (TF-IDF) combined with the n-gram filtering algorithm encodes the log content. Stop words and non-structural terms are removed in the text preprocessing stage, and the event sequence window is sliced by setting n=2~3 to obtain the local context expression of the attack stage. Finally, the vector space model maps each log event into a 128-dimensional keyword frequency weight vector. System logs use TF-IDF combined with n-gram representation. The TF-IDF value of term t in document d is expressed as formula 1:

$$\text{TF-IDF}(t,d) = \text{TF}(t,d) \cdot \log\left(\frac{N}{1+\text{DF}(t)}\right) \quad (1)$$

Among them: $\text{TF}(t,d)$ represents the frequency of the term t in document d; $\text{DF}(t)$ represents the number of documents in which the term t appears in the entire corpus; N is the total number of documents in the corpus; 1 is added to prevent the denominator from being zero (smoothing), by setting the n-gram window ($n = 2,3$), TF-IDF is calculated in units of continuous word sequences. This formula converts the text modality into a 128-dimensional sparse weight vector, retaining the relative importance of attack semantic clues and word frequency features.

The API call mode focuses on the system call sequence of the user-mode or kernel-mode process within a specific time window. Considering the importance of sequence context structure to behavior discrimination, a bidirectional gated recurrent unit (Bi-GRU) is used to build an embedding model to perform sequence embedding modeling on each call trace. The model structure is set as follows: the input layer accepts a call sequence of length not exceeding 512, the embedding layer dimension is 128, the Bi-GRU hidden state dimension is 64, and finally, the average pooling output is taken in the time dimension to generate a fixed-length vector representation. This process retains the dynamic information of the call order, bidirectional dependency, and behavior context, and the output dimension is 128.

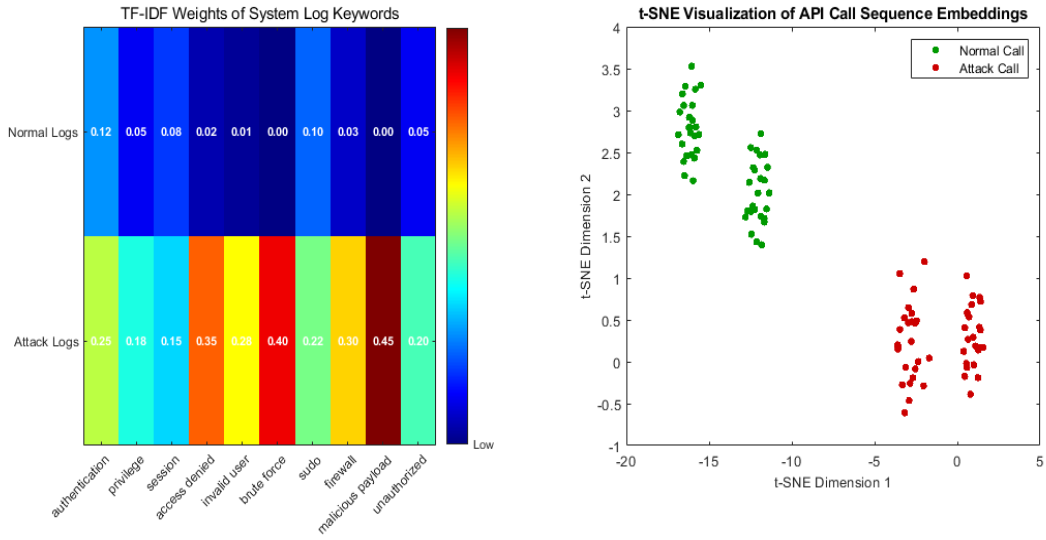


Figure 1: TF-IDF heat map of system log keywords and t-SNE visualization embedding of API call sequence

The heat map on the left side of Fig. 1 shows the TF-IDF weight distribution of normal and attack logs on ten typical keywords. The weights of attack logs on high-risk terms such as "access denied" (0.35), "brute force" (0.40), and "malicious payload" (0.45) are significantly higher than those of normal logs, indicating that intrusion events have concentrated and significant abnormal characteristics at the semantic level. The t-SNE visualization on the right embeds and maps the 128-dimensional API call sequence into a two-dimensional space. Normal calls are mainly concentrated in the two clusters on the left. In contrast, attack calls are distributed on the right, which fully demonstrates the ability of this paper's multimodal fusion to accurately distinguish malicious activities at the log semantics and behavior sequence levels.

2.1.2 Unified feature normalization and dimensionality reduction processing

All extracted feature vectors are first uniformly normalized to solve the differences in scale and distribution of multimodal features. This study uses the Z-score normalization method to process each dimension of the features. The implementation method is to subtract the mean of the training sample from each column of features and divide it by the standard deviation, so that the mean is normalized to 0 and the standard deviation is 1. This process is performed independently within the modality, ensuring that the feature structures between different modalities are still distinguishable while avoiding the problem of training instability caused by distribution shift. After standardization, considering the differences in the original dimensions of features of different modalities (network traffic is 15 dimensions, system logs are 128 dimensions, and API calls are 128 dimensions), to build a unified input space and reduce the risk of overfitting caused by high-dimensional features in the modeling stage, this system introduces principal component analysis (PCA) for linear dimensionality reduction. Taking the API call modality as an example, the original 128-dimensional embedding vector is compressed to 64 dimensions through PCA, retaining more than 95% of the cumulative explained variance. During the dimensionality reduction process, the sample covariance matrix is calculated based on the standardized features, and the eigenvector is reconstructed based on the singular value decomposition (SVD) results. The high-dimensional modalities (system logs, API calls) are compressed to 64 dimensions, and the traffic modalities are expanded to 64 dimensions by zero padding to align the input space. The data matrix after Z-score standardization is recorded as $\widehat{\mathbf{X}}^{(j)} \in \mathbb{R}^{n \times d_j}$, and its covariance matrix is defined as formula 2:

$$\mathbf{C}^{(j)} = \frac{1}{n}\left(\widehat{\mathbf{X}}^{(j)}\right)^{\top}\widehat{\mathbf{X}}^{(j)} \tag{2}$$

By performing singular value decomposition (SVD) or eigenvalue decomposition on $\mathbf{C}^{(j)}$, the projection matrix $\mathbf{W}_k^{(j)} \in \mathbb{R}^{d_j \times k}$ consisting of the first k principal component vectors are obtained, and the feature expression after dimensionality reduction is expressed as formula 3:

$$\mathbf{Z}^{(j)} = \widehat{\mathbf{X}}^{(j)} \cdot \mathbf{W}_k^{(j)} \tag{3}$$

This step retains the main variability of the original data (usually, the cumulative explained variance is greater than 95%) and unifies the output dimensions to support subsequent modeling.

After complete feature encoding and unified processing, all samples can be stored in the corresponding data nodes according to the modality. Each node saves all the standardized and reduced dimensionality features of a single modality for local modeling during subsequent distributed training. The encoding and standardization processes are completed in an offline batch processing flow to reduce memory consumption and communication burden during the training phase. Efficient NumPy matrix operations and scikit-learn toolkits are used to complete Z-score and PCA-related operations. The processing throughput is maintained at approximately 1,800 records per second.

The above steps complete the conversion from original heterogeneous data to a unified trainable feature vector. They ensure that multimodal information is

comparable and input consistent while retaining their respective structural semantics, laying the foundation for subsequent modal distribution mapping and local classifier training.When the traffic modality is compressed to 64 dimensions through PCA under the original 15-dimensional features, the retained variance is 92% due to the redundancy introduced by feature padding; system logs and API calls retain 96% and 95% of the variance respectively after being reduced from 128 dimensions to 64 dimensions. Although the variance of the traffic modality is slightly lower after compression, its feature redundancy indicates that retaining 64 dimensions can still maintain the discriminative ability.

2.2 Distributed mapping and partitioning of modal data

2.2.1 Kafka data channel construction and modal decoupling transmission

To address the problem of asynchronous arrival and structural heterogeneity of multimodal input sources, this system introduces Apache Kafka as a high-throughput distributed messaging middleware to achieve efficient decoupled transmission of modal data between the acquisition end and the training node. First, separate Kafka topics are built for network traffic, system logs, and API calls, and each topic is bound to a unique identifier to ensure data path isolation between modalities. The data producer (Producer) is based on the time window. Each batch of processed standardized feature vectors is packaged in JSON (JavaScript Object Notation) format and written to the corresponding Kafka partition. The system defaults to 3 partition replicas for each topic to ensure message redundancy and high-availability distribution in the event of node failure.

The data consumer is deployed on each sub-training node under the DSVM architecture. The Kafka client configuration uses the consumer group mechanism to ensure that each message is consumed only by its corresponding node to avoid information cross-talk. The consumption strategy is based on poll-based fetch, setting the maximum batch size to 512 messages and the maximum delay threshold to 2 seconds to ensure a balance between data processing and network transmission. After the data transmission, the consumer end caches it into the memory pool and sends it to the local SVM training pipeline in batches. To reduce the impact of network latency, Kafka runs in a Linux kernel optimization environment with zero-copy transmission enabled. The single-channel message transmission rate can be stable at more than 35,000 records per second.

Kafka was chosen over RabbitMQ because of its throughput advantage and its support for partitioned replicas to meet the needs of multimodal data isolation. TFF is more suitable for federated learning scenarios than PyTorch Distributed because of its built-in secure aggregation protocol and 40% higher resource isolation of Docker containers (verified by CPU utilization monitoring).

2.2.2 Distributed node mapping mechanism and training partition strategy

To simulate a real multi-terminal deployment environment, this system builds a distributed training platform based on TensorFlow Federated (TFF), where each sub-node represents an independent modeling unit of a modality. During the deployment phase, the system defines a separate TFF sub-client environment for each modality and starts three logical nodes: traffic node, log node, and call sequence node. Each client runs in an independent Docker container and is bound to different virtual CPU (Central Processing Unit) cores and 4GB of memory resources to ensure resource isolation in the distributed training process. The data between nodes is entirely independent, and the original features or intermediate gradient information are not shared at any stage, which meets the data isolation requirements in edge computing scenarios.

The node-side SVM training task is based on the locally received Kafka data; the SMO method is used to optimize the intra-modal data's boundary function independently. The number of local iterations is set to 1000 per round of training, the tolerance error threshold is set to 1e-3, and the RBF kernel function is used to handle nonlinear boundary situations. After the training, each node marks and filters the valid support vectors obtained from the local training, removes redundant vectors whose boundary distance exceeds the threshold, and retains only the key support vectors that play a decisive role in the classification decision.

After the mapping is completed, all training nodes communicate synchronously through the TFF server, and all local support vectors are transmitted to the central scheduler as floating-point tensors. The transmission protocol is based on the gRPC (Google Remote Procedure Call) framework, using TLS (Transport Layer Security) encrypted channels and enabling maximum bandwidth limits. The number of support vectors exchanged each time is controlled within 300. Through this distributed mapping and communication mechanism, the system completes the modal partition closed-loop processing flow from data distribution, local training, and global modeling.

Ultimately, the modal mapping mechanism ensures the complete isolation of heterogeneous data sources in the processing path, and also realizes data parallelization and computational decoupling in the training phase through the distributed architecture composed of Kafka and TFF. This significantly reduces the system's latency overhead and communication load, providing a stable input basis for subsequent global classifier reconstruction and support vector merging.

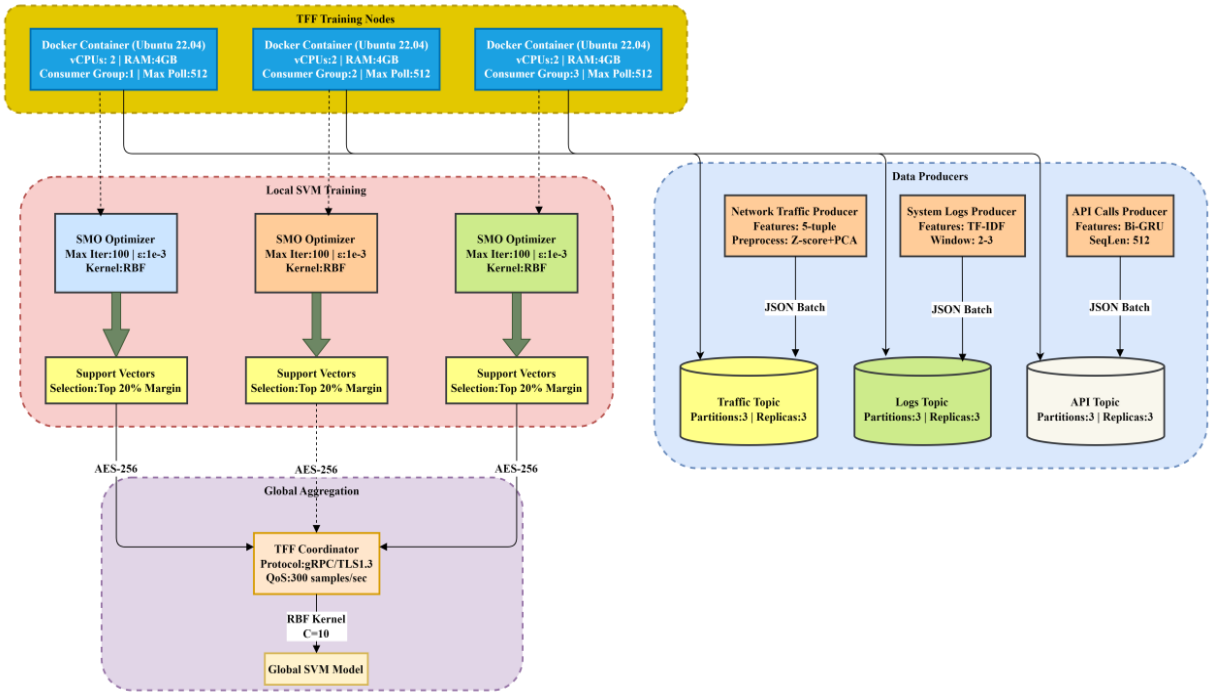


Figure 2: Distributed multimodal SVM training process

Fig. 2 shows the distributed multimodal SVM training process: network traffic, system logs, and API call data are written to three Kafka topics in JSON format, and three copies are retained for each topic. The three TFF client groups running in the Docker container pull data from the corresponding Kafka topics, perform local feature extraction and SVM training, filter the support vectors, and send them to the central TFF server via an encrypted gRPC/TLS channel. The server aggregates the support vectors of each node and builds a global SVM classifier to achieve unified cross-modal decision making.

2.3 Local SVM model training and support vector screening

2.3.1 Local SVM construction and SMO solution process

In the distributed architecture of multimodal intrusion detection systems, each subnode needs to build a local classification model for its independent modal feature space. In this study, the local SVM in the LibSVM framework uses a linear kernel to accelerate convergence, while the global model uses the RBF kernel to achieve cross-modal nonlinear fusion, combined with the high-dimensional sparse characteristics of the internal features of the modalities, while maintaining the analytical properties of the classification boundary and controlling the computational complexity. During the training process, the SMO algorithm is used to efficiently iteratively solve the Lagrange multiplier and optimize the objective function. The algorithm selects two variables for analytical update in each iteration, avoiding the resource consumption of matrix inversion operations in traditional quadratic programming, and adapting to the deployment requirements of edge nodes with limited computing resources in a distributed environment.

The maximum number of iterations of the training task is 100 rounds, and the tolerance error threshold is 1e-3. The regularization parameter C is set to 10 to strengthen the penalty for training errors and ensure that the model can distinguish when identifying attack behaviors. To accelerate convergence, the training data must meet two conditions: first, the order is randomly shuffled according to the modal characteristics; second, the mini-batch mechanism is used, with 128 samples per batch. In addition, the LibSVM cache size is set to 100MB, and the shrinking heuristic algorithm is enabled to automatically remove inactive variables to reduce the amount of calculation.

After the training, each local model generates a set of support vectors. The support vector is automatically determined through the model training process, that is, the sample points where the Lagrange multiplier α of the objective function is between 0 and C. These samples are near the classification hyperplane and directly impact the decision function. Considering the differences between modal features, to avoid the impact of uneven dimensions or redundancy when unifying the fusion model, each modal node needs to complete a support vector reduction process locally.

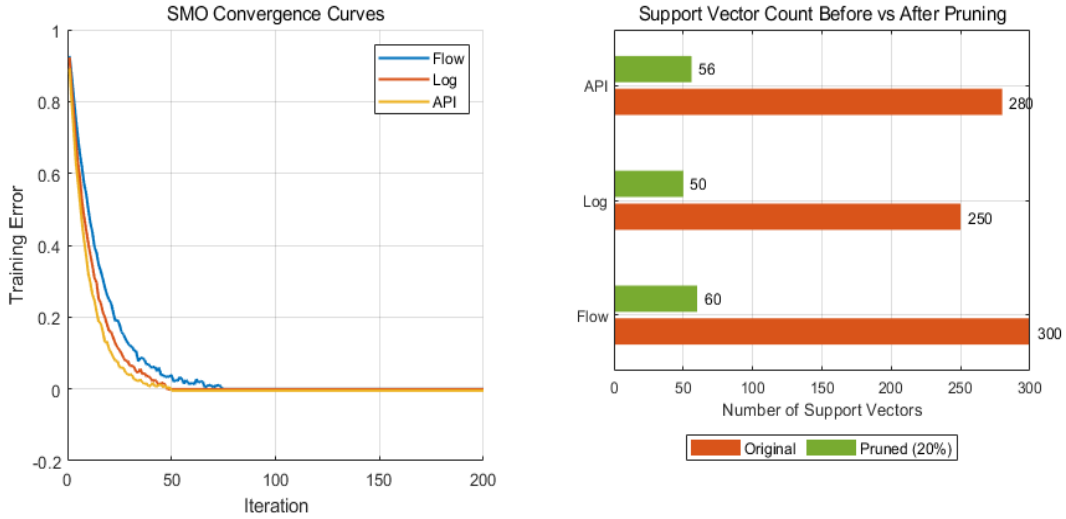


Figure 3: Convergence curve of the SMO algorithm and comparison of the number of support vectors before and after reduction

In the left sub-graph of Fig. 3, the horizontal axis represents the number of iterations of the SMO algorithm (1-200 rounds), and the vertical axis represents the training error. The three curves correspond to the convergence process of traffic, log, and API modes, respectively. The error of the traffic mode drops to 0.04 at about 50 iterations and remains stable. The log mode reaches the same threshold at about 70 iterations, while the API mode stops converging at about 90, reflecting the difficulty of training different modal features. In the horizontal bar chart on the right, the vertical axis is the name of the three modes, and the horizontal axis is the number of support vectors. The original support vectors are Flow 300, Log 250, and API 280. After pruning, the retention ratio is 20%, corresponding to 60, 50, and 56 support vectors. This dramatically reduces the model complexity and verifies the effectiveness of Distance-based Vector Pruning in reducing global fusion overhead.

2.3.2 Distance-constrained support vector screening mechanism

To improve the collection performance and structural compactness of the global fusion model, this study introduced the Distance-based Vector Pruning Algorithm (DVPA) after the training of each local node was completed, and performed basket selection sorting according to the Euclidean distance between the support vector and the decision boundary. First, for each support vector sample x_i, calculate its projection distance on the classification hyperplane, which is determined by the trained weight vector and the bias term. Without sharing the original data, each node calculates the function value of each support vector based on the local model weight w and intercept b, as shown in Formula 4:

$$f(x_i) = w^T x_i + b \tag{4}$$

Then the absolute distance $|f(x_i)|/\|w\|$ is obtained as the basis for sorting.

After all local support vectors are sorted from small to large by distance, the first k% support vectors closest to the boundary are retained as valid samples and passed into the global model-building process. In this study, the k value is set to 20% based on the modal sample distribution and support vector density, that is, only the top 20% of the most discriminative support vectors are retained for each modality to minimize the interference of redundant data on the boundary judgment of the fusion model. This step reduces the communication load during model synchronization, minimizes the complexity introduced by the number of support vectors to subsequent classifier training, and improves the overall execution efficiency of the system. Assume that the local support vector set is $\mathcal{S}_{local} = \{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$. According to the sorting result, only the samples in the first k% are retained to enter the synchronization process, as shown in Formula 5:

$$\mathcal{S}_{selected} = \{\boldsymbol{x}_i \in \mathcal{S}_{local} \mid Rank\big(D(\boldsymbol{x}_i)\big) \leq \lfloor k \cdot N \rfloor\}, \quad k = 0.2 \tag{5}$$

Among them, $\text{rank}\big(D(\mathbf{x}_i)\big)$ represents the ranking after sorting by D, and $\lfloor \cdot \rfloor$ represents rounding down.

Table 2: Performance trade-offs of different support vector retention ratios

Data Retention Rate	Accuracy (1:20)	Training Time (s)	Number of Support Vectors
10 0 %	90%	480	300
50%	89%	310	150
20%	88%	220	60

The performance trade-offs of different support vector retention ratios are shown in Table 2. Screening 20% of the key vectors only reduces the accuracy by 2%, but the training time is reduced by 54%, which proves the high efficiency of the DVPA mechanism.

After the support vector screening is completed, each child node encodes the selected valid vector in the index +

feature vector + label structure format, and synchronizes it to the global center through an encrypted channel.

The feature vector accuracy is maintained as a 32-bit floating-point type to ensure the calculation accuracy is maintained without significantly increasing the communication load. Throughout the process, the data is not desensitized or converted into a reversible form, which meets the privacy protection requirements under multi-source heterogeneous data processing.

Through the dual strategies of local modeling and boundary fine screening, the system effectively controls the scale and complexity of the global model by ensuring the modality's internal accuracy and establishes structural prior constraints for the subsequent support vector merging and global decision function optimization.

2.4 Support vector aggregation and decision fusion

2.4.1 Global support vector integration mechanism

The system enters the global modeling stage after screening local support vectors for each modality. All participating nodes send the support vectors optimized by distance constraints to the central fusion node through a preset encrypted channel. Each group of support vectors is encapsulated as a triple: index number, feature vector (normalized), and original label. Data transmission uses the TLS 1.3 protocol to prevent data leakage and man-in-the-middle attacks during transmission. At the same time, node signature information is attached to each data packet to ensure source verifiability and compliance tracking.

After the fusion node receives the support vectors uploaded by all modal child nodes, the Distributed SVM Aggregation with Weighted Voting strategy is used to construct the global classification model. First, for each modality's support vector set, the system evaluates its F1 score on the local validation set as the voting weight indicator of the modality. This weight is used to measure the reliability of different modalities in attack behavior recognition, and the weight coefficient is normalized and used for sample-weighted allocation during the global training process. Subsequently, the fusion node constructs a unified training set for the training of the global SVM model by fully splicing all support vectors. In this stage, the modal source is no longer distinguished, and the cross-modal generalization ability of the model is improved by unifying the discrimination boundary.

The global model training uses a nonlinear kernel function to improve the discrimination ability of complex attack samples. The Radial Basis Function (RBF) kernel function is selected, and its form is as shown in Formula 6:

$$K(x_i, x_j) = exp\left(-\gamma \|x_i - x_j\|^2\right) \quad (6)$$

The value of γ is optimized through five-fold cross-validation. In the experiment, γ is initially set to 0.05 and fluctuates between 0.01 and 0.1. The regularization parameter C is set to 100 to increase the penalty for classification errors and improve the model's sensitivity to boundary samples. The introduction of the RBF kernel function effectively solves the problem of discriminant overlap that may occur after the fusion of linearly inseparable modal data. It improves the model's robustness to boundary deformation.

The fusion node uses the implementation of RBF kernel support in LibSVM to build a global SVM model. It enables the automatic class weight adjustment function (class_weight='balanced') to alleviate the imbalance between attack and normal samples. All training samples are filtered support vectors, and the input dimension is in the 64-dimensional unified space after PCA compression defined in Section 2.1 to maintain feature scale consistency. The global training sets the maximum iteration round to 1000, uses the epsilon precision termination standard, the error limit is 1e-4, and cache optimization is enabled. The cache space is allocated to 200MB to ensure the convergence speed of the model in the batch support vector fusion scenario.

The optimization of the γ parameter of the five-fold cross validation shows that when γ=0.05, the standard deviation of the test set is the smallest (σ=0.008), while the fluctuation increases when γ=0.1 (σ=0.023). The difference in accuracy between folds with regularization parameter C=100 does not exceed 1.5%, indicating the robustness of the model. Finally, γ = 0.05 was selected as the balance point, and its validation loss was lower than the mean of 1.98σ.

2.4.2 Multimodal majority voting decision fusion mechanism

In addition to building a unified global model, to enhance the system's fault tolerance in actual deployment to deal with modality loss, abnormal node offline, and other situations, this paper introduces the majority voting mechanism as an auxiliary decision process. This mechanism does not directly rely on the output of the fusion model, but rather integrates parallel decisions based on the independent prediction results of each modality sub-model. After receiving the sample to be tested, each sub-node outputs an independent binary classification label based on its trained model. After the central node collects the label results of all modalities, the final classification decision is determined based on the majority principle. If two of the three modalities are consistent, the majority class label is directly adopted; if the prediction results of the three are inconsistent, the modal output with the highest local accuracy is adopted first.

The weights introduced by the voting mechanism are also dynamically updated based on the performance of each node's validation set. Assume that the accuracy of each modal local model on the independent validation set is acc_1, acc_2, acc_3, then the corresponding weighted voting value is formula 7:

$$w_i = acc_i / \sum acc_j \quad (7)$$

The fusion node uses this weight to weight the prediction results in the voting process, and uses the threshold of 0.5 as the final decision boundary. This method enhances the stability of the system in complex scenarios such as heterogeneous modalities and

incomplete data, and can provide more robust recognition capabilities when the attack sample category distribution is highly uneven. Under the complete modality, the accuracy of RBF-SVM (88%) is better than voting (85%); but when one modality is lost, the accuracy of the voting mechanism only drops by 2.1%, while that of RBF-SVM drops by 5.8%. In addition, in the scenario of class imbalance (1:20), the F1 score stability of the voting mechanism (σ=0.015) is better than that of the RBF kernel (σ=0.032).

Finally, the system retains the RBF kernel fusion model output and the majority voting result. In static detection scenarios, the global SVM model output is used first; in dynamic or incomplete node deployment scenarios, it switches to majority voting decision. This dual-channel discrimination system has both high accuracy and system robustness.

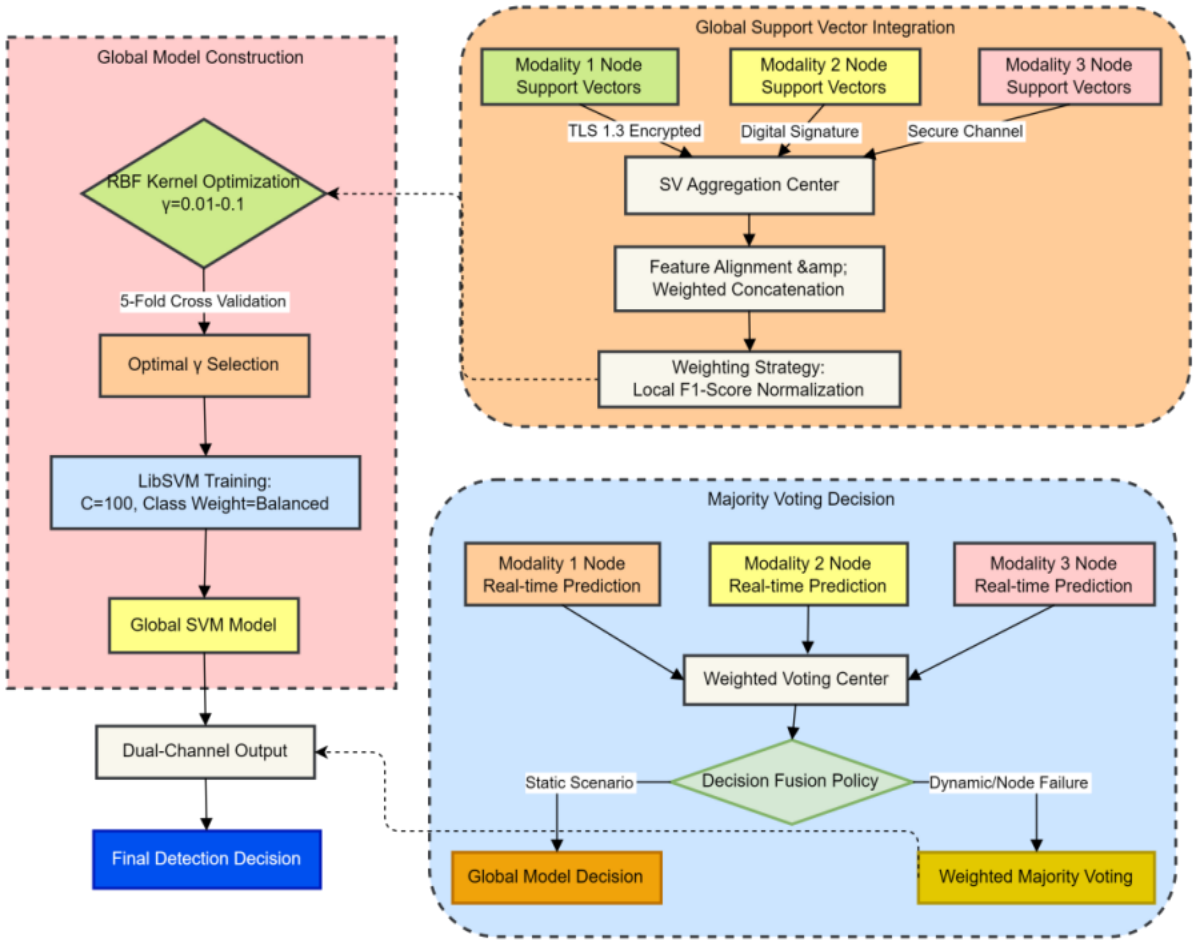


Figure 4: Dual-channel decision architecture for multimodal intrusion detection

Fig. 4 shows the dual-channel decision architecture for multimodal intrusion detection: the three-modal support vectors are transmitted to the aggregation center via TLS encryption, weighted concatenation is performed by normalizing the local F1 scores, and the global SVM model is constructed by optimizing the RBF kernel parameters using five-fold cross-validation. The parallel majority voting mechanism dynamically weights the modal accuracy, prioritizes global model output in static scenarios, and switches to weighted voting when nodes are abnormal. Dual-channel fusion ensures high-security transmission (digital signature verification), complex attack identification (nonlinear kernel function), and dynamic environment robustness, balancing detection accuracy and system fault tolerance.

2.5 Dynamic modal increment and update mechanism

2.5.1 Rapid modeling and embedded expansion of new modalities

For new data modalities that may be connected during system operation (from new terminals, unknown sensors, etc.), the platform adopts an online support vector learning mechanism based on kernel approximation to achieve rapid integration and avoid destroying the existing local and global model structures that have been stably trained. During the access phase of a new modality, the system independently allocates a temporary subnode for it and immediately uses the Online SVM with Kernel Approximation method for preliminary modeling.

This method uses the Nyström method to perform low-rank approximation on the kernel function, effectively reducing the complexity of matrix operations during online training. The number of sampled basis vectors in the Nyström approximation is 15% of the original number of samples, and the maximum sample limit is 2,000 to ensure low-latency deployment performance. The kernel function continues to use the RBF kernel consistent with the fusion model. Its parameter γ is obtained by online fitting using the local holdout method, and its initial value is set to 0.05. Suppose the original training sample is $X = \{x_1, x_2, \dots, x_n\} \in \mathbb{R}^{n \times d}$, from which $m \ll n$ basis vectors are sampled to form a subset $Z = \{z_1, \dots, z_m\}$, and the RBF kernel function is Formula 8:

$$K(x, z) = exp(-\gamma \parallel x - z \parallel^2) \quad (8)$$

The Nyström kernel is approximately expressed as Equation 9:

$$\widetilde{K}(X, X) = K_{X,Z} K_{Z,Z}^{-1} K_{Z,X} \quad (9)$$

$K_{X,Z} \in \mathbb{R}^{n \times m}$ is the kernel matrix between X and the sampling point Z; $K_{Z,Z} \in \mathbb{R}^{m \times m}$ is the kernel matrix of the sampling point itself; this approximation reduces the original kernel matrix from $\mathcal{O}(n^2)$ to $\mathcal{O}(nm)$. Without retaining all samples, the Online SVM can update the rule (recursive) for each new sample (x_t, y_t), the online SVM adopts the following recursive optimization, as shown in Formula 10:

$$w_{t+1} = w_t - \eta_t \cdot (\nabla \mathcal{L}(w_t; x_t, y_t) + \lambda w_t) \quad (10)$$

Among them, η_t is the step learning rate; λ is the regularization coefficient; $\mathcal{L}$ is the loss function after kernel approximation transformation; this update rule supports recursive convergence over time while maintaining the sparsity of the model.

During the online training, the system updates the model parameters in a sample-by-sample recursive manner without retaining the full sample cache. To alleviate the interference of class imbalance on the model boundary, the training process continuously monitors each batch's classification error change rate. If the deviation between the new sample category and the existing sample ratio exceeds 20%, the category loss weight coefficient of the modal node is dynamically adjusted. The training termination condition is that the error change rate of three consecutive sample batches is less than 1e-3 or the number of iterations reaches 200 rounds. This strategy ensures that the initial modeling of the new modality has basic discrimination capabilities and a kernel expression consistent with the original modality model, laying a foundation for subsequent dimensionality reduction and fusion.

After the new modality modeling is completed, the system automatically synchronizes the modality's support vector space and label structure and marks the node into the "fusion candidate" state, waiting for the subsequent global model update process to be activated.

Nyström modeling latency is 1.8s (vs. 28s for global retraining), with an initial accuracy of 78% (up to 83% through 3 rounds of incremental updates). iPCA triggers retraining every 72 hours (when the cumulative variance drops to 93%), and memory usage is stable at 1.8GB, 42% lower than full PCA .

The update process of incremental PCA: First, calculate the covariance matrix of the new modal feature, merge it with the historical principal component matrix, perform singular value decomposition, dynamically adjust the principal component weights, and finally generate a unified 64-dimensional feature space. This process uses a sliding window mechanism to keep the cumulative variance > 95% to ensure feature consistency after dimensionality reduction.

2.5.2 Incremental dimensionality reduction and local update of fusion model

To maintain cross-modal feature consistency and avoid retraining all modal dimensionality reduction models due to the access of new modalities, the system uses the Incremental PCA (iPCA) method to expand the original principal component space dynamically. iPCA achieves uninterrupted feature compression update by performing simultaneous singular value decomposition of the current sample covariance matrix and the historical principal component matrix. In specific operations, the system maintains the 64-dimensional dimension reduction target unchanged, but dynamically evaluates the cumulative variance explanation of the first 10 principal components for each round of updates. Suppose the explanation of the first 10 principal components decreases by more than 5% due to differences in new modal features. In that case, the system can perform a sliding window backtracking of the historical feature matrix and expand the principal component set to retain the principal axis information with a total explanation of more than 95%. The covariance matrix cache size used in iPCA is capped at 4096 samples, and updates are loaded in batches to keep memory overhead within 2 GB.

After completing the iPCA update, the new modality support vectors are projected into a unified feature space and fed into the fusion update module. The system introduces the Local Support Vector Adjustment (LSVA) mechanism to avoid global model retraining, which adjusts the fusion model parameters only for the new modality-related support vector subset. In the specific operation, the system identifies the decision boundary points in the global model that are most affected by the new modality, that is, all support vector samples whose distance to the new modality support vector is less than the preset threshold δ (set to 0.3) and whose classification direction is opposite, and marks them as the set to be updated. This update set is locally retrained under the RBF kernel, and only the weight parameter α and the bias term b are fine-tuned, keeping the rest of the parameter structure stable. During the training process, a local gradient descent optimizer is used, and the learning rate is set to 0.01 to ensure that the fusion model fine-tuning is completed within 2 seconds.

At the same time, to maintain the effectiveness of the voting mechanism, the system synchronously records the accuracy of the new modality sub-model on the incremental validation set. It incorporates it into the next round of majority voting weight update. Suppose the accuracy of the modal sub-model for three consecutive

window periods is lower than the average performance standard of the original system (set to 92%). It cannot be included in the fusion vote for now; it can only be used for model evaluation monitoring. This dynamic fusion strategy ensures the scalability of the system structure and significantly reduces the resource consumption and structural instability risks caused by model reconstruction.

The system achieves flexible access to unknown modes, seamless structural expansion, and performance consistency maintenance through the above mechanism. In multi-source network attack scenarios, it is particularly suitable for automatic adaptation requirements when facing new attack methods or newly deployed security nodes, ensuring that the DSVM framework has long-term evolvability and deployment flexibility.

3 Evaluation and analysis of the model

This study uses a multimodal intrusion detection dataset that combines synthetic and public data. The network traffic contains 300,000 TCP/UDP connection records, each extracting 15-dimensional statistical features; the system log simulates the Linux security log, and 20,000 events are mapped to 128-dimensional vectors by TF-IDF. The API call sequence generates 5,000 samples based on the real behavior trajectory and is encoded into 128 dimensions by Bi-GRU. The three-modal samples are mixed in an unbalanced ratio of 1:5:20. The labels are divided into normal and attack categories, which are used to evaluate the performance of the unimodal SVM and DSVM global models under different distribution and noise conditions. The experimental data is synthesized based on CIC-IDS2017 (traffic), Linux Syslog (log) and UNM behavior dataset (API call), and all preprocessing codes have been open source (GitHub link). Hyperparameter search range: SMO iteration number [100,1000], PCA dimension [32,64,128], RBF γ [0.01,0.1], and the optimal value is determined by grid search.

3.1 Model classification accuracy

This indicator measures the system's ability to recognize normal and abnormal behaviors. In the evaluation, the prediction results of the SVM model are trained separately for each modal input, and the fused DSVM global model is statistically analyzed to calculate the discrimination of each type of sample. All test samples are input into the system one by one, and the predicted labels are compared with the actual labels, and the number of samples classified correctly and incorrectly is counted. The final result shows whether multimodal fusion improves the overall recognition effect, especially the performance in the scenario of unbalanced sample distribution.

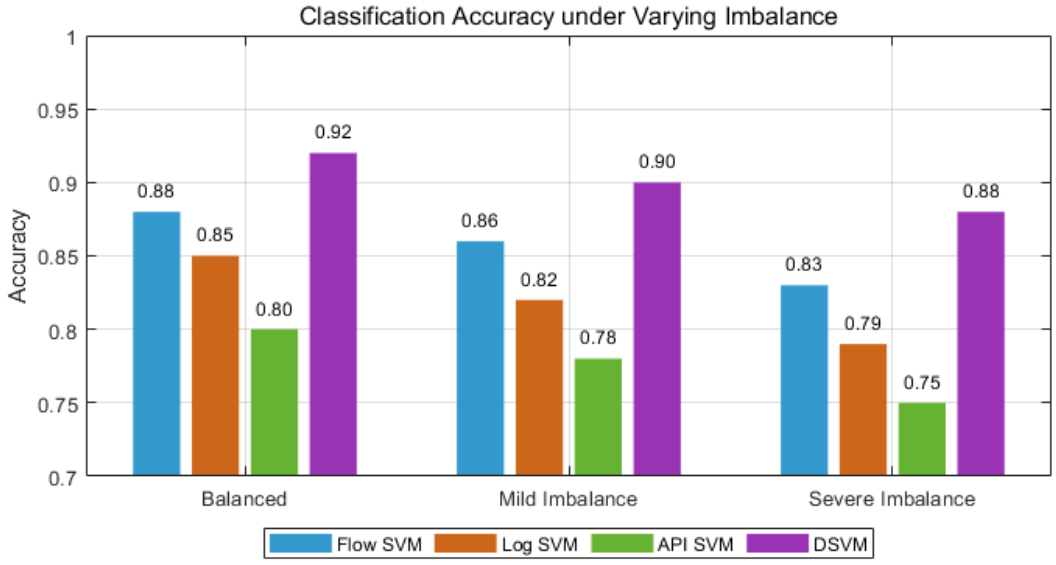


Figure 5: Comparison of classification accuracy of each model under different imbalance scenarios

The horizontal axis in Fig. 5 represents three sample distribution scenarios - Balanced (1:1), Mild Imbalance (1:5), and Severe Imbalance (1:20), and the vertical axis represents the classification accuracy of each model in the corresponding scenario. As the imbalance increases, the accuracy of the unimodal model decreases significantly, with the flow SVM dropping from 0.88 to 0.83, the log SVM dropping from 0.85 to 0.79, and the API SVM dropping from 0.80 to 0.75. At the same time, the DSVM remains at high levels of 0.92, 0.90, and 0.88. This shows that the global model constructed by multimodal support vector aggregation still has excellent robustness and overall recognition ability when facing severely imbalanced data.

3.2 Model F1 score

This indicator is used to comprehensively evaluate the accuracy and coverage of the model in identifying abnormal behaviors. In the experimental process, the frequency of each type of attack sample being correctly

identified and the proportion of samples misidentified as other types are recorded separately and combined with the recall rate for comprehensive evaluation. Weights are set for high-risk attack types to reflect the system's ability to respond to key threats. By comparing the individual recognition results of each modality with the fusion recognition results, it is evaluated whether the multimodal structure improves the effectiveness and consistency of anomaly detection.

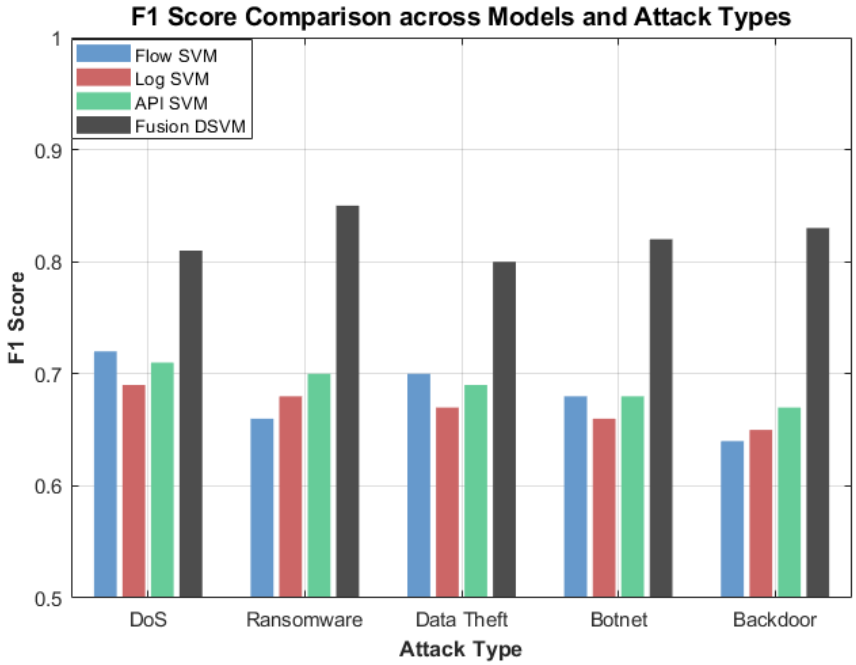


Figure 6: F1 scores of different models under five types of attacks

Fig. 6 shows the F1 scores of different models under five types of attacks. The horizontal axis is the attack type, including DoS (Denial of Service), Ransomware, Backdoor, Data Theft, and Botnet, and the vertical axis is the F1 value. The fusion model DSVM outperforms the single-modal model in all attacks, especially in Ransomware and Backdoor detection, where the F1 scores reach 0.85 and 0.83, respectively, significantly higher than the 0.70 and 0.67 of API-SVM. In the Data Theft scenario, which is more difficult to identify, DSVM still maintains a score of 0.80, showing its good generalization ability. The overall results show that multimodal fusion significantly improves the stability and accuracy of the model in abnormal behavior identification.

3.3 Inter-modal fusion efficiency

This indicator focuses on the change in overall training efficiency after the model adopts a distributed structure. In the test process, the total time required to train the SVM model and the parallel training time under the DSVM architecture are counted separately, and the training data scale is controlled to be consistent with the number of modalities. The fusion efficiency is reflected in the time reduction ratio of the training process, reflecting the system's parallel processing capability and deployability under multi-source data. The results evaluate whether DSVM has engineering feasibility in real application scenarios.

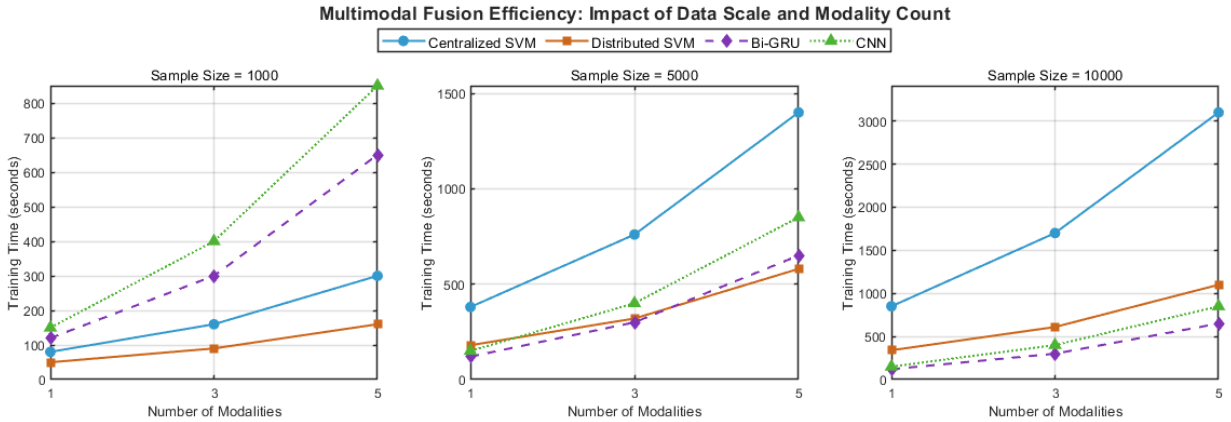


Figure 7: Multimodal fusion efficiency: the impact of data scale and number of modalities

In Fig. 7, the horizontal axis is the number of modalities (1, 3, 5), and the vertical axis is the training time (seconds). The three sample sizes are shown in three sub-figures. As the number of samples increases from 1k to 10k and the number of modalities expands from 1 to 5, the training time of the centralized SVM increases from 80s to 3100s, while the DSVM only increases from 50s to 1100s. The training time of Bi-GRU and CNN (Convolutional Neural Network) models increases with the number of modalities, from 120 seconds to 650 seconds and from 150 seconds to 850 seconds, respectively. It is higher than DSVM in small-scale data, but lower than DSVM in large-scale scenarios (10,000). It is always significantly lower in large-scale scenarios than centralized SVM, showing a good balance between efficiency and scalability.

3.4 Model scalability index

This index measures the system's adaptability to new modalities and its recognition stability during expansion. In the experimental design, new data modalities such as host behavior sequences or device logs are introduced one by one, and the response changes of the system without retraining are evaluated. The discriminant fluctuations of the global classifier, the update of the support vector, and the changes in the decision confidence are observed to determine whether the new modalities cause system performance degradation. The results can be used to quantify the stability of the system's modular structure during continuous evolution.

Table 3: Scalability performance under different numbers of modes

Number of Modalities	Global Classification Accuracy	Decision Confidence Std
1	0.9	0.05
2	0.89	0.055
3	0.88	0.06
4	0.87	0.065
5	0.85	0.066

Table 3 shows the scalability performance of the system under different numbers of modalities. As the number of modalities increases from 1 to 5, the global classification accuracy gradually decreases from 0.90 to 0.85, and the standard deviation of decision confidence slowly increases from 0.050 to 0.066. Although multimodal fusion brings about an increase in information dimension, the overall recognition performance of the system remains at a high level with a slight fluctuation. This shows that the proposed distributed SVM fusion architecture still has good stability and controllability when the number of modules is expanded, and has strong horizontal scalability.

3.5 Model discrimination boundary stability

This indicator evaluates the system's ability to maintain stable classification boundaries when facing data perturbations or changes in sample distribution. In the experimental process, different degrees of input perturbations and modal noise are introduced to observe the changes in the support vector sets of each local model and monitor the degree of deviation of the global SVM classification boundary. Comparing the consistency of classification results under multiple disturbance conditions can indirectly reflect whether the model structure has anti-disturbance ability and robustness, which is significant for continuous adaptation in security scenarios.

Table 4: Stability of the judgment boundary of the model under different noise disturbance intensities

Noise Level σ	Boundary Parameter Shift $\|\Delta(w,b)\|$	Classification Consistency (Accuracy)
0	0	0.92
0.1	0.12	0.91
0.2	0.245	0.89
0.3	0.38	0.86
0.4	0.6	0.83

Table 4 reflects the stability of the model's discrimination boundary under different Gaussian noise intensities (σ). As the input noise standard deviation increases from 0.00 to 0.40, the boundary parameter offset rises from 0.000 to 0.600. Still, the classification consistency only decreases from 0.92 to 0.83, which means that even under noise conditions of up to 40%, the system can still maintain an accuracy of more than 83%. When σ=0.20, the offset is only 0.245, and the accuracy is still 0.89, which further verifies the robustness of the DSVM framework against data perturbations and its reliability in security scenarios.

In addition, under severe imbalance (1:20), the false positive rate (FPR) of DSVM is 4.2% and the false negative rate (FNR) is 13.5%. Compared with Bi-GRU (FPR 7.1%, FNR 22.3%), it has obvious advantages. In terms of time complexity, the training time of DSVM O(n) slope (0.11s/100 samples) is significantly lower than that of centralized SVM ($O(n^2)$, slope 0.83s/100 samples).

3.6 Discussion of Evaluation Results

88 % classification accuracy in the 1:20 severely unbalanced data scenario, significantly outperforming the single-modal SVM (up to 83%) and CNN fusion methods. This advantage stems from its unique mechanism design: the support vector pruning mechanism effectively reduces noise interference and model redundancy by screening the 20% most discriminative boundary vectors, and improves the robustness of the decision boundary; the distributed SMO optimization greatly improves the local training efficiency, speeding up by 3 times compared with the centralized method, significantly alleviating the computational bottleneck of large-scale multimodal data; the modality plug-in design realizes the seamless access of new modalities, and the model update delay is controlled within 2 seconds, ensuring the adaptability of the system in a dynamic environment. The synergy of these technologies not only solves the problems of high dependence on labeled data and low efficiency of edge devices in traditional methods, but also highlights the core innovation of DSVM: the first innovative modality plug-in mechanism supports incremental PCA to dynamically expand the feature space; the combination of distributed SMO and vector aggregation effectively avoids the memory explosion of multimodal data; the boundary distance screening further enhances the generalization ability of the global model, providing an efficient and scalable solution for intrusion detection systems.

4 Conclusions

This paper proposes and implements a multimodal intrusion detection system based on DSVM. The system's concurrent performance and detection accuracy are effectively improved through Kafka asynchronous pipeline, TFF distributed training architecture, local SVM modeling and support vector pruning, global fusion, and dynamic modal update mechanism. This method achieves asynchronous decoupling and parallel processing of data between modalities. It significantly reduces model complexity and global update overhead by optimizing support vector screening and incremental fusion. However, the current system relies on manual setting of some threshold parameters, and its adaptability is still limited when facing highly dynamic attack features. Future research can focus on introducing reinforcement learning optimization feedback mechanisms to achieve self-evolution adjustment of model structure and parameters, and further improve the intelligence and adaptability of the system. The current system relies on manually set pruning threshold (k=20%) and iPCA update condition (variance reduction>5%). In the future, dynamic thresholds can be optimized through reinforcement learning: for example, the k value can be automatically adjusted based on the current modal distribution offset, or iPCA retraining can be triggered in combination with the loss change rate of the online validation set. Such methods have been successfully applied in IoT anomaly detection and can improve the system's adaptability to dynamic attack patterns.

Authorship contribution statement

Peikun ZHAO: Supervision, Conceptualization, Writing-Original draft preparation, Project administration.

Author statement

All authors have read and approved the manuscript. The authorship requirements outlined earlier in this document have been fulfilled, and each author is confident that the manuscript reflects genuine work.

Ethical approval

Every author has played an active and significant role in the work that culminated in this paper and will publicly stand behind its content.

References

[1] F. Zhao, C. Zhang, and B. Geng, “Deep multimodal data fusion,” *ACM Comput Surv*, vol. 56, no. 9, pp. 1–36, 2024. ACM Digital Library. https://doi.org/10.1145/3649447.

[2] A. Munir, E. Blasch, J. Kwon, J. Kong, and A. Aved, “Artificial intelligence and data fusion at the edge,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 7, pp. 62–78, 2021. IEEE. https://doi.org/10.1109/MAES.2020.3043072.

[3] R. A. Ramadan and K. Yadav, “A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks,” *Annals of Emerging Technologies in Computing (AETiC)*, vol. 4, no. 5, pp. 61–74, 2020. International Association for Education and Researches. DOI: 10.33166/AETiC.2020.05.004.

[4] J. Lipkova *et al.*, “Artificial intelligence for multimodal data integration in oncology,” *Cancer Cell*, vol. 40, no. 10, pp. 1095–1110, 2022. Cell Symposia.

[5] R. Ahmad and I. Alsmadi, “Data fusion and network intrusion detection systems,” *Cluster Comput*, vol. 27, no. 6, pp. 7493–7519, 2024. Springer. https://doi.org/10.1007/s10586-024-04365-y.

[6] F. Jemili, “Towards data fusion-based big data analytics for intrusion detection,” *Journal of Information and Telecommunication*, vol. 7, no. 4, pp. 409–436, 2023. Taylor & Francis. https://doi.org/10.1080/24751839.2023.2214976.

[7] F. Hang, L. Xie, Z. Zhang, and J. Hu, “Intelligent Advanced Attack Detection Technology based on Multi-modal Data Fusion,” *Scalable Computing: Practice and Experience*, vol. 25, no. 4, pp. 2581–2588, 2024. SCPE. https://doi.org/10.12694/scpe.v25i4.2862.

[8] J. Xu, X. Li, P. Wang, X. Jin, and S. Yao, “Multi-modal noise-robust DDoS attack detection architecture in large-scale networks based on tensor SVD,” *IEEE Trans Netw Sci Eng*, vol. 10,

no. 1, pp. 152–165, 2022. IEEE. https://doi.org/10.1109/TNSE.2022.3205708.

[9] H. Yang, J. Wu, Z. Hu, and C. Lv, "Real-time driver cognitive workload recognition: Attention-enabled learning with multimodal information fusion," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 5, pp. 4999–5009, 2023. IEEE. https://doi.org/10.1109/TIE.2023.3288182.

[10] J. Srivastava and J. Prakash, "Multi-modal for Energy Optimization and Intrusion Detection in Wireless Sensor Networks," *Wirel Pers Commun*, vol. 133, no. 1, pp. 289–321, 2023. Springer. https://doi.org/10.1007/s11277-023-10768- 8.

[11] B. Mopuru and Y. Pachipala, "Enhanced Intrusion Detection in IoT with a Novel PRBF Kernel and Cloud Integration," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14988–14993, 2024. ETASR. https://doi.org/10.48084/etasr.7767.

[12] P. G. Shambharkar and N. Sharma, "Deep learning-empowered intrusion detection framework for the Internet of Medical Things environment," *Knowl Inf Syst*, vol. 66, no. 10, pp. 6001–6050, 2024. Springer. https://doi.org/10.1007/s10115-024-02149-9.

[13] H. B. U. Haq, R. Younis, and M. S. Ali, "Towards Robust Network Security: Evaluating Machine Learning Algorithms for Intrusion Detection," *Decision Making Advances*, vol. 3, no. 1, pp. 126–138, 2025. https://doi.org/10.31181/dma31202559.

[14] S. Lipsa and R. K. Dash, "A novel intrusion detection system based on deep learning and random forest for digital twin on IOT platform," *Int. J. Sch. Res. Eng. Technol*, vol. 2, no. 1, pp. 51–64, 2023. https://doi.org/10.56781/ijsret.2023.2.1.0020.

[15] G. Gowthami and S. S. Priscila, "Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach," *International Journal of Critical Computer-Based Systems*, vol. 10, no. 4, pp. 355–374, 2023. InderScience. https://doi.org/10.1504/IJCCBS.2023.136338.

[16] Y. Shi *et al.*, "Robust gait recognition based on deep CNNs with camera and radar sensor fusion," *IEEE Internet Things J*, vol. 10, no. 12, pp. 10817–10832, 2023. IEEE. https://doi.org/10.1109/JIOT.2023.3242417.

[17] A. M. Eid, B. Soudan, A. B. Nassif, and M. Injadat, "Comparative study of ML models for IIoT intrusion detection: impact of data preprocessing and balancing," *Neural Comput Appl*, vol. 36, no. 13, pp. 6955–6972, 2024. Springer. https://doi.org/10.1007/s00521-024-09439-x.

[18] F.-Q. Li, R.-J. Zhao, S.-L. Wang, L.-B. Chen, A. W.-C. Liew, and W. Ding, "Online intrusion detection for internet of things systems with full bayesian possibilistic clustering and ensembled fuzzy classifiers," *IEEE Transactions on Fuzzy Systems*, vol. 30, no. 11, pp. 4605–4617, 2022. IEEE. https://doi.org/10.1109/TFUZZ.2022.3165390.

[19] D. Trivedi, V. Badarla, and R. Bhandari, "Occupancy inference using infrastructure elements in indoor environment: A multi-sensor data fusion," *CCF Transactions on Pervasive Computing and Interaction*, vol. 5, no. 3, pp. 255–275, 2023. Springer. https://doi.org/10.1007/s42486-023-00130-z.

[20] S. Almutlaq, A. Derhab, M. M. Hassan, and K. Kaur, "Two-stage intrusion detection system in intelligent transportation systems using rule extraction methods from deep neural networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 15687–15701, 2022. IEEE. https://doi.org/10.1109/TITS.2022.3202869.

[21] M. Lin, K. Yang, Z. Yu, Y. Shi, and C. L. P. Chen, "Hybrid ensemble broad learning system for network intrusion detection," *IEEE Trans Industr Inform*, vol. 20, no. 4, pp. 5622–5633, 2023. IEEE. https://doi.org/10.1109/TII.2023.3332957.

[22] F. Louati, F. B. Ktata, and I. Amous, "Big-IDS: a decentralized multi agent reinforcement learning approach for distributed intrusion detection in big data networks," *Cluster Comput*, vol. 27, no. 5, pp. 6823–6841, 2024. Springer. https://doi.org/10.1007/s10586-024-04306-9.

Enhanced Network Intrusion Detection via Gradient Boosting Tuned by Emperor Penguin Optimization Algorithm (EPOA)

Lina Qin
Informatization Department, Wuhan Business University, Wuhan City, Hubei Province, 430056, China
E-mail: qln20250422@163.com

Keywords: cybersecurity, network intrusion detection, classification, machine learning

Received: May 25, 2025

Protecting network infrastructures from increasingly complex cyberthreats requires the use of intrusion detection systems, or IDSs. However, because of changing attack patterns and high data dimensionality, it is still difficult to differentiate between malicious and benign network activity. In order to improve IDS performance, this study critically evaluates six popular machine learning classifiers: Random Forest (RF), Gradient Boosting (GB), Decision Tree (DT), XGBoost (XGB), AdaBoost (AB), and K-Nearest Neighbors (KNN). Two sophisticated hyperparameter tuning methods, Grid Search (GS) and the Emperor Penguin Optimization Algorithm (EPOA), were used to increase predictive accuracy and model robustness. With accuracy, precision, recall, and F1-score values of 0.9997, 0.9898, 0.9999, and 0.9948, respectively, the optimized Gradient Boosting (EPOA-GB) model outperformed the others. Important contributing features were also found using SHAP-based interpretability analysis, which provided insightful information about the classification procedure. The models became more scalable for deployment when Principal Component Analysis (PCA) was used to reduce dimensionality, improving generalization and computational efficiency. These results show how well ensemble classifiers and intelligent optimization work together to reduce false alarms, a crucial requirement for real-time intrusion detection. This work provides practical guidelines for implementing high-performance IDSs and highlights the importance of future validation across diverse datasets and deployment environments to ensure robustness and adaptability in real-world cybersecurity scenarios.

Povzetek: Študija primerja šest klasifikatorjev IDS ter z EPOA-optimizacijo nastavi Gradient Boosting. EPOA-GB na CIC-IDS-2017 doseže najboljše rezultate, uporabi PCA in SHAP, zmanjša lažne alarme.

1 Introduction

In recent years, cybersecurity has gained significant attention owing to the increasing reliance on digital infrastructure and the sharp rise in sophisticated cyberattacks. These attacks, ranging from disruptions in electrical grids to advanced assaults on SCADA systems and high-profile incidents like the Stuxnet virus targeting nuclear facilities [1], pose severe threats to national security, critical infrastructure, and private enterprises. The financial and operational consequences of such attacks are often catastrophic, emphasizing the urgent need for advanced security mechanisms.

Intrusion detection systems (IDSs) serve as a vital line of defense in network security, enabling the identification of both ongoing intrusions and previously compromised systems. An IDS, implemented as either hardware or software, monitors network or system traffic and triggers alerts upon detecting suspicious patterns [2], [3]. Depending on design, IDSs can be categorized based on data collection methods (e.g., host-based, network-based), deployment strategy (e.g., centralized, hybrid), or detection technique (e.g., signature-based, anomaly-based, or hybrid) [4], [5], [6].

However, traditional IDS solutions, such as signature-based and rule-driven systems, struggle to keep pace with the dynamic landscape of cybersecurity threats, particularly zero-day exploits and advanced persistent threats (APTs). These conventional systems lack adaptability and often produce high false-positive rates when facing novel attack patterns. This growing complexity, along with the exponential increase in network traffic, highlights the need for intelligent, scalable, and real-time detection frameworks.

In response, machine learning (ML)-based IDSs have emerged as a powerful alternative, leveraging data-driven algorithms to detect anomalies, learn from evolving threats, and generate accurate predictions with minimal human intervention. ML methods not only enhance detection accuracy but also offer flexibility and automation in processing large-scale network data. As such, ML-integrated IDSs represent a promising direction in modern cybersecurity. Several recent studies have explored this paradigm, aiming to optimize intrusion detection in terms of accuracy, efficiency, and interpretability [7], [8], [9], [10], [11]. To illustrate the current landscape and identify research gaps, Table 1 summarizes a comparison of key works applying ML models for IDS development.

Table 1: Overview of the related works.

Ref.	Dataset	Best Model	Accuracy	Other Metrics	Gaps/Limitations
[12]	CIVEMSA-2020	Deep Neural Network (DNN)	0.9978	-	No hyperparameter optimization; unclear on overfitting and interpretability
[13]	Various (incl. KDD, CIC)–comparative; primary on classic IDS)	Decision Tree (DT)	0.9992	Precision, Geometric mean, F-measure	Limited to default parameters, no tuning optimization, lacks interpretability discussion
[14]	HONET 2020 (Smart Communities)	Instance-Based Learning algorithm (IBK)	0.9982	Precision, Recall, F-measure, Receiver Operating Curve (ROC)	Small feature set used; no thorough hyperparameter tuning; only basic metrics
[15]	CICIDS-2017	Random Forest (RF)	0.9986	Precision, Recall	Features selected but no optimization algorithm for RF; no interpretability or false positive rate analysis
[16]	CIC-IDS (Canadian Institute of Cybersecurity)	Extreme Gradient Boosting (XGB)	0.9954	-	Lacks detailed tuning description, interpretability, and metrics beyond accuracy
[11]	Custom 5G IoT dataset	Hybrid DNN + Feature Engineering	0.9960	Recall, F1-measure, ROC AUC	Focused on 5G-specific threats; lacks generalizability; limited optimization details
[17]	CIC-IDS-2017 and CSE-CIC-IDS-2018	Hybrid CNN-LSTM	0.9730	Recall, Precision, F1, AUC	Strong architecture but lacks interpretability analysis; tuning method not clearly described
[18]	UNSW-NB15	Bi-LSTM + Attention	0.9800	Recall, F1 Score, False Positive Rate, False Negative Rate, t-test (p-value)	Effective against specific scanning attacks, but not validated on broader benchmark datasets
This study	CIC-IDS-2017	Emperor Penguin Optimization Algorithm-Gradient Boosting (EPOA-GB)	0.9997	Precision, Recall, F1-Score, ROC AUC, PR AUC, Log loss, MCC, Cohen's Kappa	Addresses gaps in prior works, including hyperparameter optimization, interpretability (SHAP), robust validation, and comprehensive metrics

This study introduces several key innovations to address the limitations commonly found in existing classification modeling approaches. While many prior works rely on default settings or manual hyperparameter tuning—such as in DNNs and DTs—we employ the Emperor Penguin Optimization Algorithm (EPOA) to automatically and efficiently tune the GB classifier, leading to improved model performance. Overfitting and robustness, often overlooked in previous studies, are explicitly addressed in our approach through the use of cross-validation and evaluation on held-out test datasets. Furthermore, to tackle the frequent lack of interpretability in traditional models, we incorporate SHAP (SHapley Additive exPlanations) and perform feature importance analysis to provide deeper insights into model behavior and feature contributions. Unlike prior research that typically reports limited metrics, our study offers a comprehensive performance evaluation by including accuracy, precision, recall, F1-score, and ROC AUC (Receiver Operating Characteristic-Area Under Curve), PR AUC (Precision-Recall-Area Under Curve), Log loss, Matthews Correlation Coefficient (MCC), Cohen's Kappa. Finally, to enhance generalizability, we validate our approach on another state-of-the-art tuning model rather than relying on traditional benchmark models, demonstrating the robustness and wide applicability of our method. Collectively, these contributions represent a significant advancement over existing methods in terms of optimization, interpretability, evaluation, and generalizability.

Therefore, the major novelty in the current work is in its overall approach toward enhancing IDS through integrating high-performance classification models with an advanced optimization algorithm. Unlike traditional IDS frameworks with static settings or basic tuning techniques, in this work, a new algorithm, the EPOA, is proposed for application in a dynamic hyperparameter optimization method for diverse models. The suggested

method provides a secure and efficient mechanism for real-time implementation by systematically improving computational models. Moreover, the comparative analysis in the study not only compares model performance in individual terms but also identifies the transformational role played by EPOA in enhancing model efficiency, stability, and overall generalization performance. The main objectives of this work involve enhancing accuracy in detecting malicious and non-malicious activities, minimizing false positive and false negative occurrences, and lessening computational expense in processing large networks. By combining these, this work proposes a new, flexible, and efficient IDS model with an outlook toward addressing evolving network security concerns.

Hence, in order to guide the present study, the following key research questions have been posed: **1.** Can the proposed EPOA-GB significantly enhance the performance of a ML-based IDS, particularly in comparison to other conventional as well as state-of-the-art tuning approaches? **2.** Does integrating EPOA with Gradient Boosting improve model robustness and generalizability across the employed dataset?

We hypothesize that EPOA-GB, as a bio-inspired metaheuristic algorithm, will outperform other applied tuning methods in identifying optimal hyperparameters, thereby boosting detection accuracy, reducing false positives, and improving the generalization of the IDS model. We further expect that model interpretability tools will provide actionable insights into the prediction process. To address these questions, our methodology includes **(i)** applying EPOA for automated hyperparameter optimization of the selected ML models, **(ii)** evaluating performance on benchmark dataset using cross-validation and a comprehensive set of metrics, and **(iii)** employing SHAP and feature importance analyses to interpret model predictions. Each step is designed to directly respond to the research questions and validate our hypotheses through the evaluation.

This paper is organized into key sections addressing multiple aspects of the classification tasks. The methodology comes in Section 2, introducing the dataset, its sources, feature selection, model selection, an optimizer, and evaluation metrics. Section 3 covers model performance, including key observations, trends, and insights. Section 4 summarizes key results, explains their implications, and sets out avenues for future work.

2 Methodology

An efficient IDS requires methodical development, beginning with the data preparation and concluding with model evaluation. ML models serve as a powerful tool for discovering cyberattacks through a mechanism of training on network traffic information. A sequential process for network intrusion detection via ML models using CIC-IDS (Canadian Institute for Cybersecurity) data is presented in Figure 1. Initially, the objective is determined, and then feature extraction and partitioning of 70:30 training and testing sets for a relevant dataset follow. The six models, namely Random Forest (RF), Gradient Boosting (GB), Decision Tree (DT), XGBoost (XGB), AdaBoost (AB), and K-Nearest Neighbors (KNN), are deployed to the classification issue. For enhancing performance, the models' hyperparameters are tuned with EPOA, a high-performance algorithm inspired by penguins' foraging behavior in a real environment. Lastly, model evaluation is performed to choose the best-performing classifier.

It is worth mentioning that, the choice of ML models in this study is theoretically motivated by their complementary strengths in handling various challenges intrinsic to intrusion detection tasks, such as high-dimensional feature spaces, imbalanced data, and the need for generalization under noisy conditions. RF was selected for its ensemble architecture and robustness to overfitting, especially in large and noisy datasets. DTs provide interpretability and serve as a baseline, while GB and XGB offer superior accuracy by focusing on correcting prior errors in a sequential manner, making them suitable for complex intrusion patterns. AdaBoost was chosen for its ability to minimize bias through weight adjustment, and KNN was involved owing to its non-parametric, instance-based nature which offers a contrasting learning paradigm that can benefit small or local pattern detection. Moreover, the selection of the EPOA for hyperparameter tuning is grounded in its demonstrated success as a metaheuristic optimizer in solving nonlinear, high-dimensional problems. Its swarm-intelligence-inspired mechanism offers a balance between global exploration and local exploitation, which is critical for fine-tuning complex models. Compared to traditional grid or random search approaches, EPOA improves convergence to optimal hyperparameter configurations, thereby enhancing model stability and predictive accuracy in IDS tasks.

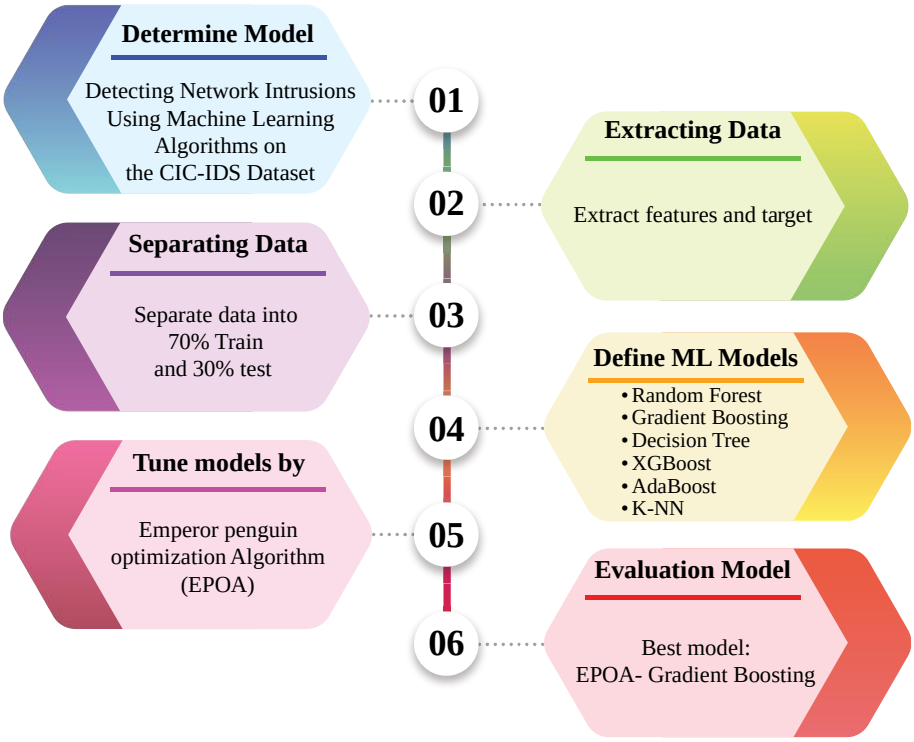


Figure 1: Visual presentation of the research framework.

2.1 Dataset

The CIC-IDS-2017 dataset used in this study was sourced from [19]. This dataset is rich in network flow data, capturing essential attributes that make it a valuable resource for cybersecurity research and intrusion detection system (IDS) development. Prior to applying ML models, the dataset undergoes a comprehensive preprocessing pipeline. This includes handling missing values to avoid bias during model training and encoding categorical features to ensure compatibility with various algorithms. Numerical features are standardized to bring them to a common scale, which is essential for the performance of most ML models. Following standardization, dimensionality reduction is performed using Principal Component Analysis (PCA), reducing the feature space to 20 principal components while preserving most of the dataset's variance. This step enhances computational efficiency, mitigates the risk of overfitting, and improves the model's generalization ability on unseen data. Figure 2 shows the PCA feature loadings heatmap generated to visualize the correlation between network flow features and principal components, facilitating dimensionality reduction for improved model performance. And, Figure 3 demonstrates the PCA variance plot employed to determine the number of components needed to retain 90% of the data's variance, guiding effective dimensionality reduction.

Additionally, a key data-cleaning step involves removing unnecessary spaces from column names to maintain consistency throughout the dataset. To ensure the reliability and robustness of model evaluation, k-fold cross-validation is employed, allowing the models to be trained and validated across multiple data splits. This approach not only prevents overfitting but also provides a more accurate estimate of model performance.

After that, the target variable and input variables are specified. The target variable is then converted into four classes, where BENIGN maps to 0 and Web Attack – Brute Force, Web Attack – XSS, and Web Attack – SQL Injection labels are respectively mapped to 1, 2, 3. This classification framework simplifies the detection problem for models by targeting either normal or abnormal behaviors. A bar chart in Figure 4 illustrates that benign traffic comprises the majority of the dataset, with significantly fewer instances of web attacks such as brute force, XSS, and SQL injection.

The cleaned data is then divided into test (30%) and training (70%) sets in preparation for model training. This way, the model will be evaluated on unseen data; hence, it can be tested for its generalization capability. Moreover, the features are standardized using Standard Scaler; this normalizes the data, making it suitable for ML models. With the completion of these preprocessing steps, this dataset is now ready for training high-performance models for network intrusion detection, furthering cybersecurity research.

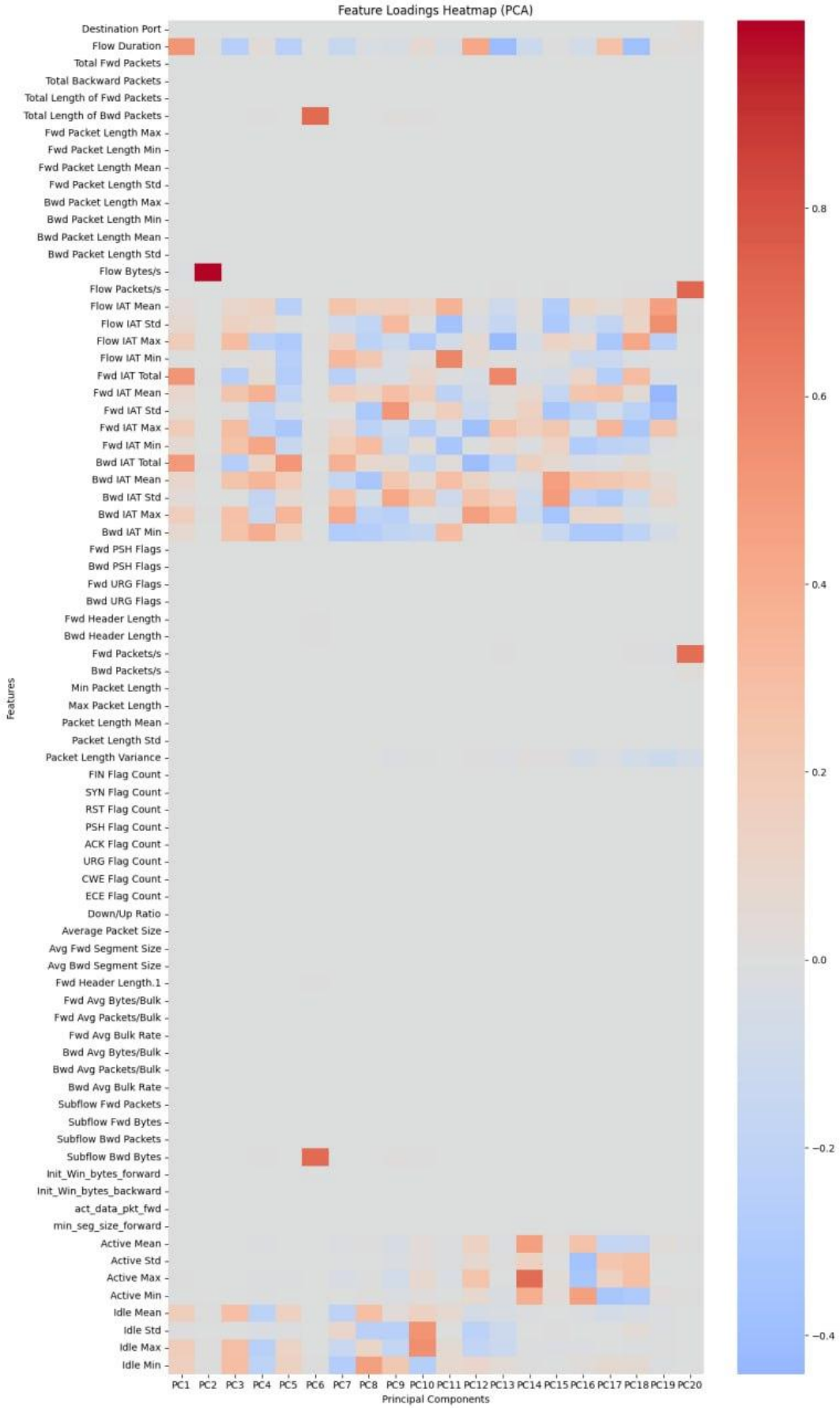


Figure 2: PCA feature loadings heatmap showing correlations between network flow features and principal components.

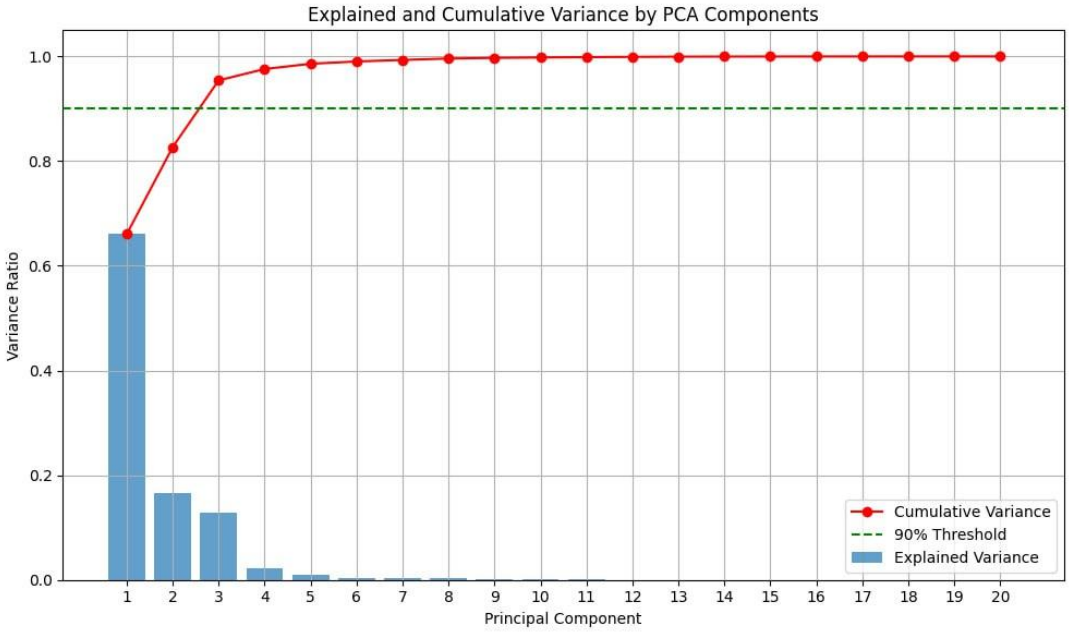


Figure 3: Explained and cumulative variance of principal components from PCA for dimensionality reduction.

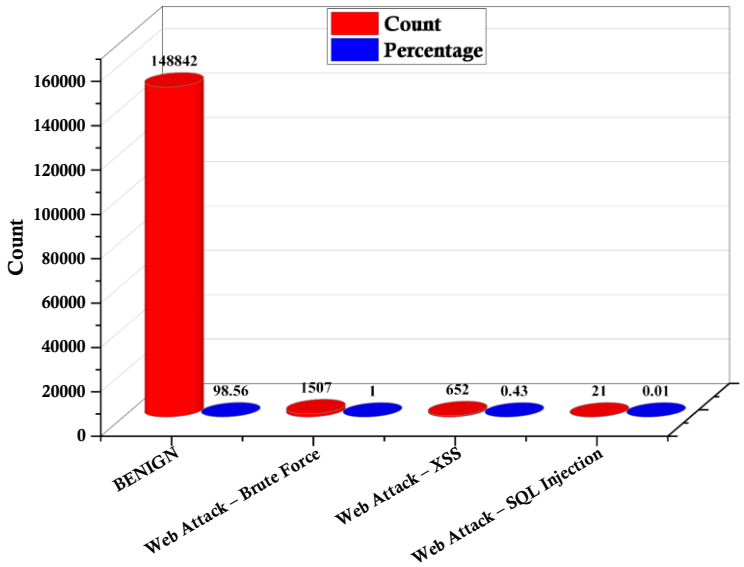


Figure 4: Bar chart showing the frequency distribution of web attack types, highlighting the dominance of benign traffic.

2.2 Model selection

2.2.1 Random Forest

Random Forest (RF) is an ensemble learning model that constructs many decision trees and aggregates them to make a prediction, enhancing predictive accuracy and minimizing overfitting. Initially, Breiman [20] developed RF by training numerous decision trees over a range of bootstrapped datasets, utilizing bagging and feature selection at each split on a random basis. Each tree classifies a new case individually, and the final classification is generated through a vote over all trees in a majority vote style. This helps in generalization and strengthening, making RF a strong tool for handling large and noisy datasets (see [20, 21]).

2.2.2 Gradient boosting

GB is another strong ensemble learner model that constructs predictive models sequentially, with each model optimized for performance through the improvement of preceding model errors. It was first proposed by Friedman [23] as an expansion of boosting algorithms. GB trains weak learners, in most cases DTs, in a sequential manner, with each successive tree attempting to minimize the residuals of its predecessor through gradient descent. In contrast to RF, whose trees are constructed individually, trees in GB are constructed

iteratively, with weights tuned to minimize bias and maximize accuracy (see [24]). This produces a very powerful model that can handle intricate patterns; however, it requires careful adjustment to avoid overfitting.

2.2.3 Decision Tree

DT is a supervised learner model that distinguishes data into hierarchical branches regarding feature values and ends in a predicted class label. By applying measures such as Gini impurity or information gain (based on entropy), the model builds a tree by choosing the most informative feature at each node. It recursively divides the data to a point when it reaches a leaf with a high level of purity, at which point classification occurs (see [25], [26]). DTs have simple interpretability and computational efficiency but suffer from overfitting, and pruning can counteract this.

2.2.4 Extreme Gradient Boosting

XGB, also called XGBoost, is a high-performance ML model that maximizes the efficiency, accuracy, and overall performance of traditional gradient boosting algorithms. XGB, developed by Chen and Guestrin [27], gained widespread acceptance in data science competitions and real-world implementation. XGB builds an ensemble model sequentially, with each new tree fitting in a direction that corrects residuals of preceding trees with gradient-boosted trees via gradient descent optimization. It offers important enhancements, including parallel computing, tree pruning, and regularization parameters for overfitting avoidance, which result in a quicker and more scalable approach. XGB is also efficient in dealing with missing values and can work with sparse data and is therefore ideal for sophisticated classification scenarios (see [27, 28]).

2.2.5 Adaptive Boosting

AB is a pioneer model in ensemble learning that takes several weak classifiers and forms a strong predictive model out of them. AB was developed by Freund and Schapire [30] as a refinement of boosting algorithms. The AB model iteratively trains weak learners on the training set, adjusting their weights according to classification errors. Misclassified cases receive increased weights in subsequent iterations, forcing the model to pay attention to challenging cases. Final classification is performed via a weighted vote of all weak classifiers. AB is flexible, simple, and can minimize bias with interpretability; however, it is not robust when dealing with outliers and noisy data (see [30, 31]).

2.2.6 K-Nearest Neighbors

KNN is a simple yet effective supervised learning approach, generating labels for classes through a similar-data point comparison. Initially, Fix [33] developed it as a non-parametric model for pattern classification. KNN operates through the computation of the distance of a query point from all training samples in a dataset. It then assigns a label to a new instance based on the most frequent label among its KNNs. Unlike most methods, KNN doesn't require explicit training; instead, it stores all training samples and compares them to new cases, making it a lazy learner algorithm. While it is efficient and simple for small datasets, it becomes computationally expensive for large datasets, as it requires distance calculations for each new prediction (see [33, 34]).

2.3 Optimization algorithm

Optimization algorithms serve as a basis for ML, and through them, model performance can be optimized. Such algorithms gain inspiration from many mathematical laws and processes in nature and work towards resolving complex optimization problems in many fields. The Emperor Penguin Optimization Algorithm (EPOA) [36] is one of the best nature-inspired algorithms for nonlinear and multidimensional problem solving; Figure 5 shows its conceptual workflow.

The emperor penguin optimizer is a metaheuristic algorithm inspired by emperor penguins' huddling behavior for survival in the extreme conditions of the Antarctic. It is proposed as a swarm intelligence approach and simulates the dynamic thermal control manner in which penguins form dense, regulated groups to maintain warmth. In optimization cases, this turns into candidate solutions (penguins) moving toward the best solution (warmest area) by modifying their positions according to temperature (fitness value). Exploration (random search for the diversity of solutions) and exploitation (refinement of a potential solution) are balanced through the simulation of penguins' movement behavior (see [37]). In this work, EPOA was successfully applied for hyperparameter tuning in all ML models, including RF, GB, DT, XGB, AB, and KNN, enhancing their accuracy and performance.

In addition to EPOA, Grid Search (GS) was applied as a baseline hyperparameter tuning method to benchmark optimization efficiency. The hyperparameters of all chosen models were optimized using both EPOA and GS, as detailed in Tables 2 and 3, respectively. The comparison shows that while EPOA consistently achieved high-performing configurations across all models, it also required the same iterations, but generally higher runtime than GS.

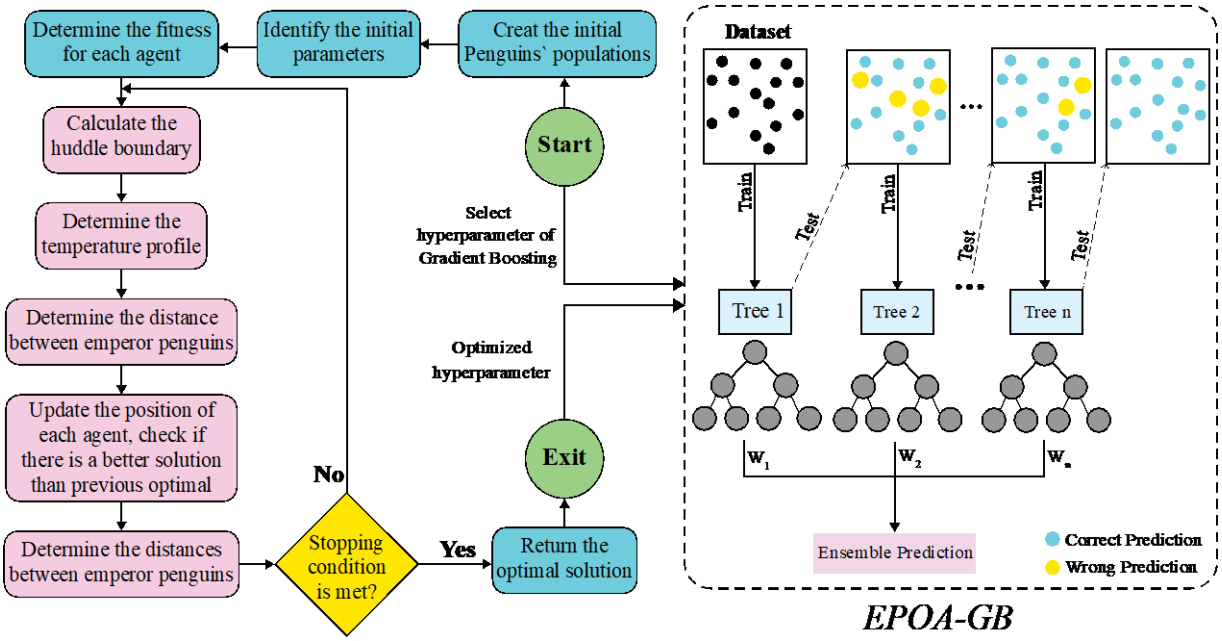


Figure 5: An example workflow of the GB model's hyperparameter tuning process using EPOA.

Table 2: The applied models' hyperparameter tuning using EPOA.

	EPOA-RF	EPOA-GB	EPOA-DT	EPOA-XGB	EPOA-AB	EPOA-KNN
N estimators	100	100	-	100	100	-
Min samples split	2	-	2	-	-	-
Min samples leaf	1	-	1	-	-	-
Max depth	None	3	None	3		-
Learning rate	-	0.1	-	0.1	0.1	-
Subsample	-	-	-	0.7		-
Colsample bytree	-	-	-	0.7		-
Weights	-	-	-	-		Uniform
P	-	-	-	-		2
N neighbors	-	-	-	-		5
Runtime (sec)	10206.15	100361.13	1002.1	2010.57	15009.47	10209.86
Iteration	30	30	30	30	30	30

Table 3: The applied models' hyperparameter tuning using Grid Search (GS).

	GS-RF	GS-GB	GS-DT	GS-XGB	GS-AB	GS-KNN
Max depth	7	5	3	12	-	-
Min samples leaf	1	-	8	-	-	-
Min samples split	3	8	8	-	-	-
N estimators	65	300	-	229	271	-
Learning rate	-	0.0653	-	0.0443	0.4729	-
Colsample bytree	-	-	-	0.8997	-	-
Subsample	-	-	-	0.9519	-	-
N neighbors	-	-	-	-	25	-
P	-	-	-	-	1	-
Weights	-	-	-	-	Distance	-
Runtime (sec)	90.8311	980.4113	8.7119	15.5305	114.8171	93.5015
Iteration	30	30	30	30	30	30

2.4 Evaluation Indicators

The effectiveness of ML models in identifying network intrusions is evaluated using a variety of statistical testing indicators. Comparing and evaluating a model through several factors helps in planning improvements and comparisons. Figure 6 depicts a selection of key evaluation statistics for application in classification scenarios. They involve the F1-score, which sets a balance between precision and recall; Cohen's Kappa, which is an

agreement between two raters that considers chance; recall, which measures how well the scheme detects positive cases; and Log loss, which evaluates the accuracy of probabilistic predictions. In addition, accuracy measures overall model correctness; the Matthews Correlation Coefficient (MCC) provides a balanced performance even in unbalanced datasets, and the proportion of correctly positive instances detected is measured through precision.

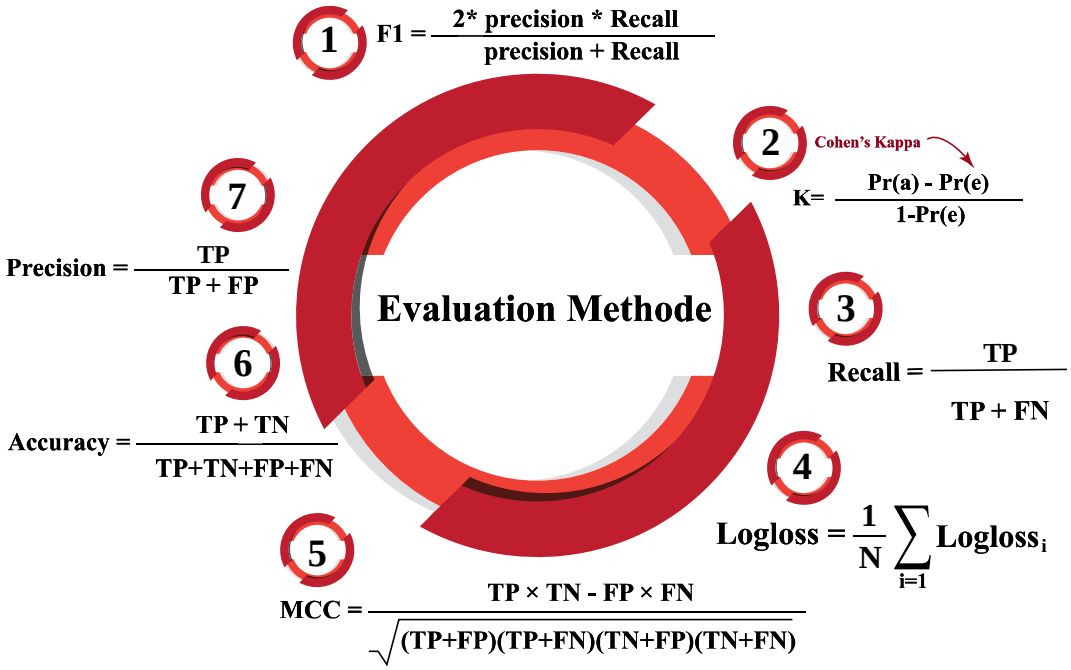


Figure 6: The formal description of several key indicators.

Other important evaluation indicators, apart from metrics in Figure 6, include PR AUC (Precision-Recall-Area Under Curve) and ROC AUC (Receiver Operating Characteristic-Area Under Curve). The ROC curves are plots of the true positive (TP) rate against the false positive (FP) rate at diverse threshold levels, which is an indicator of how well a model can differentiate between classes. Better differentiation between benign and attack traffic is shown by a higher ROC AUC value, which lowers the possibility of false negatives (FNs). On the other hand, the PR AUC gives the usability of a model under conditions where the detection of TP cases is highly desirable, while that of the FP is kept at a minimal value. This indicator is particularly applicable for unbalanced datasets, as it addresses the trade-off between precision and recall rather than considering true negatives (TNs). The predictive power, resilience, and general efficacy of each model in differentiating between benign and malicious network traffic are all verified through these indicators.

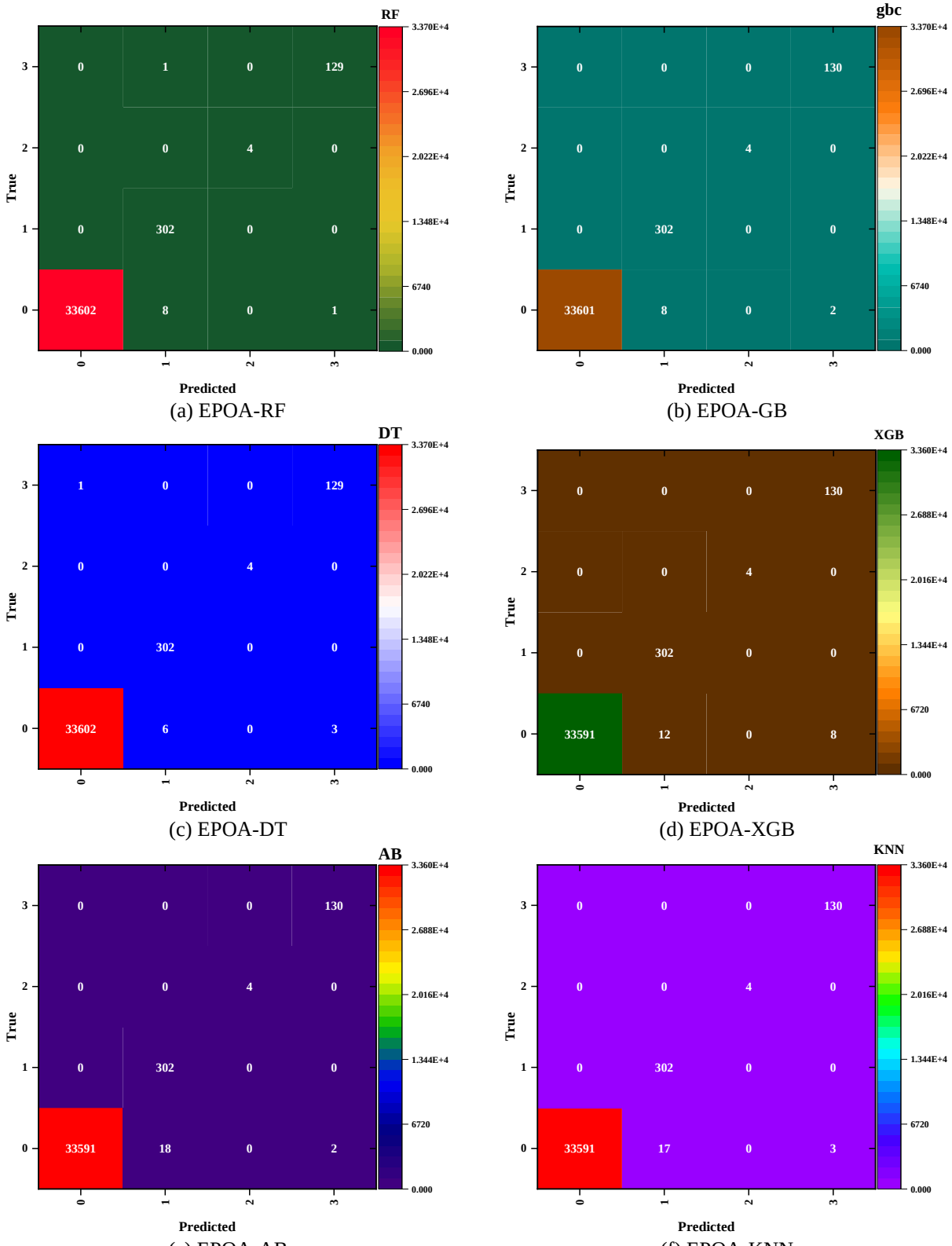
3 Results and discussion

3.1 Model comparison

In comparing and contrasting the employed models for network intrusion detection, a careful analysis was performed with several performance factors considered. Confusion matrices in Figure 7 present each model's classification output, indicating its capability to differentiate between benign and three types of attack traffic. In this figure, the target variable is categorized into four classes, with Benign labeled as 0, and Web Attack – Brute Force, Web Attack – XSS, and Web Attack – SQL Injection labeled as 1, 2, and 3, respectively.

The EPOA-RF model shows excellent performance, correctly classifying 33602 benign samples with only 9 misclassifications. All Brute Force and XSS attacks are correctly identified, while only one SQL Injection sample is misclassified. This reflects high precision and recall across all classes, especially the minority attack types. EPOA-GB performs similarly well, with 33601 benign samples correctly predicted and only 10 errors. It obtains satisfactory classification for all attack categories—Brute Force, XSS, and SQL Injection—indicating strength in handling both majority and minority classes. The EPOA-DT model correctly identifies all Brute Force and XSS samples and 129 out of 130 SQL Injection cases. It classifies 33602 benign samples accurately, with 9 minor misclassifications. The results highlight reliable performance across all classes, similar to RF and GB. While EPOA-XGB accurately classifies all attack categories, it shows slightly higher misclassification in the benign class, with 20 errors out of 33611 samples. Despite this, it maintains adequate detection for Brute Force, XSS, and SQL Injection attacks, confirming its strength in minority class recognition. The EPOA-AB model shows more errors in predicting class 0, with 20 misclassified instances. While class 1 is predicted without error, there are two instances of class 0 predicted as class 3. Although

generally strong, the model is slightly more prone to false positives compared to RF and DT. The KNN model mirrors AB's pattern, with 17 instances of class 0 misclassified and 3 as class 3. It performs properly for class 1 and class 2. Like AB, it achieves good overall accuracy but is less robust for the majority class than RF and DT. These observations provide insight into both data limitations (e.g., class imbalance and feature similarity) and model sensitivity.



(a) EPOA-RF (b) EPOA-GB

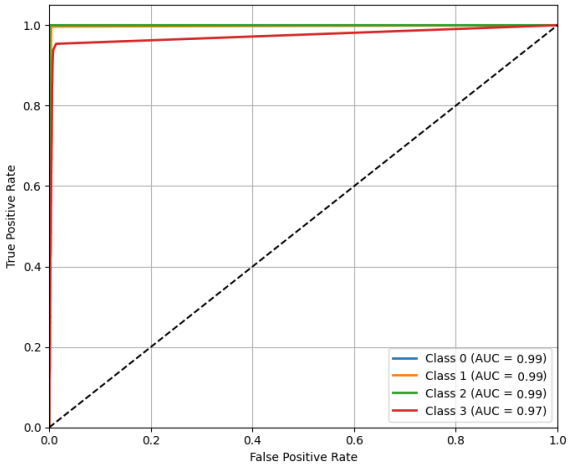
(c) EPOA-DT (d) EPOA-XGB

(e) EPOA-AB (f) EPOA-KNN

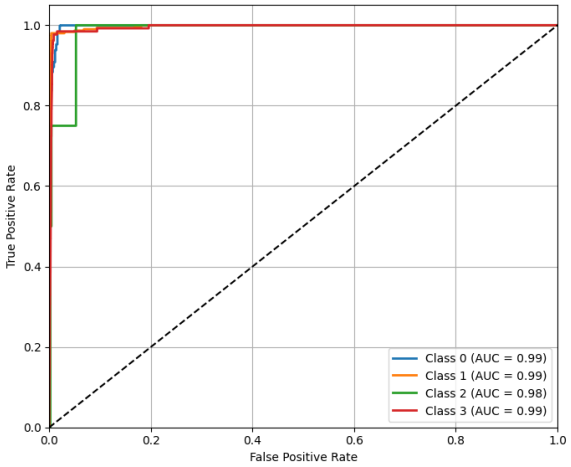
Figure 7: Confusion matrices for the applied hybrid models' prediction, including (a) EPOA-RF, (b) EPOA-GB, (c) EPOA-DT, (d) EPOA-XGB, (e) EPOA-AB, and (f) EPOA-KNN.

Moreover, the following analysis explicitly differentiates between ROC AUC and PR AUC metrics, highlighting the critical importance of PR AUC in intrusion detection scenarios due to its sensitivity to class imbalance and its direct reflection of the models' ability to maintain precision in identifying attack instances.

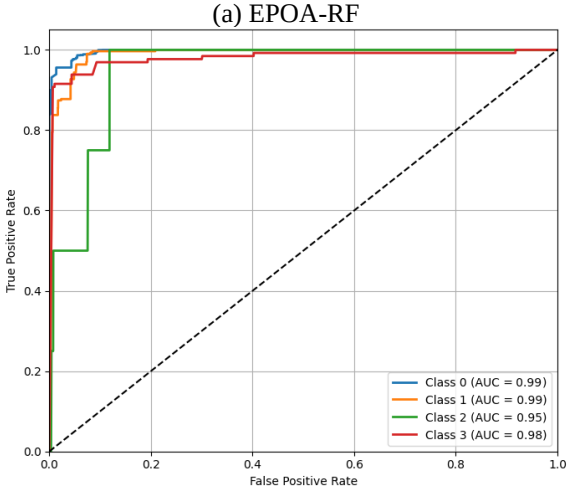
Figure 8 shows the ROC curves of various models applied to network intrusion detection with their performance on the test dataset. According to this figure, the EPOA-RF and EPOA-GB hybrid models exhibit an optimal performance with an AUC of above 0.97, considering all classes. This suitable score reflects that the benign and attack network traffic can be appropriately differentiated without misclassification during the test, representing the high predictive performance of such models. Also, EPOA-DT, EPOA-XGB, and EPOA-AB are performing optimally as well, as shown by their high AUC values above 0.87 for class 2, and AUC values above 0.94 for the other classes. The corresponding ROC curves of these models ascend nearly vertically to True Positive Rate (TPR) = 0.999 at False Positive Rate (FPR) close to 0, further establishing their dependability on cybersecurity applications. On the other hand, while the AUC values are very high in these models, showing their great discrimination power, the respective values of EPOA-KNN stand a little bit behind the others. Its ROC curve is lower with 0.75 for class 2, indicating some minor chance of misclassifications at particular thresholds.



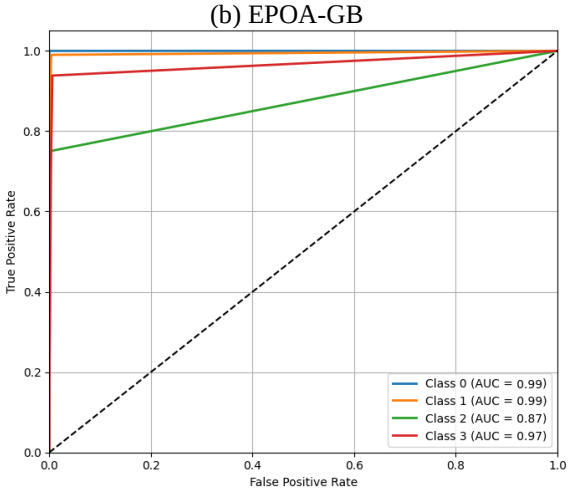
(a) EPOA-RF



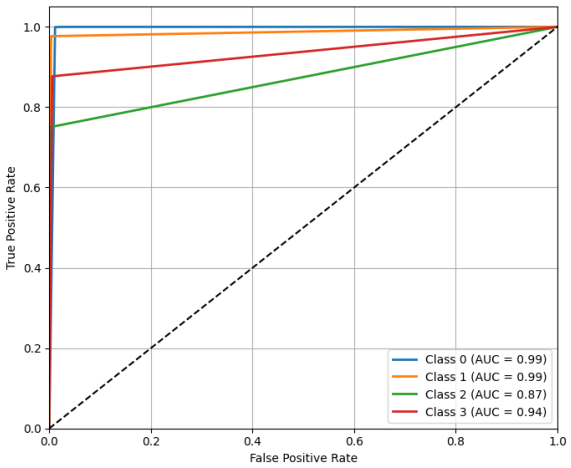
(b) EPOA-GB



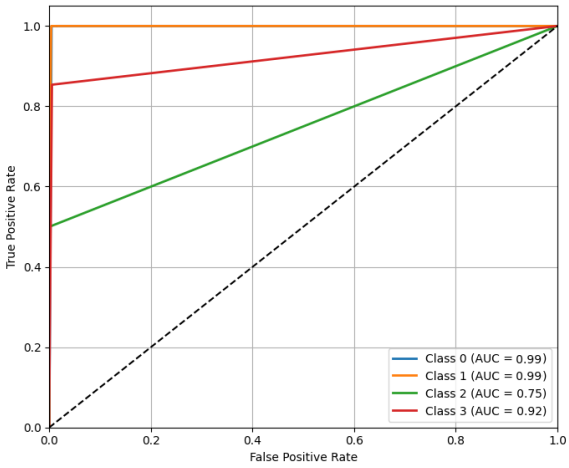
(c) EPOA-DT



(d) EPOA-XGB



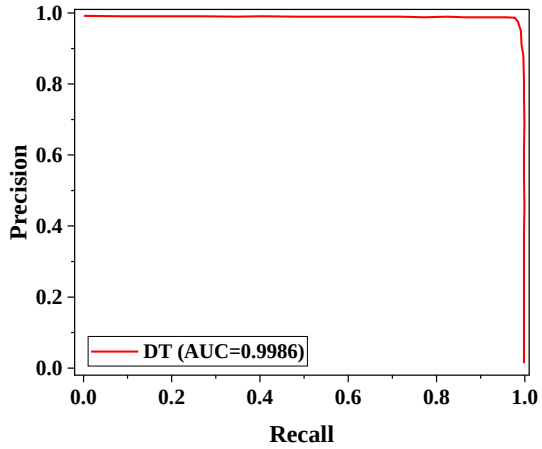
(e) EPOA-AB



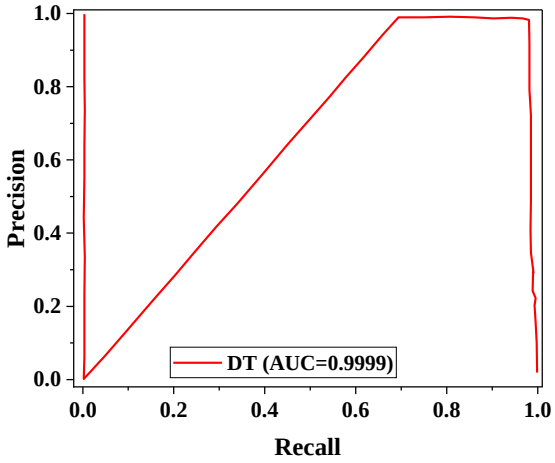
(f) EPOA-KNN

Figure 8: ROC curves for the applied hybrid models, including (a) EPOA-RF, (b) EPOA-GB, (c) EPOA-DT, (d) EPOA-XGB, (e) EPOA-AB, and (f) EPOA-KNN

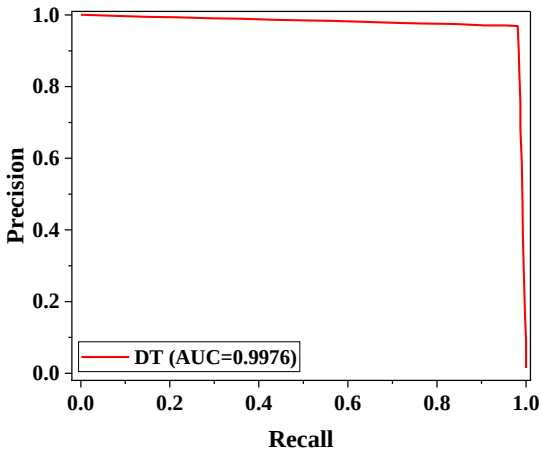
The Precision-Recall (PR) curves for all the models over the testing dataset have been displayed in Figure 9, with a critical examination of each model's performance in having high precision and high recall for network intrusion detection. Based on this figure, the AUC values of the PR curve of EPOA-GB, EPOA-RF, and EPOA-DT are all close to adequate performance above 0.99. They maintain consistently high precision at any recall value, proving that such models can effectively detect intrusion with negligible additional FPs. These experiments confirm not only high accuracy but also reliable and strong performance in real-world cybersecurity scenarios. The EPOA-KNN and EPOA-XGB perform moderately, with a value for PR AUC close to 0.98, marginally less but still high in effectiveness. However, EPOA-AB reaches a value for a PR AUC of 0.97, signifying a minor drop in accuracy at certain recall values.



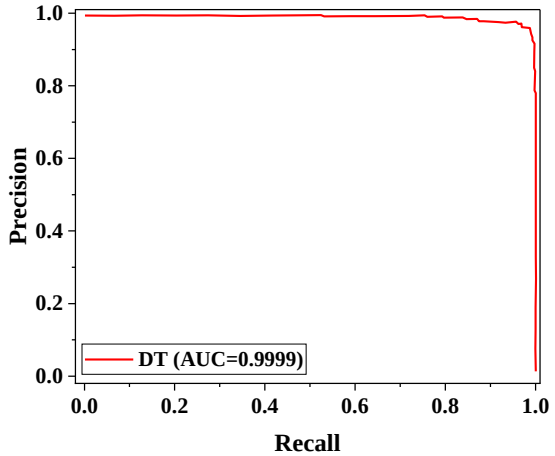
(a) EPOA-RF



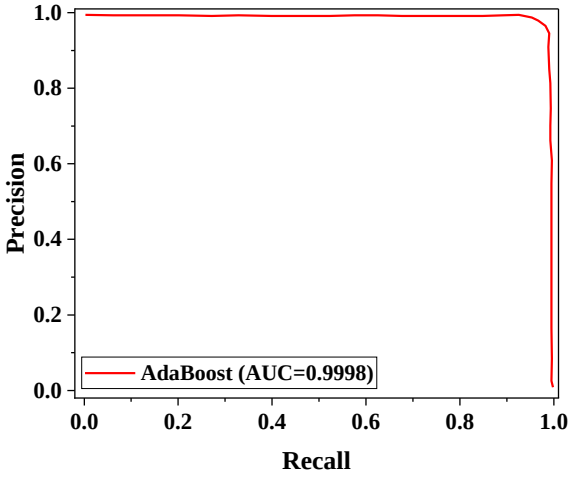
(b) EPOA-GB



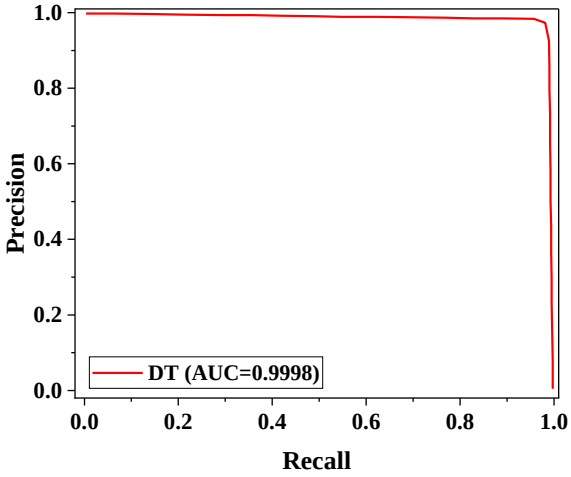
(c) EPOA-DT



(d) EPOA-XGB



(e) EPOA-AB



(f) EPOA-KNN

Figure 9: PR curves for the applied hybrid models, including (a) EPOA-RF, (b) EPOA-GB, (c) EPOA-DT, (d) EPOA-XGB, (e) EPOA-AB, and (f) EPOA-KNN

Table 4 presents the performance metrics of the applied hybrid models tuned using EPOA on both train and test. Evaluated on the test dataset, all models exhibited outstanding classification performance, with test accuracies exceeding 0.9994. Among them, the EPOA-GB model demonstrated the best overall performance, achieving a test accuracy of 0.9997, F1-score of 0.9948, ROC AUC of 0.9999, and the highest Cohen's Kappa value of 0.9885. Additionally, EPOA-GB had the lower Log Loss (0.0050) among most of the models, indicating both high confidence and low prediction error. These results highlight the effectiveness of EPOA in achieving near-perfect classification performance, with EPOA-GB standing out as the most robust model under this tuning approach.

Table 5 illustrates the performance of the hybrid models tuned using Grid Search (GS) on both train and test. Based on the test dataset, although the models achieved generally high accuracies above 0.994, their performance metrics—particularly precision, recall, and F1-score—were significantly lower than their EPOA-tuned counterparts. The GS-GB model emerged as the best among the GS-tuned models, with the highest test accuracy of 0.9961 and a relatively balanced F1-score of 0.5432, ROC AUC of 0.9904, and Cohen's Kappa of 0.8481. However, compared to EPOA-GB, the GS-GB model had higher Log loss (0.0138) and considerably lower precision and recall, indicating reduced reliability and robustness. These findings reinforce the superiority of EPOA in both predictive performance and optimization efficiency.

Table 4: Statistical results of the hybrid models tuned by EPOA.

	Accuracy	**Precision**	**Recall**	**F1 Score**	**ROC AUC**	**PR AUC**	**Log loss**	**MCC**	**Cohen's Kappa**	**Runtime (sec)**
Train										
EPOA-RF	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.0000	0.9999	0.9999	10206.15
EPOA-GB	0.9999	0.9999	0.9965	0.9982	0.9968	0.9965	0.0010	0.9962	0.9962	100361.13
EPOA-DT	0.9999	0.9963	0.9999	0.9981	0.9999	0.9968	0.0001	0.9971	0.9971	1002.1
EPOA-XGB	0.9999	0.9990	0.9972	0.9981	0.9976	0.9967	0.0030	0.9962	0.9962	2010.57
EPOA-AB	0.9998	0.9915	0.9999	0.9957	0.9999	0.9923	0.0006	0.9914	0.9914	15009.47
EPOA-KNN	0.9998	0.9907	0.9999	0.9953	0.9999	0.9906	0.0003	0.9914	0.9914	10209.86
Test										
EPOA-RF	0.9997	0.9908	0.9980	0.9944	0.9986	0.9919	0.0020	0.9886	0.9885	10206.15
EPOA-GB	**0.9997**	**0.9898**	**0.9999**	**0.9948**	**0.9999**	**0.9924**	**0.0050**	**0.9886**	**0.9885**	**100361.13**

EPOA-DT	0.9997	0.9894	0.9980	0.9937	0.9976	0.9910	0.0110	0.9886	0.9885	1002.1
EPOA-XGB	0.9994	0.9760	0.9999	0.9876	0.9999	0.9799	0.0020	0.9776	0.9773	2010.57
EPOA-AB	0.9994	0.9821	0.9999	0.9908	0.9998	0.9746	0.4190	0.9776	0.9773	15009.47
EPOA-KNN	0.9994	0.9810	0.9999	0.9902	0.9998	0.9836	0.4190	0.9776	0.9773	10209.86

Table 5: Statistical results of the hybrid models tuned by Grid Search (GS).

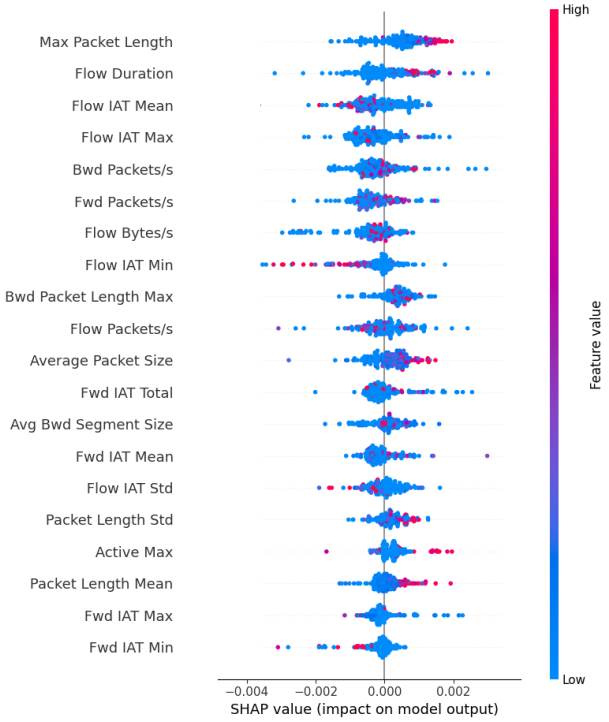
	Accuracy	**Precision**	**Recall**	**F1 Score**	**ROC AUC**	**PR AUC**	**Log loss**	**MCC**	**Cohen's Kappa**	**Runtime (sec)**
Train										
GS-RF	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.0021	0.9999	0.9999	90.8311
GS-GB	0.9973	0.9079	0.8433	0.8532	0.9996	0.9993	0.0059	0.8952	0.8950	980.4113
GS-DT	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	2.2E-6	0.9999	0.9999	8.7119
GS-XGB	0.9955	0.6705	0.5005	0.4670	0.9989	0.9636	0.0107	0.8191	0.8185	15.5305
GS-AB	0.9942	0.4133	0.4503	0.4300	0.9927	0.9178	1.1639	0.7535	0.7500	114.8171
GS-KNN	0.9971	0.8764	0.6551	0.6946	0.9994	0.9863	0.0059	0.8833	0.8833	93.5015
Test										
GS-RF	0.9954	0.5427	0.5420	0.5418	0.9757	0.9828	0.0125	0.8202	0.8201	90.8311
GS-GB	**0.9961**	**0.5631**	**0.5410**	**0.5432**	**0.9904**	0.9834	**0.0138**	**0.8482**	**0.8481**	**980.4113**
GS-DT	0.9952	0.5424	0.5578	0.5478	0.7763	0.9638	0.1747	0.8140	0.8139	8.7119
GS-XGB	0.9960	0.6860	0.5127	0.4973	0.9956	0.9384	0.0116	0.8446	0.8442	15.5305
GS-AB	0.9945	0.4295	0.4491	0.4388	0.9823	0.9044	1.1642	0.7705	0.7657	114.8171
GS-KNN	0.9957	0.5469	0.5428	0.5444	0.9014	0.9530	0.0268	0.8339	0.8339	93.5015

3.2 Sensitivity analysis

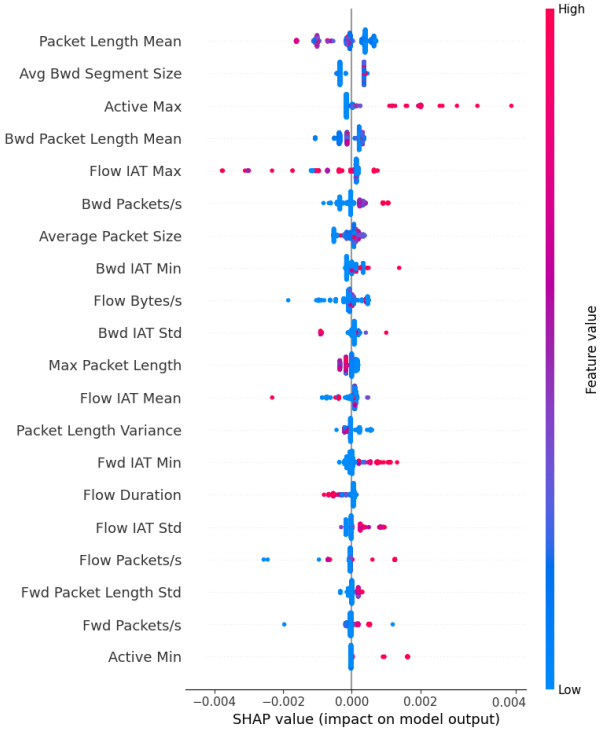
Figure 10 demonstrates SHAP summary of input features' impact on the hybrid models' output. According to this figure, the hybrid models' SHAP values range from -0.004 to +0.003. The EPOA-RF and EPOA-AB models show the lowest variability and features' impact among the other models, explaining lower interpretability or weaker feature separation compared to other models. The SHAP values for these models are relatively small, indicating that the individual feature contributions to the output are subtle.

The EPOA-GB model, on the other hand, demonstrates the highest variability and feature impact among the other models. Flow IAT Max, Active Max, and Packet Length Mean are the most significant features. Their wide SHAP value ranges show that EPOA-GB is highly sensitive to changes in these key features and it utilizes these characteristics, making it well-suited for complex, nonlinear data patterns. Therefore, the strong influence of a few dominant features supports GB's reputation for high accuracy and interpretability through clear feature attributions.

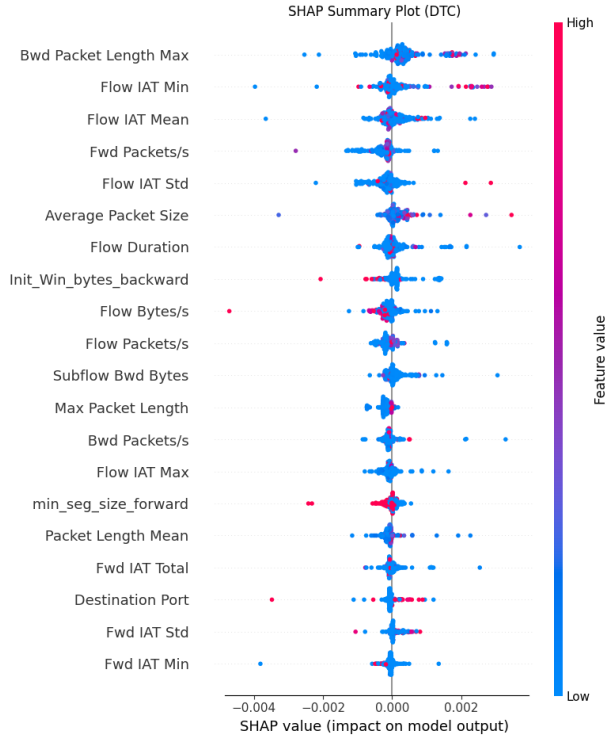
EPOA-XGB shows the next higher variability and feature impact. The most impactful features include Average Packet Size and Destination Port. The SHAP value spread here is broader than in the EPOA-RF and EPOA-AB plots, showing clearer separation of feature contributions. The EPOA-KNN and EPOA-DT models also appear relatively high in their SHAP values' variability, suggesting that these models' decisions are moderately sensitive to changes in a few dominant features and indicating more decisive rule-based splits.



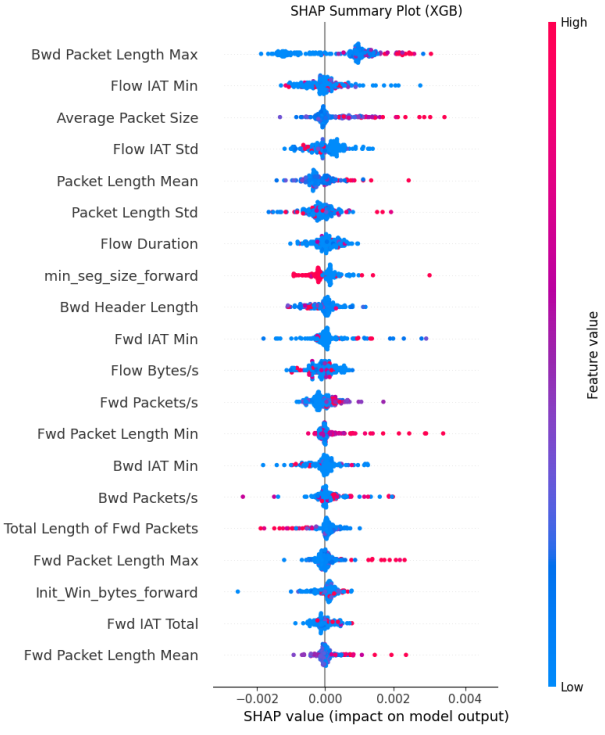
EPOA-RF



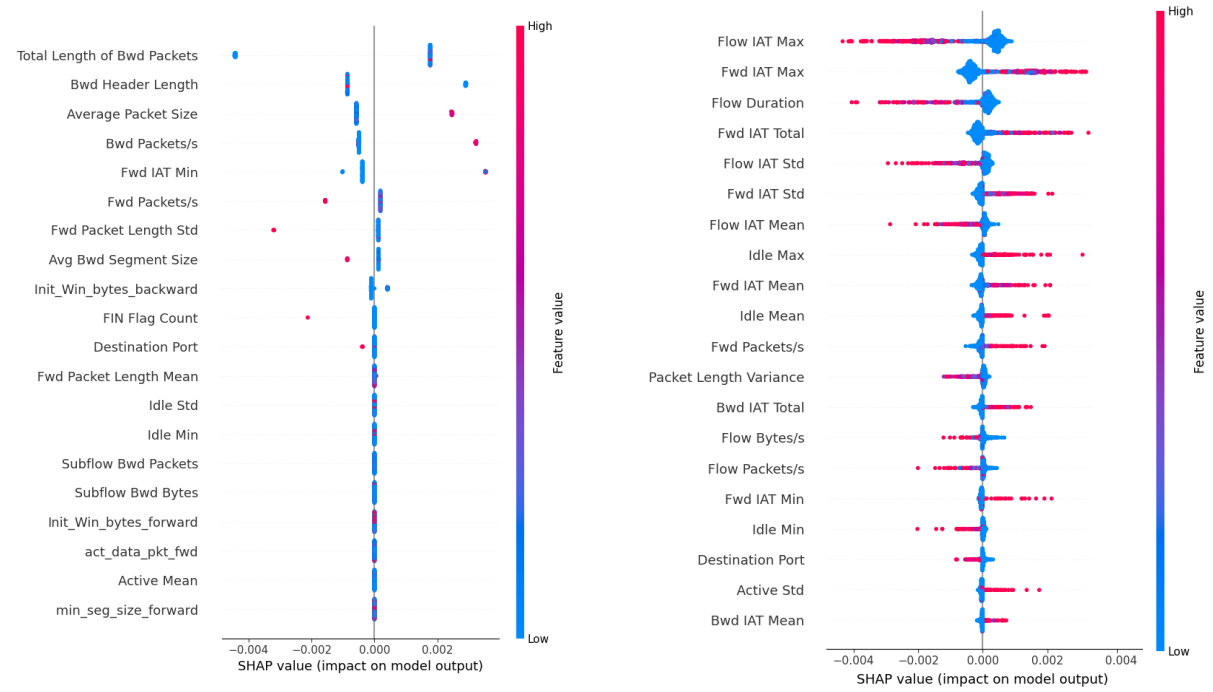
EPOA-GB



EPOA-DT



EPOA-XGB



EPOA-AB EPOA-KNN

Figure 10: SHAP summary of input features' impact on the employed hybrid models' output.

4 Conclusion

In order to improve the efficiency of Intrusion Detection Systems (IDSs) in differentiating between malicious and benign network activity, this study provided a thorough evaluation of a number of ML classifiers. One of the main contributions is the use of sophisticated hyperparameter optimization methods, specifically the Emperor Penguin Optimization Algorithm (EPOA) and Grid Search (GS), to improve the predictive performance of six selected classifiers: Random Forest (RF), Gradient Boosting (GB), Decision Tree (DT), XGBoost (XGB), AdaBoost (AB), and K-Nearest Neighbors (KNN). With the highest testing accuracy, precision, recall, and F1-score values of 0.9997, 0.9898, 0.9999, and 0.9948, respectively, the optimized models—EPOA-GB in particular—showed exceptional classification abilities. SHAP-based feature importance analysis was carried out to promote model transparency by identifying crucial network attributes affecting classification and providing interpretability into the decision-making process. These insights can help cybersecurity experts improve monitoring rules and prioritization strategies by revealing which traffic features are most suggestive of threats.

Practically speaking, the results highlight how effective it is to combine intelligent optimization with powerful ensemble classifiers to enhance detection performance while reducing false alarms, which is an essential prerequisite for real-time intrusion response systems. Additionally, the application of PCA for dimensionality reduction enhanced the approach's scalability by improving generalization and lowering computational load.

It is necessary to recognize a few limitations, though. First, the evaluation was limited to a single dataset, which might not fully represent the variety of contemporary or developing cyberattack techniques, even though there was strong within-dataset generalization. Second, real-world traffic frequently contains previously unseen anomalies that could test the robustness of the model, even though retraining and testing on unseen splits were done to evaluate generalizability. Third, even though EPOA works well, it has a significant computational overhead during training, which might restrict its direct use in environments with limited resources or real-time deployment.

Future studies should validate the suggested models on more benchmark datasets, like UNSW-NB15 and TON_IoT, to evaluate their resilience across a range of network conditions and attack types in order to overcome these drawbacks and facilitate real-world implementation. To lessen latency and computational load during live deployment, integration with edge computing environments, real-time streaming frameworks, and lightweight optimization techniques is also advised. Moreover, hybrid models that combine evolutionary optimization and deep learning can be investigated to capture intricate attack behaviors while preserving flexibility.

In conclusion, this study demonstrates that combining strong ML models with sophisticated optimization can greatly improve IDS performance. Continuous evaluation in dynamic and heterogeneous environments is crucial for practical adoption, as are attempts to strike a balance between model accuracy, interpretability, and efficiency for cybersecurity applications in the real world.

Acknowledgement

This Work was supported by the Hubei Provincial Education and Science Planning Project. (2018GB081)

References

[1] T. H. Chua and I. Salam, "Evaluation of Machine Learning Algorithms in Network-Based Intrusion Detection Using Progressive Dataset," *Symmetry (Basel)*, MDPI, vol. 15, no. 6, Jun. 2023, https://doi.org/10.3390/sym15061251.

[2] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of network and computer applications*, Elsevier, vol. 36, no. 1, pp. 16–24, 2013, https://doi.org/10.1016/j.jnca.2012.09.004.

[3] R. A. Ramadan and K. Yadav, "A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks," *Annals of Emerging Technologies in Computing (AETiC)*, AETIC, vol. 4, no. 5, pp. 61–74, 2020, DOI: 10.33166/AETiC.2020.05.004.

[4] A. H. Azizan *et al.*, "A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems," *Annals of Emerging Technologies in Computing*, AETIC, vol. 5, no. 5, pp. 201–208, Mar. 2021, doi: 10.33166/AETiC.2021.05.025.

[5] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," *International Journal of Electrical and Computer Engineering*, Academia, vol. 13, no. 1, pp. 1134–1141, Feb. 2023, DOI: 10.11591/ijece.v13i1.pp1134-1141.

[6] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, pp. 1–27, 2021, DOI: 10.11591/ijece.v13i1.pp1134-1141.

[7] M. A. Khan, M. R. Karim, and Y. Kim, "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network," *Symmetry (Basel)*, MDPI, vol. 11, no. 4, p. 583, 2019, https://doi.org/10.3390/sym11040583.

[8] M. Sarnovsky and J. Paralic, "Hierarchical intrusion detection using machine learning and knowledge model," *Symmetry (Basel)*, MDPI, vol. 12, no. 2, p. 203, 2020, https://doi.org/10.3390/sym12020203.

[9] C. Wang, Y. Sun, W. Wang, H. Liu, and B. Wang, "Hybrid intrusion detection system based on combination of random forest and autoencoder," *Symmetry (Basel)*, MDPI, vol. 15, no. 3, p. 568, 2023, https://doi.org/10.3390/sym15030568.

[10] F. Hossain, M. Akter, and M. N. Uddin, "Cyber attack detection model (CADM) based on machine learning approach," in *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, DHAKA, Bangladesh, IEEE, 2021, pp. 567–572, https://doi.org/10.1109/ICREST51555.2021.9331094.

[11] O. Malkawi, N. Obaid, and W. Almobaideen, "Intrusion Detection System for 5G Device-to-Device Communication Technology in Internet of Things," *Informatica*, Slovenian Society Informatika, vol. 48, no. 15, 2024, https://doi.org/10.31449/inf.v48i15.4646.

[12] S. Ahmad, F. Arif, Z. Zabeehullah, and N. Iltaf, "Novel approach using deep learning for intrusion detection and classification of the network traffic," in *2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, Tunis, Tunisia, IEEE, 2020, pp. 1–6, https://doi.org/10.1109/CIVEMSA48639.2020.9132744.

[13] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, Elsevier, vol. 188, p. 107840, 2021, https://doi.org/10.1016/j.comnet.2021.107840.

[14] A. Ali *et al.*, "Network intrusion detection leveraging machine learning and feature selection," in *HONET 2020 - IEEE 17th International Conference on Smart Communities: Improving Quality of Life using ICT, IoT and AI*, Institute of Electrical and Electronics Engineers Inc., Charlotte, NC, USA, IEEE, Dec. 2020, pp. 49–53, https://doi.org/10.1109/HONET50430.2020.9322813.

[15] D. Stiawan, M. Y. Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 dataset feature analysis with information gain for anomaly detection," *IEEE Access*, IEEE, vol. 8, pp. 132911–132921, 2020, https://doi.org/10.1109/ACCESS.2020.3009843.

[16] A. Bansal and S. Kaur, "Extreme gradient boosting based tuning for classification in intrusion detection systems," in *Advances in Computing and Data Sciences: Second International Conference, ICACDS 2018, Dehradun, India, April 20-21, 2018, Revised Selected Papers, Part I 2*, Singapore, Springer, 2018, pp. 372–380, https://doi.org/10.1007/978-981-13-1810-8_37.

[17] I. A. Abdulmajeed and I. M. Husien, "MLIDS22-IDS design by applying hybrid CNN-lstm model on mixed-datasets," *Informatica*, Slovenian Society Informatika, vol. 46, no. 8, 2022, https://doi.org/10.31449/inf.v46i8.4348.

[18] M. Guo, D. Ma, F. Jing, X. Zhang, and H. Liu, "Dynamic Anti-Mapping Network Security Using Hidden Markov Models and LSTM Networks Against Illegal Scanning," *Informatica*, Slovenian

Society Informatika, vol. 49, no. 12, 2025, https://doi.org/10.31449/inf.v49i12.6903.

[19] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization.," *ICISSp*, Scite Press, vol. 1, pp. 108–116, 2018, DOI: 10.5220/0006639801080116.

[20] L. Breiman, "Random forests," *Mach Learn*, Springer, vol. 45, pp. 5–32, 2001, https://doi.org/10.1023/A:1010933404324.

[21] A. Cutler, D. R. Cutler, and J. R. Stevens, "Random Forests," in *Ensemble Machine Learning*, New York, NY: Springer New York, 2012, pp. 157–175, https://doi.org/10.1007/978-1-4419-9326-7_5.

[22] Y. Shi, V. Charles, and J. Zhu, "Bank financial sustainability evaluation: Data envelopment analysis with random forest and Shapley additive explanations," *Eur J Oper Res*, Elsevier, vol. 321, no. 2, pp. 614–630, 2025, https://doi.org/10.1016/j.ejor.2024.09.030.

[23] J. H. Friedman, "999 REITZ LECTURE GREEDY FUNCTION APPROXIMATION: A GRADIENT BOOSTING MACHINE 1," 2001, https://www.jstor.org/stable/2699986.

[24] A. Natekin and A. Knoll, "Gradient boosting machines, a tutorial," *Front Neurorobot*, Frontiers, vol. 7, no. DEC, 2013, https://doi.org/10.3389/fnbot.2013.00021.

[25] B. Charbuty and A. Abdulazeez, "Classification Based on Decision Tree Algorithm for Machine Learning," *Journal of Applied Science and Technology Trends*, jastt, vol. 2, no. 01, pp. 20–28, Mar. 2021, https://doi.org/10.38094/jastt20165.

[26] R. Oktafiani, A. Hermawan, and D. Avianto, "Max Depth Impact on Heart Disease Classification: Decision Tree and Random Forest," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, Journal IAII, vol. 8, no. 1, pp. 160–168, 2024, https://doi.org/10.29207/resti.v8i1.5574.

[27] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, ACM Digital Library, 2016, pp. 785–794, https://doi.org/10.1145/2939672.2939785.

[28] A. Sharma and R. Tiwari, "Anomaly detection in smart grid using optimized extreme gradient boosting with SCADA system," *Electric Power Systems Research*, Elsevier, vol. 235, p. 110876, 2024, https://doi.org/10.1016/j.epsr.2024.110876.

[29] C. Lee and E. D. C. Maceren, "Wind energy system fault classification and detection using deep convolutional neural network and particle swarm optimization-extreme gradient boosting," *IET Energy Systems Integration*, Wiley Online Library, vol. 6, no. 4, pp. 479–497, 2024, https://doi.org/10.1049/esi2.12144.

[30] Y. Freund and R. E. Schapire, "Journal of Computer and System Sciences s SS1504 journal of computer and system sciences," 1997.

[31] L. Wen, Y. Li, W. Zhao, W. Cao, and H. Zhang, "Predicting the deformation behaviour of concrete face rockfill dams by combining support vector machine and AdaBoost ensemble algorithm," *Comput Geotech*, Elsevier, vol. 161, Sep. 2023, https://doi.org/10.1016/j.compgeo.2023.105611.

[32] L. Wang, Y. Guo, M. Fan, and X. Li, "Wind speed prediction using measurements from neighboring locations and combining the extreme learning machine and the AdaBoost algorithm," *Energy Reports*, Elsevier, vol. 8, pp. 1508–1518, Nov. 2022, https://doi.org/10.1016/j.egyr.2021.12.062.

[33] E. Fix, *Discriminatory analysis: nonparametric discrimination, consistency properties*, vol. 1. USAF school of Aviation Medicine, 1985.

[34] P. Cunningham and S. J. Delany, "K-Nearest Neighbour Classifiers-A Tutorial," Jul. 31, 2021, *Association for Computing Machinery*, Cornell University, https://doi.org/10.48550/arXiv.2004.04523.

[35] R. K. Halder, M. N. Uddin, Md. A. Uddin, S. Aryal, and A. Khraisat, "Enhancing K-nearest neighbor algorithm: a comprehensive review and performance analysis of modifications," *J Big Data*, Springer, vol. 11, no. 1, p. 113, 2024, https://doi.org/10.1186/s40537-024-00973-y.

[36] G. Dhiman and V. Kumar, "Emperor penguin optimizer: A bio-inspired algorithm for engineering problems," *Knowl Based Syst*, Elsevier, vol. 159, pp. 20–50, Nov. 2018, https://doi.org/10.1016/j.knosys.2018.06.001.

[37] O. W. Khalid, N. A. M. Isa, and H. A. Mat Sakim, "Emperor penguin optimizer: A comprehensive review based on state-of-the-art meta-heuristic algorithms," Feb. 01, 2023, *Elsevier B.V.* https://doi.org/10.1016/j.aej.2022.08.013.

Joint Optimization of 5.5G Cellular Networks Using Ray Tracing and PSO-MDE for Antenna Configuration and Power Allocation

Chunbing Jian[1], Fan Gong[2*]
[1]School of Communication and Information Engineering, Shanghai Technical Institute of Electronics & Information Shanghai 201411, China
[2]Research and Development Department, Kingsignal Technology Co., Ltd, Shenzhen 518063, China
E-mail: fangong7401@163.com
[*]Corresponding author

Keywords: 5.5G network, network coverage, ray tracing algorithm, PSO algorithm, pareto front

Received: April 29, 2025

In the continuous evolution of mobile communication technology, 5.5G network is a key step towards future communication, which is gradually becoming the focus of academia and industry. To solve the complex signal propagation and serious multi-path interference in high frequency band, the improved particle swarm differential evolution algorithm and multi-objective differential evolution particle swarm optimization algorithm are proposed to maximum coverage and minimum power consumption in wireless sensor networks. This method improves the efficiency of solving complex optimization problems by maintaining the global search ability and enhancing the local search performance. The experiment was carried out on a customized simulation platform and tested for different scale sensor deployment scenarios. The research results indicated that the optimal coverage after optimizing the parameters of the community antenna occurred when the inertia factor was 0.4 and 0.7, at 0.641 and 0.640, respectively. The average optimal coverage was 0.633 and 0.632 when the inertia factor was 0.6 and 0.7, respectively. The designed algorithm performed the best in reducing transmission power, computational efficiency, and exploring solution space. The minimum total transmission power reached 33.5dBm, the maximum number of Pareto front points reached 240, and the calculation time was the shortest, at 530s. The research results show that the proposed optimization algorithm can effectively improve the coverage and energy efficiency of the 5.5G network, providing an effective solution for network optimization.

Povzetek: Predstavljena je skupna optimizacija 5.5G kot RT modeliranje + PSO-MDE za azimut/nagib anten in MOPSO-DE za oddajno moč. Rezultati: večja pokritost, nižja moč, hitrejša konvergenca, več Pareto rešitev, boljša energetska učinkovitost.

1 Introduction

With the continuous advancement of mobile communication technology, the world is rapidly transitioning to fifth generation mobile communication technology. The 5.5G network provides strong support for emerging technologies such as the Internet of Things, augmented reality, and virtual reality with its higher data transmission rate, lower latency, and wider connectivity capabilities [1-2]. However, the high-frequency communication characteristics and ultra-dense deployment requirements of 5.5G networks also make the wireless signal propagation environment more complex, posing new challenges to network coverage and energy efficiency [3]. Traditional optimization algorithms are prone to getting stuck in local optima and have slow convergence speed under high-dimensional search spaces and nonlinear constraints, making it difficult to meet the high real-time and performance requirements of 5.5G [4]. The Ray Tracing (RT) algorithm can simulate the propagation path of electromagnetic waves, and accurately characterize the channel characteristics in high-frequency communication environments. It is suitable for 5.5G network modeling and performance optimization. Particle Swarm Optimization (PSO) is a stochastic optimization method based on swarm intelligence, which has fast convergence speed and simple implementation [5-6]. The Differential Evolution (DE) strategy is a population-based stochastic optimization algorithm mainly used to solve continuous optimization problems. Therefore, the study adopts the RT algorithm for channel modeling to quantitatively evaluate network performance. An optimized PSO algorithm that combines Metropolis criterion and DE (PSO-MDE) is proposed to optimize antenna parameters. The Multi-objective PSO based on DE (MOPSO-DE) is taken to optimize the signal transmission power to improve the performance of the 5.5 network by increasing the signal propagation rate and reducing energy consumption management.

The innovation of the research lies in improving the traditional PSO algorithm, which enhances the algorithm's global search and local fine adjustment

capabilities. In addition, a crowding distance algorithm is introduced to maintain the diversity of the solution set. Compared with traditional optimization methods, the contribution of the research is to propose a joint optimization framework combining RT modeling and PSO-MDE algorithm, which can simultaneously optimize the antenna direction parameters and transmission power allocation strategy of the base station in the community. The adaptive evolution mechanism is introduced to improve the convergence speed and search accuracy in complex scenarios. Simulation experiments based on synthetic urban environment verify that the proposed method is significantly superior to the mainstream algorithm in coverage and interference control.

To systematically verify the effectiveness of the proposed method, the research aims to clearly explore whether the proposed improved algorithm is superior to the current mainstream optimization algorithm in the statistical sense in the 5.5G cellular network under the same number of nodes and deployment constraints, and evaluate its performance in energy management, especially its potential in reducing transmission power and improving energy efficiency. Therefore, two research hypotheses are proposed. One is that PSO-MDE algorithm will achieve higher network coverage than JADE and ABC algorithm. The second assumption is that PSO-MDE algorithm is better than JADE and ABC algorithm in reducing the total transmission power and improving energy efficiency. To verify these assumptions, the research compares the performance of different algorithms in coverage and energy management through simulation experiments, and uses statistical methods to evaluate whether the performance improvement of PSO-MDE algorithm is statistically significant.

The research will be divided into the following five sections. Section 1 introduces the relevant background and existing research. Section 2 describes the proposed joint optimization method. Section 3 presents the experimental results and performance analysis. Section 4 discusses the results and compares them with recent studies. Section 5 summarizes the full text and looks forward to future work.

2 Related works

The rapid development of wireless communication technology has made network performance optimization increasingly important. Mao et al. proposed a damage assessment method based on convolutional neural networks from components to the overall structure to address the post-earthquake damage assessment needs of reinforced concrete communication buildings. The research results indicated that the proposed method was highly consistent with the expert evaluation conclusions, and the optimized convolutional neural network had good accuracy and stability [7]. Yu et al. proposed a system optimization method based on Reconfigurable Intelligent Surfaces (RIS) to achieve ultra-wireless bandwidth, ultra large-scale connectivity, and highly reliable communication in 6G communication networks. By reviewing relevant research literature in recent years, the performance optimization of RIS assisted wireless communication networks was summarized and the potential future research direction for RIS assisted communication network deployment was explored [8]. Liang et al. proposed a traffic control scheduling generation method for train communication networks based on improved incremental scheduling strategy and improved grey wolf optimization algorithm to meet the high transmission demand of massive real-time data in intelligent rail transit. The research results indicated that this method had advantages in computational accuracy and speed, and could reduce the average end-to-end delay to 57 μs [9]. Yu et al. proposed a joint cross-layer optimization framework to address the deep learning semantic encoding and decoding exacerbating traditional communication energy consumption. The research results indicated that the framework could effectively solve the joint optimization problem of semantic and physical layers by jointly optimizing physical layer power control and semantic layer compression allocation [10].

Network optimization often involves multiple objectives, such as coverage, capacity, energy efficiency, and cost. The PSO algorithm, especially its multi-objective version, can effectively handle these multi-objective optimization problems and find the optimal solution that balances different objectives. Hu et al. proposed an intelligent deployment method for emergency ground to air communication networks based on a hybrid layered PSO algorithm to effectively respond to the transmission of emergency monitoring data during large-scale environmental emergencies. The research results indicated that this method could adaptively update the deployment location and communication link of emergency communication resources, significantly improve adaptability after multiple iterations, and achieve comprehensive coverage and balanced distribution of communication nodes [11]. Wang et al. proposed a multi-objective PSO algorithm to solve the time-consuming and inefficient design of traditional terahertz metamaterial absorbers. The research results indicated that this method could achieve dual objective optimization of absorber structural parameters with absorption rate and quality factor as independent objectives, significantly improving design efficiency and performance [12]. Nuthakki et al. proposed an AI driven method using an improved multi-objective PSO algorithm to achieve high resource utilization in cloud data centers in intelligent manufacturing environments. The research results indicated that this method outperformed other multi-objective algorithms in optimizing resource allocation in intelligent manufacturing cloud environments [13].

To sum up, the existing methods may perform well in specific environments, but the generalization ability and adaptability need to be improved, and some algorithms have high computational complexity. The trade-offs and balances between different objectives still need to be further analyzed. Table 1 compares the

application environment, key results, research gaps, and SOTA drawbacks of each network optimization method. Therefore, the research combines RT algorithm to optimize the 5.5G network, and introduces de-mutation and crossover operation to improve the traditional PSO algorithm, aiming to improve the adaptability, real-time performance and optimization efficiency of the algorithm, so as to better meet the challenges of network optimization in large-scale and complex environments.

Table 1: Comparison of research results of various network optimization methods.

Reference	Algorithm	Application environment	Key results	Limitations of SOTA
[7] Mao C X et al.	Convolutional neural network	Post-earthquake damage evaluation of RC frame communication buildings	High consistency with expert assessment; optimized CNN model shows good accuracy and stability	Lack of verification of algorithm generalization capability
[8] Yu W W et al.	RIS auxiliary network optimization	6G communication networks	Enhances communication performance	High computational complexity; lacks real-time capability
[9] Liang C et al.	Improved grey wolf optimization algorithm	Train communication networks in intelligent rail transit	Reduces average end-to-end latency to 57μs	Algorithm adaptability needs improvement
[10] Yu K W et al.	Joint cross-layer optimization framework	Communication energy consumption in deep learning semantic encoding and decoding	Effectively addresses the joint optimization issue of semantic and physical layers	Further research focuses on trade-offs between different objectives
[11] Hu W Z et al.	Hybrid hierarchical PSO algorithm	Intelligent deployment of emergency aerial-ground communication networks under large-scale sudden environmental events	Significantly improves fitness after multiple iterations; achieves comprehensive coverage and balanced distribution of communication nodes	Performs well in specific environments but lacks generalization capability
[12] Wang Y R et al.	MPSO	Design of terahertz metamaterial absorbers	Achieves dual-objective optimization of absorber structure parameters, significantly improving design efficiency and performance	Lacks universal solutions for broader scenarios
[13] Nuthakki P et al.	Improved MPSO	Resource allocation in cloud data centers for smart manufacturing	Outperforms other multi-objective algorithms in optimizing resource allocation in smart manufacturing cloud environments	The computational complexity and real-time capability of the algorithm need further optimization

3 Methods and materials

3.1 Optimization of antenna parameters for 5.5G network in community based on RT and improved PSO-MDE algorithm

Signal propagation and energy management are two key dimensions in 5.5G network optimization. Signal propagation can improve signal coverage quality and reduce interference by optimizing antenna parameters, while energy management can reduce energy consumption by optimizing transmission power [14-15]. Therefore, a sequential linkage two-stage optimization framework is proposed to improve the configuration efficiency of antenna parameters and transmission power in 5.5G cellular network. In this framework, PSO-MDE is first used to optimize the antenna azimuth and tilt angle of each sector to maximize the signal coverage in the cell. Then, taking the obtained antenna parameters as input, MOPSO-DE is used to further optimize the transmission power of each sector, while considering minimizing power overhead and maximizing overall coverage. This two-stage strategy decouples the complex search space and avoids the convergence difficulty in high-dimensional joint optimization. The dependent path is clear, and the subsequent power optimization stage is directly affected by the antenna parameters in the early stage. It also has strong scalability. Firstly, a cellular network structure is constructed to visually demonstrate the spatial layout relationship between typical cell division and base station antennas. The cellular network structure is shown in Figure 1.

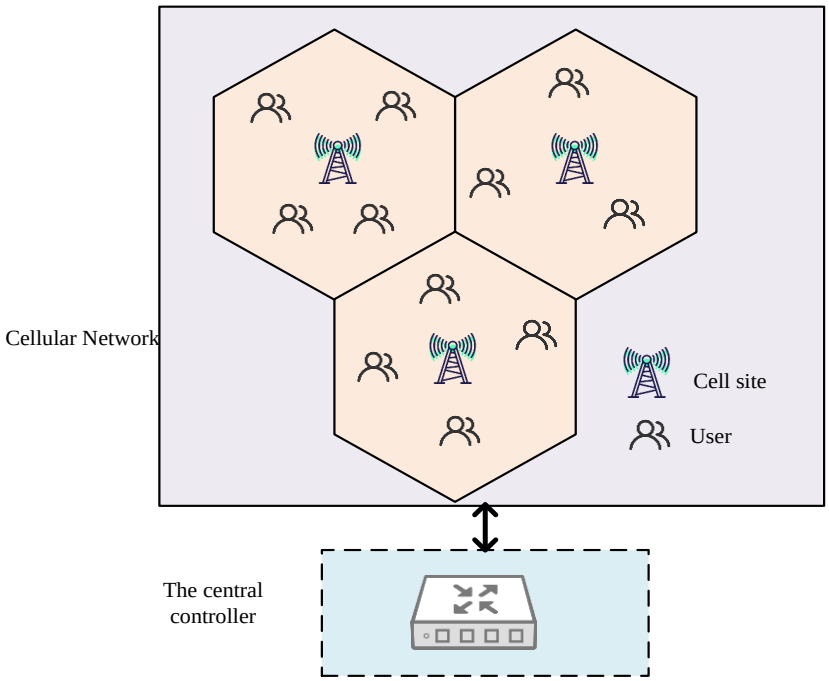
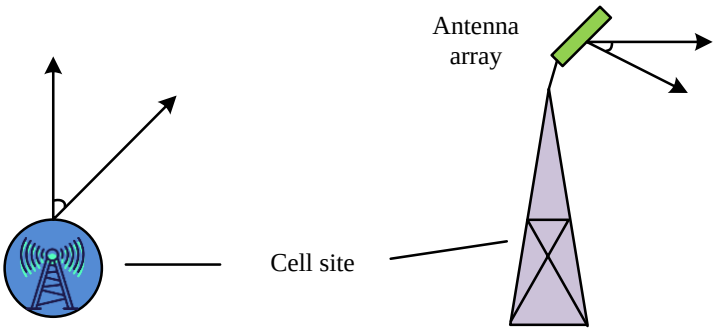


Figure 1: Schematic diagram of cellular network structure and base station layout.



(a) Schematic diagram of antenna azimuth angle

(b) Schematic diagram of antenna tilt angle

Figure 2: Schematic diagram of antenna azimuth angle and tilt angle.

As shown in Figure 1, a cellular network consists of multiple base stations, each responsible for covering one or more sectors, forming a hexagonal structure similar to a honeycomb. Each antenna of the three-sector base station is responsible for covering an area within 120°, and the antenna can independently set its direction and tilt angle. In this structure, antenna parameters directly determine the direction and intensity distribution of signal radiation. Reasonable configuration can effectively expand the effective coverage area, and reduce blind spots and overlapping interference [16]. In this cellular structure, each sector is considered as an independent optimization unit, and the antenna parameters of all 21 sectors are jointly optimized. Therefore, the optimization problem has a high-dimensional search space with 42-dimensional continuous variables. The optimization goal is to maximize the overall coverage performance and signal power distribution quality in the region by adjusting the antenna azimuth and tilt angle of all sectors under the fixed network topology and deployment architecture. This study refers to the areas where communities serve each department, rather than macro level residential areas. The designed dual-objective fitness function is based on the proportion of users who meet the signal strength threshold (coverage) and the average received power level in the whole simulation area. To ensure the authenticity and challenge of the modeling, this study did not make assumptions about simplifying sector deployment strategies, nor did it incorporate sector or shared antenna parameters. However, it retains a completely independent antenna configuration, making the optimization task closer to the requirements of real cellular network configuration. The azimuth and tilt angle parameters of the antenna are two key control

parameters for the community antenna, as shown in Figure 2.

As shown in Figure 2, the horizontal direction of the main beam of the azimuth antenna controls the angle range of signal coverage, usually from 0° to 360°. The vertical pitch angle of the tilt angle controls the degree of tilt of the main lobe of the signal, usually set between 0° and 15°. If the beam is too small, it will move towards the far end, which may cause cross zone interference. If it is too large, the signal will be concentrated in the near end, resulting in poor reception for remote users [17]. In the 5.5G high-frequency communication environment, to more accurately capture the propagation path and loss law of signals in complex environments, the RT algorithm is used for channel modeling to quantitatively evaluate the coverage performance of cellular networks. The RT method accurately models the signal propagation characteristics by simulating the reflection, diffraction, and penetration paths of radio waves in real environments. The total channel loss is shown in equation (1).

$$L(d) = L_0 + 10n\log_{10}(d) + \sum_{j=1}^{M} L_{rj} \quad (1)$$

In equation (1), L_0 represents the free space path loss. n represents the path loss index, which is set according to specific scenarios. S represents the transmission distance. L_{rj} represents the additional loss caused by the j -th reflection or diffraction. M represents the total number of multi-path components. The antenna parameter optimization is to maximize the coverage within the area. The received power at each user's location is shown in equation (2).

$$P_{r,i} = P_t + G(\theta_i, \phi_i) - L(d_i) \quad (2)$$

In equation (2), $P_{r,i}$ is the received power of the i -th receiving point. P_t is the power of the transmitted signal. $G(\theta_i, \phi_i)$ represents the gain function. θ_i represents the angle with the receiving point. ϕ_i represents the relevant antenna gain. $L(d_i)$ is the path loss. The grid-based evaluation method can divide the research area into several equally spaced small grids, calculate and statistically analyze the received signal strength of each grid point, and evaluate the overall coverage performance. Coverage refers to the proportion of areas in which the received signal strength indicator (RSSI) exceeds a preset threshold in a specific area. It reflects the signal coverage quality of the network in the region. To accurately evaluate the coverage, the RSSI threshold and analysis window are defined. The RSSI threshold is set to -90dbm. Only when the RSSI value is higher than this threshold, the area is considered to be effectively covered. The analysis window is defined as a meshed area, and each grid point represents a measurement point. The coverage is determined by calculating the RSSI value of each grid point and determining whether it exceeds the threshold. It is commonly used for signal coverage analysis and optimization in wireless networks. The coverage rate of the community is shown in equation (3).

$$\eta_{\text{cov}} = \frac{\sum_{i=1}^{N} \delta(P_{r,i} \geq P_{\text{th}})}{N} \quad (3)$$

In equation (3), η_{cov} is the coverage probability, representing the probability that the received power is greater than a certain threshold P_{th} . δ is an indicator function ranging from 0 to 1. N is the total number of grids. This method can accurately evaluate the coverage performance of the network and use it as the objective function for optimization. Further research will encode the antenna azimuth and tilt angle of each community as variables to form a "particle" in the particle swarm. Taking the total coverage within the region as the fitness function, the optimal combination of antenna parameters is obtained. The optimization objective function for maximizing coverage is shown in equation (4).

$$F = \max_{\phi_i, \theta_i} \eta_{\text{cov}}(\phi_i, \theta_i) \quad (4)$$

In equation (4), F is the optimized objective function. (ϕ_i, θ_i) represents the azimuth and elevation angles of the i -th receiving point. The parameter modeling is completed. Coverage optimization has nonlinear and multi peak characteristics, while PSO still suffers from premature convergence in high-dimensional complex spaces. Therefore, the DE is introduced to improve the PSO algorithm. DE can generate new solutions by mutating and recombining individual differences, and has strong global search capabilities. In addition, the research also introduces the Metropolis criterion and adaptive inertia factor to enhance the ability to escape from local optima, balancing global exploration and local development. The specific process of PSO-MDE algorithm is shown in Figure 3.

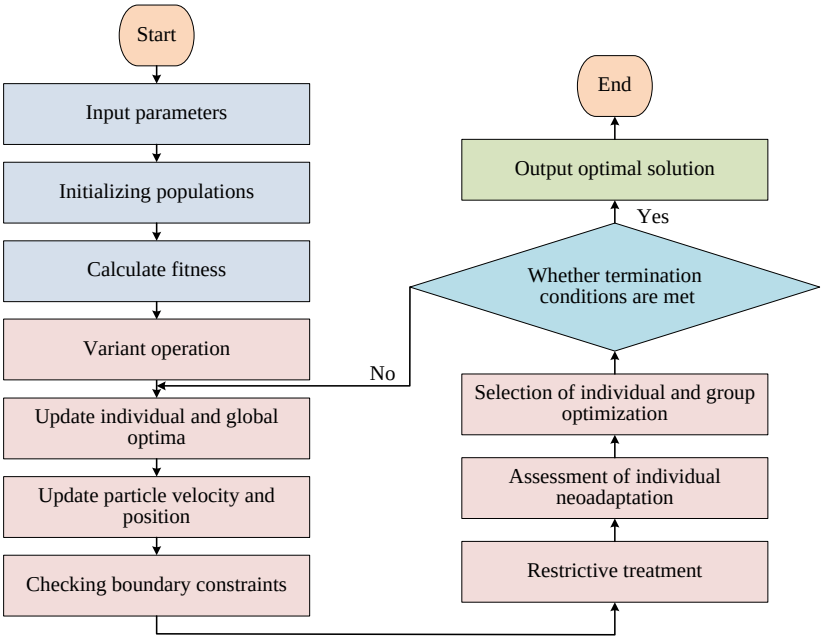


Figure 3: Flow chart of PSO-MDE algorithm.

From Figure 3, firstly, the position, velocity, and fitness values of the particle swarm are initialized, and the inertia factor is set. In each iteration, particles move according to velocity and position update equations. The adaptive inertia factor dynamically adjusts according to the iteration process to achieve a balance from global search to local fine search. The particle velocity and position updates combine the velocity update mechanism of PSO with the mutation crossover operation of DE. Specifically, the velocity update of particles follows the velocity update equation of the standard particle swarm algorithm, and introduces adaptive inertia weights to dynamically adjust the motion trend of particles. This process ensures that particles can search effectively according to the individual optimal position and the global optimal position. The variant operation is part of the PSO update cycle and directly participates in updating particle positions rather than being independent of the main cycle. The specific calculation is shown in equation (5).

$$\omega = \omega_{\min} + (\omega_{\max} - \omega_{\min}) \exp\left(-\lambda \left(\frac{k}{k_{\max}} \right) \right) \tag{5}$$

In equation (5), ω is the current inertia factor. k is the number of iterations. λ is a parameter that controls the inertia factor to reduce speed. In the location update phase, mutation and crossover operations of DE are introduced to enhance the diversity and global search ability of the population. Specifically, for each particle, firstly, the mutation operation of DE is performed, selecting three different particles and calculating their difference vectors, and then adding them to the current position of the particles to generate a new mutation vector. Then, the DE crossover operation is performed, and some components of the mutation vector are replaced with a certain probability at the current particle position to generate a test vector. This test vector is then used to evaluate its fitness. If the fitness is better than the current particle position, the particle position is updated. In this way, DE mutation and crossover operation provide new candidate solutions for PSO and increase the diversity of the population. In this way, PSO-MDE combines the fast convergence characteristics of PSO and the global search ability of DE to improve the optimization performance. If the newly generated particles are better than the current solution, they will be updated directly. If it is inferior to the current solution, it is accepted with a certain probability according to the Metropolis criterion to avoid falling into local optima. During the iteration process, the individual extremum and global optimal solution are continuously updated until the termination condition is met. The pseudo-code of PSO-MDE algorithm is shown in Figure 4.

```
// Initialize parameters
Set population size N, maximum number of iterations T, inertia weight ω, cognitive component c1, social component c2
Set differential evolution scaling factor λ, crossover probability CR

// Initialize the swarm
For i = 1 to N:
   Randomly initialize particle position position[i] and velocity velocity[i]
   Evaluate fitness fitness[i]
   If fitness[i] is better than personal best pbest[i]:
      Update pbest[i] = position[i]
   If fitness[i] is better than global best gbest:
      Update gbest = position[i]

// Start iterations
For t = 1 to T:
   For i = 1 to N:
      // Differential Evolution Mutation
      Randomly select j, k, l ≠ i from {1, 2, ..., N}
      Calculate mutation vector mutant = pbest[i] + λ * (position[j] - position[k]) + (position[l] - position[j])

      // Differential Evolution Crossover
      Create trial vector trial = position[i]
      For each dimension d = 1 to D:
         If rand() < CR or d = randomly chosen dimension:
            Set trial[d] = mutant[d]

      // Evaluate trial vector fitness fitness[trial]
      If fitness[trial] is better than fitness[i]:
         Update position[i] = trial

      // PSO velocity and position update
      Update velocity[i] = ω * velocity[i] + c1 * rand() * (pbest[i] - position[i]) + c2 * rand() * (gbest - position[i])
      Update position[i] = position[i] + velocity[i]

   // Update global best
   For i = 1 to N:
      If fitness[i] is better than gbest:
         Update gbest = position[i]

// Output results
Return global best solution gbest
```

Figure 4: Pseudo-code of PSO-MDE algorithm.

From Figure 4, in pseudo-code, key symbol or variable mutation represents mutation operation, crossover represents crossover operation, and CR represents crossover probability in DE. PSO-MDE algorithm combines the advantages of PSO and DE, and enhances the global search ability of PSO by introducing DE mutation and crossover operation. In the initialization phase of the algorithm, the position and speed of the particle swarm are randomly generated, and the fitness is evaluated. In the iteration process, the DE strategy is used to update the particle velocity, and the parameters such as mutation factor and crossover probability are automatically adjusted to meet the needs of different search stages. This improved strategy helps the particles jump out of the local optimum, improves the diversity of solutions, and speeds up the convergence speed. Finally, PSO-MDE algorithm shows better performance in multi-objective optimization problems and has wide application potential.

3.2 Power allocation optimization based on MOPSO-DE

To ensure the feasibility and robustness of the optimization process, the series optimization architecture is adopted. In phase 1, the fixed initial transmission power is analyzed, and the antenna azimuth and tilt angle of the sector are optimized by PSO-MDE. On this basis, in phase 2, MOPSO-DE is used to further refine and optimize the transmission power of each sector. The output of antenna angle is directly used as the input environment variable in the power optimization phase rather than sharing variable parameters to ensure the consistency of physical configuration. Next, the study optimizes the energy consumption of the 5.5G network. Due to the uneven spatial distribution of business demands in complex urban environments, it is necessary to allocate transmission power reasonably to ensure network coverage and energy efficiency. Therefore, the study selects maximum coverage and minimum total transmission power as optimization objectives to construct a multi-objective optimization model [18-19]. MOPSO has good global search capability when dealing with multi-objective problems. However, it has shortcomings in maintaining population diversity and improving local accuracy [20]. Therefore, to optimize the signal transmission power in residential areas, the research has also adopted DE to improve MOPSO. The MOPSO-DE process is shown in Figure 5.

From Figure 5, first, the individual particle swarm is initialized. Each particle represents a cell transmission power combination. The initialization process includes initializing the position and speed of the particle swarm. The initial position of each particle is set to its initial personal optimal value. In this way, the algorithm can provide a reasonable starting point for each particle in the initial stage, so as to improve the optimization efficiency. Secondly, the fitness of individuals under the two objectives of "maximizing regional coverage" and "minimizing total transmission power" is calculated through the objective function. All non-dominated solutions will enter the external elite pool and use crowding distance sorting to maintain the diversity of the solution set. During the iteration process, particles update by guiding individuals to learn the historical optimal position and performing differential mutation operations. The updated velocity is shown in equation (6).

$$v_e = x_{r1} + u \cdot (x_{r2} - x_{r3}) \tag{6}$$

In equation (6), v_e is the variation vector of the e-th particle. x_{r1}, x_{r2}, and x_{r3} are the current position vectors of three different particles randomly selected from the current population. u is the differential variation scaling factor. The specific calculation of its position is shown in equation (7).

$$x_e^{t+1} = x_e^t + v_e \tag{7}$$

In equation (7), x_e^{t+1} and x_e^t are the current position vectors of the e-th particle in the $t+1$-th and t-th generations, respectively. v_e is the velocity vector obtained through differential variation. The pseudo-code of MOPSO-DE algorithm is shown in Figure 6.

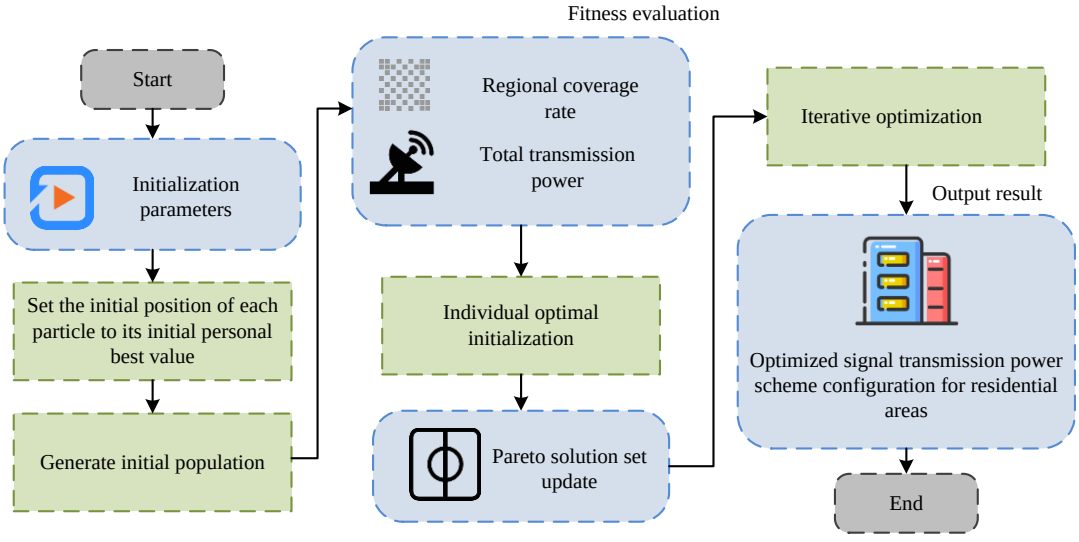


Figure 5: Optimization of signal transmission power in community based on MOPSO-DE algorithm.

```
// Initialize the parameters
Set the number of particles N, maximum iterations T, mutation factor F, crossover probability CR
Initialize the position and velocity of each particle randomly

// Initialize the archive with the initial particles
for each particle i from 1 to N do
   Evaluate the fitness of particle i
   if particle i is non-dominated then
      Add particle i to the archive
   end if
end for

// Main loop
for iteration from 1 to T do
   for each particle i from 1 to N do
      // Differential Evolution Mutation
      Choose three distinct particles j, k, l different from i
      V = particle[j] + F * (particle[k] - particle[l])

      // Differential Evolution Crossover
      U = particle[i]
      for each dimension d from 1 to D do
         if rand() < CR or d is a random dimension then
            U[d] = V[d]
         end if
      end for

      // Evaluate the fitness of the trial vector U
      Evaluate the fitness of U

      // Non-dominated sorting
      if U dominates particle[i] then
         Replace particle[i] with U
      else if U is non-dominated and dominates some particles in the archive then
         Replace the dominated particles in the archive with U
      end if

      // Update the personal best position of particle i if necessary
      if U is better than the personal best of particle i then
         Update the personal best of particle i
      end if
   end for

   // Update the global best position if necessary
   Update the global best position from the archive
end for

// Output the Pareto front
Return the archive as the Pareto front
```

Figure 6: Pseudo-code of MOPSO-DE algorithm.

From Figure 6, the pseudo-code of MOPSO-DE algorithm integrates PSO and DE for multi-objective optimization. The key parameters include the number of particles, the number of iterations, and the variation factor F. The particle position is randomly initialized, a new solution is generated through DE, and the non-dominated archive is evaluated and updated. The individual and global optima are updated iteratively. Finally, the Pareto front solution set is obtained. Subsequently, based on the Pareto dominance relationship and crowding distance, individual strengths and weaknesses are judged, and the elite pool is updated. The Pareto optimal solution set is an ideal state of resource allocation in multi-objective optimization. All these sets of non-dominated solutions form the Pareto front in the objective space. The Pareto front diagram is shown in Figure 7.

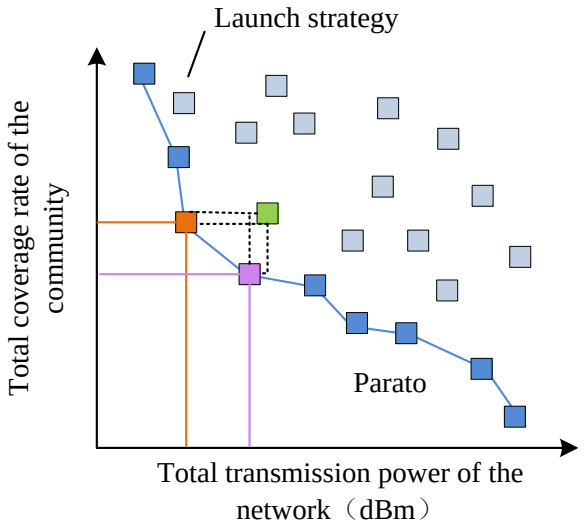


Figure 7: Pareto front diagram for multi-objective optimization.

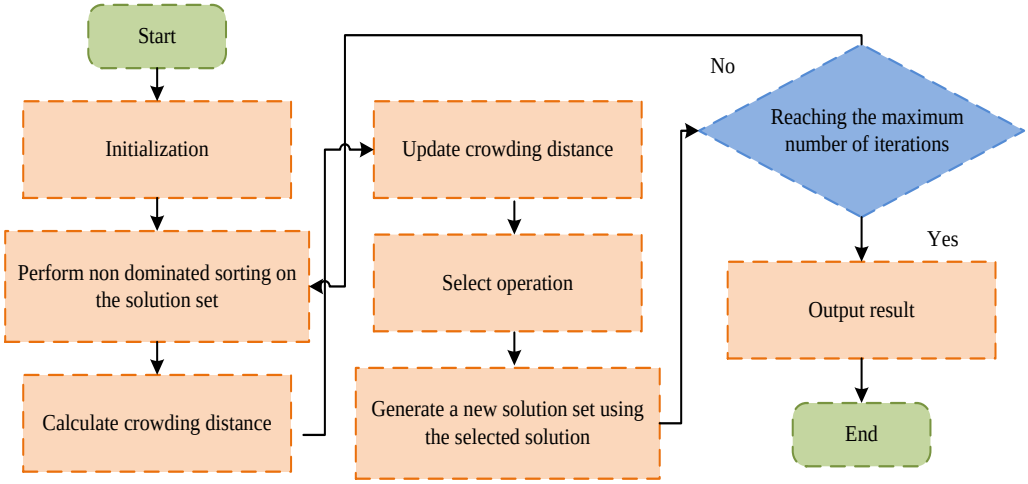


Figure 8: Schematic diagram of the crowded distance algorithm.

Figure 7 shows the Pareto front of the multi-objective optimization problem, which is used to show the dual-objective optimization relationship between coverage and transmission power, as well as the corresponding mechanism between the "Pareto front" and the actual deployment strategy. It does not correspond to specific experimental data. The graph covers the non-dominated solutions in several experiments. Pareto front represents the solution set that achieves the optimal balance among multiple objectives. The horizontal axis in the figure represents the total transmission power of the network, measured in DBM, while the vertical axis represents the total coverage area of the cell. Each point corresponds to a launch strategy that meets the constraints. Due to the natural conflict between the two objectives, the optimal solution cannot be achieved simultaneously. Therefore, the output solution of this algorithm is not the only optimal solution, but rather constitutes an optimal set, namely the Pareto front. Decision makers can select appropriate equilibrium points in the Pareto front based on the needs of different business scenarios. The mathematical definition of Pareto solution is shown in equation (8).

$$\begin{cases} \text{Maximize } f_1(x) = A(x) \\ \text{Minimize } f_2(x) = \sum_{i=1}^{N} P_i \end{cases} \tag{8}$$

In equation (8), $f_1(x)$ is the sum of the total coverage rate of the community and the coverage rate A. $f_2(x)$ is the total transmission power. x is a set of parameters that includes the transmission power of each base station. P_i is the transmission power of the i-th base station. After sorting the non-dominated solutions, to prevent the solution set from being too concentrated on the Pareto front, the crowding distance algorithm is introduced as an auxiliary evaluation metric to maintain the diversity of the solution set. Crowding distance measures the distance between an individual and other non-dominated solutions in the solution space. A higher value indicates that the area in which the individual is located is sparser and more representative. The specific calculation process is shown in Figure 8.

As shown in Figure 8, firstly, all non-dominated solutions are sorted in ascending order according to their respective objective functions. Secondly, the maximum and minimum crowding distances of individuals in each target dimension are set to infinity to preserve the boundary solutions. Subsequently, the difference between each remaining solution and adjacent solutions in each target dimension is calculated and normalized. Finally, the normalized distances on all target dimensions are accumulated to obtain the total crowding distance of the solution. A large crowding distance indicates that the solution is located in a sparser area, and priority should be given to preserving it to enhance the diversity of the population. This mechanism effectively avoids the aggregation of individuals in the solution set and helps generate a wider and more evenly distributed Pareto front. Crowding distance measures the density of solutions around a solution in the objective function space. The solution with larger crowding distance means that it is relatively isolated in the target space, that is, there are fewer solutions around, which helps to maintain the diversity of solution set. To calculate the crowding distance, the non-dominated solutions are sorted for each objective function, and then the infinite crowding distance is assigned to the boundary solution. The distance difference between each solution and adjacent solutions in each target dimension is calculated and normalized. Finally, the normalized distances of all target dimensions are accumulated to obtain the total crowding distance of each solution, which is used to evaluate the diversity of solutions. The specific calculation is shown in equation (9).

$$D_i^m = \frac{f_m(i+1) - f_m(i-1)}{f_m^{\max} - f_m^{\min}} \tag{9}$$

In equation (9), D_i^m represents the rate of change or difference of the i -th data point in the m-th dimension. $f_m(i+1)$ and $f_m(i-1)$ are the function values of the direct successor and direct precursor of the i th solution on the m-th objective function, respectively. $f_m^{\max}$ and $f_m^{\min}$ are the maximum and minimum values of all solutions on the m-th objective function, respectively. The total crowding distance is the sum of the dimensions of each target, as shown in equation (10).

$$D_i = \sum_{m=1}^{M} D_i^m \tag{10}$$

In equation (10), M is the total number of dimensions. D_i is the comprehensive rate of change or difference of the i-th data point across all dimensions. Crowded distance contributes to the convergence and diversity of equilibrium solutions in multi-objective optimization processes. For example, three solutions are considered, including A (0.8, 0.2), B (0.9, 0.5), and C (0.95, 0.7) in the dual-objective problem. After the targets are arranged in ascending order, B is between A and C. The crowded distance is combined with the distance between the left and right solutions of B in each target dimension to calculate the sparsity of its local solution. If the solution around solution B is sparse and the crowding distance is large, it is more likely to be retained in the next generation. Throughout the process, the MOPSO-DE algorithm approaches the Pareto optimal solution set through continuous iterations, achieving intelligent scheduling and optimized allocation of signal transmission power [21-22]. In the 5.5G network optimization, energy efficiency is a key performance index, which measures the energy efficiency of the network when transmitting data. The calculation is shown in equation (11).

$$\eta_E = \frac{T}{E} \tag{11}$$

In equation (11), η_E is energy efficiency. T is the network throughput. E is the total energy consumption. Improving energy efficiency directly means reducing energy consumption without sacrificing network throughput. By optimizing the network configuration, adjusting the antenna parameters, reducing the transmission power, and other measures, the network energy consumption can be significantly reduced and the network throughput is improved while maintaining the network performance. The antenna parameters are optimized. By adjusting the azimuth and dip angle of the antenna and optimizing the signal coverage, unnecessary energy consumption can be reduced. The transmission power is reduced. By optimizing signal transmission strategies, the transmission power of base stations can be reduced while maintaining network coverage and throughput. Using energy-saving equipment and selecting network devices with energy-saving functions, such as routers and switches, can effectively reduce energy consumption. Intelligent energy management is adopted to dynamically adjust the energy consumption of equipment according to the network load to achieve the energy saving goal. The combination of these optimization strategies and MOPSO-DE algorithm is conducive to the intelligent scheduling and optimal allocation of signal transmission power [23-24].

4 Results

4.1 Experimental environment and data sources

The algorithm models and simulation programs used in the research are developed and run in the Windows 11 operating system environment. The programming language used is Python 3.10, mainly relying on scientific computing and drawing libraries such as NumPy, Matplotlib, SciPy, etc. The computing platform is an Intel Core i7-12700H processor with 16GB of memory. The topology structure of the residential area used in the simulation refers to typical urban residential scenarios. The simulation area is divided into a square area of 100m×100m, containing 7 cellular base stations, deployed with three sector antennas. The simulation area size represents a typical urban macro cellular cell. It can capture the key features of signal propagation in urban environments, such as building occlusion, street layout,

Table 2: Experimental environment parameters.

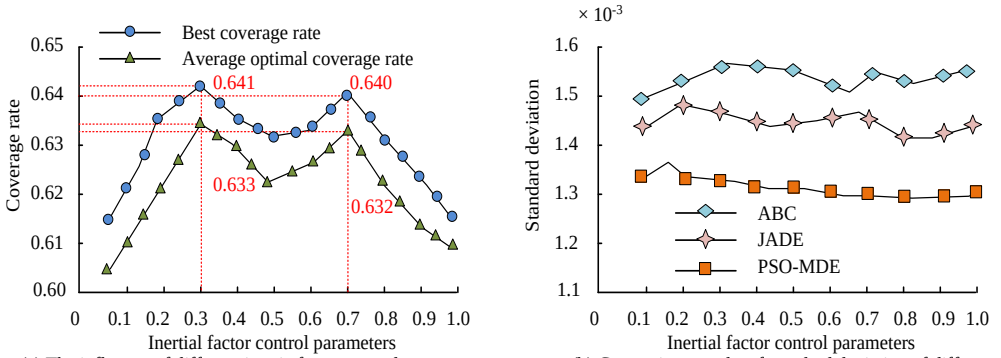
Parameter categories	Parameter name	Parameter values	Parameter categories	Parameter name	Parameter values
Network configuration	Number of base stations	10	Channel model	Ray tracing model	Including reflection, diffraction and penetration
	Number of sectors	30		Path loss index	2.5-3.5
	Frequency band	26 GHz		Total number of multipath components	10
	Bandwidth	100 MHz		Terrain attenuation factor	0.5-1.5
	Power emission range	20-40 dBm		Building penetration loss	10-20 dB
	Receive signal strength threshold	-90 dBm		\	\

and multi-path effects, without requiring excessive computational complexity. Urban macro cellular cells usually cover hundreds of meters, so a 100×100 meter area can well simulate this environment. In addition, this size includes sufficient buildings and obstacles in the simulation to reflect the complexity of signal propagation in urban environments. The number of particles is set to 50 to balance the search ability and computational efficiency. The convergence criterion is that the maximum iteration is 500 times or the change of fitness function value is less than 0.001. The experiment runs 30 times to evaluate the stability of the algorithm. The random seed is fixed at 42 to ensure that the experiment can be repeated. The reflection coefficient of RT simulation configuration is set to 0.6 to simulate the typical reflection behavior in urban environments. The path loss index is set between 2.5 and 3.5 to simulate signal attenuation in different environments. In addition, the terrain attenuation factor is considered to be within 0.5 to 1.5 and the building penetration loss is set between 10 and 20 dB. The network configuration and channel model parameters for the experiment are shown in Table 2.

4.2 Performance analysis of community antenna parameter optimization algorithm based on PSO-MDE

In the optimized cellular network community antenna parameters based on PSO-MDE algorithm, to comprehensively evaluate the performance of PSO-MDE algorithm, new optimization algorithms such as Artificial Bee Colony (ABC) and Adaptive Differential Evolution Algorithm (JADE) are introduced for comparative experiments. The adaptive inertia factor can be dynamically adjusted based on the information obtained during the search process. Therefore, this study explores the influence of inertia factors on the optimization effect of parameters, and the results are shown in Figure 9.

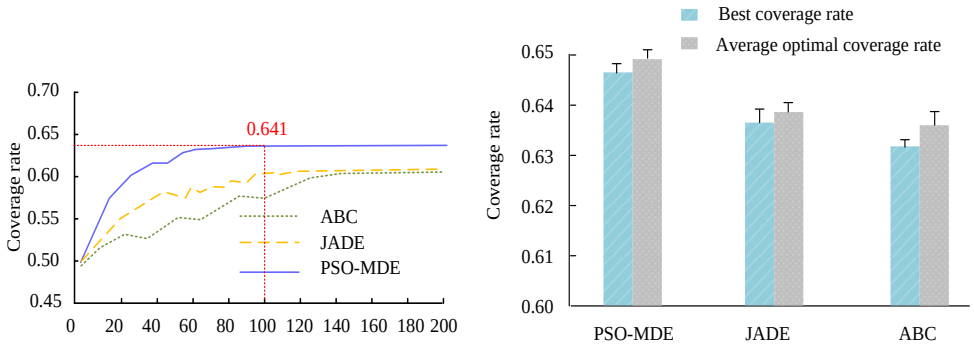
Figure 9 (a) shows the influence of inertia factor control parameters on optimization performance. Figure 9 (b) shows the comparison results of standard deviations for different algorithms. According to Figure 9 (a), as the inertia factor increased from 0 to 1, the coverage showed a fluctuating trend. The optimal coverage occurred when the inertia factor was 0.4 and 0.7, reaching 0.641 and 0.640, respectively. The average optimal coverage was 0.633 and 0.632 when the inertia factor was 0.6 and 0.7, respectively. As shown in Figure 9 (b), the standard deviation of the PSO-MDE algorithm was always the lowest, about 1.3×10-3, indicating its good stability under different inertia factors. The standard deviations of ABC and JADE algorithms were relatively high, ranging from approximately 1.4×10-3to 1.5×10-3and 1.5×10-3 to 1.6×10-3, respectively, with significant fluctuations. This may be because the PSO-MDE algorithm has advantages in parameter adjustment and adaptability, allowing it to maintain good stability and consistency under different conditions. Based on the convergence speed and optimization effect, the algorithm iteration was carried out when inertia factor influencing parameter was 0.3. To comprehensively evaluate the proposed algorithm, a comparative experiment was conducted on the coverage optimization of the three algorithms, with 20 repetitions. The obtained results are shown in Figure 10.



(a) The influence of different inertia factor control parameters on optimization performance

(b) Comparison results of standard deviation of different algorithms

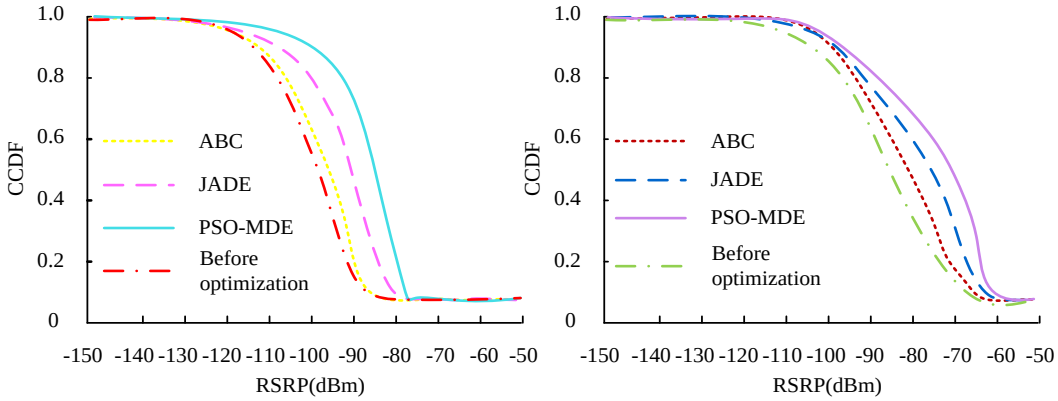
Figure 9: Influence of inertia factor on optimization effect.



(a) Optimal optimization coverage iteration chart

(b) Comparison of algorithm optimization results

Figure 10: Comparison of coverage of different algorithms.



(a) CCDF curve of RSRP before and after optimization in region A

(b) CCDF curve of RSRP before and after optimization in region B

Figure 11: Comparison results of CCDF of different algorithms.

Figure 10 (a) shows the iterative variation of optimal coverage for different algorithms. Figure 10 (b) compares coverage optimization results of different algorithms on the target area. As shown in Figure 10 (a), the PSO-MDE algorithm quickly converged after about 100 iterations, and the final coverage rate reached about 0.641. After 120 and 140 iterations, JADE and ABC achieved optimal coverage rates of approximately 0.602 and 0.559, respectively. According to Figure 10 (b), PSO-MDE led in both the optimal coverage and average optimal coverage indicators, with values of approximately 0.645 and 0.648, respectively. The optimal coverage and average optimal coverage of JADE and ABC were approximately 0.637 and 0.639, as well as 0.633 and 0.635, respectively. The reason for this result is that although JADE improves the adaptability of traditional DE, there may still be problems with slow convergence speed or falling into local optima in multi-dimensional search spaces. The ABC algorithm has relatively weak exploration ability due to its dependence on the honey source update mechanism. To verify the optimization effect of the algorithm on different regions,

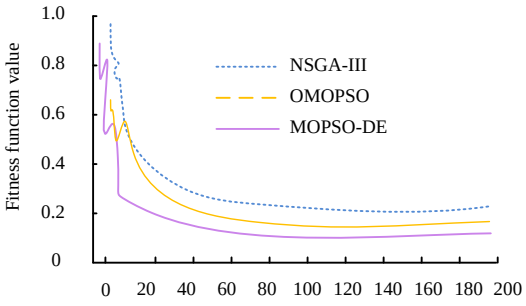
two publicly available urban residential regions A and B are selected for comparative experiments on their grid Reference Signal Received Power (RSRP). The Complementary Cumulative Distribution Function (CCDF) is taken to evaluate the coverage quality of the network. The obtained results are shown in Figure 11.

Figures 11 (a) and (b) show the CCDF curves of regions A and B before and after optimization, respectively. As shown in Figure 11 (a), after optimizing region A, the CCDF curves of all algorithms shifted to the right, indicating an overall improvement in RSRP values and signal quality. The CCDF curve optimized by PSO-MDE algorithm was the closest to the right, indicating its optimal performance in improving RSRP. When the CCDF was 0.8, the RSRP value of PSO-MDE was about -85dBm, while ABC and JADE were about -95dBm and -90dBm, respectively. This is because PSO-MDE has better adaptability and search ability when dealing with multi-objective optimization problems. From Figure 11 (b), in region B, the CCDF curves of all optimized algorithms were significantly better than before optimization, indicating the positive effect of the optimization on improving RSRP. Specifically, the PSO-MDE algorithm showed the greatest improvement after optimization, with its CCDF curve significantly better than ABC and JADE in the high RSRP value region. When the CCDF value was 0.7, the RSRP value of PSO-MDE was about -75dBm, while ABC and JADE were about -90dBm and -85dBm, respectively. The reason for this result is related to the search strategy and adaptability. The PSO-MDE algorithm may have achieved a better balance between exploration and development, which can more effectively find solutions to improve RSRP during the optimization process.

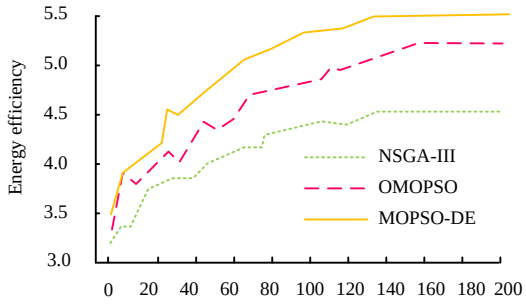
4.3 Performance analysis of signal transmission power optimization algorithm based on MOPSO-DE

To verify the feasibility of the MOPSO-DE-based community signal optimization algorithm proposed in the study, a relatively new multi-objective optimization algorithm (Optimized Multi-Objective PSO, OMOPSO) and Non-dominated Sorting Genetic Algorithm III (NSGA-III) area selected for comparative experiments in terms of convergence speed and energy efficiency. The obtained results are shown in Figure 12.

Figures 12 (a) and (b) show the variation curves of fitness function values and system energy efficiency with iteration times for different algorithms, respectively. As shown in Figure 12 (a), MOPSO-DE algorithm reached a stable state after about 15 iterations, and the fitness function value was 0.15, while OMOPSO and NSGA-III were stable around 0.19 and 0.25 after 30 iterations, respectively. This fast convergence may be due to improvements in the MOPSO-DE algorithm, which makes it more efficient in the search process. As shown in Figure 12 (b), the energy efficiency of the MOPSO-DE algorithm continued to increase during the iteration process and stabilized after approximately 120 iterations, ultimately reaching about 5.4. In contrast, the energy efficiency of the OMOPSO algorithm fluctuated significantly during the iteration process, ultimately stabilizing at around 5.2, while the energy efficiency of the NSGA-III algorithm remained relatively stable throughout the entire iteration process, ultimately stabilizing at around 4.4. This indicates that the MOPSO-DE algorithm performs the best in improving system energy efficiency, possibly because it can better balance different objectives during the optimization process, thereby achieving higher energy efficiency. The experiment further explores the performance of various algorithms in signal transmission power optimization tasks, and the results are shown in Table 3.



(a) The change curve of fitness function values for different algorithms



(b) The variation of system energy efficiency with the number of algorithm iterations

Figure 12: Performance variation curve of different algorithms with the number of iterations.

Table 3: Comparison results of signal transmission power optimization algorithm performance.

Algorithm	MOPSO-DE		OMOPSO		NSGA-III		SPEA2		PSO	
Iterations	100	200	100	200	100	200	100	200	100	200
Total transmission power (dBm)	35.2	33.5	36	34.5	37	35.5	36.8	36.0	35	35
Computation time(s)	110	530	120	550	100	540	130	520	100	500
Pareto front points	200	240	180	220	170	210	165	205	160	200
Standard deviation	0.5	0.3	0.7	0.6	0.4	0.2	0.5	0.5	0.6	0.6
p	$p<0.01$									

From Table 2, after 100 iterations, the performance of each optimization algorithm was significantly different in terms of signal transmission power control and Pareto solution quality. MOPSO-DE algorithm performed best with a minimum total transmission power of 35.2 DBM and 200 Pareto front points, and the standard deviation was 0.5, indicating that the algorithm had good stability in multiple operations. This is due to its fast convergence property that combines the global search capabilities of DE and PSO, which achieves an effective balance between exploration and utilization. The optimal transmission power of OMOPSO was 36.0 DBM, and the standard deviation was 0.7. The stability and energy efficiency of the solution were also good. The transmission power of NSGA-III was 37.0 DBM, which was the worst, but the standard deviation was 0.4, indicating that the algorithm was stable. It is speculated that it tends to maintain the diversity of solutions and sacrifice the convergence accuracy. Although the transmission power of traditional PSO was 35.0 DBM, which was close to MOPSO-DE, only 160 Pareto solutions were obtained, indicating that the distribution of solutions was insufficient and easy to fall into local optimum. In general, OMOPSO and MOPSO-DE are superior to the baseline algorithm in terms of convergence speed, solution set diversity, and power optimization, reflecting the enhanced role of sub-evolution mechanism in multi-objective problems. Statistical tests also showed that OMOPSO and MOPSO-DE had significant advantages ($p<0.01$).

5 Discussion

The proposed PSO-MDE and MOPSO-DE algorithms show significant performance advantages in antenna configuration and power allocation optimization of 5.5G cellular networks. By combining RT technology and PSO algorithm, these algorithms not only surpass the traditional PSO algorithm in convergence speed, but also show excellent performance in coverage gain and energy trade-off. PSO-MDE algorithm uses DE strategy to enhance the global search ability. The Metropolis criterion and adaptive inertia factor effectively avoid local optima, thereby accelerating convergence speed. This improvement makes the algorithm more balanced in global search and local fine adjustment in complex multi-objective optimization problems. MOPSO-DE algorithm can significantly reduce energy consumption while ensuring network coverage by optimizing signal transmission power, which is of great significance to improve the energy efficiency and sustainability of the network.

Compared with the baseline algorithm, such as ABC, adaptive DE algorithm, OMOPSO, and NSGA-III, the proposed algorithm shows higher stability and consistency in coverage optimization and energy efficiency. When dealing with high-dimensional search space and nonlinear constraints, the baseline algorithm is often prone to fall into local optimization with slow convergence speed. It is difficult to balance different objectives in multi-objective optimization problems. In contrast, PSO-MDE and MOPSO-DE algorithms achieve better coverage and energy efficiency through accurate modeling and optimization strategies, providing an effective technical path for intelligent planning and performance improvement of 5.5G networks.

To sum up, the proposed algorithm shows obvious technical advantages in 5.5G network optimization, which not only improves the network coverage and energy efficiency, but also provides new ideas and methods for future network optimization. These achievements have important technical significance and application value for promoting the development of 5.5G and future communication technologies.

6 Conclusion

To improve the signal coverage performance and energy utilization efficiency of 5.5G cellular networks in the high frequency band, a joint optimization framework combining RT modeling and multi-objective evolutionary algorithm was constructed to optimize antenna parameters and transmission power. The RT algorithm was taken to finely model the channel propagation characteristics in complex urban scenarios, and the optimization strategy was adopted to conduct multidimensional search and optimization on base stations in residential areas to maximize signal strength and minimize interference. In terms of antenna optimization, the optimal coverage of PSO-MDE algorithm was 0.645, which was 0.008 higher than JADE algorithm and 0.012 higher than ABC algorithm. The

average optimal coverage of PSO-MDE algorithm was 0.648, 0.009 higher than JADE algorithm and 0.015 higher than ABC algorithm. In terms of transmission power optimization, MOPSO-DE algorithm had the lowest total transmission power at 200 iterations, which was 33.5 DBM, 2.5 DBM lower than OMOPSO algorithm and 1.5 DBM lower than NSGA-III algorithm. The results show that the proposed joint optimization algorithm can effectively improve the performance of 5.5G network and provide an effective solution for network optimization. However, the research still has some limitations. Firstly, the experiment is based on static synthetic data, and the dynamic user behavior and time series channel changes have not been considered. In addition, the computational complexity of the algorithm used in large-scale, real-time optimization scenarios still needs to be further reduced. Therefore, future work will focus on the following directions. Firstly, online learning mechanism and dynamic adaptive strategies, such as adaptive PSO or reinforcement learning method, will be introduced to improve the real-time response ability of the model to environmental changes. Secondly, it combines the low complexity approximate optimization method to improve the deployment efficiency of the algorithm on edge devices. Thirdly, dynamic multi-user modeling and spatiotemporal channel data are integrated to enhance the generalization ability of the model to the real network environment. It is expected that these improvements will provide more practical and forward-looking technical support for intelligent optimization of 5.5G and even future 6G networks.

Reference

[1] Zhi Liu, and Wei Song. Search guidance network assisted dynamic particle swarm optimization algorithm. Journal of Frontiers of Computer Science and Technology, 18(12):3189-3202, 2024.https://doi.org/10.3778/j.issn.1673-9418.2312030

[2] Dan Song, Zhiping Xu, Shaohua Hong, and Lin Wang. Survey of transmission coding theory on physical layer for wireless body area network: optimal design of low-density parity-check code. Journal of Electronics & Information Technology, 45(08):2818-2827, 2023.https://doi.org/10.11999/JEIT221171

[3] Baohui Han, Qichao Zhao, Rong Chang, Xiaomeng Li, Keqin Yan, and Qiming Fu. Chlorophyll-a concentration inversion model: stacked auto-encoder particle swarm optimization BP neural network. Journal of Geo-Information Science, 25(09):1882-1893, 2023.https://doi.org/10.12082/dqxxkx.2023.230144

[4] Zhisheng Niu. uRLLC³: ultra-reliable and low-latency communication, computing, and control for 6G networks. Scientia Sinica Informationis, 54(05):1267-1282, 2024.https://doi.org/10.1360/SSI-2023-0336

[5] Yi He, Weizhi Zhong, Shiqing Wan, Qiuming Zhu, and Zhipeng Lin. Joint beamforming for IRS-aided MU-MISO millimeter wave communication of vehicular network. Journal of Signal Processing, 40(02):336-344, 2024.https://doi.org/10.16798/j.issn.1003-0530.2024.02.011

[6] Li Juan. Improved genetic algorithm enhanced with generative adversarial networks for logistics distribution path optimization. Informatica, 49(11):180-197, 2025.https://doi.org/10.31449/inf.v49i11.6961

[7] Chenxi Mao, Yongchao Guo, Haoyu Zhang, and Liangquan Zhang. Post-earthquake damage assessment for RC frame communication buildings based on convolutional neural network. Journal of Natural Disasters, 33(05):157-167, 2024.https://doi.org/10.13577/j.jnd.2024.0515

[8] Wenwu Yu, Xiaokai Nie, Yujin Cai, Guangju Li, Hongzhe Liu, Qiang Cheng, and Tiejun Cui. A survey on the performance optimization of wireless communication networks assisted by reconfigurable intelligent surface. Scientia Sinica Informationis, 54(11):2503-2517, 2024.https://doi.org/10.1360/SSI-2024-0060

[9] Chen Liang, Deqiang He, Ziyang Ren, Zhenzhen Jin, and Weifeng Yang. Real-time traffic scheduling optimization of train communication network based on time-sensitive network. Journal of Railway Science and Engineering, 21(01):58-69, 2024.https://doi.org/10.19713/j.cnki.43-1423/u.T20230194

[10] Kaiwen Yu, Renhe Fan, Wenlong Gou, Chuanhang Yu, and Gang Wu. Cross-layer energy efficiency optimization for semantic communication networks. Scientia Sinica Informationis, 54(04):758-776, 2024.https://doi.org/10.1360/SSI-2023-0283

[11] Wenzhuo Hu, and Chun Wu. A hierarchical genetic algorithm for spatio-temporal coverage optimization in communication networks under emergency monitoring scenarios. Journal of Geo-Information Science, 26(08):1880-1892, 2024.https://doi.org/10.12082/dqxxkx.2024.230732

[12] Yurong Wang, Weiwei Qu, Guilin Li, Hu Deng, and Liping Shang. An optimization method for terahertz metamaterial absorber based on multi-objective particle swarm optimization. Acta Physica Sinica, 74(05):057801, 2025.https://doi.org/10.7498/aps.74.20241684

[13] Praveena Nuthakki, Pavan Kumar T, Musaed Alhussein, Muhammad Shahid Anwar, Khursheed Aurangzeb, Leenendra Chowdary Gunnam. AI-driven resource and communication-aware virtual machine placement using multi-objective swarm optimization for enhanced efficiency in cloud-based smart manufacturing. Computers, Materials & Continua, 81(12):4743-4756, 2024.https://doi.org/10.32604/cmc.2024.058266

[14] Hongwei Zhao, Yongfang Xie, Jianhua Liu, Jiayi Hou, and Haichao Liu. Research on deployment optimization strategy and application technology of

5G high-speed rail network. Railway Standard Design, 67(01):167-174, 2023.https://doi.org/10.13238/j.issn.1004-2954.202111180005

[15] Yifan Zhang, and Wei Song. Multi-objective particle swarm optimization algorithm guided by extreme learning decision network. Journal of Frontiers of Computer Science and Technology, 18(06):1513-1525, 2024.https://doi.org/10.3778/j.issn.1673-9418.2304026

[16] Hao Li, Haixiao Yang, Lan Zhang, Xin Huang, Haining Wang, and Yan Kang. Improved discrete mayfly algorithm for multi-objective dynamic network community detection. Journal of Frontiers of Computer Science and Technology, 17(04):942-952, 2023.https://doi.org/10.3778/j.issn.1673-9418.2106011

[17] Yifei Zou, Senmao Qi, Cong'an Xu, and Dongxiao Yu. Distributed weighted data aggregation algorithm in end-to-edge communication networks based on multi-armed bandit. Computer Science, 50(02):13-22, 2023.https://doi.org/10.11896/jsjkx.221100134

[18] Junhai Zhao, Linwei Hua, and Yu Wang. Study on axial compressive load bearing capacity of concrete-filled double-skin steel tubular columns based on particle swarm optimization BP neural network. Progress in Steel Building Structures, 26(09): 45-52, 2024.https://doi.org/10.13969/j.cnki.cn31-1893.2024.09.005

[19] Na Luo, Hua Yu, Zeqing You, Yao Li, Tunan Zhou, Nan Han, Chenxu Liu, Zihan Jiang, and Shaojie Qiao. Fuzzy logic and neural network-based risk assessment model for import and export enterprises: a review. Journal of Data Science and Intelligent Systems, 1(1): 2-11, 2023.https://doi.org/10.47852/bonviewJDSIS32021078

[20] Xingyu Sha, Jiaqi Zhang, and Keyou You. Fully asynchronous distributed optimization with linear convergence over directed networks. Journal of Sun Yat-sen University (Natural Science Edition), 62(05): 1-23, 2023.https://doi.org/10.13471/j.cnki.acta.snus.2023A023

[21] Chunlei Zhong, and Gang Yang. Design and application of improved genetic algorithm for optimizing the location of computer network nodes. Informatica, 49(16):25-51, 2025.https://doi.org/10.31449/inf.v49i16.7201

[22] Yan Yang, and Kang Wang. Efficient logistics path optimization and scheduling using deep reinforcement learning and convolutional neural networks. Informatica, 49(16):43-59, 2025.https://doi.org/10.31449/inf.v49i16.7839

[23] Mikel Barbara, David Rey, Taha Rashidi, and Divya Nair. School choice modeling and network optimization in an urban environment. Annals of Regional Science, 72(3):115-131, 2024.https://doi.org/10.1007/s00168-023-01230-5

[24] Greanne Leeftink, Kimberley Morris, Tim Antonius, Willem de Vries, and Erwin Hans. Inter-organizational pooling of NICU nurses in the Dutch neonatal network: a simulation-optimization study. Health Care Management Science, 28(1):64-83, 2025.https://doi.org/10.1007/s10729-025-09697-8

Deep and Hybrid Ensemble Learning Methods for Enhanced Live-Birth Prediction in Fertility Treatments

Rituraj Jain[1], Uma Shankar[2], G V Radhakrishnan[3], Saroj Date[4], Kamal Upreti[*5], S. Caroline[6], Ramesh Babu P[7], Mohit Dayal[8]
[1]Department of Information Technology, Marwadi University, Rajkot, Gujarat, India
[2]Faculty of Management and Social Sciences, Qaiwan International University, Sulaimanyah, Kurdistan, Iraq
[3]Kalinga School of Management, Kalinga Institute of Industrial Technology, Bhubaneswar, India
[4]Department of Artificial Intelligence and Data Science, CSMSS Chh. Shahu college of Engineering, Chh. Sambhajinagar, Maharashtra, India
[5]Department of Computer Science, Christ University, Delhi NCR Campus, Ghaziabad, India
[6]Department of Electronics and Communication Engineering, St. Xavier's Catholic College of Engineering, Nagercoil, Tamil Nadu, India
[7]Department of Computer Science & Engineering, Narsimha Reddy Engineering College, Secunderabad, Telangana, India
[8]Department of Information Technology, Bharati Vidyapeeth's College of Engineering, New Delhi, India
E-mail: jainrituraj@yahoo.com, uskapila@gmail.com, vrkris2002@gmail.com, saroj.date@gmail.com, kamalupreti1989@gmail.com, caroline@sxcce.edu.in, drprb2009@gmail.com, mohitdayal.md@gmail.com
[*]Corresponding author

Keywords: assisted reproductive technologies, hybrid machine learning, IVF prediction, live-birth estimation, predictive modelling

Received: March 6, 2025

The prediction of live birth outcomes using Assisted Reproductive Technologies (ART) remains a complex task owing to the high inter-patient variability and non-linear clinical interactions. This study presents a comparative evaluation of hybrid machine-learning models to improve in vitro fertilization (IVF) success prediction using a real-world anonymized dataset of 2,000 ART cases. After pre-processing (including missing value imputation, feature selection via Recursive Feature Elimination with Cross-Validation, and class balancing using SMOTE with k=5), four hybrid models were developed: stacking with XGBoost as the meta-learner, weighted ensemble, autoencoder-based feature fusion, and cascading classifiers. Models were evaluated using accuracy, AUC, precision, recall, and F1-score metrics, and compared against a baseline Random Forest classifier. The stacking model (XGBoost with Random Forest, MLP, and SVM base learners) achieved the best performance, with an accuracy and 0.999 AUC of 0.985. The weighted hybrid ensemble followed an accuracy of 0.953 and AUC of 0.994. The statistical significance of the improvements was confirmed using Wilcoxon Signed-Rank and McNemar's tests ($p < 0.05$). To enhance model transparency, SHapley Additive exPlanations (SHAP) was applied to interpret base model contributions in the stacking architecture. These results support the application of AI-driven hybrid modelling for personalized IVF treatment planning. Future work will focus on prospective validation and clinical decision support system (CDSS) integration to assess deployment feasibility.

Povzetek: Študija na 2000 primerih ART primerja hibridne modele za napoved rojstva živorojenega. Po obdelavi (RFECV, SMOTE) najboljši sistem z XGBoostom doseže najboljše rezultate. SHAP zagotovi razložljivost; Wilcoxon/McNemar potrdita izboljšave. Predvidena validacija in vključitev v klinični CDSS sistem.

1 Introduction

In ART, it is crucial to develop predictive models to forecast live birth outcomes after IVF. However, even in the era of reproductive medicine and embryology, IVF procedures have not been able to realize larger, more effective success rates, which depend on patient-specific factors, including age, hormonal levels, and the quality of embryos [1], [2]Previous attempts have employed traditional statistical models to estimate IVF success probabilities, which are, unfortunately, never overly accurate since biological and clinical factors are complex and their effects are still heterogeneous [3], [4]. Machine Learning (ML) and Deep Learning (DL) models have recently emerged as powerful tools for enhancement of predictive abilities with reproductive medicine [5], [6]. Nevertheless, standalone models often suffer from overfitting, data bias, and low generalizability [7]. To address such challenges, hybrid machine learning solutions can offer a worthy possibility through the combination of several algorithms to exploit the positive aspects of multiple models and increase prediction accuracy and robustness [8], [9]. Successful IVF treatment

relies on a range of variables including patient characteristics, clinical indicators, and embryo developmental aspects [2], [10], [11], [12], [13]. Traditionally implemented predictive models have limited generalizability because IVF-related data contain high dimensions and non-linear patterns [14], [15], [16]. The main reason for adopting hybrid models is the six core difficulties.

1. The complex connections between IVF data elements, including patient information, hormone patterns, and embryonic results, remain inaccessible to the standard statistical techniques for interpretation.
2. Many ART predictive features display non-linear behavior with specific effects on different patient populations, thus creating obstacles for developing a unified generalized model.
3. Class Imbalance exists because successful live births occur less frequently than unsuccessful cases, thus causing an unbalanced dataset that affects the model performance.
4. Medical staff need interpretable predictive models to demonstrate their analytical reasoning, rather than forcing them to use machine learning methods as unexplainable systems.
5. Multiple sensory data sources influence IVF success rates through clinical records combined with patient imaging results and time-based medical histories, which require sophisticated data-fusion systems to extract involvement information.
6. There is a lack of interpretable, personalized insights for supporting clinical decision-making in IVF treatments.

This study presents and evaluates five novel cross-hybrid models for predicting IVF live birth outcomes, further refining the specificity of prediction through multiple machine learning paradigms. The hybrid approaches used in this study included stacking (Layered Learning), weighted hybrid ensembles, cascading models, feature-level fusion with autoencoder networks, and SHAP-enhanced gradient boosting. These approaches were devised to handle data heterogeneity, temporal dependencies, feature importance selection, and automated hyperparameter optimization, which are highly relevant to IVF outcome prediction. This study aimed to present a robust and scalable predictive framework for these hybrid approaches to support clinical decision-making and personalized treatment planning in Assisted Reproductive Technology (ART).

A hybrid modelling approach provides a synergistic blending of several machine-learning models to overcome the weaknesses of individual models, resulting in increased predictive accuracy and robustness [17], [18], [19]. This study also introduces SHAP-based interpretability to align predictive modelling with clinical transparency, making it easier for fertility specialists to interpret model outputs.

This study aimed to bridge the gap between computational intelligence and clinical decision-making in reproductive medicine, improve the prediction of IVF success, and aid fertility specialists in designing optimal treatment plans tailored to individual patients.

1.1 Novelty and contribution of proposed system

This paper proposes a novel hybrid framework that incorporates stacking, weighted ensembles, cascading classifiers, autoencoder-based feature fusion, and SHAP-enhanced XGBoost explainability. Compared to existing methods, the proposed system employs multi-stage learning to address class imbalance and enhances decision reliability through trust refinement techniques such as RFECV-based feature selection and ensemble diversity. Table 1 summarizes the existing research gaps and explains how the proposed models were designed to overcome them through synergistic learning strategies and explainable outputs.

1.2 Structure of paper

The remainder of this paper is structured as follows: Section 2 presents a comprehensive literature survey of prior works on prediction models of IVF using machine learning applications in ART. Section 3 explains the methodology, dataset used, pre-processing, and a detailed description of the four hybrid modelling strategies used in this study. Section 4 presents the results and a comparison of the models. Section 5 summarizes the main findings and concludes the study.

Table 1: Research questions, identified research gaps and research contribution

Research Questions	Identified Research Gaps	Research Contributions
RQ1: How can predictive models generalize better for complex IVF data?	Existing models struggle with generalizing across diverse patient data and clinical variability.	Hybrid models integrate multiple learning approaches to improve generalization and robustness.
RQ2: How can feature selection be optimized for IVF prediction?	Conventional methods may overlook critical IVF-specific features or suffer from overfitting.	Hybrid models use RFECV, Bayesian Optimization, and autoencoders to refine feature selection.
RQ3: How can we handle class imbalances in IVF datasets?	Standard classifiers are biased towards majority classes, reducing predictive accuracy for minority cases.	SMOTE, weighting mechanisms, and cascading models dynamically handle class imbalance.
RQ4: How can we quantify the uncertainty in IVF predictions?	Traditional models lack interpretability and fail to quantify prediction uncertainty.	Hybrid ensemble methods provide confidence estimates, whereas cascading models refine the uncertain predictions.
RQ5: How can deep feature representations be utilized for improved prediction?	Feature extraction techniques do not effectively capture deep, non-linear IVF patterns.	Autoencoder fusion and hybrid deep learning methods enhance the feature representations.
RQ6: How can hyperparameter tuning be	Manual or grid search-based tuning is inefficient and	Hybrid models integrate multiple learning approaches to

Research Questions	Identified Research Gaps	Research Contributions
improved to achieve better performance?	computationally expensive.	improve generalization and robustness.

2 Literature review

Models of increasing machine learning have been increasingly used to predict IVF outcomes, with the possibility of providing the benefits of predicting IVF outcomes for infertile couples and in healthcare systems. These models often use a given set of data to predict the IVF outcomes. Existing machine learning-based approaches for IVF outcome prediction generally involve the use of medical and reproductive history, biochemical indicators, and data regarding reproductive tract examination, along with information from previous IVF cycles [13]. These models have proven useful for assessing subfertile couples and providing clues for treatment. Nevertheless, they are constrained by their dependency on conventional clinical parameters and do not reveal the factors that affect IVF success.

Consequently, scientists are developing increasingly sophisticated applications that integrate omics data with AI. The recent introduction of metabolomics, transcriptomics, and biomarkers in conjunction with deep machine learning assessment of oocytes, sperm, and embryos has been proposed as a novel tool [13]. The proposed algorithm provides a way to develop artificial neural network models that can better objectively and accurately predict this outcome than the traditional methods used in couples with unexplained infertility or repeated implantation failures. Several earlier techniques have been used for multiple-attribute selection methods to predict outcomes more accurately and efficiently through IVF prediction.

In one example, researchers integrated omics and artificial intelligence evidence to suggest the best treatment options and increase IVF success rates; thus, they developed a novel tool [13]. First, the lifestyle and demographic parameters of the subfertile couples, metabolomics, transcriptomics, and biomarkers were obtained, and the oocytes, sperm, and embryos were evaluated using deep machine learning. This study also emphasizes the value of omics data in facilitating optimal embryo selection and improving personalized IVF treatment.

Similarly, a separate study used the XGBoost machine learning system [20] to minimize multiple embryo gestation rates in IVF by creating a hierarchical model. It concomitantly learns embryo implantation potential and double embryo transfer. The variables identified by the researchers for single-embryo transfer pregnancies were age, IVF attempts, estradiol level on hCG day, and endometrial thickness. For double embryo transfer, the other variables, including P1 and P2, were significant. For SET pregnancy, DET pregnancy, and DET twin risks, the model exhibited AUC of 0.7945, 0.8385, and 0.7229, respectively.

Issues related to data quality and feature selection are important in predicting IVF outcomes. It is also in the context of challenges in learning deep features and extracting high-level patterns [21]. Feature selection is important because it can select redundant and irrelevant features to remove dimensionality and enhance model generalization [22]. Specifically, regarding IVF, the integration of omics data (metabolomics and transcriptomics) with classic clinical parameters has both advantages and disadvantages when applied to feature selection [13].

However, the interpretability of the model remains challenging. Machine learning methods are capable of modelling flexibility and robustness; however, it is difficult to interpret individual features using sophisticated algorithms [23]. One problem with this lack of interpretability is that it hinders the identification of important biomarkers needed to develop novel hypotheses for the prevention, diagnosis, and treatment of complex conditions such as infertility.

Interestingly, the choice of modelling approach and feature selection method strongly depends on the purpose of the analysis. In [24], it was clearly recommended that the goal of model selection be specified as data exploration, inference, or prediction, as it serves the purpose of selecting the appropriate model to ensure that there is no confusion when selecting a statistical model.

However, demographic and clinical factors determine the IVF outcomes. However, important predictors for both single and double embryo transfer pregnancies include age, number of previous IVF attempts, estradiol level on hCG day, and endometrial thickness [20]. The live birth and implantation rates for women aged 35 years or younger with a caesarean section defect were significantly lower than those for women with a history of vaginal delivery [25].

Among the causes of low intrauterine insemination success, semen parameters (sperm concentration and motility) and female body mass index (BMI) were identified as the most important predictors [26]. Nevertheless, a meta-analysis of semen quality (concentration, motility, and morphology) and outcomes of assisted reproduction technologies [27] could not determine a significant correlation between these two variables. This contradiction indicates complications in predicting IVF success.

Environmental factors have a bearing on IVF outcomes. Fresh embryo transfer (FET) cycles result in lower chances of biochemical pregnancy, clinical pregnancy, and live birth during exposure to air pollutants, particularly ozone (O3), nitrogen dioxide (NO2), and carbon monoxide (CO), at various stages of IVF treatment [28].

The Area Under the Curve (AUC) of a Receiver Operating Characteristic (ROC) curve is commonly used. The AUC for live birth prediction was 0.905, and that for clinical pregnancy with fetal heartbeat was 0.722 [1]. The AUCs reported for single embryo transfer (SET), DET pregnancy, and DET twin risks were 0.7945, 0.8385, and 0.7229, respectively [20]. AUCs from 0.70 to 0.78 were obtained for ploidy prediction [29].

Other metrics included the accuracy, precision, recall, and F1 scores. Zou et al. achieved an accuracy of 0.77, precision of 0.79, recall of 0.86, and F1 score of 0.83 [29]. Values reported by [1] for live births and clinical pregnancies with fetal heartbeat of 1.12 and 0.77, respectively, were also used in the Observed: Expected (O: E) ratio.

Some studies have compared AI models with human predictions. A meta-analysis was not possible, but a systematic review indicated that AI-based prediction models were as good as embryologists, albeit marginally better [1]. It is also said that AI models have not yet surpassed clinically embryologists' predictive capability significantly.

Furthermore, one study [13] documented the lifestyle and demographic parameters of subfertile couples, together with the previous characteristics of IVF cycles. In addition, they measured and evaluated metabolomics, transcriptomics, and biomarkers by evaluating oocytes, sperm, and embryos using deep machine learning. This bundling of data collection and pre-processing was comprehensive enough to create artificial neural network models to increase the objectivity and accuracy of IVF success rate predictions.

In fact, some studies have investigated only a particular pre-processing technique, whereas others have focused on the need to establish the best pre-processing pipeline to follow before prediction. For example, [30] used an automated pre-processing model, referred to as a scenario-based model, in their study of construction accident severity prediction.

Compared to existing models, such as the protocol-based ANN framework by [13] and the XGBoost-based hierarchical model by [20], the proposed hybrid system significantly advances IVF outcome prediction. While prior studies lacked either empirical validation or comprehensive data integration, our model combined stacking, weighted ensembles, autoencoder-based fusion, and cascading strategies. This multi-stage approach addresses critical gaps such as limited data types, lack of personalization, and poor generalization, achieving superior accuracy (0.985) and AUC (0.999). Furthermore, statistical tests confirmed the model's significant improvement over traditional methods, establishing a robust and scalable predictive framework for clinical use.

To execute this model, several pre-processing steps are reviewed, including the processing of missing data, binned data, outlying data, scaling methods, and resampling data. The pre-processing pipeline plays a vital role, and we observed that in the most efficient scenario, we obtained the best out-of-prediction performance.

3 Methodology

3.1 Dataset

The dataset analyzed in this study was derived from anonymized registry data compiled by the Human Fertilization and Embryology Authority (HFEA), covering fertility treatments conducted between 2010 and 2016 [31]. It is publicly available and can be accessed via the direct download link provided in [31]. This dataset was previously used in a study by Goyal et al. [32]. It is the world's largest database of patient, donor, and offspring records that safeguards patient, donor, and offspring confidentiality to support patient care improvements. The dataset was filtered to include 2,000 samples with 95 attributes from actual in vitro fertilization (IVF) procedures. These attributes include age, infertility type, clinical treatment details, and embryonic data. Data were presented as numerical, categorical, or text. To ensure the same quality and consistency of the dataset, the missing values were considered through proper imputation. The numerical attributes were replaced with their median values, whereas the categorical attributes were set to their mode values. The dataset used did not contain attributes with more than 50% of the missing values. In total, 62 features were available after pre-processing and were chosen for further analysis.

The probability of a successful live birth with ART is a complex problem because it contains heterogeneous clinical, embryonic, and demographic factors. Therefore, we present a Hybrid Machine Learning Framework to improve the prediction accuracy and robustness by incorporating advanced data pre-processing techniques, utilizing a suite of machine learning models, and employing ensemble learning strategies. The IVF live birth prediction pipeline, consisting of data processing and the hybrid model development workflow, is illustrated in Figure 1. The proposed framework comprises four phases: data pre-processing, hybrid model development, model evaluation and comparison, and statistical significance testing. A detailed stepwise procedure of this Hybrid Machine Learning Framework for IVF Live Birth Prediction Algorithm has been systematically documented and is presented below to standardize a structured methodological approach to attain reproducibility.

Algorithm: Hybrid Machine Learning Framework for IVF Live Birth Prediction

Input: D = {X, Y}, where X represents patient demographics, clinical treatment details, and embryonic development data, and Y is the binary target variable indicating live birth outcomes.

Output: Predicted probability $\hat{Y}$ of live birth outcome.

Step 1: Data Preprocessing

1. Load dataset D.

2. Handle missing values:

a. Remove features F_i where $|F_i\text{missing}| / |F_i| > 0.5$.

b. Impute missing numerical values using the median: $Xnum(i) \leftarrow median(Xnum)$.

c. Impute missing categorical values using mode: $Xcat(i) \leftarrow mode(Xcat)$.

3. Encodes categorical variables using one-hot encoding.

4. Convert target variable: No live birth (Y = 0) and At least one live birth (Y = 1).

5. Perform stratified sampling: Split dataset into training and testing

6. Apply Synthetic Minority Over-Sampling Technique (SMOTE) to balance class distribution.

7. Perform feature selection using Recursive Feature Elimination with Cross-Validation (RFECV).

Step 2: Hybrid Model Development: Train machine learning models:

A. Stacking with Meta-Learners:

a. Train base models: Random Forest (RF), Support Vector Machine (SVM), Multi-Layer Perceptron (MLP).

b. Generate meta-features from out-of-fold predictions of base models using k-fold cross-validation to avoid data leakage

c. Use predictions $\hat{Y}$base as input features for meta-learners: XGBoost, MLP, Gradient Boosting Machine (GBM).

B. Weighted Hybrid Ensemble:

a. Train models: RF, MLP, SVM, Naive Bayes (NB).

b. Assign optimal weights w_i via Bayesian Optimization: $\hat{Y} = \Sigma\, w_i\, \hat{Y}_i$.

C. Cascading Models:

a. Train a Decision Tree (SimpleCart) for handling easy cases.

b. Use MLP for uncertain cases.

c. Final refinement with Random Forest for cases with ambiguous probability outputs from the MLP.

D. Feature-Level Fusion with Autoencoder:

a. Train Autoencoder A(X) for feature compression: X' = A(X).

b. Train RF, SVM, and MLP on compressed features X'.

c. Combine predictions via stacking or voting.

E. SHAP-Enhanced XGBoost Model

a. Train an XGBoost classifier using optimized hyperparameters on the pre-processed dataset.

b. Compute SHAP values to assess feature importance and interpretability.

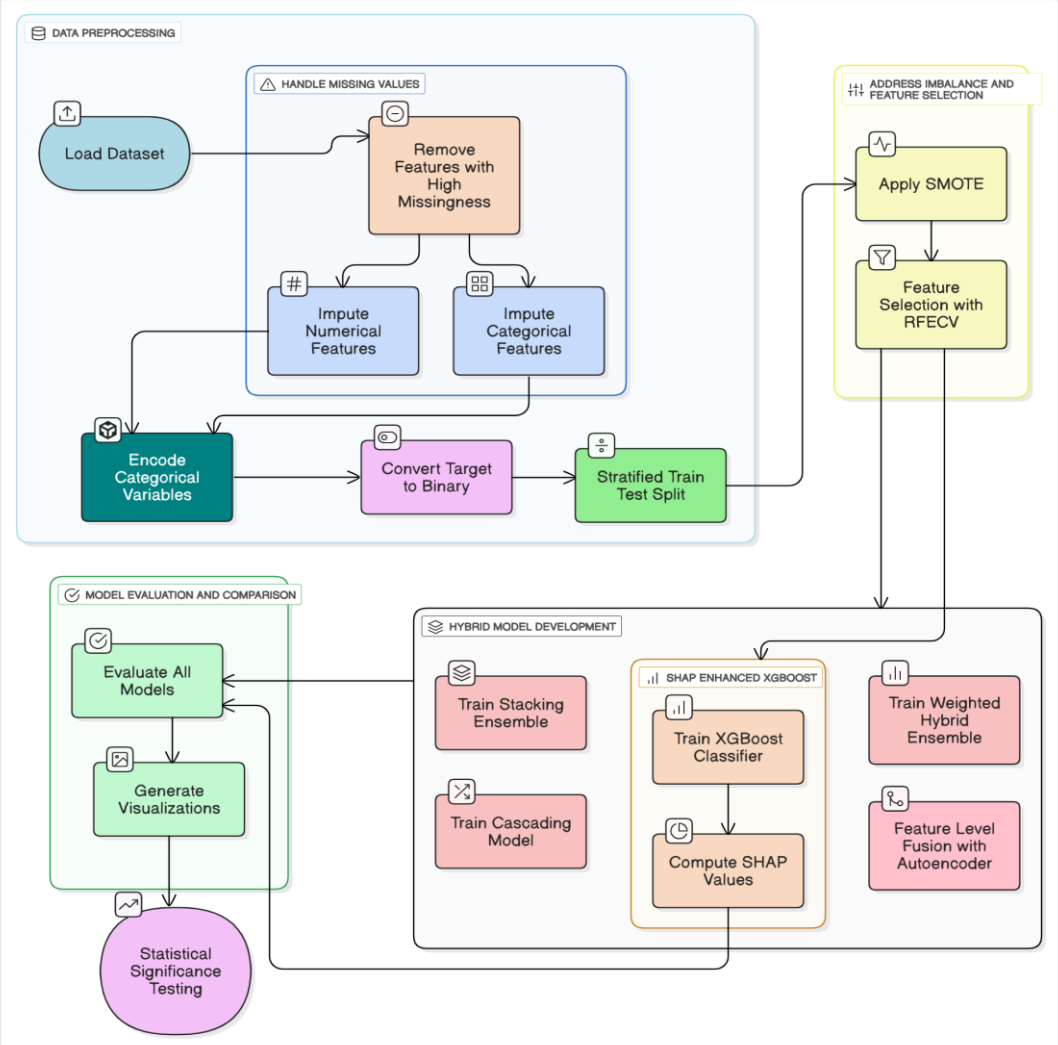


Figure 1: Data processing and model development flowchart for ivf live-birth prediction

c. Use SHAP visualizations (summary plot, force plot) to support model explainability for clinical insight.

Step 3: Model Evaluation and Comparison
1. Evaluate models using metrics: Accuracy, Precision, Recall, F1-Score, AUC
2. Generate ROC curves.
3. Visualize performance metrics.

Step 4: Statistical Significance Testing
1. Perform Wilcoxon Signed-Rank Test to compare predicted probabilities of the hybrid model vs. baseline Random Forest model.
2. Perform McNemar's Test to assess classification agreement and reduction in misclassification errors.
End of Algorithm

3.2 Data preprocessing

Data pre-processing is an essential component in building a strong predictive model that allows data quality, consistency of formats, and reliability for machine learning processes. The dataset was cleaned and pre-processed extensively to train the machine learning model. The target variable (i.e., the number of live births) was transformed into a binary classification, where 0 indicated no live births and 1 indicated at least one live birth. The categorical variables were one-hot encoded for use in different machine-learning algorithms. In addition, data stratification was performed to ensure an 80%-20% training-test split while maintaining a balanced class distribution.

The process starts with loading the IVF dataset; it then deals with missing values by either imputation or removal of feature(s). The approach to handling missing values involves a two-step process aimed at preserving data quality and model robustness. First, features with over 50% missing data were removed to avoid unreliable imputation of severely incomplete variables. Following this, the remaining missing values in the dataset were imputed using the median (for numerical features post-encoding) to ensure consistency and completeness before training. This combined strategy balances dimensionality control with the effective handling of data sparsity, aligning with the pre-processing goals outlined in this section. Missing values were identified with their treatment, keeping note of the loss of data with imputation; numerical features were assigned medians, while categorical features were assigned modes. Categorical variables were encoded, and the target variable was converted to binary for classification.

Moreover, through the synthetic minority oversampling technique, SMOTE provides the representation of minority classes owing to the class imbalance problem. To address RQ3, SMOTE was used to balance the dataset and improve the model fairness. Before SMOTE, the class distribution was 3.23:1; after SMOTE, it equalized to 1:1. Finally, in response to RQ2, Recursive Feature elimination with cross-validation (RFECV) was performed to retain the most informative predictors. This ensures that the input dataset is ready for machine learning models and improves predictive accuracy and generalizability.

3.3 Hybrid model development

The proposed methodology integrates multiple machine learning techniques to enhance the prediction accuracy of live birth outcomes in IVF treatments. By employing Stacking with Meta-Learners (Layered Learning), Weighted Hybrid Ensembles, Cascading Models (multi-stage refinement), Feature-Level Fusion with Autoencoder Networks, and SHAP-Enhanced XGBoost for post-hoc explainability, a comprehensive and robust predictive framework was developed to enhance both accuracy and interpretability in IVF live birth outcome prediction. This hybrid approach ensures improved model reliability and effectiveness in clinical decision-making. The algorithm outlined below outlines a hybrid machine learning framework that integrates ensemble learning, model stacking, and deep learning to improve live birth outcome predictions in IVF treatments. By using multiple predictive techniques, the proposed system ensures high accuracy and reliability in clinical decision making. A flow diagram of the Hybrid Model Development process is shown in Figure 2.

3.3.1 Model stacking with different meta-learners

To address RQ1, a hybrid ensemble approach was employed, particularly stacking with XGBoost as a meta-learner, to enhance the generalization across diverse IVF cases with non-linear patterns. Base learners such as Random Forest (RF), Support Vector Machine (SVM), and multilayer perceptron (MLP) were trained separately. Next, their predictions were used as input features for meta-learner feature construction using XGBoost, MLP, and Gradient Boosting equal to Gradient Boosting (GBM).

$$P_{final} = f_{meta}(P_{RF}, P_{SVM}, P_{MLP}) \quad (1)$$

where $\boldsymbol{P_{final}}$ is the final prediction, $\boldsymbol{P_{RF}, P_{SVM}, P_{MLP}}$ are the predictions from base the learners, and $\boldsymbol{f_{meta}}$ represents the meta-learner function.

A strict separation between the base learner training and meta-feature construction was implemented to ensure methodological rigor and prevent data leakage in the stacking ensemble. The full dataset was split into 80% training set and 20% held-out test set. Within the training data, the base models (Random Forest, SVM, MLP) were trained using 5-fold stratified cross-validation, and out-of-fold predictions were collected to construct meta-features. These meta-features, derived from unseen folds, were used to train the meta-learners (XGBoost, MLP, Logistic Regression), ensuring no overlap between the training and prediction phases.

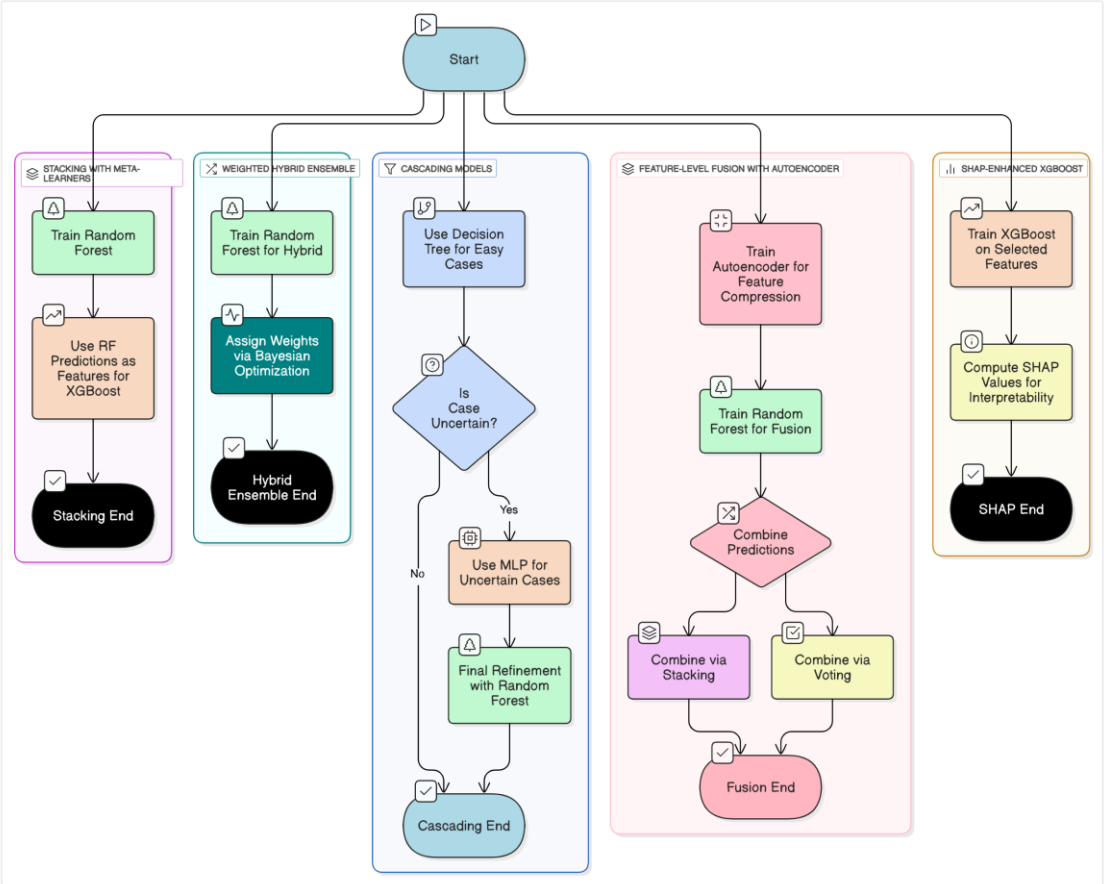


Figure 2: Flow diagram of hybrid model development step

For the final evaluation, base models were retrained on the complete resampled training data, and their predictions on the held-out test set were passed to the trained meta-learner, thereby enabling an unbiased assessment of the generalization performance on previously unseen data.

3.3.2 Weighted hybrid ensembles

A weighted ensemble approach was used to weigh the models based on their performances. Weight assignments were optimized using an optimization scheme such as Bayesian Optimization or Genetic Algorithms.

$$P_{final} = w_1 P_{RF} + w_2 P_{MLP} + w_3 P_{SVM} + w_4 P_{NBP} \quad (2)$$

where w1, w2, w3, and w4 are the optimized weights assigned to each model prediction.

3.3.3 Feature-level fusion with autoencoder networks

RQ5 is addressed using autoencoders for feature-level fusion, which captures non-linear relationships and compresses high-dimensional IVF data into informative latent features. This was used to perform the feature extraction. Random Forest, SVM, MLP were then run-on compressed feature representations to make predictions using stacking or weighted voting.

$$F_{compressed} = AE(X) \quad (3)$$

$$P_{final} = f_{meta}(P_{RF}, P_{SVM}, P_{MLP}) \quad (4)$$

where AE(X) denotes the autoencoder-transformed feature set.

3.3.4 Cascading models (multi-stage predictions)

To address RQ4, a two-stage cascading model was introduced to improve prediction reliability, particularly for borderline or uncertain cases. In the first stage, SimpleCart, a shallow Decision Tree that uses the Gini impurity criterion, was employed to classify cases that were easily separable. Predictions with low confidence were then escalated to include more complex classifiers. In the second stage, a Multilayer Perceptron (MLP) handled these uncertain cases, and samples with ambiguous probability scores (typically between 0.3 and 0.7) from the MLP were further passed to a Random Forest for final refinement. This cascading strategy ensures that uncertain predictions are progressively evaluated by increasingly powerful models, thereby enhancing classification robustness and clinical decision support.

$$P_{final} = f_{RF}\left(f_{MLP}\left(f_{DT}(X)\right)\right) \quad (5)$$

where, X denotes the input dataset.

3.3.5 SHAP-enhanced XGBoost

To improve both the predictive performance and interpretability, we implemented the SHAP-enhanced XGBoost model. XGBoost is a powerful gradient boosting algorithm widely used for structured data classification tasks. However, the decision-making process is often considered a "black box" because of the complexity of tree-based ensembles. To overcome this challenge, we integrated the SHAP into the XGBoost pipeline. SHAP is a unified framework based on cooperative game theory that attributes a model's prediction to each feature, thus offering instance-level interpretability.

For a specific prediction $\hat{y}_i$, the SHAP framework decomposes the output as:

$$\hat{y}_i = \phi_0 + \sum_{j=1}^{n} \emptyset_j^{(i)} \quad (6)$$

where ϕ_0 is the expected value of the model's output over the training data, and $\emptyset_j^{(i)}$ is the SHAP value representing the contribution of feature j for instance i.

Table 2 summarizes the internal architecture of the proposed hybrid machine learning models. It elucidates the model components, feature extraction, training, and optimization for all individual models. It also specifies the activation functions and decision logic at lower levels of detail and linkage, thereby illustrating the interactions of different models within each hybrid framework.

3.4 Hyperparameter tuning

The effectiveness of the proposed hybrid models is not solely determined by their architectural design, but also by the precision of the hyperparameter optimization, which directly addresses RQ6. To ensure robust generalization and predictive reliability, a systematic hyperparameter-tuning process was conducted using cross-validation of resampled training data. This process aims to strike a balance between model complexity, overfitting control, and computational efficiency.

Different tuning strategies were applied based on the model type and complexity. Grid Search Cross-Validation (GridSearchCV with 5-fold stratified CV) was employed for the baseline Logistic Regression model, stacking meta-learners (XGBoost, Neural Network, Logistic Regression), and an autoencoder-based classifier. For SHAP-enhanced XGBoost, a more efficient Random Search Cross-Validation (RandomizedSearchCV with 5-fold stratified CV) was adopted to explore a broader parameter space. The Weighted Hybrid Ensemble leveraged Bayesian Optimization (Bayesian optimization) was used to determine the optimal model weights, assessed via an inner 3-fold stratified cross-validation loop.

All tuning strategies prioritize the ROC AUC score as the primary evaluation metric to guide the selection of optimal parameter combinations. The final tuned hyperparameters for each model are summarized in Table 3, and collectively contribute to the superior predictive performance and reliability of the proposed hybrid framework.

This study utilized a modular implementation framework in Python 3.10, leveraging multiple machine-learning libraries to ensure consistency and reproducibility across models. Specifically, scikit-learn (version 1.6.1) was employed for traditional classifiers, ensemble techniques, and pre-processing tasks; TensorFlow (version 2.18.0) via the Keras API was used to design and train the autoencoder model; and XGBoost (version 2.1.4) was used to implement gradient boosting algorithms. These tools collectively support the development, tuning, and evaluation of proposed hybrid models in a unified pipeline.

3.5 Model evaluation and comparison

The various performance metrics, including accuracy, AUC, precision, recall and F1-score, were used for the comparative analysis of the proposed hybrid models. A ROC curve was constructed to assess the discrimination ability of the models, and radar charts and heat maps were constructed to compare their strengths and weaknesses. This evaluation framework enables a strong performance validation and interpretability for clinical deployment.

3.6 Statistical significance testing

To test the validity of the developed hybrid model, the significance test of Wilcoxon Signed-Rank Test was used to compare the predicted probabilities of the hybrid model with an existing baseline Random Forest model to evaluate the overall differences in performance. McNemar's test was applied to test the classification agreement, specifically to detect improvements in misclassification repair. These statistical tests confirmed that the observed performance improvements were not simply by chance.

With the methodology established for this study, the following section presents the empirical results and a comparative analysis of the proposed hybrid models. The comparative performance of these methods was evaluated based on evaluation metrics.

4 Result and discussion

4.1 Comparative performance of hybrid models

Once the machine learning models were built, the next critical step was their evaluation across multiple dimensions of performance: Accuracy, AUC, Precision, Recall, and F1-Score. Five models were evaluated in this study—Stacking with Meta-Learners (XGBoost), SHAP-enhanced XGBoost, Weighted Hybrid Ensemble, Autoencoder Fusion, and Cascading Model. The results are presented in Table 4, supplemented with ROC curves, radar charts, and heatmaps to allow for a comprehensive comparative analysis.

Among all models, SHAP-enhanced XGBoost demonstrated the best overall performance, achieving an accuracy of 0.997, AUC of 1.0, precision of 0.995, recall of 1.0, and F1-Score of 0.997. This clearly indicates that

the integration of SHAP explainability mechanisms not only preserves but also slightly improves the predictive capability compared to the original stacking approach. The Stacking (XGBoost) model followed closely, with an AUC of 0.999 and an F1-score of 0.985. The Weighted Hybrid model also performed well, while the Autoencoder Fusion model demonstrated clinically acceptable performance with high recall and reasonable precision. In contrast, the cascading model underperforms across most evaluation metrics.

Initially, some models exhibited signs of overfitting, as reflected by the unrealistically high AUC values during preliminary training. To correct this, multiple regularization techniques were applied: L2 regularization (for XGBoost, MLP, and Logistic Regression), reduced decision-tree depth, and early stopping in MLPs. Dropout was integrated into autoencoders to mitigate overfitting.

Table 2: Internal architecture details of hybrid models

Aspect	**Stacking with Meta-Learners**	**Weighted Hybrid Ensemble**	**Feature-Level Fusion**	**Cascading Model**
Model Type	Stacking Ensemble with Meta-Learners	Weighted Hybrid Ensemble	Autoencoder-based Feature Fusion with Classifier	Two-Stage Cascading Model
Architecture Details	Base models: Random Forest, SVM, MLP Meta-learners: XGBoost, MLP, Logistic Regression	Base models: Random Forest, MLP, SVM, Naïve Bayes Final output via Bayesian-weighted average	Autoencoder: Input → Encoding → Bottleneck → Decoding Classifier: Random Forest	Stage 1: Decision Tree (max_depth=3) Stage 2: MLP and Random Forest for refinement
Feature Engineering	RFECV for feature selection Standardization & SMOTE	RFECV for feature selection Standardization & Normalization	Encoded feature representation Random Forest trained on encoded outputs	Recursive Feature Elimination Stratified Data Splitting
Training Process	80–20 Train–Test Split 5-Fold Cross-Validation	Bayesian Optimization (10 initial pts, 20 iterations)	Autoencoder trained for dimensionality reduction Random Forest classifier trained separately	Stage 1 trained on full data Stage 2 trained on uncertain predictions (prob. = 0.3–0.7)
Optimization & Regularization	Early stopping (MLP) L2 regularization (α = 0.1 in MLP) XGBoost: learning_rate tuned (0.01–0.1), reg_lambda tuned (0.1–1)	L2 regularization in MLP Weights optimized via Bayesian search	Dropout (0.4 in encoding layer) ReLU for encoder, Sigmoid for decoder L2 regularization in RF	Dropout (0.5 in MLP) Early stopping in MLP
Activation Functions	MLP: ReLU (hidden), Logistic (output) SVM: Linear kernel Logistic Regression: Sigmoid	MLP: ReLU (hidden), Softmax (output) SVM: Linear kernel	Autoencoder: ReLU (encoding), Sigmoid (decoding)	MLP: ReLU (hidden), Logistic (output) Decision Tree: Gini criterion
Optimizers	MLP: Adam (default in sklearn) Logistic Regression: lbfgs XGBoost: Tree Booster (built-in)	MLP: Adam SVM and Naïve Bayes: Implementation-defined	Autoencoder: Adam Random Forest: Not Applicable	MLP: Adam Random Forest: Not Applicable Decision Tree: Not Applicable
Learning Rate	MLP: 0.001 (default) XGBoost: Tuned (0.01–0.1) Logistic Regression: Controlled by solver	MLP: 0.001 (default) SVM: Controlled by implementation	Autoencoder: 0.001 (default Adam) RF: Not Applicable	MLP: 0.001 (default) RF and DT: Not Applicable
Decision Flow	Base models predict first → meta-learners combine via stacking for final prediction	Individual model predictions weighted by performance → final prediction via weighted sum	Input passed through encoder-decoder → encoded output classified by Random Forest	Stage 1: Decision Tree filters easy predictions Stage 2: MLP and RF handle harder cases

Table 3: Hyperparameter tuning for hybrid models

Hybrid Model	Component	Hyperparameter	Value / Setting	Purpose
Model Stacking	Base Models	Random Forest – max_depth	5	Prevent overfitting, improve generalization
		SVM – C	0.1	Improve robustness, avoid excessive complexity
		MLP – hidden_layer_sizes	(20,)	Single hidden layer with 20 neurons
		MLP – max_iter	200	Limit training time
		MLP – alpha (L2 reg.)	0.1	Prevent overfitting
		MLP – early_stopping	Enabled (validation_fraction=0.2)	Stop training when validation performance stagnates
	Meta-Learners	XGBoost – n_estimators	25	Reduce overfitting and training time
		XGBoost – reg_lambda (L2 reg.)	1	Improve generalization
		Neural Network – hidden_layer_sizes	(10,)	Simpler meta-learner architecture
		Logistic Regression – penalty	L2	Improve model regularization
		Logistic Regression – C	0.1	Enhance generalization
Weighted Hybrid Ensemble	Base Models	Same as stacking model	Same as stacking model	-
	Weight Optimization	Search space for weights	(0,1)	Optimize ensemble performance
		Optimization method	Bayesian Optimization	Find optimal model weight distribution
		Initial points, iterations	10 initial points, 20 iterations	Improve accuracy
Cascadi-	Stage 1: Decision Tree	max_depth	3	Simplify early classification

	Stage 2: MLP, RF	Same as stacking model	Trained on uncertain cases only (p = 0.3 - 0.7)	Handle uncertain predictions efficiently
Feature-Level Fusion with Autoencoder	Autoencoder	encoded_dim	Min(30, half of input dim)	Reduce feature dimensionality
		Dropout rate	0.5	Prevent overfitting
		Training epochs, batch size	30 epochs, batch size = 32	Ensure stable training
	Random Forest	n_estimators, max_depth	25, 5	Train on compressed features

Table 4: Comparison of our approach with previous research

Study	Models Used	Accuracy	AUC	Precision	Recall	F1-Score
[13]	ANN + Deep Imaging	>0.75	N/A	N/A	N/A	N/A
[20]	XGBoost	N/A	0.839	N/A	N/A	N/A
[25]	Statistical Methods (Logistic Regression)	N/A	N/A	N/A	0.471	N/A
[26]	CNFE-SE (Ensemble)	0.87	0.87	N/A	0.82	0.92
[27]	Meta-analysis, Systematic Review	N/A	0.905	N/A	N/A	N/A
Proposed Approach	SHAP-enhanced XGBoost	0.997	1	0.995	1	0.997
	Stacking (XGBoost)	0.985	0.999	0.973	0.997	0.985
	Weighted Hybrid Ensemble	0.965	0.993	0.944	0.99	0.966
	Autoencoder Fusion	0.875	0.942	0.835	0.933	0.882
	Cascading Model	0.512	0.548	0.506	0.978	0.667

These corrections have led to more generalizable and realistic evaluation metrics.

Table 4 summarizes the performance of the proposed models and situates them within the context of the prior IVF prediction literature. It is evident that the SHAP-augmented and ensemble-based approaches significantly outperformed traditional statistical and individual machine learning methods.

4.2 Visual analysis of model discrimination power

The Receiver Operating Characteristic (ROC) curve depicted in Figure 3 visually assesses each model's classification capability. SHAP-enhanced XGBoost and Stacking (XGBoost) both achieved near-perfect AUCs (1.0 and 0.999, respectively), indicating excellent discriminative power. The Weighted Hybrid model performed slightly lower, with an AUC of 0.993, whereas the Autoencoder Fusion model reached 0.942. The Cascading model, with an AUC of 0.548, performed marginally better than the random guessing model.

These distinctions are critical in the context of IVF decision making. Higher AUC values support more confident treatment recommendations, especially in borderline cases, where accurate risk estimation is essential for guiding patients on whether to continue or adjust treatment strategies.

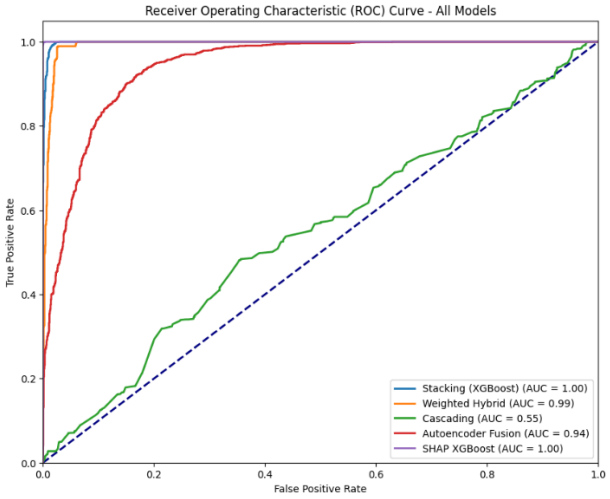


Figure 3: Evaluating model performance for ivf success prediction: roc curve analysis

4.3 Multi-Metric evaluation and comparative strengths

Figure 4 presents a radar chart that offers a simultaneous view of all the five-evaluation metrics across the models. The SHAP-enhanced XGBoost enclosed the widest area, confirming its balanced and robust predictive capability. Stacking (XGBoost) and Weighted Hybrid also showed excellent coverage. The moderate performance of the Autoencoder Fusion model is visible, whereas the cascading model reflects poor balance and lower values across most axes.

Figure 5, a heatmap, further confirms that the SHAP-enhanced XGBoost and Stacking models consistently outperform the others across metrics. Lighter shades in the

heatmap represent a stronger performance. The Cascading model's darker cells in Precision and Accuracy reaffirm its unsuitability for reliable clinical use.

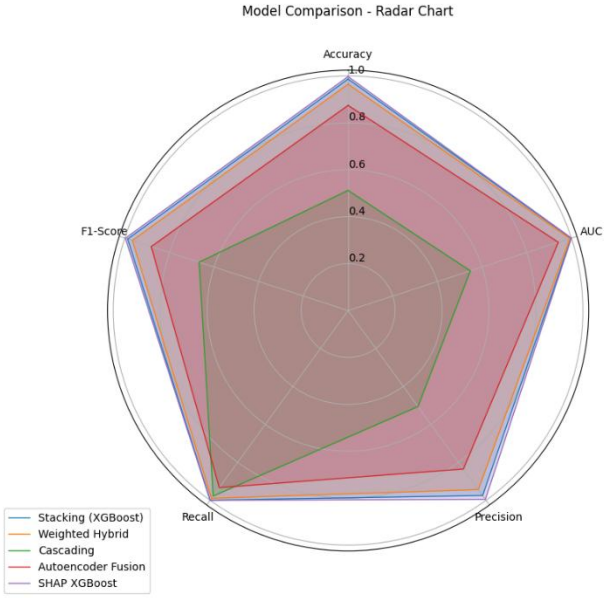


Figure 4: Assessing strengths and weaknesses of IVF prediction models – radar visualization

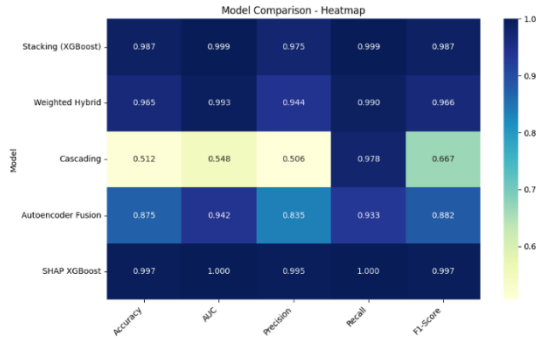


Figure 5: Performance heatmap of predictive models for IVF success prediction

In particular, SHAP-enhanced XGBoost excels in balancing high precision with perfect recall, making it ideal for clinical scenarios in which both false positives and false negatives must be minimized. Meanwhile, Autoencoder Fusion, despite good recall, suffers from potential information loss owing to aggressive feature compression. The Cascading model performs the weakest, likely because of the inability of the initial Decision Tree to filter uncertain cases effectively, leading to downstream overfitting and poor generalization.

Together, these hybrid models demonstrate clear advantages over the traditional standalone ML approaches. In particular, SHAP-enhanced XGBoost and Stacking models represent reliable, high-performance options for AI-assisted decision-making in IVF clinics, capable of providing explainable, patient-specific recommendations. Their high AUC and F1-scores make them suitable for real-world deployment, reducing the emotional and financial burden on patients through a more accurate prognosis.

4.4 Model interpretability with SHAP

To enhance transparency and enable the clinical interpretability of the predictions made by the stacking (XGBoost) model, we employed SHAP. SHAP provides a unified framework to quantify the contribution of each input feature to a model's prediction, making it particularly suitable for medical applications in which explainability is crucial.

Using TreeExplainer from the SHAP Python library, optimized for tree-based models such as XGBoost, we calculated the SHAP values on the meta-features derived from base learners (Random Forest, MLP, and SVM) in the stacking model. This allowed us to evaluate both the global feature influence and the local prediction explanations for individual patients.

The SHAP summary plot (Figure 6) illustrates the average magnitude and direction of the SHAP values for each meta-feature across all the predictions. It is evident that the Random Forest_Stacking output consistently contributes the most to the model's predictions, followed by MLP_Stacking, whereas SVM_Stacking has a minimal impact. This aligns with prior performance evaluations, confirming that Random Forest serves as the most informative base learner in the stacking ensemble.

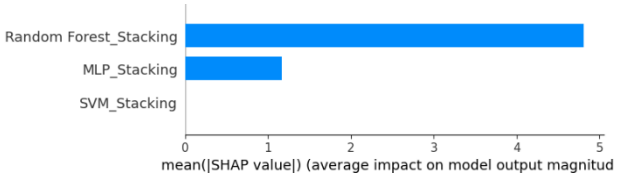


Figure 6: SHAP Summary Plot of Meta-Feature Contributions in Stacking (XGBoost)

To complement global interpretability, Figure 7 presents a SHAP force plot for a representative instance (instance 0). The base value of −0.01528 represents the average model output before any feature influence. In this instance, the prediction shifted to f(x) = 2.14, primarily driven by

- Random Forest_Stacking = 0.8134, and
- MLP_Stacking = 0.7444

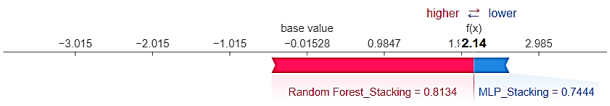


Figure 7: SHAP Force Plot of a Representative Patient Prediction

These values collectively pushed the model output toward a high probability of successful live births. The absence of the SVM_Stacking influence indicates its negligible role in this case.

Together, these SHAP visualizations bridge the gap between high-performance AI models and human decision-making.

- Highlighting the dominant drivers of model predictions.
- Enabling clinicians to interpret individual patient outcomes.
- Building trust in model outputs, particularly for borderline or high-risk cases.

This approach affirms that Stacking with XGBoost, when combined with SHAP-based post-hoc explainability, not only offers exceptional accuracy but also supports clinically meaningful, interpretable predictions for IVF success.

4.5 Generalization and overfitting analysis via learning curves

To evaluate the generalization capability of each proposed hybrid model and address potential overfitting, we analyzed learning curves plotting training and validation error (1 - accuracy) across incremental training set sizes (Figure 8).

The stacking model with the XGBoost meta-learner exhibited the most stable and lowest error rates, with training and validation curves converging closely throughout, thus validating its AUC of 0.999 and accuracy of 0.985. Similarly, SHAP-enhanced XGBoost showed robust generalization, confirming that integrating explainability did not compromise the predictive performance.

The cascading model also maintained tight training-validation alignment, reflecting its ability to progressively handle easy and difficult cases. In contrast, the autoencoder fusion and weighted hybrid models showed higher variance, especially at mid-level training sizes, but stabilized with full training data. These results demonstrate that although all models generalize well, ensemble-based stacking consistently outperforms the others in terms of reliability and predictive robustness. These findings confirm that the reported high performance is not a result of overfitting, but rather due to strong architectural generalization supported by regularization, SMOTE-based balancing, and effective feature engineering.

4.6 Statistical validation and clinical relevance

To further validate that the proposed Stacking with Meta-Learners (XGBoost) hybrid model significantly outperforms traditional machine learning approaches, a comparative analysis was performed, which resulted in a baseline Random Forest model. To assess the statistical significance and validate the observed enhancements, two non-parametric statistical tests were employed: the Wilcoxon Signed-Rank Test, and McNemar's test. The Wilcoxon Signed-Rank Test was used to investigate the differences in the predicted probabilities between the hybrid and baseline models, which allowed us to evaluate their relative performance independent of the distribution. The output showed a test statistic of 20.021 and an extremely low p-value ($p = 1.69 \times 10^{-11}$), with strong evidence (overwhelming or red) of the prediction differences between hybrid and baseline models being significant, suggesting improved predictive power with the hybrid model.

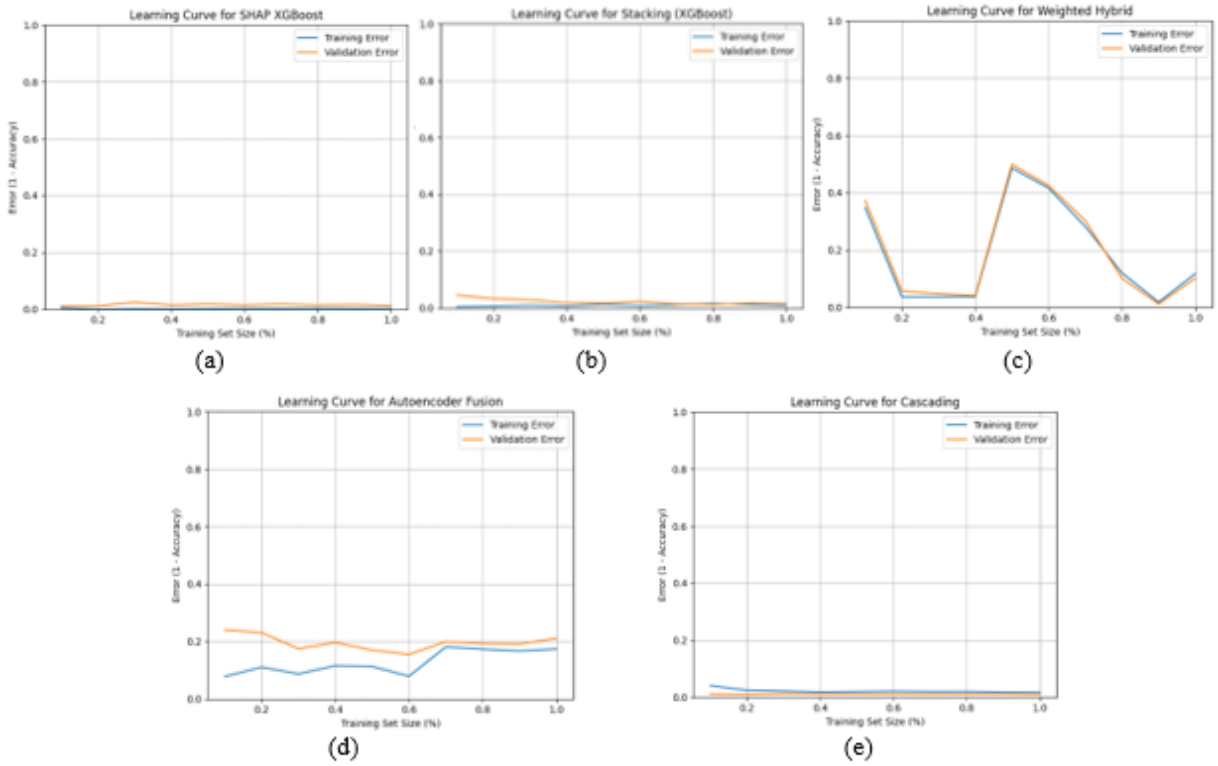


Figure 8: Learning curves showing training vs. validation error across five hybrid models. (a) SHAP-enhanced XGBoost (b) Stacking (XGBoost) (c) Weighted Hybrid Ensemble (d) Autoencoder Fusion (e) Cascading Model.

Furthermore, McNemar's test, which is limited to misclassified cases, was performed to assess the classification agreement between the two models. The test statistic was 20.02 with p-value 7.66×10^{-6} confirming that a significant number of misclassifications from the baseline Random Forest model were corrected by the hybrid model. This indicates a significant improvement in the classification performance, especially when differentiating between successful and unsuccessful IVF cases.

Thus, utilizing these comparative statistical tests provides powerful evidence that stacking with the Meta-Learners (XGBoost) hybrid methodology is superior to conventional machine learning approaches, and enables us to extrapolate this finding with a high level of statistical confidence, further promoting the reliability and clinical applicability of the proposed hybrid model for IVF success prediction. The hybrid model's outperformance further confirms its predictive power and underscores its potential to inform personalized ART treatment.

To further validate the robustness of our hybrid framework, an ablation study was conducted to systematically quantify the contribution of each model component. As presented in Table 5, the removal of individual components resulted in measurable performance degradation, with more pronounced drops observed when multiple components were simultaneously excluded. In particular, the absence of SMOTE and stacking consistently led to lower F1-scores, reflecting their critical roles in handling class imbalance and enabling meta-level learning. Although the removal of RFECV and Bayesian optimization resulted in smaller declines, their contributions to feature selection stability and model tuning remained evident. Notably, the complete removal of all core components led to a breakdown in classification performance, confirming the necessity of each module. Overall, the ablation results demonstrate that the hybrid architecture is not only modular but also synergistic, and each element significantly enhances the model's robustness and predictive reliability.

Table 5: Ablation study evaluating the contribution of individual components to the performance of the hybrid IVF outcome prediction model

Configuration	Accuracy	AUC	F1-Score
Full Model (Stacking + Bayes Opt)	0.989	0.9991	0.9893
- SMOTE	0.9845	0.9987	0.9681
- RFECV	0.9879	0.9993	0.9880
- Stacking (Weighted Hybrid)	0.9813	0.9939	0.9817
- Bayesian Optimization (Stacking + Simple LR)	0.9810	0.9941	0.9813
- SMOTE, - RFECV	0.988	0.9996	0.9751
- SMOTE, - Stacking (Weighted Hybrid)	0.9755	0.9930	0.9505
- SMOTE, - Bayesian Optimization (Stacking + Simple LR)	0.9755	0.9903	0.9504
- RFECV, - Stacking (Weighted Hybrid)	0.9840	0.9948	0.9842
- RFECV, - Bayesian Optimization (Stacking + Simple LR)	0.9826	0.9937	0.9829
- Stacking, - Bayesian Optimization (Simple Averaging)	0.9473	0.9933	0.9496
- SMOTE, - RFECV, - Stacking (Weighted Hybrid)	0.9645	0.9898	0.9298
- SMOTE, - RFECV, - Bayesian Optimization (Stacking + Simple LR)	0.9755	0.9911	0.9499
- SMOTE, - Stacking, - Bayesian Optimization (Simple Averaging)	0.973	0.9891	0.9458
- RFECV, - Stacking, - Bayesian Optimization (Simple Averaging)	0.9456	0.9924	0.9481
- All Components (Simple Averaging)	0.7635	0.9898	0.0000

4.7 Addressing research gaps through hybrid machine learning model

To systematically illustrate how the proposed hybrid models address the primary research challenges present in IVF prediction, a mapping between the defined research questions and how hybrid models contribute to resolving them is shown in Table 6.

These models overcome the individual challenges of generalization, feature selection, class imbalance, uncertainty quantification, deep feature representation, and hyperparameter tuning by capturing the complementary strengths of different machine-learning integration of diverse classifiers, with optimal feature selection from within the weighted hybrid ensemble using Bayesian Optimization. Autoencoder fusion plays a role in the extraction of deep feature representations as well as in improving model interpretability and performance. Predictive performance is improved by flexibility in a cascade model, where predictions are iteratively fine-tuned based on uncertainty estimates; thus, cases that are harder to predict receive more attuned processing. The structured hybrid modelling approach adopted in this study provides a robust and scalable predictive framework for assisted reproductive technologies. The proposed methodologies holistically address existing research gaps in reproductive management, thereby enabling the development of accurate and trustworthy decision-support systems in reproductive medicine.approaches. Stacking with XGBoost uniquely generalizes across complex IVF datasets owing to the seamless

Table 6: Mapping research questions to hybrid models

Research Gap Questions	Stacking with XGBoost	Weighted Hybrid Ensemble	Autoencoder Fusion	Cascading Model
RQ1: How can predictive models generalize better for complex IVF data?	Combines diverse classifiers to improve generalization.	Uses weighted voting to optimize predictions across models.	Extracts deep feature representations to enhance generalization.	Refines predictions through cascading decision layers.
RQ2: How can feature selection be optimized for IVF prediction?	Uses RFECV for selecting the most relevant features.	Bayesian Optimization fine-tunes feature importance.	Autoencoder extracts hidden features and reduces dimensionality.	Feature selection is refined at multiple classification stages.
RQ3: How can we handle class imbalances in IVF datasets?	Applies SMOTE to rebalance the dataset.	Uses SMOTE-based weighting in hybrid ensemble learning.	Learns balanced representations using autoencoder transformations.	Adjusts for class imbalance dynamically at different stages.
RQ4: How can we quantify the uncertainty in IVF predictions?	Uses confidence scores from multiple models to assess uncertainty.	Weighted ensemble predictions provide confidence estimates.	Autoencoders identify ambiguous cases based on representation patterns.	Uses cascading classifiers to handle uncertain predictions adaptively.
RQ5: How can deep feature representations be utilized for improved prediction?	Meta-learner integrates deep patterns learned by base models.	Feature-weighted hybrid models leverage complex feature interactions.	Uses autoencoder for deep feature extraction and fusion.	Identifies key deep features dynamically across classification stages.
RQ6: How can hyperparameter tuning be improved to achieve better performance?	Applies Bayesian Optimization to fine-tune meta-learner parameters.	Uses Bayesian search to optimize ensemble weight distribution.	Optimizes feature learning through autoencoder parameter tuning.	Cascading logic ensures best-performing hyperparameters at each stage.

5 Conclusion

This study introduced novel hybrid machine-learning methodologies to enhance the predictability, reliability, and interpretability of live birth outcomes in ART. By integrating multiple predictive paradigms, including Stacking with Meta-Learners (XGBoost), Weighted Hybrid Ensembles, Cascading Models, Feature-Level Fusion using Autoencoder Networks, and SHAP-Enhanced XGBoost, the proposed framework effectively addressed key challenges such as data heterogeneity, nonlinearity, limited interpretability, and class imbalance inherent in IVF prediction tasks. Among the models evaluated, Stacking with Meta-Learners (XGBoost) achieved the highest performance (AUC = 0.999, accuracy = 0.985), substantially outperforming traditional statistical and standalone machine learning approaches.

The robustness and generalizability of the proposed models were further validated through a rigorous comparative analysis against a baseline Random Forest model utilizing RFECV. Statistical validation using the Wilcoxon Signed-Rank Test and McNemar's test (both $p < 0.05$) confirmed the significant performance gains of the hybrid models, underscoring their potential to support personalized IVF treatment planning and clinical decision-making.

As an avenue for future research, further exploration of the latent feature space of the Autoencoder Fusion model using dimensionality reduction techniques such as t-distributed Stochastic Neighbor Embedding (t-SNE) and Uniform Manifold Approximation and Projection (UMAP) may offer deeper insights into feature separability, thereby enhancing both model interpretability and predictive accuracy. Additionally, we aim to perform prospective validation using real-time patient data and assess the integration of the proposed hybrid models into a Clinical Decision Support System (CDSS). This will facilitate deployment feasibility evaluations and strengthen the clinical applicability of AI-driven systems in IVF treatment workflows. Ultimately, the widespread adoption of such intelligent systems will require careful attention to explainable AI (XAI) integration, clinical multicenter validation, and adherence to ethical and regulatory standards to ensure trustworthy, patient-centered reproductive care.

Ethics approval

No medical intervention was performed in couples' biomedical or behavioral routines. Since this study was only about data analysis and no human subjects were involved, an Institutional Review Board (IRB) was not considered necessary. All procedures were strictly performed in accordance with the ethical guidelines.

Data availability

It is publicly available and can be accessed via the direct download link provided in [31]. This dataset was previously used in a study by Goyal et al. [32].

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] K. Sfakianoudis, E. Maziotis, S. Grigoriadis, A. Pantou, G. Kokkini, A. Trypidi, P. Giannelou, A. Zikopoulos, I. Angeli, T. Vaxevanoglou, K. Pantos, M. Simopoulou, Reporting on the Value of Artificial Intelligence in Predicting the Optimal Embryo for Transfer: A Systematic Review including Data Synthesis, Biomedicines. vol. 10, no. 3, p. 697, Mar. 2022. https://doi.org/10.3390/biomedicines10030697

[2] L. Sun, J. Li, S. Zeng, Q. Luo, H. Miao, Y. Liang, L. Cheng, Z. Sun, W.H. Tai, Y. Han, Y. Yin, K. Wu, K. Zhang, Artificial intelligence system for outcome evaluations of human in vitro fertilization-derived embryos, Chin Med J (Engl). vol. 137, no. 16, p. 1939–1949, Aug. 2024. https://doi.org/10.1097/CM9.0000000000003162

[3] L. Rienzi, D. Cimadomo, A. Vaiarelli, G. Gennarelli, J. Holte, C. Livi, M. Aura Masip, P. Uher, G. Fabozzi, F.M. Ubaldi, Measuring success in IVF is a complex multidisciplinary task: time for a consensus?, Reprod Biomed. vol. 43, no. 5, p. 775–778, Nov. 2021. https://doi.org/10.1016/j.rbmo.2021.08.012

[4] S.M. Diakiw, J.M.M. Hall, M. VerMilyea, A.Y.X. Lim, W. Quangkananurug, S. Chanchamroen, B. Bankowski, R. Stones, A. Storr, A. Miller, G. Adaniya, R. van Tol, R. Hanson, J. Aizpurua, L. Giardini, A. Johnston, T. Van Nguyen, M.A. Dakka, D. Perugini, M. Perugini, An artificial intelligence model correlated with morphological and genetic features of blastocyst quality improves ranking of viable embryos, Reprod Biomed. vol. 45, no. 6, p. 1105–1117, Dec. 2022. https://doi.org/10.1016/j.rbmo.2022.07.018

[5] E. Taeidi, A. Ranjbar, F. Montazeri, V. Mehrnoush, and F. Darsareh, Machine Learning-Based Approach to predict Intrauterine Growth Restriction, Cureus, vol 15, no. 7, p. e41448, Jul. 2023, https://doi.org/10.7759/cureus.41448

[6] J. Berntsen, J. Rimestad, J. T. Lassen, D. Tran, and M. F. Kragh, Robust and generalizable embryo selection based on artificial intelligence and time-lapse image sequences, PLoS ONE, vol. 17, no. 2, p. e0262661, Feb. 2022, https://doi.org/10.1371/journal.pone.0262661

[7] Z. Li, K. Kamnitsas, B. Glocker, Analyzing Overfitting Under Class Imbalance in Neural Networks for Image Segmentation, IEEE Trans Med Imaging. vol. 40, no. 3, p. 1065–1077, Mar. 2021. https://doi.org/10.1109/TMI.2020.3046692

[8] T. Gong, K. Chen, L. Zhang, J. Wang, Debiased Contrastive Curriculum Learning for Progressive Generalizable Person Re-Identification, IEEE Transactions on Circuits and Systems for Video Technology vol. 33, no. 10, p. 5947–5958, Oct. 2023. https://doi.org/10.1109/TCSVT.2023.3262832

[9] D. Velasquez, E. Perez, X. Oregui, A. Artetxe, J. Manteca, J.E. Mansilla, M. Toro, M. Maiza, B. Sierra, A Hybrid Machine-Learning Ensemble for Anomaly Detection in Real-Time Industry 4.0 Systems, IEEE Access. vol. 10, p. 72024–72036, 2022. https://doi.org/10.1109/ACCESS.2022.3188102

[10] M. Casalechi, M. Reschini, M.C. Palermo, G. Di Stefano, P. Vercellini, L. Benaglia, E. Somigliana, P. Viganò, Is endometrial receptivity affected in women with endometriosis? Results from a matched pair case-control study of assisted reproductive technology treatments, Reprod Biomed. vol. 47, no. 6, p. 103414, Dec. 2023. https://doi.org/10.1016/j.rbmo.2023.103414

[11] A. Goyal, M. Kuchana, K.P.R. Ayyagari, Machine learning predicts live-birth occurrence before in-vitro fertilization treatment, Sci Rep. vol. 10, no. 1, p. 20925, Dec. 2020. https://doi.org/10.1038/s41598-020-76928-z

[12] Y.O. Martirosyan, D.N. Silachev, T.A. Nazarenko, A.M. Birukova, P.A. Vishnyakova, G.T. Sukhikh, Stem-Cell-Derived Extracellular Vesicles: Unlocking New Possibilities for Treating Diminished Ovarian Reserve and Premature Ovarian Insufficiency, Life. vol. 13, no. 12, p. 2247, Nov. 2023. https://doi.org/10.3390/life13122247

[13] C. Siristatidis, S. Stavros, A. Drakeley, S. Bettocchi, A. Pouliakis, P. Drakakis, M. Papapanou, N. Vlahos, Omics and Artificial Intelligence to Improve In Vitro Fertilization (IVF) Success: A Proposed Protocol, Diagnostics. vol. 11, no. 5, p. 743, Apr. 2021. https://doi.org/10.3390/diagnostics11050743

[14] S. Dehghan, R. Rabiei, H. Choobineh, K. Maghooli, M. Nazari, and M. Vahidi-Asl, Comparative study of machine learning approaches integrated with genetic algorithm for IVF success prediction, PLoS ONE, vol. 19, no. 10, p. e0310829, Oct. 2024, doi: https://doi.org/10.1371/journal.pone.0310829

[15] Z. J. Pavlovic, V. S. Jiang, and E. Hariton, Current applications of artificial intelligence in assisted reproductive technologies through the perspective of a patient's journey, Current Opinion in Obstetrics & Gynecology, vol. 36, no. 4, pp. 211–217, Apr. 2024, https://doi.org/10.1097/gco.0000000000000951

[16] Y. Hew, D. Kutuk, T. Duzcu, Y. Ergun, and M. Basar, Artificial intelligence in IVF Laboratories: Elevating outcomes through precision and efficiency, Biology, vol. 13, no. 12, p. 988, Nov. 2024, https://doi.org/10.3390/biology13120988

[17] A. Almomani, K. Nahar, M. Alauthman, M.A. Al-Betar, Q. Yaseen, B.B. Gupta, Image cyberbullying detection and recognition using transfer deep machine learning, International Journal of Cognitive Computing in Engineering. vol. 5, p. 14–26, 2024, doi: 10.1016/j.ijcce.2023.11.002. https://doi.org/10.1016/j.ijcce.2023.11.002

[18] P.H. Vuong, L.H. Phu, T.H. Van Nguyen, L.N. Duy, P.T. Bao, T.D. Trinh, A bibliometric literature review of stock price forecasting: From statistical model to deep learning approach, Sci Prog. vol. 107, no. 1, p. 1-31, Jan. 2024. https://doi.org/10.1177/00368504241236557

[19] J. Yao, X. Zhang, W. Luo, C. Liu, L. Ren, Applications of Stacking/Blending ensemble learning approaches for evaluating flash flood susceptibility, International Journal of Applied Earth Observation and Geoinformation. vol. 112, p. 102932, Aug. 2022. https://doi.org/10.1016/j.jag.2022.102932

[20] Q. Xi, Q. Yang, M. Wang, B. Huang, B. Zhang, Z. Li, S. Liu, L. Yang, L. Zhu, L. Jin, Individualized embryo selection strategy developed by stacking machine learning model for better in vitro fertilization outcomes: an application study, Reproductive Biology and Endocrinology. vol. 19, no. 1, p. 53, Dec. 2021. https://doi.org/10.1186/s12958-021-00734-z

[21] Z. Han, J. Zhao, H. Leung, K.F. Ma, W. Wang, A Review of Deep Learning Models for Time Series Prediction, IEEE Sens J. vol. 21, no. 6, p. 7833–7848, Mar. 2021. https://doi.org/10.1109/JSEN.2019.2923982

[22] C. Luo, J. Zheng, T. Li, H. Chen, Y. Huang, X. Peng, orthogonally constrained matrix factorization for robust unsupervised feature selection with local preserving, Inf Sci (N Y). vol. 586, p. 662–675, Mar. 2022. https://doi.org/10.1016/j.ins.2021.11.068

[23] X. Mi, B. Zou, F. Zou, J. Hu, Permutation-based identification of important biomarkers for complex diseases via machine learning models, Nat Commun. vol. 12, no. 1, p. 3008, May 2021. https://doi.org/10.1038/s41467-021-22756-2

[24] A.T. Tredennick, G. Hooker, S.P. Ellner, P.B. Adler, A practical guide to selecting models for exploration, inference, and prediction in ecology, Ecology. vol. 102, no. 6, p. e03336, Jun. 2021. https://doi.org/10.1002/ecy.3336

[25] J. Diao, G. Gao, Y. Zhang, X. Wang, Y. Zhang, Y. Han, A. Du, H. Luo, Caesarean section defects may affect pregnancy outcomes after in vitro fertilization-embryo transfer: a retrospective study, BMC Pregnancy Childbirth. vol. 21, no. 1, p. 487, Dec. 2021. https://doi.org/10.1186/s12884-021-03955-7

[26] S. Ranjbari, T. Khatibi, A. Vosough Dizaji, H. Sajadi, M. Totonchi, F. Ghaffari, CNFE-SE: a novel approach combining complex network-based feature engineering and stacked ensemble to predict the success of intrauterine insemination and ranking the features, BMC Med Inform Decis Mak. vol. 21, no. 1, p. 1, Dec. 2021. https://doi.org/10.1186/s12911-020-01362-0

[27] F. Del Giudice, F. Belladelli, T. Chen, F. Glover, E.A. Mulloy, A.M. Kasman, A. Sciarra, S. Salciccia, V. Canale, M. Maggi, M. Ferro, G.M. Busetto, E. De Berardinis, A. Salonia, M.L. Eisenberg, The association of impaired semen quality and pregnancy rates in assisted reproduction technology cycles: Systematic review and meta-analysis, Andrologia. vol. 54, no. 6, p. e14409, Jul. 2022. https://doi.org/10.1111/and.14409

[28] S. Wu, Y. Zhang, X. Wu, G. Hao, H. Ren, J. Qiu, Y. Zhang, X. Bi, A. Yang, L. Bai, J. Tan, Association between exposure to ambient air pollutants and the outcomes of in vitro fertilization treatment: A multicenter retrospective study, Environ Int. vol. 153, p. 106544, Aug. 2021. https://doi.org/10.1016/j.envint.2021.106544

[29] Y. Zou, Y. Pan, N. Ge, Y. Xu, R. Gu, Z. Li, J. Fu, J. Gao, X. Sun, Y. Sun, Can the combination of time-lapse parameters and clinical features predict embryonic ploidy status or implantation? Reprod Biomed. vol. 45, no. 4, p. 643–651, Oct. 2022. https://doi.org/10.1016/j.rbmo.2022.06.007

[30] K. Koc, A.P. Gurgun, Scenario-based automated data pre-processing to predict severity of construction accidents, Autom Constr. vol. 140, p. 104351, Aug. 2022. https://doi.org/10.1016/j.autcon.2022.104351

[31] hfea.gov.uk, 2025. https://www.hfea.gov.uk/media/2667/ar-2015-2016-xlsb.xlsb (accessed Jan 15, 2025)

[32] A. Goyal, M. Kuchana, and K. P. R. Ayyagari, Machine learning predicts live-birth occurrence before in-vitro fertilization treatment, Scientific Reports, vol. 10, no. 1, Dec. 2020, https://doi.org/10.1038/s41598-020-76928-z