IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 September 2023, accepted 15 November 2023, date of publication 24 November 2023,
date of current version 1 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336701

RESEARCH ARTICLE

A Privacy-Preserving Method Based on Artificial Immune Computing in MCS

HAO LONG[1], **JIAWEI HAO**[1], **SHUKUI ZHANG**[2], **YANG ZHANG**[2], **AND LI ZHANG**[2]

[1]School of Information Engineering, Xuzhou College of Industrial Technology, Xuzhou, Jiangsu 221140, China
[2]School of Computer Science and Technology, Soochow University, Suzhou, Jiangsu 215006, China

Corresponding author: Shukui Zhang (zhangsk@suda.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62072321 and Grant 61672370, in part by the Jiangsu Province 333 Talents Training Project Youth Talent Program, in part by the Doctoral Teaching and Scientific Research Project of the Xuzhou College of Industrial Technology, in part by the Xuzhou Key Research and Development Plan (Modern Agriculture) Project "Research on Key Technology of Meat Intensive Processing Quality Monitoring," and in part by the Jiangsu Natural Science Foundation General Project under Grant BK20231206.

ABSTRACT Due to the widespread use of mobile intelligent terminal devices, Mobile Crowd Sensing (MCS) applications have gained significant research attention. However, ensuring users privacy remains a critical challenge, as it can hinder users' willingness to participate actively in tasks. To address the limitations of existing differential privacy protection methods, this paper proposes a novel privacy protection approach based on Artificial Immune Computing (AICppm). Specifically, private information is concealed within a masking carrier, and data scrambling is avoided. The proposed method involves two main steps: first, a carrier preprocessing approach based on a high-pass filter bank is designed to identify candidate positions for perturbation. Then, a carrier steganography algorithm based on multi-objective optimization is used, transforming the perturbation position into an antibody using the artificial immune algorithm. By iteratively searching for antibodies with higher fitness, the optimal perturbation of the offspring population is identified using the improved Strength Pareto Evolution Algorithm (SPEA2). The experimental results demonstrate that the proposed algorithm can withstand the attacks of malicious steganalysis tools, preserving the integrity of the sensing data and enabling real-time processing of private information.

INDEX TERMS Mobile crowd sensing, privacy-preserving, edge computing, artificial immune computing, sensing data.

I. INTRODUCTION

Currently, the MCS task collects a significant amount of sensitive data, particularly the user's identity and location information, putting the user's privacy at risk of being leaked. The method of protecting data through differential privacy by scrambling data with noise is currently widely used. This method hides sensitive information by distorting the perception data collected from users. However, it has several drawbacks, including high time and space complexity, computational overhead, and the possibility of information loss and data distortion due to noise addition [1]. In reality, only a small percentage of the sensing data contains private information. Therefore, it is possible to extract this private information and transmit it covertly to protect the user's sensitive data. To achieve this, we propose using data steganography technology to conceal the user's private information in multimedia carriers during transmission, thus preventing attackers from accessing it.

Given that MCS imposes stringent requirements on real-time performance and computing resources [2], mobile edge computing is employed to enable data steganography. Mobile devices are limited in terms of computing resources, and cannot handle complex applications and large volumes of data. By employing mobile edge computing, the complex computing processing can be offloaded to the edge server of the mobile terminal, which is closer to the data source

The associate editor coordinating the review of this manuscript and approving it for publication was Huan Zhou.

and users, thereby facilitating the deployment of complex applications on the mobile terminal. Mobile edge computing enables the identification of redundant locations in the multimedia carrier that are not noticeable to human perception systems [3], through low-latency, low-bandwidth, and high-performance computing. These locations on the mobile edge server can be used for embedding sensitive user information, which effectively mitigates the communication delays and memory resource imbalances that data steganography can cause [4].

Once data steganography is assigned to an edge server, it becomes challenging to guarantee the data transmission time. This is especially true when imperceptibility, capacity, and security (defined in this article as privacy entropy) are essential indicators for data steganography. To address this challenge, we have analyzed and modeled the transmission time, imperceptibility, capacity, and privacy entropy collectively as a multi-objective optimization problem. To solve this problem, we use the artificial immune algorithm based on the principle of natural defense. This algorithm offers several advantages such as anti-noise, unsupervised learning, memory, self-organization, and other evolutionary learning methods. Therefore, in this article, we propose to use the artificial immune algorithm to handle the multi-objective optimization problem of data steganography. The implementation module diagram of AICppm is shown in Figure 1.

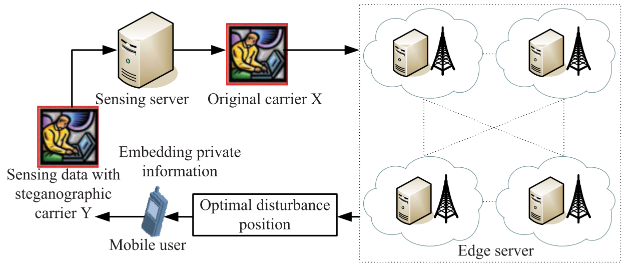
Sensing server
Original carrier X
Sensing data with steganographic carrier Y
Embedding private information
Optimal disturbance position
Mobile user
Edge server

FIGURE 1. AICppm module diagram.

To optimize conflicting goals and achieve privacy protection for perception data in MCS, a privacy protection method called AICppm based on artificial immune calculation is proposed. This method embeds user's private information in masked multimedia carriers, such as videos, audios, images, web pages, and text files, while ensuring the quality of the carrier. The proposed method has several key steps. Firstly, a carrier preprocessing method is proposed based on high-pass filter bank. This method uses multi-directional and non-directional high-pass filter bank to preprocess the masked carrier and aggregates the filter residuals to form candidate positions for disturbance. The aggregated residuals correspond to noise and texture regions that are difficult to model. Secondly, a carrier steganography algorithm based on multi-objective optimization is proposed. This algorithm defines a multi-objective optimization problem by taking embedding capacity and task migration probability as constraints and minimizing imperceptibility and task average transmission time while maximizing privacy entropy. Finally, the artificial immune algorithm is used to search for antibodies with higher adaptability through feature extraction and adaptive evolution operator. SPEA2 is used to solve the optimal perturbation of the offspring population. The proposed algorithm is implemented on a mobile edge server to meet the real-time and bandwidth requirements of MCS. Experimental results show that the proposed algorithm can resist attacks of malicious attackers' steganalysis tools, avoid the scrambling of perception data, and realize the real-time processing of private information. Compared with similar methods, it performs better in terms of imperceptibility, average transmission time, and privacy security. We have made significant contributions in this research project, which can be summarized as follows:

- For the first time, we have applied the artificial immune algorithm to the MCS network, utilizing its feature extraction capabilities and adaptive evolution operator to search for antibodies with higher adaptability. We use SPEA2 to solve the optimal perturbation of the progeny population, achieving hidden protection of private information.
- We introduce the mobile edge server to search for the disturbance location of the masked carrier, addressing the problem of insufficient bandwidth and real-time performance of mobile networks and smart devices.
- We have theoretically and experimentally verified and analyzed that the proposed method can resist the attacks of malicious attackers' steganalysis tools, while avoiding the scrambling of the sensing data and enabling the real-time processing of private information.

The rest of this paper is organized as follows: Section II presents related works, Section III introduces the system model and analyzes the relevant problems of the proposed method, Section IV describes the proposed privacy-preserving method based on artificial immune computing in MCS, Section V evaluates the method's performance through extensive experiments, and finally, Section VI concludes the paper and presents future work.

II. RELATED WORK

MCS has garnered significant research interest in various applications such as personalized recommendations, intelligent transportation, environmental monitoring, and health care. With just the utilization of smartphones, physical world sensing becomes achievable through MCS. Within smartphones, diverse sensors are already integrated, such as accelerometers, ambient temperature and humidity sensors, Global Positioning System (GPS), cameras, etc. By employing Bluetooth, cellular networks, or Wi-Fi, smartphones can establish connections with other devices or networks. As a result, users can readily employ their smartphones anytime, anywhere, to perceive, gather, process, and disseminate ambient data. Ang et al. [5] conducted a comprehensive investigation of this new paradigm of MCS Internet of

Things (IoT) from four different perspectives: (1) The architecture of MCS IoT; (2) Trust, privacy, and security in MCS IoT for the masses; (3) Considerations for resources, sharing, storage, and energy in crowdsourced IoT for the masses; (4) Applications of crowd-sourced IoT for the masses. De et al. [6] designed a MCS-based physical distance monitoring model leveraging federated learning for pandemic. They proposed an edge-based MCS strategy for physical distance monitoring and taking initiative to alert people. Dimitriou et al. [7] has designed an MCS framework that enables users to submit data in a privacy-preserving manner and receive Bitcoin payments. It ensures the fairness of transactions in a completely trustless manner, eliminating the need for trust in third parties through reliance on the blockchain in contrast to traditional fair transaction protocols. Sun et al. [8] applied MCS to smart agriculture, extensively evaluated agricultural mobile crowd sensing, and provided insights for agricultural data collection solutions. In MCS applications, privacy concerns are the main obstacles to their development, and how to protect users' privacy information is the main focus of this article.

In 2018, prominent internet companies such as Apple, Google, and Facebook experienced privacy breaches, which has led to users becoming increasingly sensitive and aware of the importance of protecting their personal information. As a result, there has been a growing interest in privacy protection research, which is a critical component of the entire MCS network. Effective user privacy protection is also essential for attracting users to participate in perception tasks. While traditional wireless sensor networks have various technologies to protect user privacy, they are no longer suitable for the MCS network due to issues related to execution efficiency and computational complexity. Currently, the differential privacy method is the most widely used privacy protection method in the MCS system. This method involves adding random noise to the perception data before uploading it, which effectively disrupts the data and prevents malicious attackers from reconstructing it. Xiong et al. [9]. proposed a differential privacy protection algorithm for location data publishing applications that uses privacy location clustering and shrinking to hide participants' real location and frequency of visiting a certain location. Jin et al. [10]. developed a differential privacy protection method for data fusion that generates highly accurate aggregation results while maintaining user privacy. Fan et al. [11]. proposed a real-time differential multidimensional time series privacy protection framework to protect the privacy of different users. Meanwhile, Daniele et al. [12]. developed a privacy protection method for information scrambling based on a differential privacy method combined with a pre-filtering process to protect user privacy. Chen et al. [13]. proposed a data privacy protection method based on dynamic group management in a mobile-aware dynamic environment and introduced a data aggregation integrity verification protocol to verify the correctness of the results. However, scrambling the entire perception data can cause distortion of the data and require more computing and storage overhead, as the privacy information contained in the perception data itself is minimal. This article primarily addresses the issues arising from data perturbation in differential privacy protection methods, concealing users' privacy information within a masking carrier, thereby avoiding data perturbation and recovery.

Currently, an increasing number of researchers are recognizing the importance of protecting users' private information through the concealment of private data in hidden carriers. In one method proposed in the literature [14], an image steganography approach that uses the particle swarm optimization (PSO) algorithm has been developed to enhance the embedding capacity and data security. This method partitions the overlay image and the steganographic image into four parts and utilizes the particle swarm algorithm to efficiently calculate the fitness function dependent on the cost matrix. However, this method's complexity is relatively high as it depends on the speed of particles. Another image steganography approach, as proposed in [15], combines the strengths of visual saliency and SDS-based steganography technology and uses genetic algorithms to determine the optimal balance between pixel saliency and embedding capacity to reduce embedding distortion and increase embedding capacity. Nonetheless, the fixed crossover and mutation process in genetic algorithms can lead to degradation during the iterative search process of the population. To address the need for increased embedding capacity while maintaining steganographic image security, Joshi et al. [16] utilize DCT and its wavelet (DCTW) to embed in the image at an appropriate position without causing low-energy transformation regions through genetic algorithms. However, this approach's computational efficiency is limited. In contrast, artificial immune systems (AIS) have more applications in the fields of network intrusion detection, network diagnosis, and privacy protection due to their adaptive learning, memory, and recognition pattern characteristics. Li et al. [17] propose a new distributed intrusion detection method based on immune mobile agents, which utilizes the intelligence and mobility of mobile agents to address the issues of poor real-time performance and single point of failure in distributed intrusion detection systems. Currently, research institutions and university project teams worldwide have conducted investigations on security and privacy protection systems using various algorithms, models, and system designs based on immune function, immune system, immune theory, and immune agents. The AIS optimization process searches for solutions across the entire search space to avoid premature convergence of local minima, making artificial immune algorithms more robust than genetic algorithms and particle swarm algorithms. This article employs the artificial immune algorithm to search for the optimal perturbation position of the covert carrier and enhances the algorithm's computational efficiency and real-time performance through edge computing. The summary of related work is given below in Table 1.

TABLE 1. Summary of related work.

Ref. Works	Techniques	Contribution	Limitation
[9]	Differential privacy protection	Hide participants' real location	Conventional method
[10, 13]	Data fusion	Generate highly accurate aggregation results	High computational cost
[11]	Differential multidimensional time	Protect the privacy of different users	High computational cost
[12]	Information scrambling	Hide participants' real information	Cause distortion of the data
[14]	Particle swarm optimization	Enhance the data security	High complexity
[15, 16]	Genetic algorithms	hide participants' real location	Resulting in population degradation

III. SYSTEM MODEL AND PROBLEM DEFINITION

A. CORRELATION THEORY

In the implementation process of the existing algorithm, one performance index is prioritized at the expense of others. Consequently, the objective that requires optimization in the algorithm can be regarded as a multi-objective optimization problem. To address this issue, evolutionary multi-objective optimization can be used to balance all objectives and control the complexity of the algorithm with conditional constraints. In this paper, we propose to use the artificial immune algorithm to achieve evolutionary multi-objective optimization and search the disturbed location. The antibody population is employed to explore the solution space of the problem, where each antibody represents a coding solution and is assigned a fitness function value based on its performance. The higher the fitness, the better the antibody. The AIS involves various processes, such as selection, cloning, and mutation. The mutation operator is crucial as it modifies the antibody. Figure 2 presents the module diagram of AIS, and the implementation steps are described below [18]. To begin the process of generating antibodies for the hidden image block, we must first initialize several key parameters. These parameters include the population size F, which refers to the set of antibodies that will be used in each generation. Additionally, we must determine the number of antibodies that will be selected for cloning operations, which is referred to as the select quantity σ. Other important parameters to consider include the crossover rate E_{rate}, which determines the size of the offspring population, the clone rate C_{rate}, which is used to obtain the number of antibody clones, and the mutation rate M_{rate}, which represents the probability of a certain feature mutation.

After initializing these parameters, we move on to step two, which involves randomly generating the initial population of antibodies and then calculating their fitness function after secretly embedding the hidden image block.

Step three is the selection process, where we choose antibodies based on the selection rate, clone them, and obtain the total number of clones produced by the antibodies using the following formula.

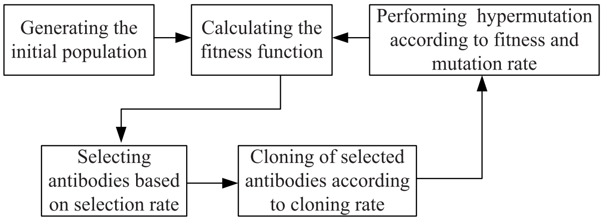
Generating the initial population
Calculating the fitness function
Performing hypermutation according to fitness and mutation rate
Selecting antibodies based on selection rate
Cloning of selected antibodies according to cloning rate

FIGURE 2. AIS immune operation module diagram.

$$SUM_{clone} = round(C_{rate} \times F \times \frac{F - \sigma + 1}{F}). \tag{1}$$

Moving on to step four, we begin the process of mutating the cloned antibodies. Each clone is mutated by changing the value of some bits, allowing us to explore nearby possible solutions. The number of bits to mutate is calculated using formula 2, where Ω represents the normalization of the antibody's fitness.

$$SUM_{mutation} = exp(-|M_{rate} \times \Omega|). \tag{2}$$

Finally, in step five, we establish the algorithm's ending condition. Specifically, we continue the algorithm until the difference between the average fitness of the current population and that of the final population is less than a specified ending parameter.

B. SYSTEM MODEL

To achieve AICppm in an MCS network environment, a mobile edge server with high computing power is employed to search for the optimal disturbance. This search is completed using a framework consisting of a mobile client and an edge server. In AICppm, images are used as carriers for concealing sensitive information, such as the user's identity, location, and equipment, in the perception data for transmission. We represent the original image and steganographic image with n channels and m elements separately as $X = (x_{i,j}^k)_{w\times h}^n \in \{0, \cdots, 2^{m-1}\}$ and $Y = (y_{i,j}^k)_{w\times h}^n \in \{0, \cdots, 2^{m-1}\}$, where each element of each channel is a pixel value of m in the finite set $\{0, \cdots, 2^{m-1}\}$. The converted binary secret information with a length of d is represented as $S = \{0, 1\}^d$, where s_l represents the secret information at the l position. In the process of embedding private information, $e(X) = (e_{i,j}^k)_{w\times h}^n \in \{0, 1\}$ represents the embedded position of the original image X. A value of 1 in $e_{i,j}^k$ represents the embedding of 1-bit secret information at the position of the embedded image k channel (i, j), while a value of 0 indicates that there is no secret embedding in the corresponding position. Formula 3 expresses the embedding process of 1-bit secret information.

$$y_{i,j}^k = \begin{cases} x_{i,j}^k - 1, & e_{i,j}^k = 1 \wedge s_l \neq x_{i,j}^k \wedge x_{i,j}^k \equiv 1(mod2) \\ x_{i,j}^k + 1, & e_{i,j}^k = 1 \wedge s_l \neq x_{i,j}^k \wedge x_{i,j}^k \equiv 0(mod2) \\ x_{i,j}^k, & otherwise. \end{cases} \tag{3}$$

Among them, $y_{i,j}^k$ is the pixels generated by the steganographic image Y, $x_{i,j}^k$ is the pixels of the original image X, $e_{i,j}^k$ is a certain position of disturbing e, and s_l is the l-bit of the secret information.

In image steganography, the embedding process needs to ensure the quality of the image, so that changes are imperceptible to the human visual system. For digital images, various methods are used to analyze the statistical characteristics of the image and evaluate the distortion between the original and steganographic images, such as mean, standard deviation, average gradient, information fidelity criteria, visual information fidelity, peak signal-to-noise ratio, mean square error, and structural similarity index (SSIM). However, mean, standard deviation, and average gradient are not suitable for evaluating the difference between the two images, and although the information fidelity criterion and visual information fidelity have theoretical support, they cannot reflect the structural information of the image. Based on experimental results presented in [19], SSIM $S(X, Y)$ is a more suitable evaluation metric as it takes into account human visual characteristics and reflects the impact of modifications on the perception of the image.

$$S(X,Y)=\frac{2(\mu_{(X)_{W\times W}}\mu_{(Y)_{W\times W}}+\theta_1)(\sigma_{(X,Y)_{W\times W}}+\theta_2)}{(\mu^2_{(X)_{W\times W}}+\mu^2_{(Y)_{W\times W}}+\theta_1)(\theta^2_{(X)_{W\times W}}+\theta^2_{(Y)_{W\times W}}+\theta_2)},\tag{4}$$

$$\mu_{(X)_{W\times W}}=\frac{1}{n\times W^2}\sum_{i=1}^{W}\sum_{j=1}^{W^2}\sum_{k=1}^{n}x_{i,j}^k,\tag{5}$$

$$\mu_{(Y)_{W\times W}}=\frac{1}{n\times W^2}\sum_{i=1}^{W}\sum_{j=1}^{W^2}\sum_{k=1}^{n}y_{i,j}^k,\tag{6}$$

$$\sigma_{(X)_{W\times W}}=\sqrt{\frac{1}{n\times(W-1)^2}\sum_{i=1}^{W}\sum_{j=1}^{W^2}\sum_{k=1}^{n}(x_{i,j}^k-\mu_{(X)_{W\times W}})^2},\tag{7}$$

$$\sigma_{(Y)_{W\times W}}=\sqrt{\frac{1}{n\times(W-1)^2}\sum_{i=1}^{W}\sum_{j=1}^{W^2}\sum_{k=1}^{n}(y_{i,j}^k-\mu_{(Y)_{W\times W}})^2},\tag{8}$$

$$\sigma_{(X,Y)_{W\times W}}=\frac{1}{n\times(W-1)^2}\sum_{i=1}^{W}\sum_{j=1}^{W^2}\sum_{k=1}^{n}(x_{i,j}^k-\mu_{(X)_{W\times W}})\times(y_{i,j}^k-\mu_{(Y)_{W\times W}}).\tag{9}$$

Among them, n represents the number of image channels, while $0<\varphi_1,\varphi_2\leq 1$, $\theta_1=(2^m\varphi_1)^2$ and $\theta_2=(2^m\varphi_2)^2$ are constants that divide the stable weak denominator. The maximum value of the image element is represented by 2^m. The structural similarity index of $W\times W$ image blocks is calculated separately, and the average value of the structural similarity indexes of all image blocks constitutes the global structural similarity index between the original image and the steganographic image. In this calculation, $\mu_{(X)_{W\times W}}$ and $\mu_{(Y)_{W\times W}}$ represent the average value of the image elements in the corresponding block, while $\sigma_{(X)_{W\times W}}$ and $\sigma_{(Y)_{W\times W}}$ represent the standard deviation of the elements in the corresponding block. The covariance of the elements in the corresponding block is represented by $\sigma_{(X,Y)_{W\times W}}$.

The structural similarity index $S(X, Y)\in[0, 1]$, where the smaller the value, the less likely the human perception system can detect image changes between X and Y. We define the structural similarity index as a measure of the imperceptibility of image steganography. If $S(X, Y)=1$, then X and Y are exactly the same. If $S(X, Y)=0$, then X and Y are completely different. To ensure the imperceptibility of the image, the structural similarity index $S(X, Y)$ should be maximized and approach 1.

C. PRIVACY ENTROPY ANALYSIS

To ensure the protection of user privacy information, it is essential to consider both the security of image steganography and task transmission. The privacy entropy is a quantitative measure used to assess the security of both these aspects. A higher privacy entropy indicates increased security of the user's private information. In [20], the security of image steganography is defined based on hypothesis testing and information entropy, and is measured using cross entropy and KL looseness. Cross entropy $H(X, Y)=-\sum XlogY$ measures the amount of information generated by Y simulating X, while KL looseness $D_{KL}(X||Y)=H(X, Y)-H(X)$ represents the amount of information lost in the process of Y simulating X, and can be used to measure the impact of each modified image element on security. Similarly, the security of task transmission refers to the security of transmitting the result of finding the disturbance location from the edge server to the mobile terminal. Assuming that the image element v is an independent and identically distributed random value, $v\in G, G=\{0,\cdots,2^{m-1}\}$, KL looseness $D_{KL}(X||Y)$ measures the security definition under passive attack, as shown in formula 10.

$$D_{KL}(P_x||P_y)=\sum_{k=1}^{|G|}P_x(v)\log\frac{P_x(v)}{P_y(v)}.\tag{10}$$

Among them, $P_x(v)$ and $P_y(v)$ represent the probability of occurrence of v in X and Y, respectively.

In the AICppm method, the corresponding relationship between the task set $T_{n,m}$ and the task migration probability $L_{n,m}$ migrated to the edge server can be expressed as:

$$\begin{pmatrix}T_{n,m}\\L_{n,m}\end{pmatrix}=\begin{pmatrix}T_{1,1},\cdots,T_{i,j}\\L_{1,1},\cdots,L_{i,j}\end{pmatrix},\quad i\in[1,n], j\in[1,m].\tag{11}$$

The task transmission security is calculated by the following formula:

$$H=-\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{m}L_{i,j}\log_2 L_{i,j}.\tag{12}$$

Finally, the privacy entropy U is expressed as:

$$\begin{aligned} U &= 1 - D_{KL}(P_x||P_y) + H \\ &= 1 - \sum_{k=1}^{|G|} P_x(v) \log \frac{P_x(v)}{P_y(v)} + (-\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{m} L_{i,j} \log_2 L_{i,j}). \end{aligned} \tag{13}$$

According to the statistical security theory of steganographic images, the difference between the original image X and the steganographic image Y can be measured by $D_{KL}(P_x||P_y)$. The smaller the value of $D_{KL}(P_x||P_y)$, the higher the security under passive attack. To improve the security of image steganography, our optimization goal is to minimize $D_{KL}(P_x||P_y)$ and approach 0, which can be expressed as maximizing $1 - D_{KL}(P_x||P_y)$. Additionally, the security of task transmission can be improved by decomposing the task into more detailed and randomized subtasks. The specific privacy entropy can be realized through algorithm 1.

Algorithm 1 Privacy Entropy Evaluation Algorithm

```
Input: $P_x(v)$, $P_y(v)$, $T_{n,m}$, $L_{n,m}$
Output: $U$
$D_{KL}(P_x||P_y)$ is calculated by the formula 10
for $i$ from 1 to $n$ do
    for $j$ from 1 to $m$ do
        $\Pi = L_{i,j} \log_2 L_{i,j}$
        $H+ = -\Pi$
    end for
end for
$H = H/n$
$U = 1 - D_{KL}(P_x||P_y) + H$
return $U$
```

D. TRANSMISSION TIME ANALYSIS

To find the optimal disturbance position and deliver the result to the mobile terminal, we need to migrate the task set $T_{n,m}$ to different edge servers, which can be time-consuming. The time required for task migration transmission is given by formula 14.

$$t_{n,m} = 2 \cdot \frac{1}{V_{n,m}} |T_{n,m}|(a_{start} - a_{end}). \tag{14}$$

Among them, $V_{n,m}$ represents the transfer rate of the migration, a_{start} and a_{end} denote the start and end positions of the edge server, respectively.

Finally, according to the task migration probability and transmission time, the average transmission time of $T_{n,m}$ is obtained.

$$Q = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{m} L_{n,m} t_{n,m}. \tag{15}$$

To improve user privacy protection, we refine the perturbation search task into several parts. Algorithm 2 takes the task migration probability $L_{n,m}$ and the migration rate $V_{n,m}$ as input and calculates the migration time for each task element. Finally, we obtain the average transmission time of tasks.

Algorithm 2 Average Transmission Time Calculation

```
Input: $V_{n,m}$, $L_{n,m}$
Output: $Q$
for $i$ from 1 to $n$ do
    for $j$ from 1 to $m$ do
        $t_{i,j} = 2 \cdot \frac{1}{V_{i,j}} |T_{i,j}|(a_{start} - a_{end})$
        $Q+ = L_{i,j} t_{i,j}$
    end for
end for
$Q = Q/n$
return $Q$
```

E. OBJECTIVE FUNCTION AND CONSTRAINTS

This paper aims to optimize the image steganography task to achieve user privacy protection by minimizing the average transmission time, maximizing the imperceptibility, and privacy entropy, while taking into account the edge server mobility and image embedding capacity as constraints in a multi-objective optimization problem. Based on the formulas 4, 13, and 15, AICppm is defined as a solution to this problem. 16.

$$\begin{aligned} &min \quad Q \\ &max \quad S(X, Y), U \\ &s.t. \quad \sum_{i=1}^{n}\sum_{j=1}^{m} L_{i,j} = 1 \\ &\qquad\quad \sum_{k=1}^{n} e_{i,j}^{k} \leq q. \end{aligned} \tag{16}$$

The optimal embedding position can be found by solving in formula 16, where the average transmission time Q is the smallest, and the structural similarity index $S(X, Y)$ and privacy entropy U are the largest. The constraint ensures that the task is completely migrated, and the capacity of the image to embed private information is limited, i.e., the number of bits allowed to be embedded in image elements is limited.

IV. PRIVACY PROTECTION METHOD BASED ON ARTIFICIAL IMMUNE CALCULATION

AICppm is a complex evolutionary multi-objective optimization problem that involves multiple indicators such as imperceptibility, average transfer time of migration, and privacy entropy. In this paper, artificial immune theory is utilized to achieve evolutionary multi-objective optimization. The process of AICppm begins with preprocessing the image through the high-pass filter bank, and then searching for the disturbance location based on the artificial immune theory. The optimization of the global probability search is achieved by simulating natural phenomena or processes, allowing the disturbance to possess self-organization, self-learning, and dynamic balance characteristics. However, the optimal disturbance generated by the artificial immune theory requires complex artificial immune operations, genetic operations, and population iterations. These operations increase the complexity and computational overhead of AICppm and are not suitable for the MCS network environment with limited mobile terminal performance. To address this issue, a mobile edge server with high computing power is introduced to find the optimal disturbance. This approach reduces the computational burden on the mobile terminal, which only needs to embed private information according to the disturbance position. The perception server then extracts information according to the reverse process of image steganography.

A. PREPROCESSING

Secret embedding in the noise/texture area is an effective method for ensuring the concealment and security of data steganography. The complexity of the pixel statistical characteristics of the noise/texture area has a greater tolerance for changes caused by the embedding of secret information. Since the noise/texture area is located in the high-frequency area of the image, it can be filtered through the constructed high-pass filter bank, and the filter residuals can be aggregated to enhance the noise/texture area and suppress the entity/content area. A high-pass filter bank [21] is constructed to achieve this, and the filter residual $x'_{i,j}$ is used to replace the image element $x_{i,j}$.

$$x'_{i,j} = R_{i,j} \otimes Z_k - \alpha \cdot x_{i,j}. \tag{17}$$

Here, $R_{i,j}$ is the neighborhood of $x_{i,j}$, and its size is determined by the filter core. Z_k is the kth high-pass filter core of the high-pass filter bank, and α represents the residual order of the kth high-pass filter kernel. A convolution operation is performed with the filter kernel and image pixels, and the neighborhood is used to predict the value of the central element $x_{i,j}$. The difference between the predicted value and the central element value is used to suppress the image content, making the image noise area more apparent. In this paper, multi-directional and non-directional high-pass filter banks are used to preprocess the overlay image to maximize the retention of noise/texture information in different directions. Then, the filter residuals are aggregated to increase the embedding capacity of steganography.

B. INITIALIZE POPULATION

In the theory of artificial immunity, the objective function and its constraints, as defined in formula 16, are referred to as the antigen, while the solution of the objective function, namely perturbation $e(X)$, is considered to be the antibody against the antigen. To process the data in the solution space and fit the artificial immune system, $e(X)$ is serialized into a three-dimensional decision space $w \times h \times n$, effectively converting the disturbance into a binary code. This serialization method allows any format of private data to be embedded in the original image, such as sound or digital information in other formats.

$$\Phi = ByteArray((e^k_{i,j})^n_{w\times h}) = \{0,1\}^\lambda,\ \lambda = w \times h \times n. \tag{18}$$

Among them, the serialized perturbation Φ is considered as the candidate solution in the artificial immune system. If we assume that each pixel in the perturbation has a binary code of m bits, then the total number of bits in Φ is $w \times h \times n \times m$. Each bit in Φ can take a value from the character set $\{0, 1\}$. The fitness function associated with the disturbance sequence Φ is defined as follows:

$$f(\Phi) = \frac{S(X,Y) + U}{Q}. \tag{19}$$

The corresponding relationship between the disturbance population $F = \{\Phi_1, \Phi_2, \cdots, \Phi_N\}$ and the fitness function is shown as follows:

$$\begin{pmatrix} \Phi_1, & \Phi_2, & \cdots, & \Phi_N \\ f_1(\Phi), & f_2(\Phi), & \cdots, & f_N(\Phi) \end{pmatrix}. \tag{20}$$

In AIS, the immune vaccine corresponds to the characteristic information of the solution to the problem to be solved, and its selection plays a crucial role in determining the execution efficiency and convergence speed of AIS. In AICppm, the extraction of disturbance features corresponds to the extraction of vaccine in artificial immune theory. In this regard, the disturbance pattern, rules, and dimensions are defined based on the pattern theorem and disturbance serialization. These definitions are then used to identify the constraints that the disturbance must satisfy.

Definition 1: Disturbance mode $A = \{a_1, a_2, \cdots, a_\lambda | a_i \in \{0, *\}, 1 \leq i \leq \lambda, \lambda = w \times h \times n\}$ corresponds to the serialized disturbance Φ, where 0 corresponds to the covered smooth area, these positions cannot be modified, and * Corresponding to the noise/texture area of the original image, these positions may be embedded with secrets.

Definition 2: $o(A)$ is the rule of the disturbance pattern A, which represents the number of fixed bits in the pattern, that is, the number of zeros.

Definition 3: $\omega(A)$ is the dimension of the disturbance pattern A and $\omega(A) = 2^{\lambda - o(A)}$ represents the number of disturbances that the pattern$A$ can describe.

Disturbance feature extraction based on the pattern theorem involves estimating the pattern that the disturbance can match, and each disturbance is considered as a sample generated by matching the pattern. The following constraints need to be satisfied for disturbance feature extraction based on the pattern theorem:

$$\begin{cases} \Phi = ByteArray((e^k_{i,j})^n_{w\times h}) \Rightarrow A \\ |F| \leq \omega(A) \\ ||\Phi|| \leq q. \end{cases} \tag{21}$$

Here, $\Phi \Rightarrow A$ represents that the disturbed bit sequence Φ should satisfy the pattern A, $|F| \leq \omega(A)$ represents the relationship between the disturbed population and the dimension of the disturbance pattern A, and $||\Phi|| \leq q$ means that the number of bits of the disturbance sequence should be less than or equal to the original image embedding capacity.

The perturbation feature corresponds to the basic information that the solution of the fitness function needs to satisfy. In order to ensure that each perturbation has a higher fitness and greater probability, AICppm restricts the element sites according to the formula 21, and initializes the population with the characteristic information. Initializing the population according to the characteristic information can promote the iterative evolution of the population and accelerate the algorithm's convergence to the global optimal solution. Evolutionary operations are performed based on the initialization of the disturbed population to prevent population degradation. Crossover and mutation operations can ensure the diversity of the population, while selection operations can improve the fitness of the population.

C. CROSS OPERATION

The crossover operation expands the global search space of the algorithm. The next generation of antibodies is generated by crossover. The two parent perturbations are recombined according to the crossover probability E_{rate} to form a new offspring perturbation. The crossover operation is a key component that enhances the exploration of the algorithm's search space. This is achieved by generating the next generation of antibodies through recombination of two parent perturbations based on the crossover probability E_{rate}. Specifically, E_{rate} is dynamically adjusted during the early stages of evolution to prevent premature convergence of the population.

$$E_{rate} = \begin{cases} E_{rate}^{max} - \dfrac{I}{I_{max}}(E_{rate}^{max} - E_{rate}^{min}), & f_q > f_F \\ E_{rate}^{max}, & f_q \leq f_F. \end{cases} \tag{22}$$

Among them, E_{rate}^{max} and E_{rate}^{min} represent the upper and lower bounds for the crossover probability, respectively. I and I_{max} denote the current iteration number and the maximum allowed iteration number. f_q and f_F represent the average fitness values of the parent and the population F, respectively. During the early stages of evolution, individuals with varying fitness levels are subjected to different crossover probabilities, and the crossover probability E_{rate} is dynamically adjusted to prevent premature convergence of the population.

D. MUTATION OPERATION

The mutation operation enhances the local search capability of the algorithm by introducing variation in the offspring. It is accomplished by generating a new offspring perturbation from the parent perturbation using the mutation operation, which is governed by a mutation probability M_{rate}.

$$M_{rate} = \begin{cases} M_{rate}^{min} + \dfrac{I}{I_{max}}(M_{rate}^{max} - M_{rate}^{min}), & f_q > f_F \\ M_{rate}^{min}, & f_q \leq f_F. \end{cases} \tag{23}$$

Among them, M_{rate}^{max} and M_{rate}^{min} are used to represent the maximum and minimum mutation probabilities, respectively. As the number of iterations increases, the mutation probability M_{rate} gradually increases. This approach ensures that the algorithm performs a global search in the initial stages of evolution, followed by a local search in the later stages. Specifically, AICppm applies site mutation operations to the population to generate new subgroups and introduce disturbance.

E. SELECT OPERATION

The next iteration population in AIS is formed through a process of high selection probability C_{rate}, based on the principle of survival of the fittest. The disturbance bits are represented in the 0, 1 character set, and the similarity between two disturbances can be measured using two-dimensional entropy. The two-dimensional entropy of the ith disturbance in the perturbed population F can be calculated using formula 24.

$$\Theta_F(i) = -\sum_{j=1}^{|F|} \frac{|\Phi_j^{i=1}|}{|F|} \log_2 \frac{|\Phi_j^{i=1}|}{|F|} - \sum_{j=1}^{|F|} \frac{|\Phi_j^{i=0}|}{|F|} \log_2 \frac{|\Phi_j^{i=0}|}{|F|}, \tag{24}$$

where $|F|$ represents the number of antibody populations, $|\Phi_j^{i=1}|$ represents the number of disturbances with bit i being 1, $|\Phi_j^{i=0}|$ represents the number of disturbances where the bit i is 0. If the value of the i-th bit of all disturbances is the same, then $\Theta_F(i) = 0$. The bit similarity of the two disturbances Φ_{j_1} and Φ_{j_2} can be expressed by the formula 25.

$$\Lambda(\Phi_{j_1}, \Phi_{j_2}) = \frac{1}{1 + \frac{1}{\lambda} \sum_{i=1}^{\lambda} \Theta_2(i)}, \tag{25}$$

where $\lambda = w \times h \times n$, $\Lambda(\Phi_{j_1}, \Phi_{j_2}) \in (0, 1]$. The greater bit similarity means that the two disturbances are more similar, and the bit similarity of the two disturbances is greater than the similarity coefficient $\tau \in (0.75, 1]$ [22], then the two disturbances are considered to be approximately equal.

The selection probability C_{rate} of the disturbance Φ_i is defined by the formula 26.

$$C_{rate}^{\Phi_i} = \varepsilon \cdot R_{fit} + (1 - \varepsilon) \cdot exp(-D_{\Phi_i}), \tag{26}$$

where ε is the adjustment factor, $R_{fit} = \frac{f(\Phi_i)}{\sum_{i=1}^{|F|} f(\Phi_i)}$ represents fitness rate, $D_{\Phi_i} = \frac{|\Phi_i^{\Lambda > \tau}|}{|F|}$ represents concentration rate, $|\Phi_i^{\Lambda > \tau}|$ is the number of disturbances that Φ_i is approximately equal to other disturbances in the population.

The greater the adaptability of the disturbance and the closer to the optimal solution, the greater the probability of selection of the disturbance. The greater the concentration of disturbance, the more similar the disturbance, which is not conducive to the diversity of the population, and the smaller the selection probability of disturbance. By selecting the probability, the disturbance with high adaptability is selected, and the disturbance with high concentration is suppressed, thereby promoting and suppressing the population F. This selection operation improves the shortcoming of genetic algorithm which is easy to converge prematurely [23], and accelerates the evolution of the population to the optimal disturbance.

F. OPTIMAL DISTURBANCE BASED ON SPEA2

$$(S(X,Y)_{\Phi_\beta} > S(X,Y)_{\Phi_\alpha}) \wedge (Q_{\Phi_\beta} < Q_{\Phi_\alpha}) \wedge (U_{\Phi_\beta} > U_{\Phi_\alpha}). \tag{27}$$

SPEA2 [24] has a strong ability to search for optimal results in multi-objective problems due to its improved strength. In fact, it can obtain the optimal solution of an evolutionary multi-objective optimization problem in the last generation of the population. This optimal solution can then be used to embed the user's private information. Specifically, for any disturbance $\Phi_\alpha \in F$ calculated by formula 27, there exists a disturbance $\Phi_\beta \succ \Phi_\alpha$, meaning that Φ_β is more dominant than Φ_α. We refer to Φ_β as the optimal solution for the disturbance. By calculating the optimal perturbation sequence using formula 27, we can determine the perturbation population number needed to embed private information capacity for the sensing task.

The AICppm algorithm involves a multi-step process to optimize a given objective function with constraints. The first step is to preprocess the masking vector. Next, the algorithm defines the antigen as the objective function and its constraints, while the antibody is the solution to the objective function. The characteristic information of the solution to be solved serves as the immune vaccine of the algorithm. Once the population is initialized, the algorithm performs immune operations, which include crossover, mutation, and selection. These operations ensure the diversity of the population, expand the global search space, and improve the local search ability of the algorithm. The selection operation improves the fitness of the individual and helps avoid premature degradation of the group. The algorithm is implemented using the code shown in algorithm 3.

V. EXPERIMENTAL RESULTS AND ANALYSIS

In this experiment, a simulation experiment server, the ThinkPad X1 Carbon, was used with the following specific configuration: Intel i7-10710U (maximum core frequency: 4.7GHz), memory 16GB, and solid-state drive 1T. The standard image database used in this paper was BOSSbase 1.01, which is a dataset containing 10,000 pictures acquired by 7 digital cameras. All pictures were processed into a size of 512 × 512, and 500 pictures were selected as a hidden picture for the experiment. Three algorithms, MO-GA [25], S-UNIWARD [26], and MiPOD [27], were selected as comparison methods to analyze the experimental results in detail. These approaches also utilize noise pixels to adaptively embed secret data, sharing similarities with our proposed approach. The difference lies in the way each approach identifies the locations for embedding secret data.

Algorithm 3 AICppm Implementation Algorithm

```
Input: Initialize population $F$, $E_{rate}$, $M_{rate}$, $C_{rate}$
Output: The optimally disturbed new population $F_{new}$
//Cross operation
$\Gamma = F$, generate random number $\kappa_1 \in (0,1)$
while $|\Gamma| \geq 2$ && $\kappa_1 > E_{rate}$ do
    Select $\forall \Phi_i, \Phi_j \in F$, $\Gamma = \Gamma - \{\Phi_i, \Phi_j\}$
    Randomly select bits $\kappa_2$, $1 \leq \kappa_2 \leq w \times h \times n$
    Generate cross position $\kappa_3 = \lfloor \kappa_2 / m \rfloor \times m$
    Obtain the minimum value of the non-zero string after the individual $\Phi_i, \Phi_j$ intersection $\kappa_3$
    $t = min(||\Phi_i^{\kappa_3}||_{!0}, ||\Phi_i^{\kappa_3}||_{!0})$
    Exchange the $t$ non-zero string of individual $\Phi_i, \Phi_j$ after the intersection $\kappa_3$ to generate a new individual $\Phi_i', \Phi_j'$
    $F = \Gamma \cup \{\Phi_i', \Phi_j'\}$
    Update random number $\kappa_1 \in (0,1)$
end while
//Mutation operation
$\Gamma = F$
Update random number $\kappa_1 \in (0,1)$
while $|\Gamma| \geq 1$ && $\kappa_1 > M_{rate}$ do
    Select $\forall \Phi_i \in F$, $\Gamma = \Gamma - \{\Phi_i\}$
    Replace $\Phi_i$ with the filtered residua $\Phi_i'$
    Randomly select the bits of $(\Phi_i')_{\kappa_2}$, $(\Phi_i')_{\kappa_3} = 0$ and $(\Phi_i')_{\kappa_4} = 1$ corresponding to the * value in the disturbance pattern $A$
    if $(\Phi_i')_{\kappa_2} == 0$ then
        $(\Phi_i')_{\kappa_2} = 1$, $(\Phi_i')_{\kappa_4} = 0$
    else
        $(\Phi_i')_{\kappa_2} = 0$, $(\Phi_i')_{\kappa_3} = 1$
    end if
    $F = \Gamma \cup \{\Phi_i'\}$
    Update random number$\kappa_1 \in (0,1)$
end while
//Get the optimal disturbance
$F_{new} = \emptyset$
for $i$ from 1 to $|F|$ do
    for $j$ from 1 to $|F|$ do
        The $i$-th and $j$-th disturbances $\Phi_i, \Phi_j$ in $F$
        if $(S(X,Y)_{\Phi_i} > S(X,Y)_{\Phi_j})$&&$(Q_{\Phi_i} < Q_{\Phi_j})$&&$(U_{\Phi_i} > U_{\Phi_j})$ then
            $F_{new} = F_{new} + \Phi_i$
        end if
    end for
end for
return $F_{new}$
```

First, a comparison was made between the time and space complexities of four different approaches. Our approach consists of three steps, with an overall time complexity of $O(n^2)$ and a space complexity of $O(n)$. The MO-GA approach has a time complexity of $O(n^2+n)$ and a space complexity of $O(n)$. Both the S-UNIWARD and MiPOD approaches have a time complexity of $O(n^2)$ and a space complexity of $O(n)$, similar to each other. Based on the above analysis, it can be seen that MO-GA has the highest time complexity, while the other three approaches are all better than MO-GA in terms of time complexity. The space complexity is the same for all four algorithms. Then, the experiment compared the load balancing, imperceptibility, privacy entropy, and average embedding time of the four methods. To evaluate security, SPA [28] was used as a steganalysis tool to analyze the ability of the four algorithms to resist the steganalysis of malicious attackers. Finally, the multi-objective optimization problem of algorithm evolution was analyzed, and the three conditional relations of the objective function were analyzed. The migration task was completed by simulating the edge server using virtual machine technology VM. The task was assigned to the nearest VM for completion. When the limit of the computing resource of the VM was reached, the remaining tasks were transferred to other VM until all tasks were executed. The experiment was completed using MATLAB programming, and all experimental results were averaged after at least 1000 rounds.

A. PARAMETER SETTINGS

The larger the population size N, the more iterations I, the closer the solution is to the optimal solution, and the better the diversity. However, a larger value of N and I also results in a greater computational cost for the algorithm. To strike a balance between solution quality and computational efficiency, the paper presents the results of multiple experiments with fixed $I = 600$ and varying $N \in \{25, 50, 75, 100, 125\}$. In order to ensure the validity of the experiment and promote population diversity, several basic parameters used in the evaluation are listed in Table 2.

TABLE 2. Parameter settings.

Parameter	Value
$V_{n,m}$	1600(Mb/s)
C_{rate}	roulette wheel selection
M_{rate}^{max}	0.97
M_{rate}^{min}	0.55
E_{rate}^{max}	0.15
E_{rate}^{min}	0.02
τ	0.85
ε	0.95

The size of the offspring population in the experiment is controlled by the crossover probability and mutation probability, which determine the number of population crossover and mutation as shown in the table. By adjusting these probabilities, individuals with higher fitness can be favored for the next generation while eliminating those with lower fitness. Fine-tuning these probabilities based on the experimental environment can improve the results of the experiment.

For the experiment, we selected four types of high-pass filter check images in different directions, namely $Z_{Laplacian}$, Z_{Sobel}, Z_{Kirsch}, and $Z_{NelderCMead}$ to preprocess the images in the image library $\{X_1, \cdots, X_{500}\}$. We obtained candidate positions using formula 17, and then iteratively searched for the optimal privacy embedding position in each candidate position. We used four comparison algorithms to embed the same privacy information into each hidden image, generating corresponding steganographic images. Figure 3 shows the comparison library of the original image and the steganographic image produced by our method. The first column displays the original image, the middle column shows the preprocessed image, and the third column displays the generated steganographic image.

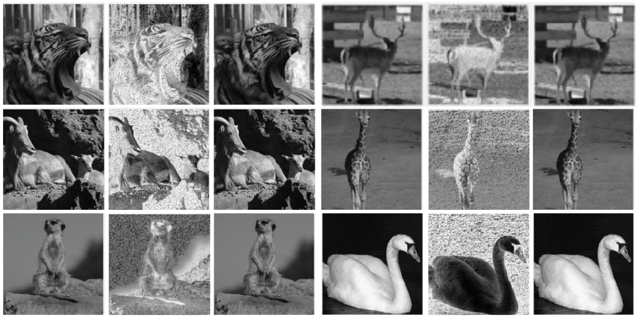

FIGURE 3. **AICppm image comparison library.**

B. LOAD BALANCING

Load balancing refers to the distribution of computing resources across edge servers. In the experiment, the computing power of edge servers depends on the scale of VM. The task of finding the location of disturbances is represented as $T_{n,m} = \{T_1, \cdots, T_N\}$, where N is the number of disturbances. $VM = \{VM_1, \cdots, VM_{AE}\}$ denotes a collection of edge servers. The average load balancing variance of edge servers in the network is calculated using formula 28.

$$LB = \frac{1}{AE} \sum_{i=1}^{M} LB_i, \tag{28}$$

where AE represents the number of edge servers required to process the task set, M denotes the number of virtual machines, and LB_i is the load balancing variance of the ith edge server, which is calculated as $(\frac{1}{AE} \sum_{i=1}^{M} AE_i - AE_i)^2$. Here, AE_i signifies the number of edge servers needed to process the ith task. A lower average load balancing variance indicates a better-balanced resource allocation among the edge servers, leading to higher resource utilization.

To compare the performance of load balancing methods, Figure 4 depicts the average load balancing variances of the $T_{n,m}$ task set for four different approaches. Among these, AICppm outperforms the other three methods, which fail to adequately address the load balancing issues of edge servers despite using them to solve population-related iterative problems. Our proposed method, on the other hand, ensures balanced resource usage among virtual machines and dynamically optimizes their load balancing.

By allocating tasks in real-time based on *VM* occupancy in the network, our approach guarantees optimal network performance.

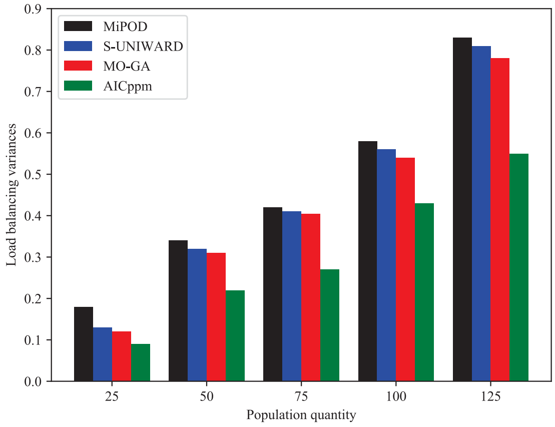

FIGURE 4. Comparison of load balancing variance of four algorithms.

C. QUALITY ASSESSMENT

Mean square error (MSE), peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM) are commonly used to evaluate the degree of image distortion. In this study, we use these three indicators to evaluate the quality of steganographic images. The results presented in Table 3 show the average values of 500 sample pairs, and summarize the comparison results of the four algorithms on MSE, PSNR, and SSIM. According to the results in Table 3, AICppm outperforms the comparison algorithms in all three indicators of MSE, PSNR, and SSIM, especially in SSIM. This is because AICppm uses SSIM as one of the population evolution goals to select the best disturbing position, which ensures that our proposed method has the least impact on image quality.

TABLE 3. Comparison of MSE, PSNR and SSIM averages.

Evaluation Index	MO-GA	S-UNIWARD	MiPOD	AICppm
MSE	0.1658	0.1768	0.1785	0.1598
PSNR	77.6578	76.9840	76.8856	78.9557
SSIM	0.9997	0.9988	0.9986	0.9999

D. PERFORMANCE COMPARISON OF PRIVACY ENTROPY

Privacy entropy is a crucial metric for quantifying privacy. Figure 5 compares four different methods for measuring privacy entropy. As the scale of the task increases, AICppm demonstrates more pronounced advantages in safeguarding user privacy and outperforms the other methods. AICppm is the best-performing method overall, owing to its minimal looseness value among the four methods, which results in the smallest difference between the original and steganographic images. Furthermore, the AICppm method's task decomposition is more intricate and random, leading to better task security during transmission.

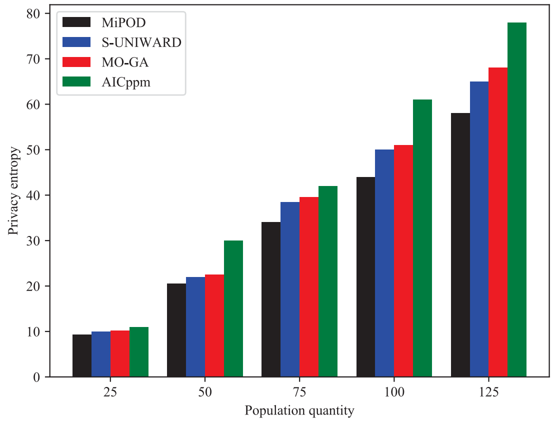

FIGURE 5. Comparison of privacy entropy of four algorithms.

E. AVERAGE TRANSMISSION TIME

In many scenarios where MCS perception tasks are involved, users need to transmit perception data in real-time. Thus, the average transmission time of the task plays a critical role in determining the user's enthusiasm to perform the perception task. As illustrated in Figure 6, the average transmission time increases as the task set size increases. AICppm leverages the iterative progress of the artificial immune system, and the transformation is conducted on the mobile edge server, making the privacy embedding on the mobile terminal highly efficient. Furthermore, the algorithm considers both global and local searches, enabling it to swiftly and efficiently locate the optimal solution. In cases where the embedded user's privacy information capacity is less than 0.1M, AICppm can achieve a low-latency of millisecond-level average transmission time. As shown in Figure 6, AICppm has a faster transmission time, which meets the real-time requirements of the MCS network environment.

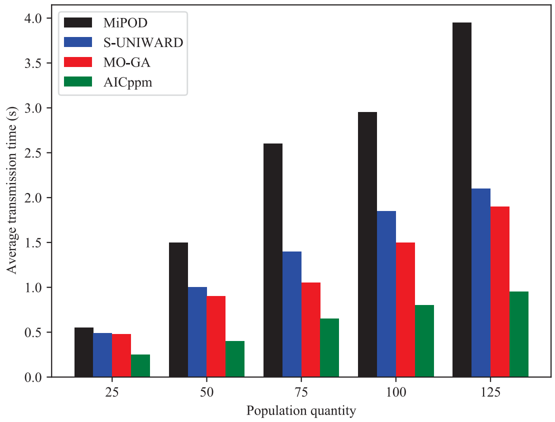

FIGURE 6. Comparison of average transmission time of four algorithms.

F. ANTI-STEGANALYSIS PERFORMANCE EVALUATION

Malicious attackers can use steganalysis tools to obtain secret information from steganographic images. Therefore, evaluating the performance of the four methods against steganalysis is a crucial indicator of algorithm security. In the four methods of the steganographic image library, SPA is utilized for steganalysis, and the detection error rate P_{ERROR} is employed to assess the algorithm's performance against steganalysis.

$$P_{ERROR} = \frac{P_{OF} + P_{FD}}{2}. \tag{29}$$

Among them, P_{FD} represents the false detection rate of the attacker, indicating the ratio of the number of original images detected as steganographic images to the total number of steganographic images. P_{OF} is the missed detection rate, representing the ratio of the number of undetected steganographic images to the total number of steganographic images. Figure 7 compares P_{ERROR} of different algorithms with a population size of 125. As illustrated in Figure 7, the algorithm proposed in this paper is robust against SPA steganalysis tools, and the less secret the steganographic image is embedded, the more robust the algorithm's anti-SPA ability becomes.

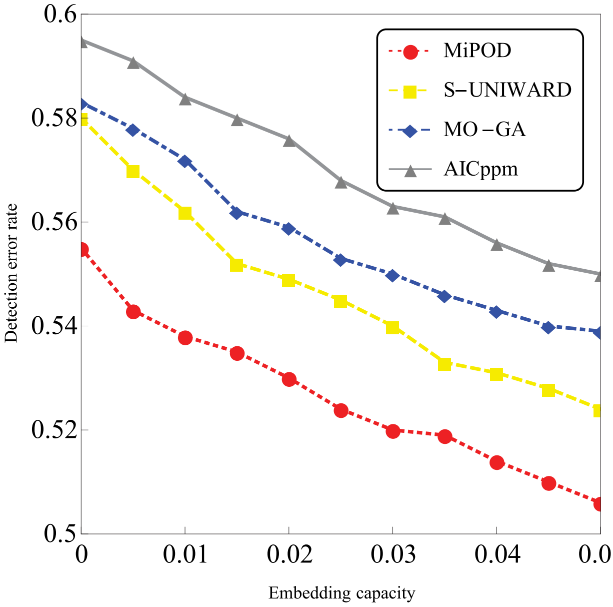

FIGURE 7. Four algorithms P_{ERROR} comparison.

G. MULTI-OBJECTIVE OPTIMIZATION RELATIONSHIP ANALYSIS

Figure 8 illustrates the relationship between imperceptibility, average transmission time, and privacy entropy, where the population size is 125, the migration rate is 1, and the original image capacity is restricted to 0.05M. The AICppm method is employed to search for the optimal disturbance position to maintain the balance between the three objectives. As depicted in Figure 8, the optimal values for the three objectives are achieved when the privacy entropy is 78.9, the transmission time is 0.96s, and the imperceptibility is 0.9999. Additionally, it can be observed that high privacy entropy and imperceptibility imply that the task is split into more modules, which requires a longer transmission time.

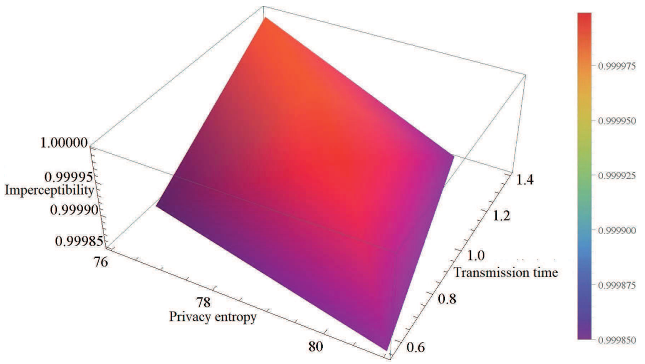

FIGURE 8. Evolutionary multi-objective optimization diagram.

VI. CONCLUSION

In this paper, we have proposed a novel privacy protection method called AICppm, which is an evolutionary multi-objective optimization algorithm based on the artificial immune system. AICppm takes into account the migration probability and embedding capacity of edge servers and defines a multi-objective optimization problem by minimizing the average transmission time, maximizing imperceptibility, and privacy entropy. This approach enables covert transmission of private information in the MCS network using image steganography technology. The mobile edge server searches for the optimal disturbance position of the carrier image, while the mobile terminal embeds the private information in real-time according to the steganography position. As a result, users' privacy information is effectively protected, and the algorithm effectively optimizes the concealment of steganographic images, better resists attacks from malicious attackers' steganalysis tools, and can achieve real-time processing of perception tasks. Future work can extend the AICppm algorithm to a general steganography method, allowing the use of other multimedia formats such as video and audio as hidden carriers. Such extensions can further enhance the security of the MCS network and make it more resilient against cyber-attacks.

REFERENCES

[1] C. Ju, Q. Gu, G. Wu, and S. Zhang, "Local differential privacy protection of high-dimensional perceptual data by the refined Bayes network," *Sensors*, vol. 20, no. 9, pp. 2516–2538, 2020.

[2] Q. Cui, Z. Zhou, Z. Fu, R. Meng, X. Sun, and Q. M. J. Wu, "Image steganography based on foreground object generation by generative adversarial networks in mobile edge computing with Internet of Things," *IEEE Access*, vol. 7, pp. 90815–90824, 2019.

[3] N. Ansari and X. Sun, "Mobile edge computing empowers Internet of Things," *IEICE Trans. Commun.*, vol. E101.B, no. 3, pp. 604–619, 2018.

[4] V. Stephanie, M. A. P. Chamikara, I. Khalil, and M. Atiquzzaman, "Privacy-preserving location data stream clustering on mobile edge computing and cloud," *Inf. Syst.*, vol. 107, Jul. 2022, Art. no. 101728.

[5] K. L. M. Ang, J. K. P. Seng, and E. Ngharamike, "Towards crowdsourcing Internet of Things (crowd-IoT): Architectures, security and applications," *Future Internet*, vol. 14, no. 2, pp. 49–100, 2022.

[6] D. De, S. Ghosh, and A. Mukherjee, "SocialSense: Mobile crowd sensing-based physical distance monitoring model leveraging federated learning for pandemic," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100872.

[7] T. Dimitriou and A. Michalas, "Incentivizing participation in crowd-sensing applications through fair and private bitcoin rewards," *IEEE Access*, vol. 10, pp. 129004–129018, 2022.

[8] Y. Sun, W. Ding, L. Shu, K. Li, Y. Zhang, Z. Zhou, and G. Han, "On enabling mobile crowd sensing for data collection in smart agriculture: A vision," *IEEE Syst. J.*, vol. 16, no. 1, pp. 132–143, Mar. 2022.

[9] P. Xiong, T. Zhu, W. Niu, and G. Li, "A differentially private algorithm for location data release," *Knowl. Inf. Syst.*, vol. 47, no. 3, pp. 647–669, Jun. 2016.

[10] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2016, pp. 344–353.

[11] L. Y. Fan, L. Xiong, and V. Sunderam, "Differentially private multi-dimensional time series release for traffic monitoring," in *Proc. 27th Data Appl. Secur. Privacy (DBSec)*, Newark, NJ, USA, 2013, pp. 33–48.

[12] D. Riboni and C. Bettini, "Differentially-private release of check-in data for venue recommendation," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2014, pp. 190–198.

[13] J. Chen, H. Ma, and D. Zhao, "Private data aggregation with integrity assurance and fault tolerance for mobile crowd-sensing," *Wireless Netw.*, vol. 23, no. 1, pp. 131–144, Jan. 2017.

[14] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, S. Nidhal, N. S. Jalood, A. N. Jasim, and A. H. Shareef, "New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity," *IEEE Access*, vol. 7, pp. 168994–169010, 2019.

[15] R. P. Sharma and R. Pal, "Saliency based image steganography with varying base SDS and multi-objective genetic algorithm," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Aug. 2015, pp. 1966–1974.

[16] S. Joshi, K. V. Sonawane, and S. Khan, "Role of genetic algorithm in performance improvement of image steganography combined with transform and its hybrid wavelet," in *Proc. 2nd Int. Conf. Commun. Syst., Comput. IT Appl. (CSCITA)*, Apr. 2017, pp. 133–138.

[17] Y. Li, M. Du, and J. Xu, "A new distributed intrusion detection method based on immune mobile agent," in *Proc. 6th Int. Conf. Adv. Cloud Big Data (CBD)*, Aug. 2018, pp. 215–219.

[18] U. Vivek, P. Madhavan, and V. Kumar, "A novel design augmentation of bio-inspired artificial immune technique in securing Internet of Things (IoT)," in *Internet of Things for Industry 4.0*, 2020.

[19] X. Ma, X. Jiang, and D. Pan, "Performance validation and analysis for multi-method fusion based image quality metrics in a new image database," *China Commun.*, vol. 16, no. 8, pp. 147–161, Aug. 2019.

[20] N. S. Hamzehkolaei and F. MiarNaeimi, "A new hybrid multi-level cross-entropy-based moth-flame optimization algorithm," *Soft Comput.*, vol. 25, no. 22, pp. 14245–14279, Nov. 2021.

[21] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.

[22] Y. Yoon and Y.-H. Kim, "Gene-similarity normalization in a genetic algorithm for the maximum k-Coverage problem," *Mathematics*, vol. 8, no. 4, pp. 1–16, 2020.

[23] Y. Lin, T. D. Liu, F. F. Chen, K. C. Li, and Y. Xie, "An energy-efficient task migration scheme based on genetic algorithms for mobile applications in CloneCloud," *J. Supercomputing*, vol. 11, no. 4, pp. 1–17, 2020.

[24] Y. Li, L. Liu, S. Yang, Z. Ren, and Y. Ma, "A multi-objective topology optimization methodology and its application to electromagnetic actuator designs," *IEEE Trans. Magn.*, vol. 56, no. 2, pp. 1–4, Feb. 2020.

[25] X. Ding, Y. Xie, P. Li, M. Cui, and J. Chen, "Image steganography based on artificial immune in mobile edge computing with Internet of Things," *IEEE Access*, vol. 8, pp. 136186–136197, 2020.

[26] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1–13, Dec. 2014.

[27] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 221–234, Feb. 2016.

[28] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777–25788, 2020.

HAO LONG received the Ph.D. degree in computer science and technology from Soochow University. Currently, he is an Associate Professor with the School of Information Engineering, Xuzhou College of Industrial Technology. His current research interests include mobile crowd sensing, privacy protection, and distributing computing.

JIAWEI HAO received the B.S. degree from the Nanjing University of Information, Science and Technology (NUIST), and the Ph.D. degree in climate system and climate change from NUIST, China, in 2022. He is currently a Lecturer with the School of Information Engineering, Xuzhou College of Industrial Technology, Xuzhou, China. His research interests include neural network algorithm, neural network application, and climate prediction.

SHUKUI ZHANG received the Ph.D. degree in computer science from the University of Science and Technology of China. Currently, he is a Professor and a Doctoral Supervisor with the School of Computer Science and Technology, Soochow University. His main research interests include ad hoc and wireless sensor networks, mobile computing, distributing computing, intelligent information processing, and parallel and distributed systems.

YANG ZHANG received the B.S. degree in electronic and communications engineering from the University of Bristol, U.K., and the M.S. degree in telecommunications electronics from the University of Glasgow, U.K. His research interests include the IoT, information security, crowd sensing computing, and intelligent information processing.

LI ZHANG received the B.S. degree in computer science and technology from Anhui Normal University, Wuhu, China, in 2008, and the B.S. degree in computer science and technology from Huaibei Normal University, Huaibei, China, in 2011. Currently, he is pursuing the Ph.D. degree with the School of Computer Science and Technology, Soochow University, Suzhou, China. His current research interests include mobile crowd sensing, mobile computing, and distributing computing.