IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 27, 2020, accepted June 15, 2020, date of publication July 20, 2020, date of current version August 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3010513

Image Steganography Based on Artificial Immune in Mobile Edge Computing With Internet of Things

XUYANG DING[1], YING XIE[1,2], PENGXIAO LI[3], MENGTIAN CUI[2], AND JIANYING CHEN[2]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]Key Laboratory for Computer Systems of State Ethnic Affairs Commission, Southwest Minzu University, Chengdu 610041, China
[3]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China

Corresponding author: Ying Xie (xieying@swun.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61902326; and in part by the Fundamental Research Funds for the Central Universities (SWUN) under Grant 2020NGD02.

ABSTRACT Mobile edge computing provides high computing power, data storage capacity and bandwidth requirements for Internet of Things (IoT) through edge servers that process data close to data sources or users. In practical, mobile edge computing can be used to implement image steganography in IoT. Considering imperceptibility, security and capacity are important indicators for image steganography, this paper propose an image steganography based on evolutionary multi-objective optimization (EMOsteg). The EMOsteg preprocesses the image through a high-pass filters bank to find noise and texture regions that are difficult to model. By perturbing the image on noise and texture regions in multiple directions, the embedded capacity is increased. By defining the imperceptibility and security as an antigen, defining the perturbation positions of the cover image as an antibody, the EMOsteg uses the artificial immune principle to heuristically obtain the perturbation population through feature extraction of the perturbation and adaptive evolution operations. And the Pareto optimal is used to find the optimal perturbation in the last generation population. The simulation experiments analyze the convergence of the algorithm and the diversity of the solutions. In simulation experiments, the MSE, PSNR and SSIM were adopted to evaluate the imperceptibility, and the results show that the MSE value of our algorithm is 0.000308, the PSNR is 82.7501 and the SSIM approaches 1, they are better than comparison algorithms. The average detection error P_E under SPA was adopted to detect the security, and the results show that our algorithm is more robust against anti-SPA steganalysis. In order to evaluate the performance of real-time, the embedding time of the same secret under different algorithms were compared, and the results show that our algorithm is faster than comparison algorithms in the terminal. In summary, the proposed algorithm can maintain the image quality while resist steganalysis tools, and realize real-time processing.

INDEX TERMS IoT security, mobile edge computing, image steganography, evolutionary multi-objective optimization, artificial immune.

I. INTRODUCTION

Security issues are always a challenge in IoT scenario. The traditional passive cryptography is easy to expose the communication process, making the sensitive data to attract the attention of attackers. While the information hiding technology hides the secret in large and complex information space, and it is even hard to discover the existence of secret. However, information hiding for the IoT has high time-space complexity and high computational overhead, especially the embedding process with image, audio and video as covers [1]. Among them, image steganography is an important branch of information hiding, and it is also an effective and safe transmission method with image as cover in IoT scenario [2]. Considering that image steganography puts higher requirements for real-time performance and privacy protection of the IoT, image steganography is implemented based on mobile edge computing in practice [3], [4]. Due to limitation of

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

computing resources, mobile terminals of IoT cannot run complex applications and process massive data. The mobile edge computing can deploy complex applications on mobile terminals by moving complex computing processing to the edge server of IoT which close to the data source and user [5]. Through low-latency, low-bandwidth, high-performance of mobile edge computing, the redundant locations of image that are not sensitive to human perception systems can be calculated at the mobile edge server, and secret can be quickly embedded in the image at mobile terminals.

There are huge different statistical characteristics for different regions in digital image. In the smooth regions, the statistical characteristics of the histogram, co-occurrence matrix and neighborhood correlation are relatively obvious. If secret was embedded in these regions, it is easy to destroy the statistical characteristics of the cover image, and detect by the steganalysis tools easily. On the other hand, the statistical characteristics of the noise and texture regions are complicated, it is difficult to model and analyze, and the elements in these regions can tolerate the perturbation caused by secret embedding. Combined 3D Color Texture Feature (CTF) was used to identify complex regions of color image in [6]. Through Discrete Cosine Transform (DCT), secret could be embedded in each of the RGB planes adaptively as per the complexity analysis of the respective regions, so that visual attack to detect hidden secret becomes quite challenging. In [7], the noisiest pixels were determined based on noise-level estimation iteratively. Then, secret were embedded into these noisy pixels using Sum and Difference Covering Set (SDCS) steganography. In [8], the change in the output of directional high-pass filters after changing one pixel was weighted and then aggregated using the reciprocal Hölder norm to define modification costs of each pixel. This method limited embedding operation to highly textured or noisy areas and avoids making modifications in smooth areas. As the pixels located in noisy regions are complicated and more tolerate to the modification caused by secret embedding, [8]–[11] take advantage of the noisy pixels to embed data adaptively.

The essence of image steganography is secure transmission while undetectable the changes of the image [2]. Therefore, security and imperceptibility are the most important indicators for evaluating image steganography. Obviously, security, imperceptibility are contradictory. To optimize one of them, it must be at the expense of others. Thus, the image steganography can be transformed into a multi-objective optimization problem. Meanwhile, the security and the imperceptibility are closely related to the embedded capacity in the actual embedding process. Embedding capacity is the ratio of bit value of secret information to bit value of the cover image. The more secret embedded in the cover, the lower the imperceptibility and security, so the embedded capacity can be used as a constraint condition in multi-objective optimization problem.

In recent years, some new evolutionary algorithms such as particle swarm optimization, artificial immune algorithm, estimation of distribution algorithm and co-evolutionary algorithm have been successfully applied in the field of multi-objective optimization, called evolutionary multi-objective optimization (EMO). The purpose of EMO is to make the population converge quickly and distributed in the non-inferior optimal domain of the problem evenly. Among EMO algorithms, artificial immune algorithm is based on the principles of natural defense, it has advantage of evolutionary learning methods, such as anti-noise capabilities, unsupervised learning, memory and self-organization [12]. In this paper, artificial immune algorithm was used to deal with multi-objective optimization problems for image steganography.

Based on the analysis above, security and imperceptibility are very important indicators for image steganography. In order to optimize these contradictory goals, an image steganography based on evolutionary multi-objective optimization (EMOsteg) was proposed. Through the principle of artificial immunity, perturbation locations on the cover image iteratively was searched to ensure image quality and resist steganalysis tools under certain embedded capacity constraints. The contributions of this paper are as follows.

1) An image preprocessing method based on high-pass filters bank is proposed. Multiple directional and non-directional high-pass filters bank is used to preprocess the cover image and filter residuals are aggregated to form the candidate locations of the perturbation. These aggregated residuals correspond to noise and texture regions that are difficult to model. In subsequent stages, perturbation locations will be searched in these aggregated residuals for embedding process.
2) An image steganography based on evolutionary multi-objective optimization (EMOsteg) is proposed. EMOsteg takes the embedded capacity as the constraint condition and formally defines the multi-objective optimization problem by minimizing the imperceptibility and maximizing the security. Based on artificial immune theory, EMOsteg transforms the multi-objective optimization problem into an antigen, transforms the perturbation locations into an antibody. Then, EMOsteg iteratively search antibodies with high fitness to eliminate antigen by feature extraction and adaptive evolution operators, and the perturbation is obtained by optimal selection among antibodies population.
3) A covert communication method that satisfies the real-time and bandwidth requirements of the IoT is proposed. Based on mobile edge computing, EMOsteg is suitable for covert communication in IoT scenarios. When deploying in IoT, the mobile edge server is used to search the perturbation of the cover image, and the mobile terminal only needs to embed the secret according to the perturbation. Through mobile edge computing, EMOsteg realizes real-time embedding in IoT.

II. RELATED WORKS

Image steganography has two categories: spatial domain algorithms and transform domain algorithms. The spatial domain algorithms embed secret by modifying the value of the image elements, such as Least Significant Bit (LSB) based methods [13]–[15], Pixel Value Difference (PVD) based methods [16]–[18], and so on. The transform domain algorithms embed secret by modifying the transform domain coefficients, that are, Discrete Cosine Transform (DCT) [19], variants of Discrete Wavelet Transform (DWT) [20], and Fast Fourier Transform (FFT) [21]. Many state-of-the-art transform domain algorithms have emerged, such as Jsteg [22], OutGuess [23], StegHide [24], F5 [25], and so on. These algorithms preserve the image statistical characteristics as much as possible during the embedding process to defense the visual-based and statistical-based steganalysis attacks.

The different embedding locations of the cover image would impact on the security of the image steganography. Image steganography based on minimizing the embedded distortion function quantifies the impact of each element change on security. The Wavelet Obtained Weights (WOW) [8] uses a wavelet-based directional filter bank to filter the spatial image, calculates the embedded distortion after the modifying the pixel on the filter residual. Then, WOW combines all the embedded distortions in each direction with the Hölder norm to measure the total embedded distortion. The Universal Wavelet Relative Distortion (UNIWARD) [9] further extend the WOW to the spatial, JPEG domain and side information JPEG domain, and the secret is embedded into the image where the distortion function tends to 0. Generalized uniform embedding was proposed in [26], [27]. By considering the relative changes of statistical model for images, this method uses all the DCT coefficients (including the DC, zero, and non-zero AC coefficients) as the cover elements to construct Uniform Embedding Revisited Distortion (UERD) function to refine the uniform embedding. In order to improve the existing distortion functions for JPEG images, [28] construct a reference image close to the image before JPEG compression. Based on the reference image and the feature distortion minimization, the existing distortion functions designed for syndrome trellis coding embedding are improved by distinguishing the embedding costs for $+1$ versus -1 embedding. In [29], a binary image steganography was proposed to improve both of imperceptibility and security by selecting more appropriate flipped pixels. This method combines the advantages of flipping distortion measurement (FDM), the edge adaptive grid method (EAG) and the Connectivity Preserving criterion (CPc). The FDM measures the distortion score by statistical features and achieves high-statistical security, while the EAG and CPc select pixels by analyzing the local texture structures based on visual quality. Above algorithms do not need to determine a specific image statistical model in advance, and they maximize the security by minimizing the total embedding distortion. However, this type of algorithms needs to be improved in terms of image integrity and image quality.

Image steganography has made great progress in the long-term confrontation with steganalysis. Due to the wide application of artificial intelligence, a kind of image steganography that attempts to deceive steganalysis tools based on neural network classifiers has emerged. Reference [30] present a steganographic operation called adversarial embedding (ADV-EMB), which achieves the goals for hiding secret and fooling a CNN-based steganalyzer at the same time. ADV-EMB adjusts the costs of image elements modifications according to the gradients back propagated from the target CNN-based steganalyzer. Therefore, modification direction has a higher probability to be the same as the inverse sign of the gradient. In order to improve the embedded capacity, an U-Net structure based image steganography scheme was proposed in [31]. In the form of paired training, the steganography algorithm and extraction algorithm are trained based on deep neural network. Depending on the adversarial training between generator and discriminator, Generative Adversarial Networks (GAN) provides an effective image generation. Considering that steganography and steganalysis are also contradictory, many state-of-the-art GAN based image steganography have emerged [32]–[34]. However, this kind of algorithms has large computational cost, and it still needs to be improved in the IoT scenario with high real-time requirements.

The EMO-based image steganography heuristically modify the pixels/coefficients and optimize the goals of the steganography by searching the optimal solution. Based on simulated annealing algorithm (SA), a multi-objective data embedding architecture which can modify pixels/coefficients to optimize correlation metrics was developed in [35]. The cost function of [35] is integrated by the mean square error (MSE), human visual system (HVS) bias and statistical feature difference (SFD), which is used to guide the correct search direction during SA optimization. However, this cost function only involves image quality metrics, and there is no consideration for embedded capacity and security during SA optimization. Based on particle swarm optimisation (PSO) algorithm, [36] propose an image steganography for the purpose of high embedment capacity and security. In this method, PSO is used to calculate fitness function efficiently that depends on the cost matrix by dividing the cover image and the stego image into four parts. The image steganography proposed in [37], [38] combines the advantages of visual saliency and SDS-based steganography, and the genetic algorithm (GA) is used to search the optimal solution between pixel saliency and embedded capacity to ensure lower embedded distortion and higher embedded capacity. In order to increase the embedding capacity while ensuring the security of the cover image, [39] also used GA to identify suitable places in cover image where embedding process will not lead to lower energy transformed regions by using DCT and its wavelet (DCTW). Through comparison experimental, both DCT and DCWT perform better when combined with genetic algorithm. The EMO-based image steganography can balance all goals and control the complexity of the algorithm

under constraints. This paper uses the EMO-based image steganography to implement covert communication in the IoT scenario, and solve the computational cost problem through edge computing.

III. PROBLEM DEFINITION

The symbols $X = (x_{i,j}^p)_{w\times h}^n \in \{0, \cdots, 2^{m-1}\}$ and $Y = (y_{i,j}^p)_{w\times h}^n \in \{0, \cdots, 2^{m-1}\}$ are used for the cover image and the corresponding stego image with n channels and $w \times h$ elements. Both grayscale and binary images are single-channel, color images include R, G, and B channels, and remote sensing images are multi-channels. Each image element of each channel is m-bit pixel value in a finite set $\{0, \cdots, 2^{m-1}\}$. The symbols $S = \{0, 1\}^d$ is used for binary secret information with length d , and S_k represents the k-th bit of the secret. In the embedding process, the perturbation $e(X) = (e_{i,j}^p)_{w\times h}^n \in \{0, 1\}$ is the embedding locations of the cover X. $e_{i,j}^p = 1$ represents that 1-bit secret is embedded on (i, j) location of the p-th channel, and $e_{i,j}^p = 0$ represents that none secret embedding on the corresponding location. Equation 1 illustrates the embedding process of 1-bit secret.

$$y_{i,j}^p = \begin{cases} x_{i,j}^p - 1, e_{i,j}^p = 1 \wedge s_k \neq x_{i,j}^p \wedge x_{i,j}^p \equiv 1(mod2) \\ x_{i,j}^p + 1, e_{i,j}^p = 1 \wedge s_k \neq x_{i,j}^p \wedge x_{i,j}^p \equiv 0(mod2) \\ x_{i,j}^p, \quad else \end{cases} \tag{1}$$

where the $y_{i,j}^p$ is generated pixel of the stego Y, the $x_{i,j}^p$ is a pixel of the cover X, the $e_{i,j}^p$ is location of the perturbation e and the s_k is the k-th bit of the secret S.

In image steganography, the embedding process needs to ensure the image quality, so that the human perception system does not perceive the change. For digital images, the mean, standard deviation, average gradient, information fidelity criterion (IFC), visual information fidelity (VIF), peak signal to noise rate (PSNR), mean square error (MSE) and structural similarity index (SSIM) are usually used to analyze the statistical characteristics and evaluate the distortion of the image. Among them, the mean, standard deviation and average gradient are evaluation indicators without reference, they cannot evaluate the difference between the cover and the stego. Although IFC and VIF have theoretical support, they cannot reflect the structural information of the image. The experimental results of [40] show that the SSIM is more in line with human visual characteristics than PSNR or MSE. So the $S(X, Y)$ from [40] was used to evaluates the impact of each element modification on the human perception system.

$$\begin{aligned} S(X, Y) = \frac{1}{M} \sum_{M} \Big(& (2\mu_{(X)_{W\times W}} \mu_{(Y)_{W\times W}} + \theta_1) \\ & \times (2\sigma_{(X,Y)_{W\times W}} + \theta_2) \\ & /(\mu_{(X)_{W\times W}}^2 + \mu_{(Y)_{W\times W}}^2 + \theta_1) \\ & \times (\sigma_{(X)_{W\times W}}^2 + \sigma_{(Y)_{W\times W}}^2 + \theta_2) \Big) \end{aligned} \tag{2}$$

$$\mu_{(X)_{W\times W}} = \frac{1}{n \times W^2} \sum_{i=1}^{W} \sum_{j=1}^{W} \sum_{p=1}^{n} x_{i,j}^p \tag{3}$$

$$\mu_{(Y)_{W\times W}} = \frac{1}{n \times W^2} \sum_{i=1}^{W} \sum_{j=1}^{W} \sum_{p=1}^{n} y_{i,j}^p \tag{4}$$

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

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

$$\begin{aligned} \sigma_{(X,Y)_{W\times W}} = & \frac{1}{n \times (W-1)^2} \\ & \cdot \sum_{i=1}^{W} \sum_{j=1}^{W} \sum_{p=1}^{n} (x_{i,j}^p - \mu_{(X)_{W\times W}})(y_{i,j}^p - \mu_{(Y)_{W\times W}}) \end{aligned} \tag{7}$$

where the SSIM of $W \times W$ image blocks are calculated separately, and the average of all blocks constitutes the global SSIM between the cover X and the stego Y. $\mu_{(X)_{W\times W}}$ and $\mu_{(Y)_{W\times W}}$ represent the mean of the image elements in the corresponding block. $\sigma_{(X)_{W\times W}}$ and $\sigma_{(Y)_{W\times W}}$ represent the standard deviation of the elements in the corresponding block. $\sigma_{(X,Y)_{W\times W}}$ represents the covariance of the elements in the corresponding block. n is the number of the channel. $\theta_1 = (2^m\xi_1)^2$ and $\theta_2 = (2^m\xi_2)^2$ are constants, 2^m represents the maximum value of the image element, $0<\xi_1, \xi_2 \leq 1$ avoids the case where the denominator is equal to 0.

$S(X, Y) \in [0, 1]$, the more similar the X and the Y, the less the human perception system perceives the change of the image. When the X and the Y are exactly the same, $S(X, Y) = 1$, otherwise $S(X, Y) = 0$. In order to guarantee the imperceptibility of the image, $S(X, Y)$ should be maximized and let it approaches to 1.

Based on hypothesis testing and information entropy, Cachin [41] defined the statistical security concept of steganography. In image steganography, the cross-entropy $H(X, Y) = -\sum XlogY$ essentially be the amount of information generated by the Y analog the X, KL-divergence $D_{KL}(X||Y) = H(X, Y) - H(X)$ represents the amount of the loss information when using the Y analog the X, and it can be used to measures the impact of each image element modification for security.

In the covert communication system based on image steganography, it is assumed that the value of image elements v is a random variable of independent identical distribution (i.i.d.), and $G = \{0, 1, \cdots, 2^m - 1\}$ is a set of all possible values of v, $v \in G$. KL-divergence $L(X, Y)$ from [41] was used to measure statistical distribution of the X and the Y for the security under passive attack.

$$L(X, Y) = D_{KL}(P_x||P_y) = \sum_{k=1}^{|G|} P_x(v) log \frac{P_x(v)}{P_y(v)} \tag{8}$$

where $P_x(v)$ and $P_y(v)$ respectively be the occurrence probabilities of value v in the cover X and the stego Y.

According to the statistical security theory and the distance measure of the statistical distribution, when $L(X, Y) = 0$, the covert communication system based on image steganography is absolutely safe, and when $L(X, Y) \leq \varepsilon$, the system is ε-safe. The smaller $L(X, Y)$, the smaller the difference between the X and the Y, and the higher the security of the system under passive attack. In order to improve the security of the system, $L(X, Y)$ should be minimized and let it approaches to 0.

According to the Equation (2) and (8), the embedded capacity was taked as the constraint and defines the multi-objective optimization problem of image steganography by minimizing the imperceptibility and maximizing the security. Therefore, the EMOsteg in IoT can be formally defined as follows.

$$\begin{cases} min : F(e(X)) = (f_1(e(X)), f_2(e(X))) \\ s.t. \quad \|e(X)\|_0 \leq d \\ \qquad \sum_{p=1}^{n} e_{i,j}^{p} \leq n \\ X, Y \subset \{0, \cdots, 2^{m-1}\}^{w \times h \times n} \\ F = (f_1, f_2) \in \Gamma \subset [0, 1]^2 \end{cases} \tag{9}$$

where perturbation $e(X)$ represents the solution for the EMOsteg. Through the L_0-norm, $\|e(X)\|_0 \leq d$ limits the embedded capacity, $\sum_{p=1}^{n} e_{i,j}^{p} \leq n$ limits the number of bits allowed to be embedded on any image elements. The objective function F defines two optimization goals: $f_1(e(X)) = 1 - S(X, Y)$ and $f_2(e(X)) = 1 - L(X, Y)$.

IV. THE PROPOSED STEGANOGRAPHY

A. DEPLOYMENT SETTING IN IoT

EMOsteg is a typical EMO problem, the artificial immune theory was used to implement EMO in this paper. However, the generation of optimal perturbation by artificial immune theory has to undergo complex artificial immune operations, gene operations and iteration of population. These operations will increase complexity and computational overhead of EMOsteg, which is not suitable for IoT environment with limited terminal performance.

In order to realize EMOsteg in the IoT environment, IoT edge server with high computing power is used to generate optimal perturbation, and the mobile terminal is used to embed the secret according to the perturbation. Through edge computing, the embedding process has low computational overhead and ensures the security of secret. The system deployment setting in IoT of the EMOsteg is shown in Figure 1.

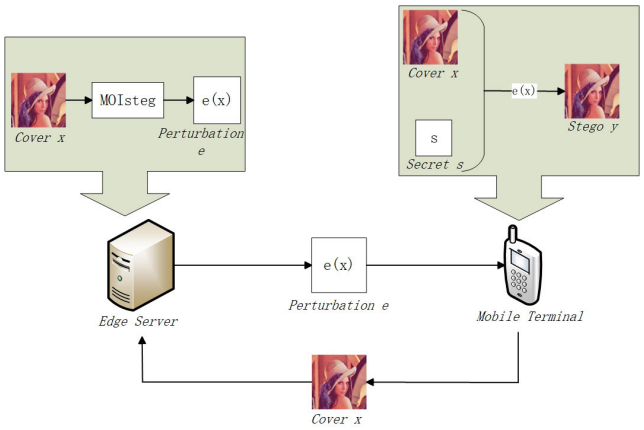

FIGURE 1. Deployment Setting in IoT.

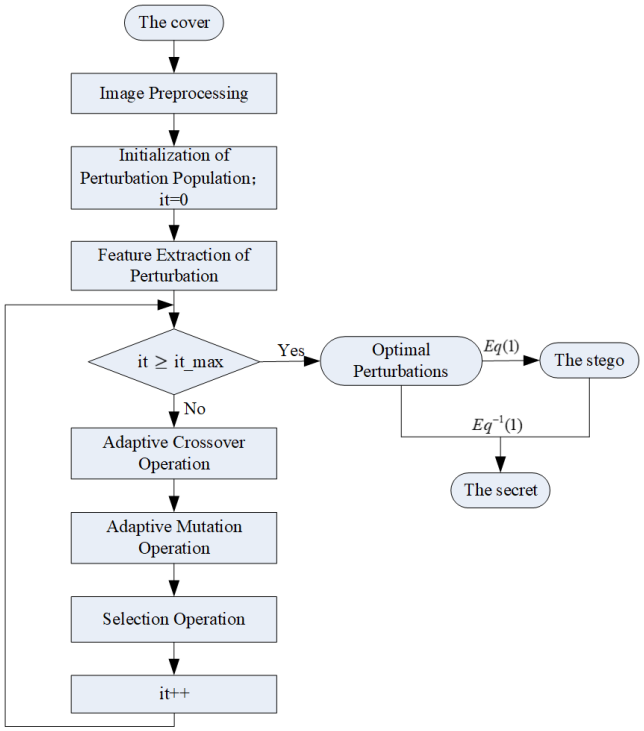

FIGURE 2. The Flow of the EMOsteg.

B. THE OVERALL FLOW

The main work of the EMOsteg is to search the perturbation locations based on artificial immune theory. The artificial immune theory performs optimization of global probability search by simulating natural phenomena or processes, and makes the perturbation has self-organizing, self-learning and dynamic balance features. The overall flow of the EMOsteg is shown in Figure 2.

According to the perturbation locations, Equation (1) and inverse of the Equation (1), the process of secret embedding and extraction are carried out in the mobile terminal.

C. IMAGE PREPROCESSING

The embedding process in the noise/texture regions is an effective way to ensure the imperceptibility and security of the image steganography. Because the noise/texture regions are located in the higher frequency regions of the cover, it can

be filtered by constructed high-pass filters bank and filter residuals are aggregated, so that the noise/texture regions are enhanced while the entity/content regions are suppressed. Through the constructed high-pass filters bank, filter residual $x'_{i,j}$ from [42] is used to instead of image element $x_{i,j}$.

$$x'_{i,j} = N_{i,j} * K_{m_1 \times m_2} - \tau \cdot x_{i,j} \tag{10}$$

where $N_{i,j}$ is the neighborhood of element $x_{i,j}$, $K_{m_1 \times m_2}$ is the kernel of the high-pass filter, m_1 and m_2 determine the type of high-pass filter, * is the convolution operation, $\tau(\tau \geq 0)$ is the order of the residual. In order to avoid the residual value is too high, it is often subtract τ times of the center element. In general, $\tau = 1$, indicating that the center element value is not taken during the calculation.

The convolution operation is performed by the filter kernel and the neighborhood is used to predict the value of the center element $x_{i,j}$. The difference operation between the predicted value and the center element value is used to suppress the image content, so that the noise regions of the image is more obvious.

In this paper, multiple directional and non-directional high-pass filters bank was adopted to preprocess the cover image, and the noise/texture information in different directions is retained to the utmost. Then the filter residuals are aggregated to increase embedded capacity of steganography.

D. INITIALIZATION OF PERTURBATION POPULATION

In the artificial immune theory, the antigen is defined as the objective function and its constraint, namely Equation (9). The antibody against the antigen is the solution of the objective function, that is the perturbation $e(X)$. In order to fit the artificial immune system and process the data of the solution space, the $e(X)$ is serialized in the three-dimensional decision space $w \times h \times n$, thereby the perturbation is represented as a binary code.

$$\delta = Serialize((e^p_{i,j})^n_{w \times h}) = \{0, 1\}^l, \quad l = w \times h \times n$$

where serialized perturbation δ is a candidate solution, perturbation δ has $w \times h \times n$ genes, and each locus can only be the value in the character set $\Phi = \{0, 1\}$.

The fitness function corresponding to the perturbation δ is defined as follows.

$$\begin{aligned} fit(\delta) &= \frac{1}{f_1(\delta) + f_2(\delta)} \\ &= \frac{1}{1 - S(X, Y) + L(X, Y)} \end{aligned} \tag{11}$$

where X is the cover image, the corresponding stego image Y is generated from the perturbation δ and the secret S based on the Equation (1).

The perturbation population $E(it)$ of size N is expressed as follows.

$$E(it) = \{\delta_1(it), \delta_2(it), \cdots, \delta_N(it)\}$$

When initializing a perturbation population, the iterations number $it := 0$.

The matrix of target values obtained from the perturbation population is expressed as follows.

$$F(it) = \begin{pmatrix} f_1(\delta_1(it)) & f_1(\delta_2(it)) & \cdots & f_1(\delta_N(it)) \\ f_2(\delta_1(it)) & f_2(\delta_2(it)) & \cdots & f_2(\delta_N(it)) \end{pmatrix}_{2 \times N}$$

E. FEATURE EXTRACTION OF PERTURBATION

Feature extraction of perturbation corresponds to the vaccine extraction of the artificial immune theory. Based on the schemata theorem and the meaning of the serialized perturbation δ, the definitions of the perturbation schema, the order and the dimension are given in this section. According to these definitions, the constraints that the perturbation needs to satisfy are given.

Definition 1: Perturbation schema $H = \{h_1 h_2 \cdots h_l | h_i \in \{0, *\}, 1 \leq i \leq l, l = w \times h \times n\}$ corresponds to the serialized perturbation δ, where 0 corresponds to the smooth regions of the cover, and these locations cannot be modified. * corresponds to the noise/texture regions of the cover, and these locations might embed the secret.

Definition 2: $o(H)$ is the order of the perturbation schema H, it represents the number of fixed bits in the schema, that is, the length of the 0.

Definition 3: $Dim(H)$ is the dimension of the perturbation schema H, and $Dim(H) = 2^{l-o(H)}$ is the number of perturbation that the schema H can describe.

The feature extraction of perturbation based on the schemata theorem is an estimation of the schema that the perturbation can match, and each perturbation is a sample generated by matching the schema.

According to the Equation (9) and Definitions (1) - (3), the perturbation needs to satisfy features as follows.

$$\begin{cases} \delta = Serialize((e^p_{i,j})^n_{w \times h}) \models H \\ |E| \leq Dim(H) \\ \left\| \delta^{k+1} \delta^{k+2} \cdots \delta^{k+n} \right\|_0 \leq n, 1 \leq k \leq w \times h \\ \|\delta\|_0 \leq d \end{cases} \tag{12}$$

where $\delta \models H$ represents that gene sequence of the perturbation should satisfy the schema H, that is, only the locations corresponding to * can be modified. $|E| \leq d(H)$ represents the relationship between the size of the population and the dimension of the schema H. Through the L_0-norm, $\left\| \delta^{k+1} \delta^{k+2} \cdots \delta^{k+n} \right\|_0 \leq n$ represents the modification of image element per channel, δ^i represents the i-th locus of the gene δ. $\|\delta\|_0 \leq d$ represents that the total embedded capacity of the cover image must be less than the length of secret.

The perturbation feature correspond to the basic information that the solution of the fitness function should satisfy. In order to guarantee each perturbation have higher fitness with greater probability, the EMOsteg initializes the perturbations in the population by constraining the loci of gene based on Equation(12). Initializing the population according to the feature information will promote the iterative evolution of the population, and accelerate the convergence of the algorithm to the global optimal solution.

Algorithm 1 Crossover Algorithm

Input:
The population $E(it)$;
The crossover probability $p_c(it)$;
Output:
The new population $E(it)$ containing progeny perturbations.

$E'(it)$=$E(it)$;
while $|E'(it)| \geq 2$ **do**
  select $\delta_i(it)$ and $\delta_j(it)$ from population $E'(it)$;
  $E'(it) = E'(it) - \{\delta_i(it), \delta_j(it)\}$;
  generate k_1 randomly, $k_1 \in (0, 1)$;
  if $k_1 > p_c(it)$ **then**
    continue;
  else
    select locus k_2 randomly, $1 \leq k_2 \leq w \times h \times n$;
    generate intersection point $k_3 = \lfloor k_2/n \rfloor \times n$;
    exchange all loci of $\delta_i(it)$ and $\delta_j(it)$ after k_3 to generate $\delta'_i(it)$ and $\delta'_j(it)$;
    $E(it) = E(it) \cup \{\delta'_i(it), \delta'_j(it)\}$;
  end if
end while
return $E(it)$;

F. ADAPTIVE EVOLUTION OF PERTURBATION

On the basis of initialized perturbation population, evolution operations prevent the population degradation. Among them, the crossover and the mutation operation ensure the diversity of the population, and selection operation improve the fitness of the population.

1) CROSSOVER OPERATION

Crossover operation expands the global search space. During crossover, two parental perturbations recombine to form new progeny perturbations with the crossover probability. The crossover probability p_c determines the number of operations and the size of the offspring population.

$$p_c(it) = \begin{cases} p_c^{max} - \dfrac{it}{it_{max}} \cdot (p_c^{max} - p_c^{min}), & f_p > f_{avg} \\ p_c^{max}, & f_p \leq f_{avg} \end{cases} \quad (13)$$

where p_c^{max} and p_c^{min} are the maximum and minimum values of the crossover probability, it and it_{max} are the current and maximum iteration number, f_p and f_{avg} are the average fitness of the parents and the population $E(it)$. Through the crossover probability $p_c(it)$, immature convergence is avoided by adopting larger crossover probability in the early stages of evolution and adopting larger crossover probability for individuals with small fitness values.

The EMOsteg algorithm uses a single-point crossover operation on population $E(it)$ to generate new progeny perturbations, which can be described as **Algorithm 1**.

Algorithm 2 Mutation Algorithm

Input:
The population $E(it)$;
The mutation probability $p_m(it)$;
Output:
The new population $E(it)$ containing progeny perturbations.

$E'(it)$=$E(it)$;
while $|E'(it)| \geq 1$ **do**
  select $\delta_i(it)$ from population $E'(it)$;
  $E'(it) = E'(it) - \{\delta_i(it)\}$;
  generate k_1 randomly, $k_1 \in (0, 1)$;
  if $k_1 > p_m(it)$ **then**
    continue;
  else
    $\delta_{new}(it) = \delta_i(it)$;
    select locus k_2 randomly where h_{k_2} equals * in the schema H;
    if $\delta_{new}^{k_2}(it) == 0$ **then**
      select locus k_3 randomly where $\delta_{new}^{k_3}(it)$ equals 1;
      let $\delta_{new}^{k_2}(it) = 1$ and $\delta_{new}^{k_3}(it) = 0$;
    else
      select locus k_4 randomly where h_{k_4} equals * in the schema H and $\delta_{new}^{k_4}(it)$ equals 0;
      let $\delta_{new}^{k_2}(it) = 0$ and $\delta_{new}^{k_4}(it) = 1$;
    end if
    $E(it) = E(it) \cup \{\delta_{new}(it)\}$;
  end if
end while
return $E(it)$;

2) MUTATION OPERATION

Mutation operation improve local search capability of algorithm. One parental perturbation produces a new offspring perturbation by mutation operation with mutation probability $p_m(it)$.

$$p_m(it) = \begin{cases} p_m^{min} + \dfrac{it}{it_{max}} \cdot (p_m^{max} - p_m^{min}), & f_p > f_{avg} \\ p_m^{min}, & f_p \leq f_{avg} \end{cases} \quad (14)$$

where p_m^{max} and p_m^{min} are the maximum and minimum values of the mutation probability. And it, it_{max}, f_p and f_{avg} have same meaning as in Equation (13). As the number of iterations increases, the p_m increases gradually, it ensure global searching in the initial stage of evolution and local searching in the late stage of evolution. The EMOsteg algorithm uses a single-point mutation operation on population $E(it)$ to generate new progeny perturbation, which can be described as **Algorithm 2**.

3) SELECTION OPERATION

Based on the survival of the fittest, perturbations with high probability were selected to form the next iteration population.

Each locus of perturbation δ_i can only be the value in the set $\Phi = \{0, 1\}$, so the bivariate entropy can be used to characterize the similarity of two perturbations. When population size is N', the bivariate entropy $H_{N'}(i)$ of locus i can be expressed as Equation (15).

$$\begin{aligned} H_{N'}(i) &= -p_i \cdot log_2 p_i - (1-p_i) \cdot log_2(1-p_i) \\ &= -\sum_{k=1}^{N'} \delta_k^i / N' log_2 (\sum_{k=1}^{N'} \delta_k^i / N') \\ &\quad -(1-\sum_{k=1}^{N'} \delta_k^i / N') log_2 (1-\sum_{k=1}^{N'} \delta_k^i / N') \end{aligned} \quad (15)$$

where the probability $p_i = \sum_{k=1}^{N'} \delta_k^i / N'$ represents the ratio of the number of perturbations for which locus $i(\delta_k^i)$ is 1 to the size N'. $1 - p_i$ is the ratio of the number of perturbations for which locus i is 0 to the size N'.

If the value of the i-th locus of all perturbations are same, the $H_{N'}(i)$ equals 0.

If $N' = 2$, the bivariate entropy of the i-th locus is $H_2(i)$. The gene similarity of the two perturbations $\delta_{k_1}(it)$ and $\delta_{k_2}(it)$ is expressed as Equation (16).

$$H_2(\delta_{k_1}(it), \delta_{k_2}(it)) = \frac{1}{1 + \frac{1}{l} \sum_{i=1}^{l} H_2(i)} \quad (16)$$

where $l = w \times h \times n$, $H_2(\delta_{k_1}(it), \delta_{k_2}(it)) \in (0, 1]$. The greater the gene similarity, the more similar the two perturbations are.

Definition 4: The relationship R on population $E(it)$ is defined as follows.

$$\begin{aligned} R = \{&\delta_i(it), \delta_j(it) | \\ &(\delta_i(it), \delta_j(it) \in E(it)) \wedge (H_2(\delta_{k_1}(it), \delta_{k_2}(it)) \geq \varepsilon)\} \end{aligned}$$

where ε is similarity coefficient, and $\varepsilon \in (0.75, 1]$.

If two perturbations $\delta_i(it)$ and $\delta_j(it)$ satisfy the relationship $\delta_i(it) R \delta_j(it)$, that is, the gene similarity of two perturbations are greater than the similarity coefficient ε, and the two perturbations are considered to be approximately equal, denoted as $\delta_i(it) \approx \delta_j(it)$. It is not difficult to prove that R is an equivalence relation on the population $E(it)$.

The concentration $D_{\delta_i(it)}$ of the perturbation $\delta_i(it)$ is the ratio of the size of the equivalence class of $\delta_i(it)$ on the relationship R to the current population size.

$$D_{\delta_i(it)} = \frac{|[\delta_i(it)]_R|}{|E(it)|} \quad (17)$$

where $|[\delta_i(it)]_R|$ is the size of the equivalence class of $\delta_i(it)$ on the relationship R, |E(it)| is the current population size.

The selection probability $p_{\delta_i(it)}$ of the perturbation $\delta_i(it)$ is defined as Equation (18).

$$p_{\delta_i(it)} = \alpha \cdot p_{fit_i}(it) + (1-\alpha) \cdot exp(-D_{\delta_i(it)}) \quad (18)$$

$$p_{fit_i}(it) = \frac{fit(\delta_i(it))}{\sum_{k=1}^{|E(it)|} fit(\delta_i(it))} \quad (19)$$

where α is the adjustment factor, $p_{fit_i}(it)$ is the fitness probability, and $exp(-D_{\delta_i(it)})$ is the concentration probability.

The greater the fitness of perturbations, the closer to the optimal solution, and the perturbations will be selected with greater probability. The greater the concentration of perturbations, the more similar perturbations are, which are not conducive to the diversity of the population, and the perturbations will be selected with smaller probability. Through the selection probabilities $p_{\delta_i(it)}$, perturbations with high fitness are selected, and perturbations with high concentrations are inhibited, thereby the population $E(it)$ was promoted and inhibited. The selection operation improves the defect that the traditional genetic algorithm is easy to immature convergence [12], and speeds up the evolution of population to optimal perturbations.

G. OPTIMAL PERTURBATIONS

The Pareto optimal method can obtain optimal solution of EMO problem in the last generation of the populations, and the obtained optimal solution is finally used for the embedding process of the secret which is placed on the mobile terminal.

For any perturbation $\delta_i(it), \delta_j(it) \in E(it)$, $\delta_i(it)$ is Pareto dominant compared to $\delta_j(it)$, if and only if:

$$\begin{aligned} \forall k_1 = 1, 2 \quad & f_{k_1}(\delta_i(it)) \leq f_{k_1}(\delta_j(it)) \\ \wedge \exists k_2 = 1, 2 \quad & f_{k_2}(\delta_i(it)) < f_{k_2}(\delta_j(it)). \end{aligned}$$

$\delta_i(it)$ is Pareto dominant compared to $\delta_j(it)$ also called perturbation $\delta_i(it)$ dominates perturbation $\delta_j(it)$, denoted as $\delta_i(it) \succ \delta_j(it)$.

Perturbation $\delta^*(it) \in E(it)$ is called Pareto optimal perturbation (or non-dominated perturbation), if and only if:

$$\neg \exists \delta_i(it) \in E(it) : \delta_i(it) \succ \delta^*(it)$$

V. EXPERIMENTS RESULT AND ANALYSIS

In experiments, four different filter kernels in different directions from SRM [42] were chose. The Figure 3 shows the $K_{5\times5}$, $K_{1\times4}$, $K_{3\times2}$ and $K_{3\times3}^{max}$, where $K_{3\times3}^{max}$ is the maximum value of the residual obtained by linear filtering in the horizontal and vertical directions.

In order to ensure the evolution of the population and the diversity of the population in the experiments, some parameters are set as follows: $p_c^{max} = 0.95, p_c^{min} = 0.45, p_m^{max} = 0.1$, $p_m^{min} = 0.01, \varepsilon = 0.8, \alpha = 0.9$.

The larger the population size N and the maximum number of iterations it_{max}, the closer the solution is to the optimal solution and the better the diversity. However, the larger values of N and it_{max} will increase the computational cost of the algorithm. In experiments, the Generation Distance (GD) and the Maximum Spread (MS) from [12] were used to determine the values of the N and the it_{max} by analyzing the convergence

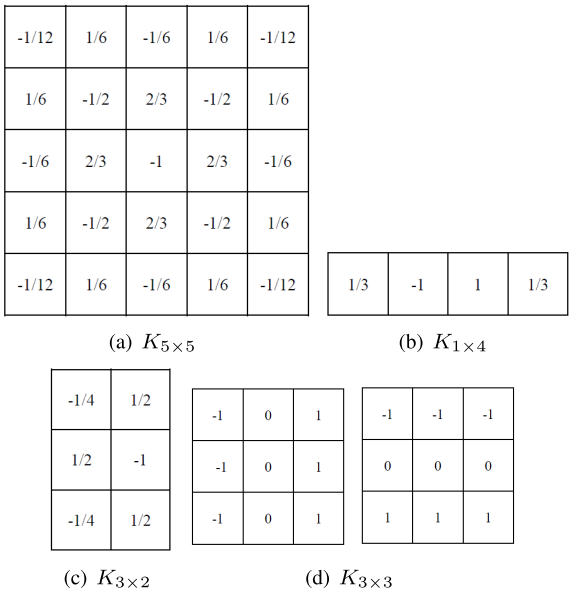

FIGURE 3. Filters bank used in the image preprocessing.

of the proposed algorithm and the diversity of the solutions.

$$GD = \frac{1}{N(it_{max})} \sum_{i=1}^{N(it_{max})} \sqrt{(\delta_i(it_{max}) - \delta^*(it_{max}))^2} \quad (20)$$

where it_{max} is the maximum iteration number, $N(it_{max})$ is the size of the population $E(it_{max})$, $\delta_i(it_{max})$ is the i-th perturbation of $E(it_{max})$, and $\delta^*(it_{max})$ is the optimal perturbation generated after it_{max} times iterations.

$$MS = \sqrt{\frac{1}{\rho} \sum_{i=1}^{\rho} \left(\frac{min(max\{F(it_{max})(i;:)\}, f_i^{max}) - min(min\{F(it_{max})(i;:)\}, f_i^{min})}{f_i^{max} - f_i^{min}} \right)^2} \quad (21)$$

where ρ is the number of the objective functions, $\rho = 2$. $F(it_{max})(i;:)$ corresponding to the values of the i-th objective function of perturbations in the it_{max}-th population. f_i^{max} and f_i^{min} are the maximum and minimum value of the i-th objective function.

When setting $N = 80$, $N = 90$ and $N = 100$, as the iteration number it_{max} continues to increase, the proposed algorithm runs 50 times, the resulting mean of GD and MS are shown in Figure 4 and Figure 5.

Figure 4 and Figure 5 show it_{max} has a significant impact on the quality and distribution of perturbations. The larger the value of it_{max}, the closer the perturbation approximates to the optimal solution, and the wider the distribution of perturbations at the Pareto front that ensures the diversity of the population. However, the change rate of GD and MS gradually decrease after $it_{max} = 500$, which indicating that the perturbations have covered the Pareto front. Considering the space and time complexity, the it_{max} is set to 500, and N is set to 90.

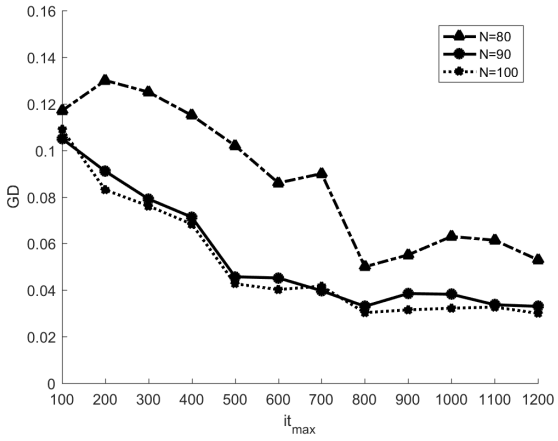

FIGURE 4. Average value of GD under different iterations number.

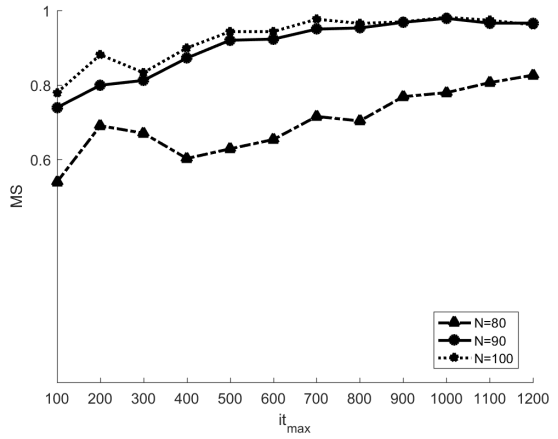

FIGURE 5. Average value of MS under different iterations number.

As the pixels located in noise/texture regions are difficult to model and more tolerate to the modification caused by secret embedding. The WOW [8], S-UNIWARD (UNIWARD for the spatial) [9], MiPOD(Minimizing the Performance of Optimal Detector) [10] and our method all take advantage of the noisy pixels to embed data adaptively, so they were chosen as the comparison methods in the simulation experiment.

The experiments compare imperceptibility, security and embedding time between our steganography and other previous works. Considering the computational power and real-time issues of IoT scenario, the embedded capacity was limited under 0.1 in the experiment. The experiments are conducted on the standard image database called BOSSbase 1.01, and there are 10000 images. 100 images were chose as the cover, the same secret are injected into each cover image under EMOsteg, WOW, S-UNIWARD and MiPOD separately, and the corresponding stego image were generated. The cover images and the corresponding stego images composed the library of sample pairs. Some sample pairs are shown in Figure 6, and the middle column are the results of the high-pass filters bank filtering.

(a) (b)

FIGURE 6. Sample pairs in our library. The first column are the cover images, the middle column are the results of the image preprocessing and the third column are the stego images generated by our method.

TABLE 1. Average values of MSE, PSNR and SSIM for previous and proposed algorithms.

	WOW	S-UNIWARD	MiPOD	EMOsteg
MSE	0.000497	0.00042	0.000333	0.000308
PSNR	81.2074	81.9423	82.6467	82.7501
SSIM	0.9997	0.9997	0.9996	1

The MSE, PSNR and SSIM were used to evaluate the imperceptibility of four algorithms, and the result of Table 1 is the average value of 100 sample pairs. Table 1 summarizes a comparison of the proposed algorithm and the previous algorithms on MSE, PSNR and SSIM.

As shown in Table 1, the proposed algorithm is superior in MSE, PSNR and SSIM, especially in the SSIM. The reason is that EMOsteg uses SSIM as one of the objective functions of the EMO problem to select the optimal perturbation during population evolution.

In order to detect the security, SPA [43]was adopted for steganalysis tool on the sample library for previous and proposed algorithms. The detection error P_E was used to evaluate the security on the library.

$$P_E = \frac{P_{FA} + P_{MD}}{2} \tag{22}$$

where P_{FA} is the false alarm rate, indicating the ratio of the number of the cover image which was detected as the stego image to the number of the cover image. P_{MD} is the missed detection rate, indicating the ratio of the number of the stego image which was detected as the cover image to the number of the stego image. Figure 7 shows a comparison of P_E for different algorithms.

As shown in Figure 7,the proposed algorithm is robust against anti-SPA steganalysis tool. The smaller the relative payload, the stronger the anti-SPA capability of proposed algorithm.

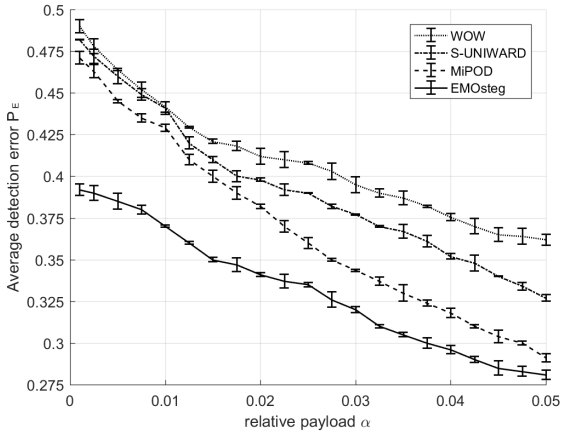

FIGURE 7. Average detection error for previous and proposed algorithms under SPA.

TABLE 2. Average embedding time for previous and proposed algorithms (Unit:second).

WOW	S-UNIWARD	MiPOD	EMOsteg
1.7318	2.0859	11.4991	0.4437

Because the iterative evolution based on artificial immune system is executed on the IoT edge server, the secret embedding on the mobile terminal is very efficient. As shown in Table 2, the proposed algorithm has the faster embedding time, and can meet real-time performance in the IoT environment.

From the perspective of information security, it is impossible that the mobile terminal give the secret to the server, so the entire execution process of previous algorithms have to be finished at the mobile terminal. However, our algorithm uses the edge server to search the perturbation locations, and uses the mobile terminal to embed secret information according to the perturbation locations. So, the embedding time of our algorithm in the mobile terminal is much better than previous algorithms.

EMOsteg expands the solution space through the multi-directional high-pass filter bank. For different cover and secret information, the artificial immune algorithm searches in the solution space iteratively through genetic operations such as feature extraction, mutation, crossover, selection and so on to find the optimal solution with minimum imperceptibility and highest security. With the help of edge computing, EMOsteg deploys complex iterative computing on the edge server, and terminals with limited resources can also realize fast secret embedding. EMOsteg satisfies the real-time and bandwidth requirements of the IoT and realizes covert communication in the IoT environment.

VI. CONCLUSION

Based on artificial immune theory, the evolutionary multi-objective optimization image steganography (EMOsteg)

was proposed. In terms of the indicators of the image steganography, EMOsteg takes the embedded capacity as the constraint condition and defines the EMOsteg by minimizing the imperceptibility and maximizing the security. Through mobile edge computing, the EMOsteg can utilize image steganography to implement covert communication in the IoT. The mobile edge server calculates the perturbation locations of the cover image, then the mobile terminal can embed the secret into the perturbation locations in real time. Compared with other algorithms, the EMOsteg effectively optimizes the imperceptibility of the stego image, resist steganalysis tool better and realize real-time processing.

In this paper, assuming that the elements of the cover image are i.i.d. model in the Equation (8), and compared the first-order statistical distribution between the cover and the stego. The usage of the first-order statistical characteristics ignores the correlation of the elements of cover, does not take into account the high-order statistical characteristics. In the next stage, further expand our algorithm to a universal algorithm for steganography with image, audio and video as covers will be our purpose.

REFERENCES

[1] 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.

[2] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Trans. Multimedia*, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.

[3] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Secur. J., Global Perspective*, vol. 25, nos. 4–6, pp. 197–212, Dec. 2016.

[4] J. H. J. Yin, G. M. Fen, F. Mughal, and V. Iranmanesh, "Internet of Things: Securing data using image steganography," in *Proc. 3rd Int. Conf. Artif. Intell., Modelling Simulation (AIMS)*, Dec. 2015, pp. 310–314.

[5] P. Corcoran and S. K. Datta, "Mobile-edge computing and the Internet of Things for consumers: Extending cloud computing and services to the edge of the network," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 73–74, Oct. 2016.

[6] R. Grover, D. K. Yadav, D. K. Chauhan, and S. Kamya, "Adaptive steganography via image complexity analysis using 3D color texture feature," in *Proc. 3rd Int. Innov. Appl. Comput. Intell. Power, Energy Controls Impact Humanity (CIPECH)*, Nov. 2018, pp. 1–5.

[7] B. Xue, X. Li, and Z. Guo, "A new SDCS-based content-adaptive steganography using iterative noise-level estimation," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Adelaide, SA, Australia, Sep. 2015, pp. 68–71.

[8] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Tenerife, Spain, Dec. 2012, pp. 234–239.

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

[10] 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.

[11] T. Denemark and J. Fridrich, "Steganography with multiple JPEG images of the same scene," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2308–2319, Oct. 2017.

[12] Y. Xie and J. Wu, "Multi-objective constraint task scheduling algorithm for multi-core processors," *Cluster Comput.*, vol. 22, no. 3, pp. 953–964, Sep. 2019.

[13] H. S. Leng and H. W. Tseng, "High payload data hiding based on just noticeable distortion profile and LSB substitution," in *Proc. 12th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Kaohsiung, Taiwan, vol. 1, Nov. 2016, pp. 59–66.

[14] R. Tavares and F. Madeiro, "Word-hunt: A LSB steganography method with low expected number of modifications per pixel," *IEEE Latin Amer. Trans.*, vol. 14, no. 2, pp. 1058–1064, Feb. 2016.

[15] J. Deng, M. Tang, Y. Wang, and Z. Wang, "LSB color image embedding steganography based on cyclic chaos," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2019, pp. 1798–1802.

[16] M. Hussain, A. W. A. Wahab, N. B. Anuar, R. Salleh, and R. M. Noor, "Pixel value differencing steganography techniques: Analysis and open challenge," in *Proc. IEEE Int. Conf. Consum. Electron.*, Taipei, Taiwan, Jun. 2015, pp. 21–22.

[17] X. Liao, S. Guo, J. Yin, H. Wang, X. Li, and A. K. Sangaiah, "New cubic reference table based image steganography," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 1–18, 2017.

[18] M. Hussain, A. W. A. Wahab, A. T. S. Ho, N. Javed, and K.-H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Process., Image Commun.*, vol. 50, pp. 44–57, Feb. 2017.

[19] W.-L. Lee and W. Sun, "Reversible steganography scheme based on position-recording in DCT coefficients," in *Proc. 15th Int. Conf. Comput. Intell. Secur. (CIS)*, Macao, Dec. 2019, pp. 424–428.

[20] S. Kamila, R. Roy, and S. Changder, "A DWT based steganography scheme with image block partitioning," in *Proc. 2nd Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Noida, India, 2015, pp. 471–476.

[21] S. K. Yadav and M. Dixit, "An improved image steganography based on 2-DWT-FFT-SVD on YCBCR color space," in *Proc. Int. Conf. Trends Electron. Inform. (ICEI)*, Tirunelveli, India, 2017, pp. 567–572.

[22] T. H. Thai, R. Cogranne, and F. Retraint, "Statistical model of quantized DCT coefficients: Application in the steganalysis of Jsteg algorithm," *IEEE Trans. Image Process.*, vol. 23, no. 5, pp. 1980–1993, May 2014.

[23] T. H. Thai, R. Cogranne, and F. Retraint, "Optimal detection of outguess using an accurate model of DCT coefficients," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2014, pp. 179–184.

[24] H. Ghasemzadeh and M. K. Arjmandi, "Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system," *IET Signal Process.*, vol. 11, no. 8, pp. 916–922, Oct. 2017.

[25] B. Zhang, F. Gianesello, S. Erba, M. Meghelli, A. Emami, and T. Shibasaki, "F5: Advanced optical communication: From devices, circuits, and architectures to algorithms," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2018, pp. 514–516.

[26] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using statistical image model for JPEG steganography: Uniform embedding revisited," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2669–2680, Dec. 2015.

[27] L. Guo, J. Ni, and Y. Q. Shi, "Uniform embedding for efficient JPEG steganography," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 814–825, May 2014.

[28] Z. Wang, Z. Qian, X. Zhang, M. Yang, and D. Ye, "On improving distortion functions for JPEG steganography," *IEEE Access*, vol. 6, pp. 74917–74930, 2018.

[29] W. Lu, L. He, Y. Yeung, Y. Xue, H. Liu, and B. Feng, "Secure binary image steganography based on fused distortion measurement," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 6, pp. 1608–1618, Jun. 2019.

[30] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-based adversarial embedding for image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2074–2087, Aug. 2019.

[31] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-Net structure," *IEEE Access*, vol. 7, pp. 9314–9323, 2019.

[32] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Access*, vol. 6, pp. 38303–38314, 2018.

[33] H. Naito and Q. Zhao, "A new steganography method based on generative adversarial networks," in *Proc. IEEE 10th Int. Conf. Awareness Sci. Technol. (iCAST)*, Oct. 2019, pp. 1–6.

[34] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "SSGAN: Secure steganography based on generative adversarial networks," in *Proc. 18th Pacific-Rim Conf. Multimedia*, Harbin, China, Sep. 2017, pp. 534–544.

[35] G.-S. Lin, Y.-T. Chang, and W.-N. Lie, "A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm," *IEEE Trans. Multimedia*, vol. 12, no. 5, pp. 345–357, Aug. 2010.

[36] A. H. Mohsin, A. N. Jasim, A. H. Shareef, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, S. Nidhal, and N. S. Jalood, "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.
[37] 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.
[38] F. R. Alonso, D. Q. Oliveira, and A. C. Z. de Souza, "Artificial immune systems optimization approach for multiobjective distribution system reconfiguration," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 840–847, Mar. 2015.
[39] 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)*, Mumbai, India, Apr. 2017, pp. 133–138.
[40] 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, 2019.
[41] C. Cachin, "An information-theoretic model for steganography," *Inf. Comput.*, vol. 192, no. 1, pp. 41–56, Jul. 2004.
[42] 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.
[43] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7, pp. 1995–2007, Jul. 2003.

XUYANG DING received the B.E. and Ph.D. degrees in computer science and engineering from the University of Electronic Science and Technology of China, in 2003 and 2008, respectively. He is currently an Associate Professor with the University of Electronic Science and Technology of China. His research interests include computer networks, cyber security, and artificial intelligence.

YING XIE received the B.E. degree in computer science and engineering from the University of Electronic Science and Technology of China, in 2006, and the Ph.D. degree from the Chengdu Institute of Computer Application, University of Chinese Academy of Sciences, in 2018. She is currently an Associate Professor with Southwest Minzu University. Her research interests include cyber security, formal verification, and distributed computing.

PENGXIAO LI received the Ph.D. degree in electronics science and technology from Tsinghua University, in 2013. He is currently a Senior Engineer with CNCERT/CC. His current research interests include communication technology, data mining, and machine learning.

MENGTIAN CUI received the Ph.D. degree from the Chengdu Institute of Computer Application, University of Chinese Academy of Sciences, in 2010. She is currently a Professor with Southwest Minzu University. Her research interests include computer networks, cyber security, and formal method. She is also reserve candidate for academic and technical leaders in Sichuan Province, in 2013.

JIANYING CHEN received the Ph.D. degree in computer science and engineering from the University of Electronic Science and Technology of China. She is currently a Professor with Southwest Minzu University. Her research interests include cyber security, artificial intelligence, distributed computing, and computer architecture. She is also undersecretary general of Sichuan Province the Internet of Things Talents Commission.