Hindawi
Security and Communication Networks
Volume 2024, Article ID 9842418, 1 page
https://doi.org/10.1155/2024/9842418

Retraction

Retracted: Image Encryption Algorithm Based on Artificial Bee Colony Algorithm and Chaotic System

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zhou, E. Wang, X. Song, and M. Shi, "Image Encryption Algorithm Based on Artificial Bee Colony Algorithm and Chaotic System," *Security and Communication Networks*, vol. 2022, Article ID 1444676, 20 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 1444676, 20 pages
https://doi.org/10.1155/2022/1444676

Research Article

Image Encryption Algorithm Based on Artificial Bee Colony Algorithm and Chaotic System

Yanqi Zhou, Erfu Wang, Xiaomeng Song, and Mengna Shi

Electrical Engineering College, Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Erfu Wang; wangerfu@hlju.edu.cn

Received 23 January 2022; Revised 9 March 2022; Accepted 1 April 2022; Published 18 May 2022

Academic Editor: Xingsi Xue

This article proposes an image encryption algorithm based on a chaotic bit-plane decomposition and optimization algorithm of a crossover operator artificial bee colony algorithm. Firstly, use the SHA-256 hash algorithm to calculate the plaintext image's hash value as the starting value of the fractional Lorenz hyperchaotic system after operation. Utilize the chaotic sequence to permutate plaintext image in a bit plane to obtain the scrambled image. Secondly, block the scrambled image into four subimages of equal size, and count the hash value of each row of each block by the SHA-256 hash algorithm as the starting value of the Sine-Tent-Logistic chaotic system. Use the obtained chaotic sequence to substitute the images. Then, stitch the four sub-block images to get the final encrypted image, and the population is obtained. Finally, use the information entropy of ciphertext image as the fitness function of the artificial bee colony algorithm based on a crossover operator. Select the ciphertext image with the best information entropy from the population as the optimal encrypted image, and then, return the position value of the best honey source meanwhile. The experimental simulation and security analysis indicate that the scheme has an excellent encryption effect and ability to oppose various general attacks.

1. Introduction

With the advancement of network technology, the era of message integration is approaching, and information and data security is becoming increasingly important [1]. Because of its intuitive, vivid, and realistic qualities, image information has become a crucial carrier in human social interactions and information transfer. The safety of photographs is really important. Image encryption is a specific technology used to address image security concerns. Traditional encryption methods, such as DES [2] and AES [3], cannot meet the present needs of picture encryption due to the characteristics of a large number of data, strong correlation, and high redundancy. Therefore, lots of encryption algorithms have been proposed, such as compressed sensing theory [4, 5], chaos theory [6–10], and DNA coding theory [11–13].

For the past few years, many scholars used chaotic systems widely in image encryption systems because of their extreme sensitivity to starting conditions and unpredictability. They outperform other encryption algorithms in terms of encryption effectiveness. Generally, this algorithm contains two main steps: permutation and substitution. The permutation operation changes the location of the pixel to reduce the correlation between neighboring pixels. The purpose of the substitution operation is to alter the size of the pixel value, and the plaintext image becomes another different image. Pan et al. [14] came up with an encryption operation using a double logistic chaotic system to achieve image substitution prior to scrambling and finally obtain the encrypted image. However, the histogram distribution and information entropy of the encrypted image by this method are poor, making it vulnerable to attackers. Liu et al. [15] put forward a new hyperbolic sine chaotic system to figure out the problem of low security of the traditional chaotic system. The generated chaotic sequence has good pseudorandom characteristics and employs it for image substitution operation and row-column operation. The algorithm has a good encryption effect. However,

compared with other encryption algorithms, the information entropy of encrypted images has some shortcomings.

However, the problems caused by chaotic systems still need to be solved. The loss of chaotic dynamic properties generated by the digital chaotic system's finite precision impact is particularly damaging, as it directly undermines the chaotic system's security in cryptographic systems. Peng et al. [16] put forward a high-dimensional chaotic map based on discrete memristor, and experimental simulation shows that the discrete memristor model can not only expand the hyperchaotic region, but also further improve the complexity of the system. Li et al. [17] discovered that the phase space of the Cat map executed on a digital computer has a severe regular pattern that differs significantly from the phase space in the infinite precision torus; Ma et al. [18] investigated the security of an image block encryption algorithm based on multiple chaotic maps and discovered it to be insecure.

The chaotic system proposed in Ref [19] is formed by fusing and cascading three one-dimensional chaotic maps. Firstly, Tent map and Logistic map are fused to generate a new chaotic system; then, the Sine map and the map generated in the first step are employed for cascade operation. The chaotic system enhances the Lyapunov exponent of the chaotic system, effectively strengthens the chaotic state, prolongs the period efficiently, and delays the degradation as much as possible. The fractional hyper-Lorenz chaotic system, as presented in Ref [20], is also used in this article. The fractional hyperchaotic dynamic system has more complex and rich dynamic characteristics than the integer-order system, with the added benefit of increasing randomness and unpredictability. Moreover, the fractional hyperchaotic system can provide more key parameters for the encryption system, expanding the key space and improving the system's security properties. Meanwhile, in view of the unique memory characteristics of the hyperchaotic system, it can effectively increase the complexity of chaotic sequence and make encryption more secure. Therefore, the chaotic systems used in this article can effectively avoid the degradation of chaotic systems under finite accuracy.

The permutation and substitution processes are two independent processes that are rarely linked to one another. Therefore, some researchers have presented a bit-plane decomposition image encryption algorithm. Bit-plane decomposition encryption is able to implement scrambling operation and change the value of pixels at the same time, allowing the scrambling and substitution processes to run concurrently. Zhou et al. [21] presented an encryption algorithm using Fibonacci p-code to decompose the plaintext image into a certain number of bit-plane images, shuffled all the bit-plane images using the key, adjusted the size of the bit plane using 2D p-Fibonacci transform, and encrypted all the bit planes, and finally, all bit planes are merged to get the last encrypted image. The experimental simulation suggests the arithmetic has an encryption effect, but as is shown from the histogram of the encrypted image that the histogram of the encryption algorithm is not flat, contains some spikes, and is likely to be subject to statistical attacks by the attacker. Rathore and Pal [22] put forward an image encryption arithmetic based on the combination of bit plane decomposition and chaotic system. The proposed method used the sequence generated by two-dimensional Henon chaos to substitute the plaintext image, decomposed the substituted image into eight-bit-plane images, and reconstructed the sequence generated by two-dimensional Henon chaos into a binary key matrix. Eight different binary edge planes are obtained by edge detection and then XOR with the corresponding bit planes after substitution. Finally, the eventual encrypted image is gained by merging the eight-bit planes. But the simulation results indicate that the encryption effect cannot achieve the optimal consequence, and the correlation between the encryption algorithm and plaintext is not good. When it is subjected to a selective plaintext assault or a differential attack, it is vulnerable to information leaking.

In recent years, many researchers have applied the heuristic evolutionary algorithm to the field of image encryption. Choosing the appropriate fitness function to optimize the generated key or ciphertext image is optimal. Abdullah et al. [23] put forward an encryption scheme based on a hybrid genetic algorithm and chaotic system. The logistic mapping function is used to encrypt the image, and multiple encrypted images create the starting population of the genetic algorithm. The genetic algorithm optimizes the encrypted image and chooses the optimal encryption image based on its low correlation coefficient and high information entropy. Ghazvini et al. [24] came up with a hybrid image encryption method based on GA and chaos. The encryption scheme contains three major steps: scrambling stage, substitution stage, and optimization stage employing GA. Mozaffari put forward a parallel image encryption algorithm based on bit-plane decomposition [25]. The original gray image is transformed into a binary image by local binary mode and bit-plane decomposition method. Use the multipopulation GA to complete the scrambling and replacement operation through crossover and mutation operation. Finally, gain the final encrypted image by merging. It is hard to select parameters of a genetic algorithm, which requires a sequence of processes such as selection, crossover, and mutation. If the parameters are not carefully chosen, they'll slip into local convergence, causing premature convergence and so on. Dua et al. [26] generate a mask sequence with the help of differential evolution technique, which is further converted to DNA and utilized in the DNA diffusion process. Saravanan and Sivabalakrishnan adopted an improved meta-heuristic algorithm termed as CI-WOA for optimizing the parameters [27]. Liu et al. proposed to use a hybrid chaos system and an artificial fish swarm neural network to encrypt images, which is used to train the hybrid random array and remove its chaotic periodicity, allowing the neural network sequence to be obtained [28].

Because of the simplicity of the chaotic system, the key space is too minor to stand up to exhaustive attack; the correlation between encryption scheme and plaintext is low,

resulting in a weak ability to resist selected plaintext attack, known-plaintext attack, and differential attack; the artificial bee colony algorithm is a simple and efficient optimization algorithm to simulate bee behavior. Role switching is a unique mechanism of the artificial bee colony algorithm. The mutual conversion and perfect cooperation between different bee species enable bees to find a better location of honey source in any environment. The artificial bee colony algorithm has a positive and negative feedback mechanism. When the hired bees find a high-quality honey source, they can recruit more observation bees to follow. If there are fewer honey sources, the number of observation bees recruited will also be reduced. In this way, the positive and negative feedback cooperate with each other to find the optimal honey source more efficiently. Particle swarm optimization has only positive feedback mechanism, and the effect and efficiency of optimization will be reduced. Compared with other optimization algorithms, the artificial bee colony algorithm has a small number of parameters, which can reduce the impact of artificial parameter setting as much as possible, and this article presents an image encryption method based on chaotic bit-plane decomposition and optimization algorithm of the crossover operator artificial bee colony algorithm. The main contributions of this article are as follows:

(1) A ciphertext image optimization algorithm based on artificial bee colony is proposed

(2) Introducing crossover operator into the artificial bee colony algorithm can generate new individuals and enrich population diversity

(3) Calculating the hash value for pixel values of each block and each line of the scrambled image strengthens the connection between bit-plane scrambling and diffusion

(4) The hash value of the plaintext image is calculated as key, which enhances the relationship between encryption and plaintext, and enhances the ability to resist selective plaintext attack

The rest of the article arranges as follows: Section 2 introduces the basic principles of the algorithm, Section 3 concretely presents the encryption method proposed in this article, the experimental results and security analysis are given in Section 4, and the conclusion is presented in Section 5.

2. Preliminary Works

Because of the randomness, ergodicity, uncertainty, and sensitivity to initial conditions and parameters, chaotic systems are extensively employed in privacy communication systems. This article uses the fractional-order super Lorenz chaotic system and the Sine-Tent-Logistic chaotic system. The artificial bee colony algorithm is a heuristic optimization algorithm, which can be used in this article to optimize the encrypted image to obtain an encrypted image with a better encryption effect.

2.1. The Fractional Hyper-Lorenz Chaotic System. The fractional-order chaotic dynamic system has more complicated and rich dynamic features than the integer-order system, with the added benefit of enhancing randomness and unpredictability. In addition, a fractional-order chaotic system can offer more significant parameters for the encryption system, thus increasing the key space and further enhancing the security characteristics of the system. The complexity of the chaotic sequence may be effectively increased, and the encryption is more safe, thanks to the fractional chaotic system's unique memory features. Many academics have employed fractional-order chaotic systems to encrypt photos in recent years. Kaur et al. [29] presented a new opto-digital color picture encryption scheme based on compound chaotic mappings, the reality-preserving fractional Hartley transformation, and the piecewise linear chaotic map for image pixel replacement, optical processing, and permutation. The presented picture encryption technique has a greater level of protection and heightened sensitivity to keys. Kaur et al. [30] proposed a multiple order optical transformation encryption scheme for two-dimensional image encryption based on chaos. The transform coefficients are calculated in the collective time-frequency domain using the multiparameter fractional Fourier transform of chaotic ordering. Two piecewise linear chaotic maps (PWLCMs) are used to generate multiple transformation orders along two dimensions. The two chaotic sequences generated by PWLCM are substituted in the proposed transform (C-MOFRFT) and then permutated in the C-MOFRFT domain based on an integrated chaotic mapping. The mathematical model of the fractional hyper-Lorenz chaotic system [20] used in this article is as follows:

$$\begin{cases} \dfrac{d^{q1}x}{\mathrm{d}t^{q1}} = \sigma(y-x) + w \\ \dfrac{d^{q2}y}{\mathrm{d}t^{q2}} = rx - y - xz \\ \dfrac{d^{q3}z}{\mathrm{d}t^{q3}} = xy - \beta z \\ \dfrac{d^{q4}w}{\mathrm{d}t^{q4}} = \mathrm{d}w - xz \end{cases}, \tag{1}$$

where x, y, z, w represent the state variables of the system, when $\sigma = 10, \beta = 8/3, r = 28, d = 1.3, q_1 = q_2 = q_3 = q_4 = 0.995$, and the system is in a chaotic state.

2.2. The Sine-Tent-Logistic Chaotic System. Integer-order chaotic systems include one-dimensional chaotic systems and hyperchaotic systems. One-dimensional chaotic systems generally contain the Logistic chaotic map, Sine chaotic map, and Tent chaotic map. Most of these one-dimensional chaotic systems only comprise one variable and some parameters, making them vulnerable to attackers and resulting in information leakage. In this article, we use the chaotic

system proposed in Ref [19]. The mathematical model of the Sine-Tent-Logistic(STL) chaotic system is

$$Z_{n+1} = \begin{cases} \sin\left[\pi\left(\left(1-2*\left|Z_n-0.5\right|\right)+\left(\mu*Z_n*\left(1-Z_n\right)\right)\right)\right]-1, & Z_n>1 \\ \sin\left[\pi\left(\left(1-2*\left|Z_n-0.5\right|\right)+\left(\mu*Z_n*\left(1-Z_n\right)\right)\right)\right]+1, & Zn<0 \end{cases}. \tag{2}$$

The Lyapunov index of the STL chaotic system is greater than 0 at any value in the parameter $\mu \in (0, 8)$. The chaotic sequence generated has good pseudorandom characteristics.

2.3. Artificial Bee Colony Algorithm. Artificial bee colony algorithm is a bionic swarm intelligence optimization algorithm based on a bee honey collection mechanism. In 2005, Professor Karaboga of Erciyes University in Turkey first proposed the artificial bee colony algorithm model [31]. It has been one of the hotspots of bionic intelligent algorithm research in recent years. Each nectar source symbolizes a feasible solution to the optimization problem in the implementation phase of the algorithm, and the pollen number of nectar sources is the fitness function value in the optimization problem. Let the feasible solution of the optimization problem be a D-dimensional vector $X = \{x_1, x_2 \ldots, x_D\}$, and the population with N feasible solutions is expressed as $S = \{X_1, X_2 \ldots, X_N\}$; specific processes of the artificial bee colony algorithm is described as follows:

(1) Colony initialization: The algorithm generates a certain number of food sources randomly at the initial stage in the feasible range. The following formula determines the initial location of the nectar source:

$$x_i^j = x_{\min}^j + r\text{and}[0,1]\left(x_{\max}^j - x_{\min}^j\right), \quad i = \{1, 2, \ldots, N\}, j = \{1, 2, \ldots, D\}, \tag{3}$$

where x_i^j represents the jth dimension of the x_i, rand$[0, 1]$ is a random digit between 0 and 1, and $x_{\max}^j, x_{\min}^j$ denote the maximum and minimum of the jth dimension of x_i.

(2) Hiring bee stage: Use equation (4) to seek the location of the nectar source near the initial food source, start a local search, judge the fitness of each nectar source, and judge the quality of the nectar source by the fitness value. Equation (5) employs a greedy approach to save the better solution:

$$v_i^j = x_i^j + \phi_i^j\left(x_i^j - x_k^j\right). \tag{4}$$

$$v_i = \begin{cases} v_i, & \text{fit}\left(v_i\right) > \text{fit}\left(x_i\right), \\ x_i, & \text{fit}\left(v_i\right) < \text{fit}\left(x_i\right), \end{cases} \tag{5}$$

where x_k represents the adjacent food source, x_i represents the current food source, $k = \{1, 2, \ldots, N\}, k \neq i, \phi_i^j \in [-1, 1]$ indicates the rate of change of food sources, and fit represents the fitness function.

(3) Observation bee stage: The observation bees select the excellent nectar sources searched by the employed bees according to the probability and then further search for the better food sources in the neighborhood. Observing bees conduct a local search near the food source according to equation (4) to generate new individuals with higher quality and use the greedy mechanism to save better solutions. Among them, the selection probability is

$$P_i = \frac{\text{fit}_i}{\sum_{i=1}^{N} \text{fit}_i}, \quad i = \{1, 2, \ldots, N\}. \tag{6}$$

(4) Investigation bee stage: Abandon a food source x_i if it does not renew after several collection. The corresponding hired bees or observation bees will transform into observation bees. The Scout bees construct a new food supply at random, move the nectar source around, and continue to search for the best answer in the global range.

3. Proposed Encryption and Optimization Algorithm

This article first uses the fractional Lorenz hyperchaotic system to scramble each bit plane of the plaintext image and then recombines the 8-bit planes into a scrambled image after scrambling. Split the scrambled image into blocks, and then, each piece is substituted by the Sine-Tent-Logistic chaotic system to generate an initial population containing multiple encrypted images. Apply the artificial bee colony algorithm based on a crossover operator to optimize the initial population and the entropy of the encrypted image used as the fitness function of the artificial bee colony algorithm. Several repetitions are used to get the best ciphertext image with the most information entropy; the position value of the best honey

source returns to facilitate subsequent decryption meanwhile. The specific encryption process is described below.

3.1. Key Generation. The key of this article consists of two parts. The first part is the key needed in bit-plane scrambling. Calculate the hash value of the plaintext image according to the SHA-256 hash algorithm. The result of the SHA-256 hash algorithm is a 256 bit hash value. Every 4 bit binary number is transformed into a hexadecimal number and finally obtained a string of 64 hexadecimal numbers: $\text{key}_1 = \{k_1, k_2, \ldots, k_{64}\}$. After an initial value substitution iteration, the fractional hyper-Lorenz chaotic system will generate four groups of different chaotic sequences X, Y, Z, and W. Because this article needs to scramble 8-bit planes, eight groups of chaotic sequences are required. It is necessary to generate 8 initial values, which are divided into two groups and substituted into the fractional hyperchaotic system to generate 8 chaotic sequences. So, it is necessary to divide the key_1 into eight blocks via the following equation:

$$\text{key}_{1i} = k_{8i-7}, k_{8i-6}, \ldots, k_{8i}, \quad i = \{1, 2, \ldots, 8\}. \tag{7}$$

Because the key_{1i} is an 8-bit hexadecimal number that must be quantized to create a decimal number between 0 and 1, use it as the initial value of the fractional hyper-Lorenz chaotic system and substitute it into the chaotic system to iteratively obtain the chaotic sequence by the following equation:

$$u_i = \frac{\text{hex 2 dec}\left(\text{key}_{1i}\right)}{\text{hex 2 dec}\underbrace{(FF \ldots F)}_{8}}, \quad i = \{1, 2, \ldots, 8\}, \tag{8}$$

where hex 2 dec is a function in MATLAB that can convert hexadecimal numbers to decimal numbers, and the $\underbrace{FF \ldots F}_{8}$ is the maximum value in eight-bit hexadecimal number. Assign $u_i, i = \{1, 2, \ldots, 8\}$ to $x_0, y_0, z_0, w_0, x_1, y_1, z_1, w_1$. By substituting them into the chaotic system as the initial values of two groups of chaotic systems for iterative operation, eight groups of chaotic sequences to scramble the bit plane of the original plaintext image are obtained.

The second part is the key needed in the substitution process after bit-plane scrambling. Get a scrambled image after the bit plane permutation operation finishes. The scrambled image divides into four sub-block images of equal size; adopt the SHA-256 algorithm to calculate the hash value of all pixel values of each block and each line to calculate the $\text{key}_{2i,j}$ via the following equation:

$$\text{key}_{2i,j} = \frac{\text{hex 2 dec}\left(\text{hash}\left(x_{i,1}, x_{i,2}, \ldots, x_{i,M/2}\right)\right)}{\text{hex 2 dec}\underbrace{(FF \ldots F)}_{64}}, \quad i = 1, 2, 3, 4,\ j = \{1, 2, \ldots, N/2\}, \tag{9}$$

where $x_{i,1}, x_{i,2}, \ldots, x_{i,M/2}$ represents all pixel values of the ith row of the block image, and hash calls the SHA-256 hash algorithm adopted in this article to get a 64 bit hexadecimal number string. Use the hex 2 dec function to convert the hexadecimal number into a decimal number, and quantize it to 0-1 as the initial value of the Sine-Tent-Logistic chaotic system.

3.2. Bit-Plane Scrambling Algorithm Based on Fractional Lorenz Hyperchaotic System. Any non-negative integer N can be described by a string of n-bit binary sequences. In gray images, the range of pixel value is between [0, 255], so each pixel value can be described by a series of 8-bit binary sequences. A gray image can be decomposed into 8-bit-plane images [32]. The ith bit plane is composed of the ith bit of the binary of each pixel value. The bit-plane decomposition of the original gray image yielded eight-bit-plane images in Figure 1.

Bit-plane scrambling not only realizes the global scrambling of image pixel position but also changes the pixel value. It can smooth out the histogram of scrambled photos, reducing the risk of information leaking.

The pseudocode of bit-plane scrambling algorithm based on the fractional Lorenz hyperchaotic system is shown in Algorithm 1.

3.3. Substitution Algorithm Based on Sine-Tent-Logistic Chaotic System. The chaotic substitution process changes the pixel value of the original image information to generate another different image. This section uses the Sine-Tent-Logistic system to perform substitution processing on the scrambled image and repeats the operation $N/2$ times to generate the initial population required for the subsequent artificial bee colony optimization operation. The specific substitution steps are as follows:

(1) The scrambled image P_{con} received in the preceding step is divided into four blocks, and the size of each block is $M/2 \times N/2$.

(2) According to Section 3.1, calculate the hash value of each block and each row after block and employ it as the chaotic initial value u_0 of Sine-Tent-Logistic after quantization.

(3) In order to get three different chaotic sequences, set three different parameters of the chaotic system—$\mu_1 = 3.9999, \mu_2 = 3.7777, \mu_3 = 3.5555$, substituting parameters and u_0 into the Sine-Tent-Logistic chaotic system. Pre-iterate the chaotic map 1000 times to eliminate the adverse consequences caused by transient reactions and continue to iterate $M/2 \times N/2$ times. Get the chaotic sequence u_1, u_2, u_3 according to the following equation:

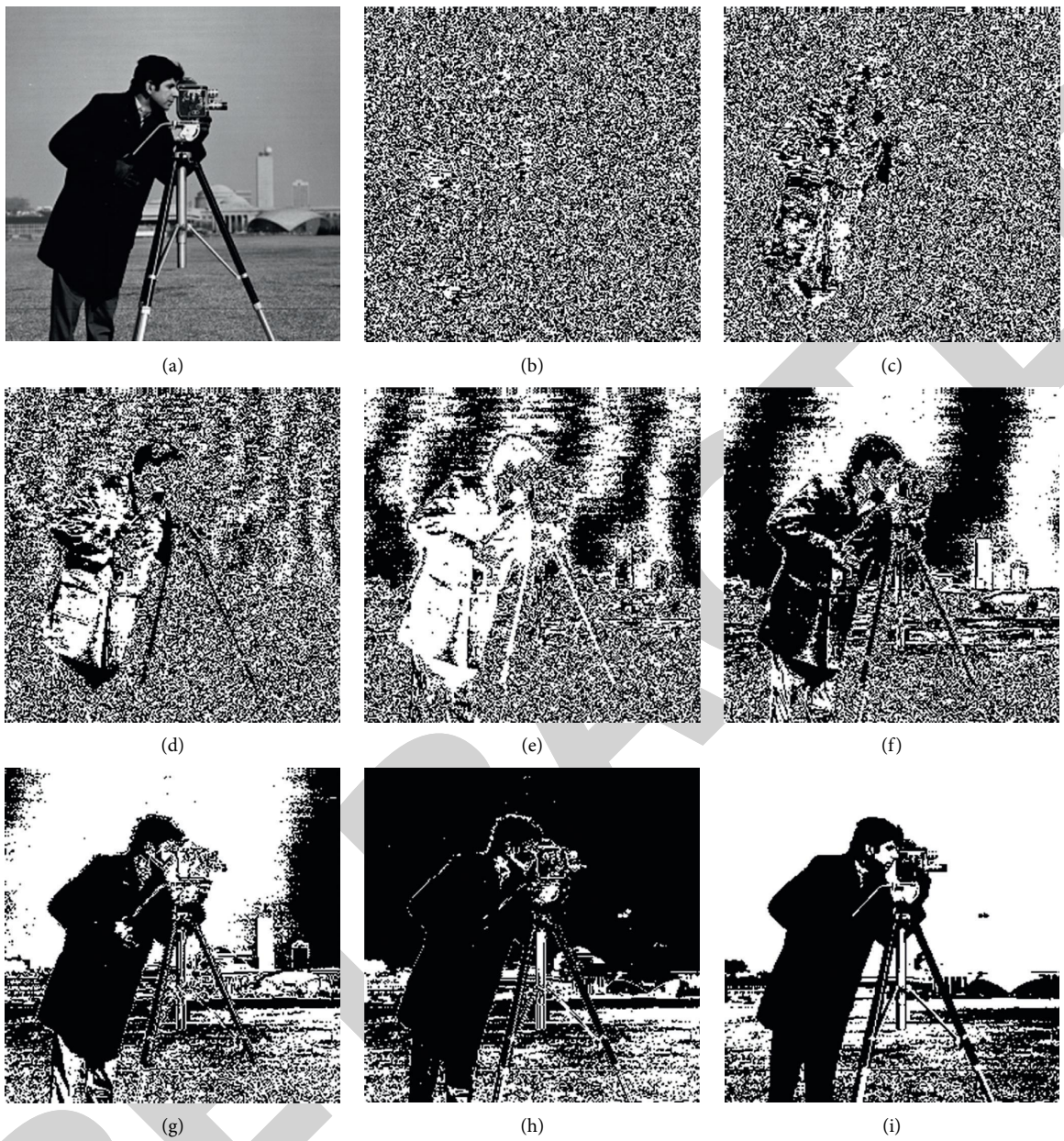


Figure 1: Bit-plane decomposition: (a) cameraman plain image; (b) first-order bit image; (c) second-order bit image; (d) third-order bit image; (e) fourth-order bit image; (f) fifth order bit image; (g) sixth-order bit image; (h) seventh-order bit image; (i) eighth-order bit image.

$$\begin{cases} u_1 = \text{round}\left(\text{STL}\left(u_0, \mu_1, \dfrac{M}{2} \times \dfrac{N}{2}\right) * 255\right), \\ u_2 = \text{round}\left(\text{STL}\left(u_0, \mu_2, \dfrac{M}{2} \times \dfrac{N}{2}\right) * 255\right), \\ u_3 = \text{round}\left(\text{STL}\left(u_0, \mu_3, \dfrac{M}{2} \times \dfrac{N}{2}\right) * 255\right). \end{cases} \tag{10}$$

In the light of the following equation, the pixel values of each block are substituted by the obtained three chaotic sequences, and the substituted image of each block is obtained:

$$\text{encrypta}(i) = \left(u_1 \oplus \left(u_2 \oplus \left(u_3 \oplus a(i)\right)\right)\right), \quad i = 1, 2, 3, 4, \tag{11}$$

where $a(i)$ is the scrambled image of each block. Finally, the four substituted images are recombined according to the following equation, and the final encrypted image is obtained:

$$\text{img} = \begin{bmatrix} \text{encrypta 1} & \text{encrypta 2} \\ \text{encrypta 3} & \text{encrypta 4} \end{bmatrix}. \tag{12}$$

Require: Plain image P, $\sigma = 10, \beta = 8/3, r = 28, d = 1.3, q_1 = q_2 = q_3 = q_4 = 0.995$
Ensure: Scrambled image P_{con}
(1) / * Calculate the hash value of the plaintext image * /
(2) $H = \text{hash}(P)$
(3) / * Calculate the initial value of the fractional chaotic system * /
(4) Calculate the initial value of the chaotic sequence according to equation (7) to equation (9)
(5) / * Calculate fractional chaotic sequence * /
(6) $Y_1, Y_2 \leftarrow$ Calculate chaotic sequence by using $h_1, h_2, \ldots, h_8$, and the given chaotic parameters into equation (1) to calculate, Pre-iterative chaotic mapping 1000 times to eliminate the adverse consequences caused by transient reactions, continue to iterate $M \times N$ times
(7) $Y = [Y_1, Y_2]$
(8) Decompose P into bit planes to get 8 bit planes $\{P_1, P_2, \ldots, P_8\}$
(9) **for** $i = 1 : 8$ **do**
(10) Arrange the ith bit plane into a one-dimensional vector X in column first
(11) Arrange the ith chaotic sequence in Y in ascending order, and generate a sequence T used to record the position of each element in the sorted sequence in the original sequence
(12) Re-arrange the vector X in the order of the sequence T to obtain a new one-dimensional vector Y after transformation
(13) Adjust the size of the newly generated Y to make it consistent with the size of the plaintext image
(14) **end for**
(15) Combine the obtained 8 scrambled bit-plane images to gain the final scrambled image P_{con}

Algorithm 1: Bit-plane decomposition and scrambling algorithm based on the fractional-order hyper Lorenz chaotic system.

To generate the initial population for artificial bee colony optimization, go back to Step 2 and repeat for $N/2$ times. It ensures that the hash value of each element in each block and line can be used as the initial value of chaos, and the initial population cellarray containing $N/2$ different encrypted images is obtained.

3.4. Image Optimization Algorithm of Artificial Bee Colony Algorithm Based on Crossover Operator. After the permutation and substitution process is completed, $N/2$ individuals of encrypted images will be generated to form the initial population optimized by the artificial bee colony algorithm. Each encrypted image in the population does not have visual visibility, so it is necessary to select specific indicators in the ciphertext image that can judge the quality of its encryption. In this article, the information entropy of the ciphertext image is selected and calculated as the fitness function to judge the quality of the ciphertext. This article presents a crossover operator shown in Figure 2, which can continuously generate new encrypted images by crossing two existing encrypted images, enhance the diversity of the population. After continuous optimization operations, the encrypted image with the largest information entropy is finally obtained. The specific optimization steps are as follows:

(1) Initialization stage: Section 3.3 generates an initial population cellarray with $N/2$ different encrypted images. Calculate the information entropy H of each encrypted image, and take it as the fitness function. The formula is as follows:

$$\text{fit} = H. \tag{13}$$

According to the order of fitness function from small to large, to sort each encrypted images in the cellarray to obtain cellimg, each individual is regarded as a honey source, and search optimization is performed by changing the position of the honey source.

(2) Hiring bee stage: Search for the location of the food source near the current nectar source x_i, x_k represents the location of other nectar sources. Update the position of the hired bee according to equation (4), and then, determine whether to choose the updated hired bee or the initially hired bee according to the greedy algorithm of equation (5). This step is equivalent to the selection stage, which can save more of the better-encrypted images in the population. Generate a new population gypop.

(3) Introducing crossover operator: Save 10% images with the highest information entropy in gypop. Then according to the crossover operator shown in Figure 2, individuals in gypop are crossed to generate the remaining 90% encrypted images. Calculate the fitness value of the newly generated individual according equation (13). According to the greedy calculation method of equation (5), the better individuals and their positions are selected for preservation and generate a new population cropop.

(4) Observation bee stage: Calculate the probability P_i according to equation (6). The follower bees choose the honey source to follow according to the follower bees. According to equation (4), the local search is carried out, and the better individuals are selected. Calculate the fitness value of the newly generated individual. According to the greedy calculation method of equation (5), the better individuals and their positions are selected for preservation and generate a new population cnew.

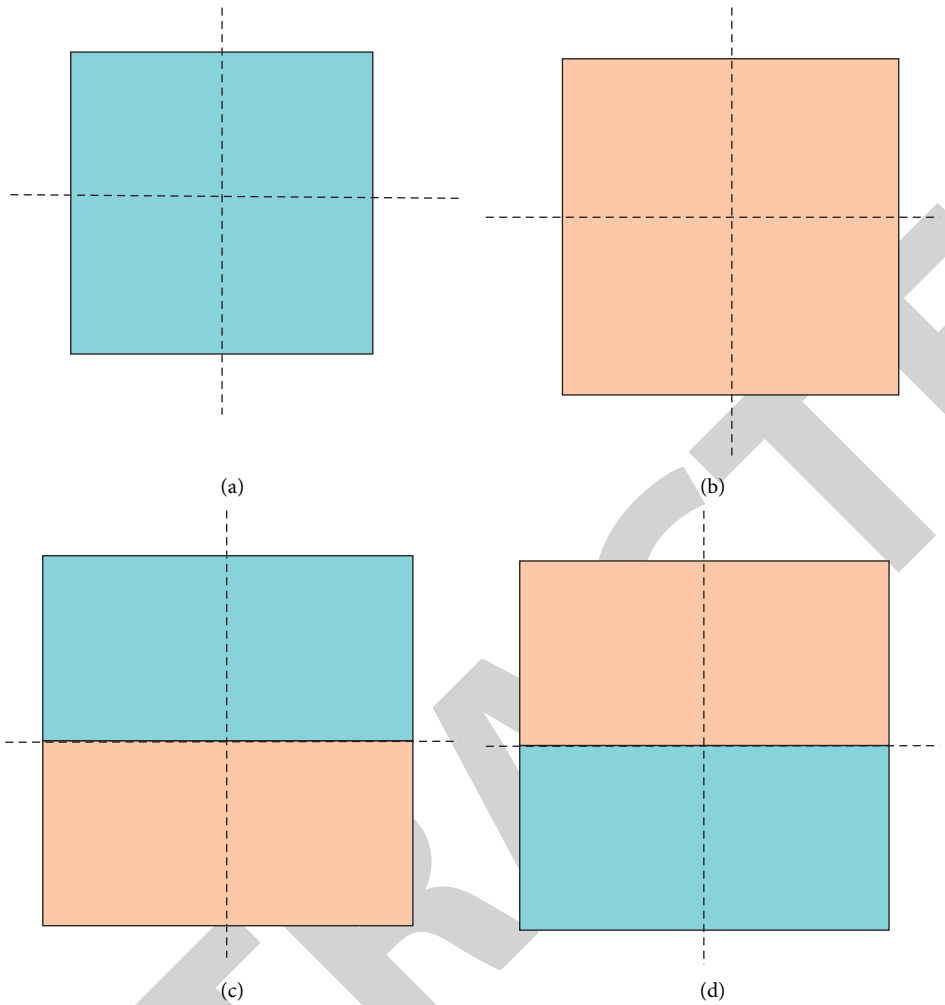


Figure 2: The crossover operator of image crossover operation: (a) input image 1; (b) input image 2; (c) output image 1; (d) output image 2.

(5) Investigation bee stage: Abandon a food source x_i if it does not renew after several collection. The corresponding hired bees or observation bees will transform into observation bees. The Scout bees randomly create a new food source, change the location of the nectar source, and continue to seek out the optimal solution in the global range.

(6) Selection stage: Calculate the information entropy of each encrypted image in cnew, where the encrypted image with the best fitness function is the optimal encrypted image obtained in this article and output its corresponding position information to facilitate subsequent decryption.

The pseudocode for image optimization based on the artificial bee colony algorithm of the crossover operator is shown in Algorithm 2.

The encryption flow diagram is shown in Figure 3.

4. Simulation Results and Analysis

An excellent encryption system may withstand various assaults, such as statistical, differential, and selective plaintext attacks, among others. To verify the efficacy and reliability of the presented encryption algorithm, we use MATLAB software for simulation. Input images are grayscale with dimensions 256×256. The plain images are tested as shown in Figure 4. Analyze the encrypted images through a series of security analysis methods, for instance, key space analysis, statistical analysis, information entropy analysis, difference analysis, and so on. The experiment consequence shows that the proposed encryption scheme has outstanding encryption characteristics.

4.1. Statistical Analysis

4.1.1. Key Space Analysis. The high-security encryption system in which key space should be large sufficient to resist all kinds of brute force attacks. The key space of the image encryption algorithm composes the key space of scrambling and substitution. The literature suggests that the encryption system can stand up to all sorts of attacks by exhaustive search only when the key space of the encryption system is not less than 2^{128} [33], so that it can reach the level of sufficient security. The accuracy of this article is double

Require: Population: cellarray, Maximum number of iterations: Gen, $\text{investigation}_{\text{size}}$, $\text{observation}_{\text{size}}$
Ensure: Optimal encrypted image and its position
(1) fitness ← According to equation (13)
(2) [cost, index] = sort (abs (fitness))
(3) cellimg ← Rearrange cellarray according index
(4) **for** $i = 1$: Gen **do**
(5) / ∗ Hiring bee stage ∗ /
(6) **for** $i = 1 : N/2$ **do**
(7) k = randi $(N/2, 1)$
(8) while $k == i$
(9) k = randi $(N/2, 1)$
(10) end
(11) ϕ = round (rand ∗ 2 − 1)
(12) gypop $\{i, 2\}$ ← Substitute cellimg into equation (4) to update its position
(13) Boundary value processing
(14) gypop$\{i, 1\}$ ← Search for the corresponding encrypted image according to gypop $\{i, 2\}$
(15) fitness 1 ← equation (13) which in gypop $\{i, 1\}$
(16) gypop ← According to equation (5) for select the better individuals
(17) **end for**
(18) / ∗ Introducing crossover operator ∗ /
(19) Sort and save the top 10% in gypop
(20) The remaining 90% ← according to Figure 2 to cross other images
(21) cropop← Calculate the fitness According to equation (13), select the better individuals according to equation (5)
(22) / ∗ Observation bee stage ∗ /
(23) **for** i = 1: observation_size **do**
(24) P_i← according to equation (6)
(25) r = rand
(26) j = find $(r < = P, 1, '\text{first}')$
(27) k = randi (gy_size, 1)
(28) while $k == j$
(29) k = randi (gy_size, 1)
(30) end
(31) cenw ← repeat 11–16
(32) **end for**
(33) / ∗ Investigation bee stage ∗ /
(34) **for** i = 1: investigation_size **do**
(35) Judge whether to give up the honey source
(36) **end for**
(37) **end for**
(38) Calculate the fitness of each encrypted image in *cnew*, select the encrypted image with the maximum fitness, and return its corresponding position

Algorithm 2: Artificial bee colony optimization algorithm based on crossover operator.

precision 10^{-16}. The parameters needed for the chaotic system are as follows: $\mu_1, \mu_2, \mu_3, \sigma, \beta, d, r, q$, and the key space is $(10^{16})^8$. The initial value of the chaotic system is hashed by SHA-256 algorithm. The size of key space provided by the SHA-256 algorithm is 2^{256}. Therefore, the key space of this article is $(10^{16})^8 * 2^{256}$, which is much larger than 2^{128}, so the encryption algorithm presented in this article has sufficient key space to stand up to any violent attack.

4.1.2. Histogram Analysis. The histogram of the digital images can directly indicate the allocation of pixel values in the image, the original plaintext information contains rich image information, so the distribution diagram of plaintext images is uneven. The ciphertext information encrypted by encryption technology is similar to noise information, and the image information can not reflect the content of the image. As a result, the ciphertext's histogram should be flat, the fluctuation amplitude should be modest, and the distribution should be close to uniform, allowing it to withstand statistical attacks. Figure 5 shows the plaintext image, plaintext image histogram, ciphertext image, and ciphertext image histogram information of Cameraman and House.

As can be seen from the figures, the histogram of the original plaintext image fluctuates greatly, and the encrypted image's histogram is very flat and approximately evenly distributed, which does not provide any favorable information. Therefore, the assailant will not be able to deduce any plaintext messages from the encrypted image and will be able to defend against the statistical analysis attack.

4.1.3. Correlation Analysis. The correlation between two neighboring pixels is called the correlation coefficient. It is

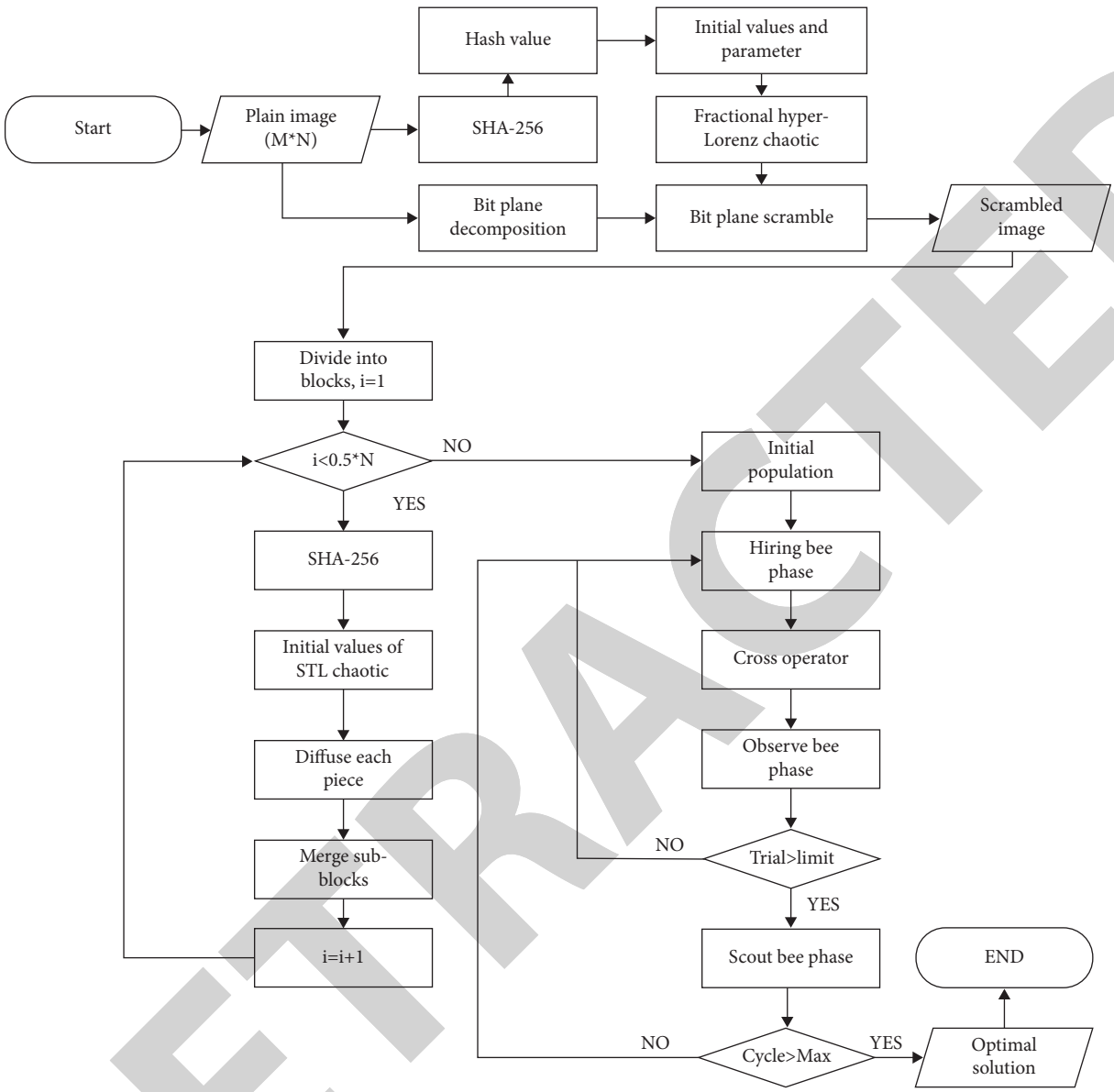
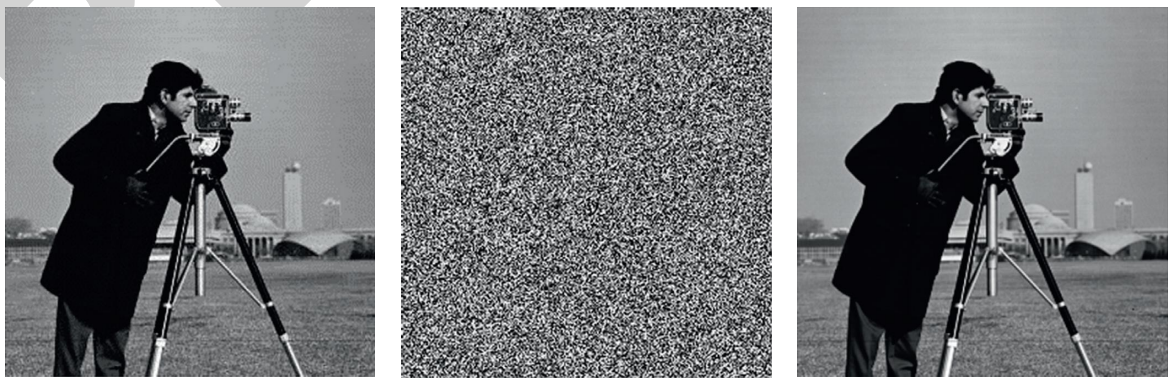
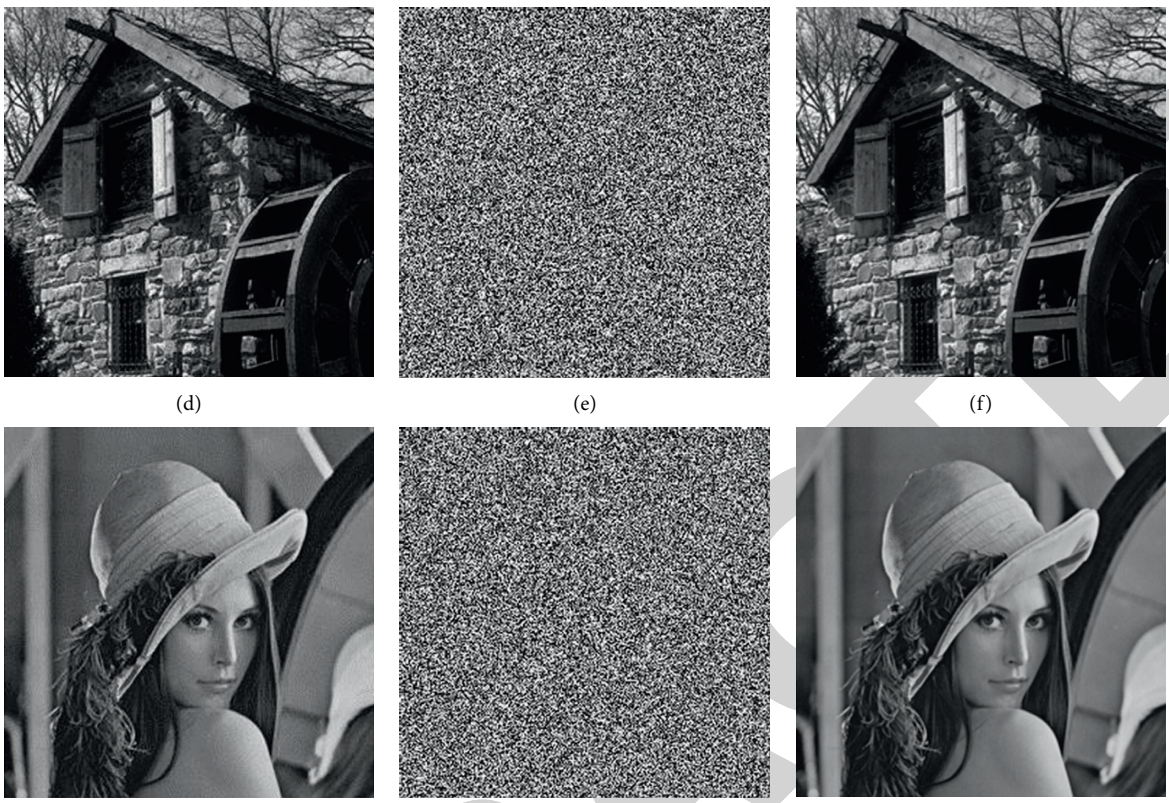


Figure 3: Flow diagram of the encryption algorithm.



(a) (b) (c)

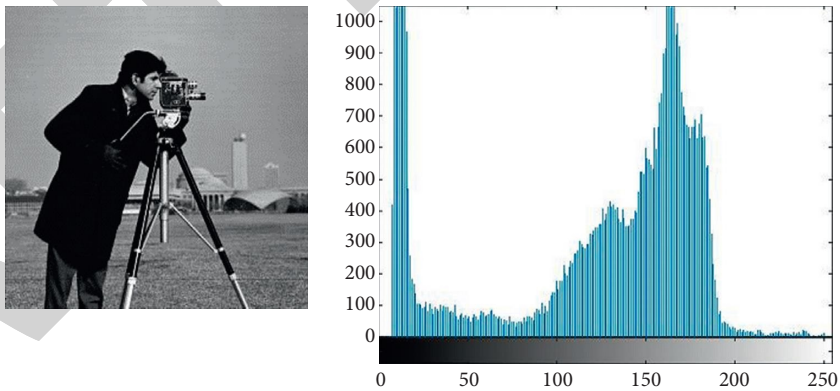
Figure 4: Continued.



(d) (e) (f)

(g) (h) (i)

Figure 4: Result images of encryption and decryption: (a) cameraman plain image; (b) cameraman ciphertext image; (c) cameraman decrypted image; (d) house plain image; (e) house ciphertext image; (f) house decrypted image; (g) Lena plain image; (h) Lena ciphertext image; (i) Lena decrypted image.



(a) (b)

Figure 5: Continued.

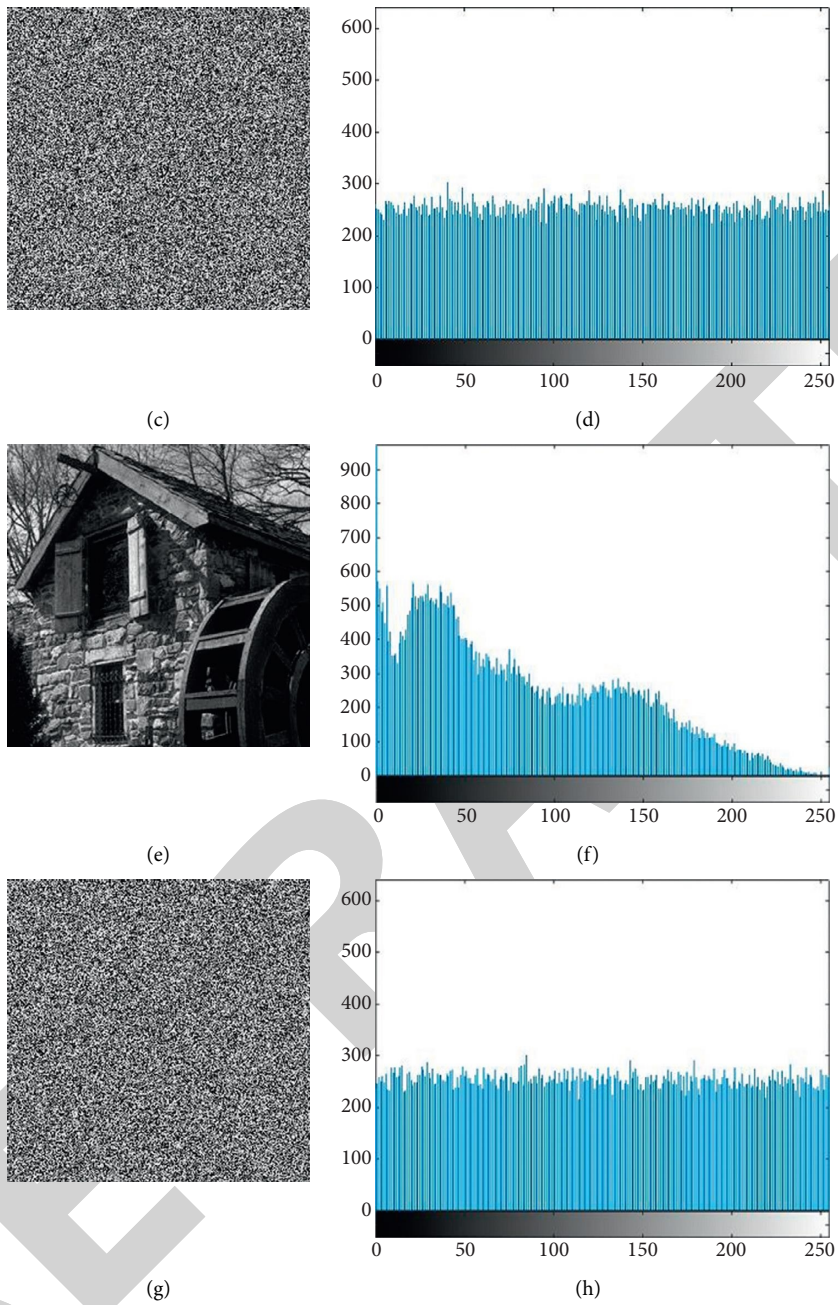


Figure 5: Histogram of original and cipher image: (a) cameraman plain image; (b) cameraman plain image histogram; (c) cameraman ciphertext image; (d) cameraman ciphertext image histogram; (e) house plain image; (f) house plain image histogram; (g) house ciphertext image; (h) house ciphertext image histogram.

one of the significant indexes in image encryption analysis. It can be used to show the amount to which image pixels have been substituted. The correlation in the original plaintext image is usually near to one, and it should be close to zero after encryption, suggesting that the encryption influence is significant. The calculation formula of the correlation coefficient is [34]

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2,$$

$$\mathrm{Cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)], \tag{14}$$

$$\rho_{xy} = \frac{|\mathrm{Cov}(x, y)|}{\sqrt{D(x)}\sqrt{D(y)}},$$

where x, y represent two neighbor pixels, and N is the whole amount of pixels chosen in the plaintext image. Compute the correlation coefficients of all adjacent elements in the image, and average them to get the correlation coefficients in the horizontal direction, vertical direction, and diagonal direction of the image. Figures 6 and 7 are the distribution maps of neighbor pixels in horizontal, vertical, and diagonal directions of Cameraman plaintext image and encrypted Cameraman image, respectively. Table 1 is the correlation coefficient values of adjacent pixels of four plaintext images and encrypted images in all directions. As indicated in Table 2, the correlation coefficient obtained by the provided encryption algorithm is compared to other literature. As a result, the suggested encryption algorithm disrupts encrypted image correlation while providing strong uniform distribution performance.

4.1.4. Information Entropy Analysis. Information entropy can estimate the allocation of gray values in an image. The more even the gray allocation is, the greater the information entropy of the image is. Plaintext image information distribution is uneven, making plaintext image data information easy to access by attackers. However, the distribution of encrypted images is uniform, and the unpredictability of images is strong. For completely ideal random images, their information entropy is 8. Assuming that m represents an information source, the information entropy can be calculated by the following formula [38]:

$$H(x) = -\sum_{i=0}^{2^n-1} p(m_i)\log_2 p(m_i), \tag{15}$$

where 2^n indicates the total number of states of the information source m and $p(m_i)$ indicates the probability of a symbol m_i appearing. Test several images to get the information entropy analysis shown in Table 3. The method put forward in this article is compared with other algorithms, and the comparison consequence is described in Table 4.

Tables 3 and 4 suggest that the information entropy of encrypted ciphertext information is closer to the ideal value of 8, and the pixels in the ciphertext are uniformly allocated. For the Cameraman image, the encryption scheme proposed in this article has greater information entropy, which proves that the attacker can obtain less useful information from the gray distribution, is more secure, and is not easy to disclose information, and has better performance than other encryption schemes.

4.2. Sensitivity Analysis

4.2.1. Key Sensitivity Analysis. Key sensitivity plays a crucial role in resisting violent attacks. On the one hand, a seemingly insignificant modification in the security key will result in completely different encrypted images. On the other hand, decrypting the encrypted image with a slightly altered key will not yield the correct decoded image.

To verify the sensitivity of the encryption key, use the set chaotic parameters to encrypt the plaintext image to obtain Figure 8(a). Then, a parameter μ in the Sine-Tent-Logistic chaotic system is changed and increased by 1×10^{-16}; ensure that other key parameters in the encryption algorithm remain unchanged, and then, encrypt the plaintext image again to get Figure 8(b). Make a difference between the two encrypted images to obtain Figure 8(c). The image illustrates that, while the encryption key changes slightly, the encrypted images generated by different encryption keys differ dramatically.

In order to verify the decryption key sensitivity, parameter μ in the Sine-Tent-Logistic chaotic system is changed and increased by 1×10^{-16}; ensure that the decryption algorithm's other key parameters remain unaltered. Figure 9 illustrates the decryption effect, which indicates that although the decryption key has a tiny modification, the ciphertext image cannot successfully decrypt and restore to the original image.

4.2.2. Differential Attack. The sensitivity of the encryption scheme to plaintext determines its power to oppose the differential attack. The sensitivity of the encryption scheme to the original image can be evaluated by two indexes: pixel change rate (NPCR) and normalized average change intensity of pixel value (UACI). NPCR and UACI separately indicate the proportion and degree of change in the pixel value of the encrypted image after altering a certain pixel value of the plaintext image at random. If the pixel values of the plaintext in ciphertext changes lead to a complete different image, which indicates that the method has a powerful ability to oppose the differential attack. For two plaintext images with only one pixel changed, let the pixels of (i, j) in their ciphertext image be $M_1(i, j)$ and $M_2(i, j)$ separately; if $M_1(i, j) = M_2(i, j)$, define $E(i, j) = 0$; or else, $E(i, j) = 1$. The calculation formulae of NPCR and UACI are [41]

$$\mathrm{NPCR} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} E(i, j) \times 100\%,$$

$$\mathrm{UACI} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|M_1(i, j) - M_2(i, j)|}{255} \times 100\%. \tag{16}$$

The formulae for calculating the ideal expected value of NPCR and UACI are [42]

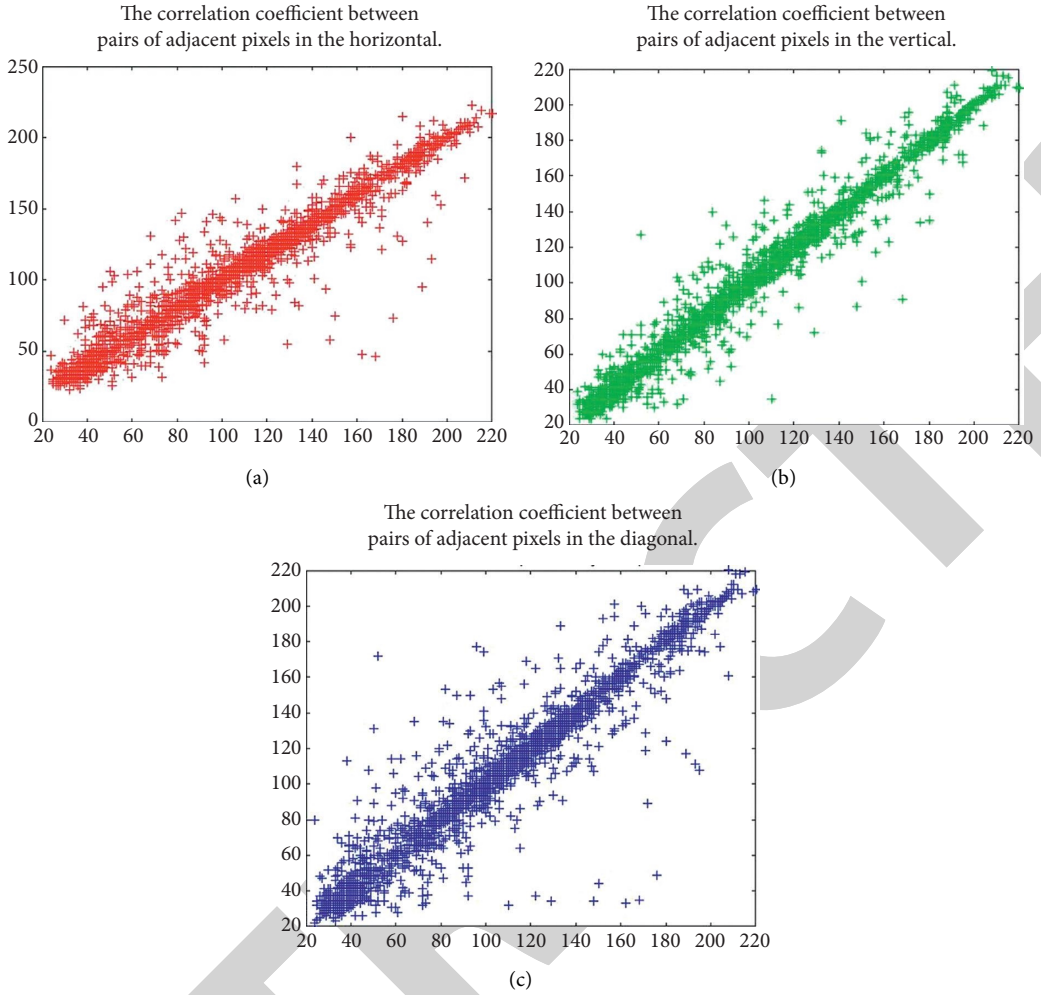


Figure 6: Horizontal, vertical, and diagonal correlation coefficient graphs of plaintext image: (a) horizontal correlation; (b) vertical correlation; (c) diagonal correlation.

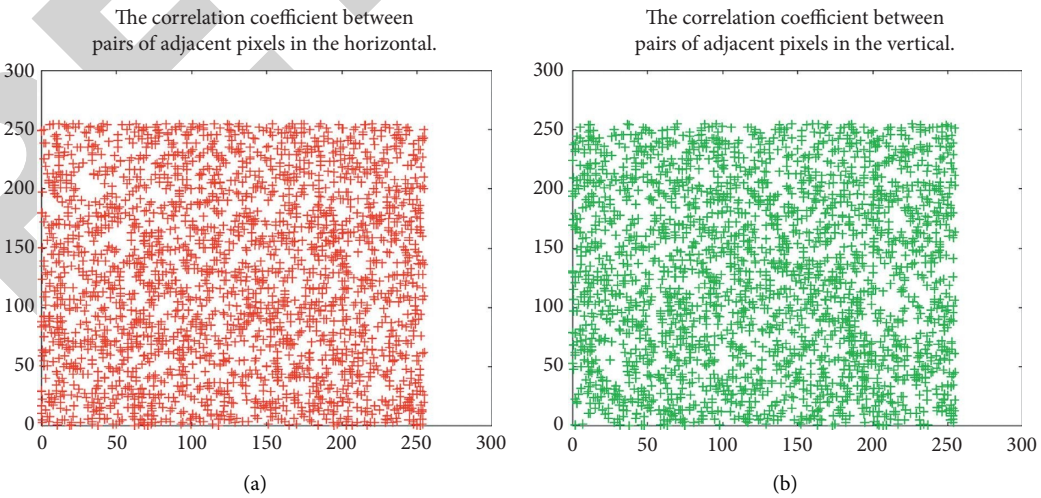
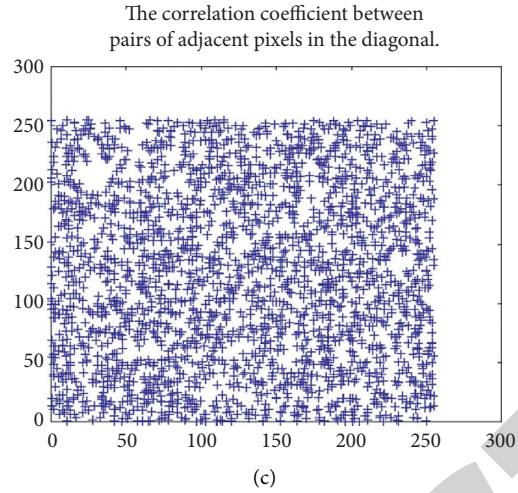


Figure 7: Continued.



(c)

Figure 7: Horizontal, vertical, and diagonal correlation coefficient graphs of ciphertext image: (a) horizontal correlation; (b) vertical correlation; (c) diagonal correlation.

Table 1: Correlation of adjacent pixels in different images.

Images		Horizontal	Vertical	Diagonal
Lena	Plain	0.9496	0.9472	0.9264
	Ciphertext	0.0029	-3.1091×10^{-4}	8.1537×10^{-4}
Barbara	Plain	0.9415	0.9619	0.9213
	Ciphertext	8.0808×10^{-4}	0.0077	8.8217×10^{-5}
House	Plain	0.8980	0.8886	0.8237
	Ciphertext	−0.0064	0.0015	−0.0019
Cameraman	Plain	0.9335	0.9592	0.9087
	Ciphertext	0.0019	−0.0018	0.0062

Table 2: Comparison of correlation coefficient of Barbara.

Direction	Proposed	Reference [5]	Reference [24]	Reference [35]	Reference [36]	Reference [37]
Horizontal	8.0808×10^{-4}	0.0053	0.0017	0.0037	0.002171	−0.0004
Vertical	0.0077	0.0035	0.0022	0.0014	0.002149	0.0061
Diagonal	8.8217×10^{-5}	−0.0017	0.0011	0.0003	−0.000587	0.0008

$$\begin{aligned} \mathrm{NPCR}_E &= \left(1 - 2^{-n}\right) \times 100\%, \\ \mathrm{UACI}_E &= \frac{1}{2^{2n}} \frac{\sum_{j=1}^{2^{n-1}} i\,(i+1)}{2^n - 1} \times 100\%, \end{aligned} \tag{17}$$

where M and N are the numbers of rows and columns of image pixels, respectively, and n is the bit depth of image color. For an 8-bit grayscale image, n is 8. The theoretical values of NPCR and UACI are 99.6094 % and 33.4635 %, respectively. We simulate the Cameraman image by randomly selecting a pixel value at a fixed location in the image and assigning it a value between 0 and 255, and then calculate the NPCR and UACI values using the formula mentioned above. The analysis of NPCR and UACI of different encrypted images and the comparison of differential attack of Cameraman are shown in Tables 5 and 6. As shown, the experimental results in this article are closer to the theoretical values, and the invention has strong sensitivity and strong resistance to difference.

4.3. Noise Attack. In the actual process of information transmission, since the transmission channel is insecurity, the data are susceptible to attack by noise, resulting in leakage of the information data and so on. Excellent encryption algorithm has better noise immunity attack performance and robustness. Use peak signal-to-noise ratio (PSNR) as an index to estimate the robustness of the algorithm. The mathematical formula is [45]

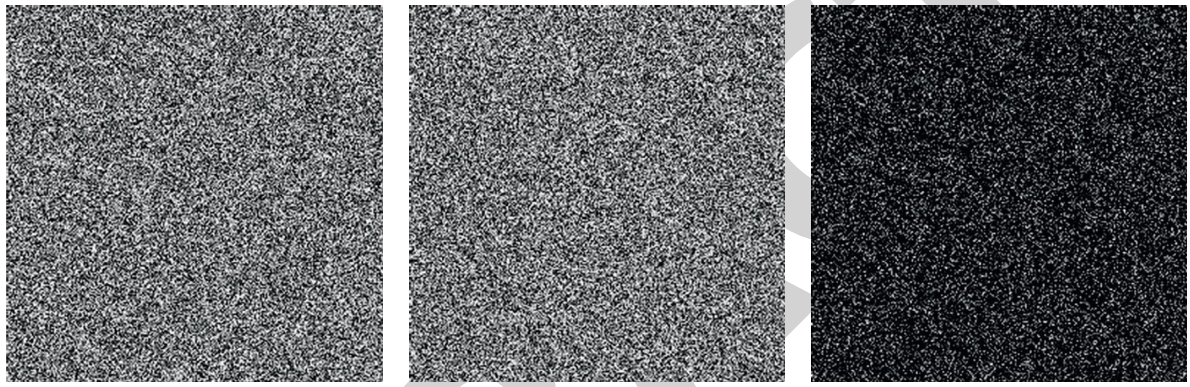
$$\begin{aligned} \mathrm{MSE} &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [a(i,j) - b(i,j)]^2, \\ \mathrm{PSNR} &= 10 \log_{10}\left(\frac{I_{\max}^2}{\mathrm{MSE}}\right), \end{aligned} \tag{18}$$

Table 3: Information entropy analysis of different encrypted images.

Images	Plain image	Ciphertext image
Lena	7.3792	7.9980
Barbara	7.7545	7.9979
House	7.4982	7.9981
Cameraman	7.0097	7.9982
Peppers	7.6049	7.9979

Table 4: Comparision of the information entropy of Cameraman.

Images	Proposed	Reference [25]	Reference [39]	Reference [30]	Reference [40]
Information entropy	7.9982	7.9904	7.9974	7.9846	7.9941



(a) (b) (c)

Figure 8: Sensitivity analysis of encryption key: (a) ciphertext image encrypted by key; (b) ciphertext image encrypted by key + 1×10^{-16}; (c) the difference between two encrypted images.

(a) (b) (c)

Figure 9: Sensitivity analysis of decryption key: (a) original plaintext image; (b) decrypted image of correct key; (c) decrypted image of false key.

where M, N is the size of the image, a is the plaintext, b is the encrypted image, and $I^2_{\max}$ represents the maximum pixel value in the image. Substituting the original plaintext and decrypted image into the above formula to calculate the PSNR value, the larger the PSNR, the better the decryption effect.

To verify the antinoise ability of the encryption algorithm presented in this article, add salt-peppers noise or Gaussian noise with different intensities to the encrypted image, and its PSNR value is calculated after decryption to judge whether it is robust or not.

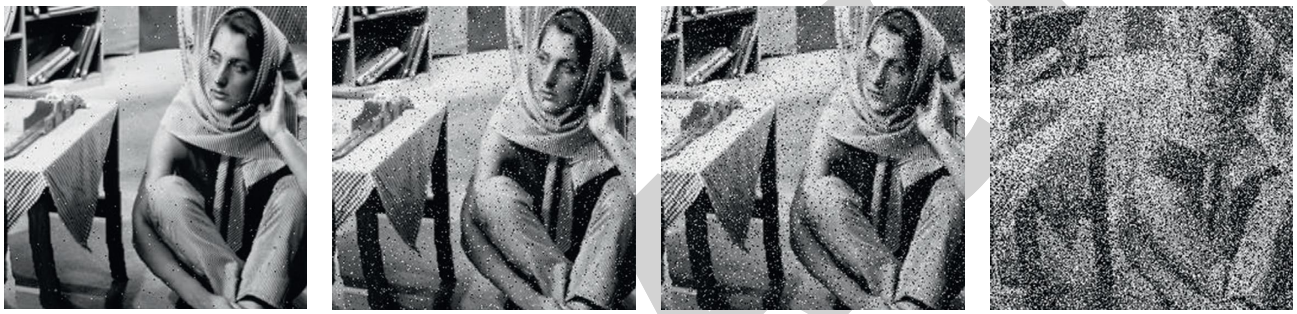
4.3.1. Salt-Peppers Noise Attack. Add salt-peppers noise with the densities of 0.001, 0.005, 0.01, and 0.1 to the Barbara encrypted image; their PSNR scores are calculated as

Table 5: Analysis of NPCR and UACI of different encrypted images.

Images	NPCR (%)	UACI (%)
Lena	99.6521	33.5907
Barbara	99.6124	33.4436
House	99.6353	33.5548
Cameraman	99.6201	33.5054

Table 6: Comparison of differential attack of Cameraman.

Images	Proposed	Reference [25]	Reference [43]	Reference [44]	Reference [30]	Reference [11]
NPCR(%)	99.6201	99.60	99.61	99.6014	99.6521	99.62
UACI(%)	33.5054	33.15	33.3638	33.3577	34.5351	33.45



(a) (b) (c) (d)

Figure 10: Results of different densities of salt-pepper noise attack: (a) 0.001; (b) 0.005; (c) 0.01; (d) 0.1.

Table 7: PSNR results after adding salt-pepper noise.

Density	Proposed	Reference [46]	Reference [47] (compressed)
0.001	37.9183	—	36.5487
0.005	30.9447	30.87	30.1789
0.01	27.6527	—	18.8745
0.1	17.8911	—	—

(a) (b) (c) (d)

Figure 11: Results of different densities of Gaussian noise attack: (a) 0.005; (b) 0.01; (c) 0.05; (d) 0.1.

37.9783, 31.0693, 27.6775, and 17.8212, respectively. The decrypted images are illustrated in Figure 10. It can be seen from Figure 10 that the decrypted image after adding noise can still clearly understand the information in the original plaintext image. The PSNR results after adding salt-peppers noise are shown in Table 7.

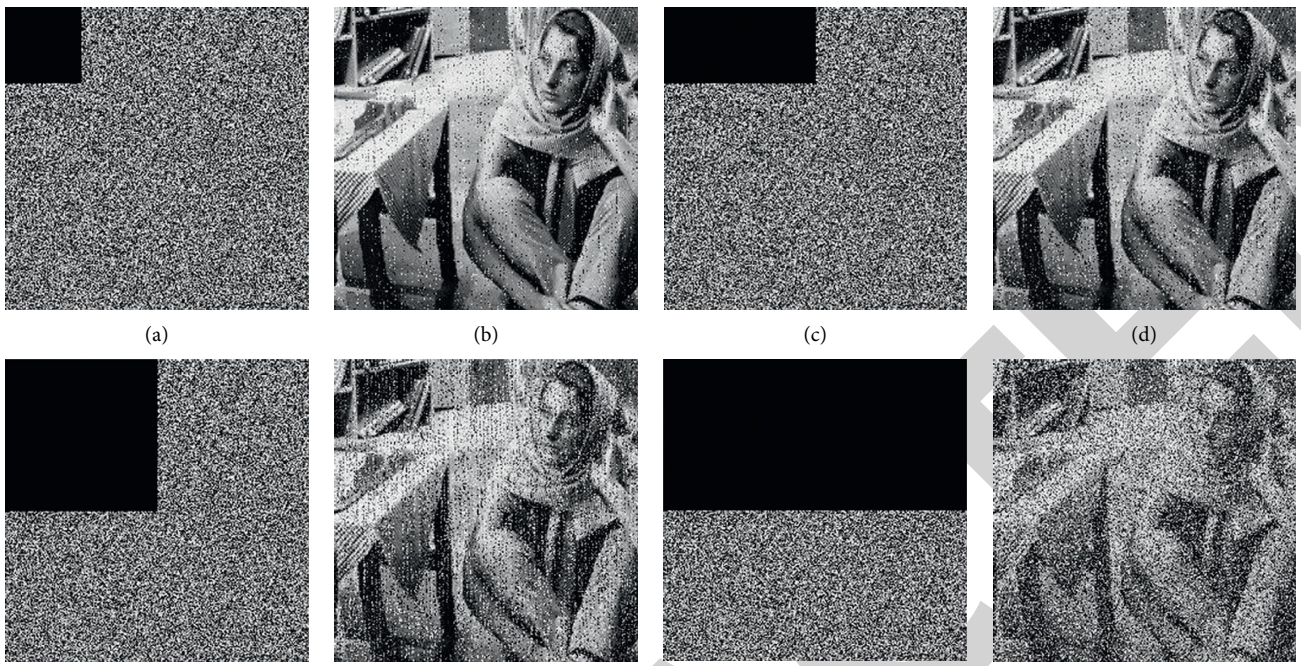


Figure 12: Results of different size of data loss attack: (a) 1/16 occlusion; (b) decrypted image with 1/16; (c) 1/8 occlusion; (d) decrypted image with 1/8; (e) 1/4 occlusion; (f) decrypted image with 1/4; (g) 1/2 occlusion; (h) decrypted image with 1/2.

Table 8: PSNR results after data loss.

Image	Cropping ratio	Reference [45]	Reference [48]	Proposed
Lena	1/16	16.6636	17.58	19.8531
	1/4	10.6747	15.03	13.9021
	1/2	10.6661	12.13	10.9435

4.3.2. Gaussian Noise Attack. Add Gaussian noise with the densities of 0.005, 0.01, 0.05, and 0.1 to the Barbara encrypted image, and their PSNR scores are calculated as 15.0117, 13.7699, 11.2407, and 10.4507 respectively. Figure 11 shows the decrypted images. The results demonstrate that decrypted images can still be recognized despite a degree of noise attack.

4.4. Data Loss Attack. Encrypted images may lose information due to clipping attacks or transmission through network and storage, which causes difficulties in the receipt of ordinary images. For purpose of verifying the anticutting performance, we replaced different sizes and positions of the encrypted image with zero value. After the cropped encrypted image is decrypted, compare the decrypted image with the plaintext information. If the similarity between the two images is high, it proves that the scheme has a strong anticutting attack performance.

Cut out 1/16, 1/8, 1/4, and 1/2 of the Barbara encrypted image at different positions, and their PSNR scores are calculated as 19.7757, 16.8110, 13.8381, and 10.9201 respectively. The decrypted images are illustrated in Figure 12. The PSNR results after data loss are shown in Table 8.

5. Conclusion

This article presented an image encryption scheme based on the artificial bee colony optimization algorithm. The significance of the encryption algorithm was to introduce the artificial bee colony optimization algorithm(ABC) after the bit-plane scrambling and block substitution. The ABC algorithm discovers the ciphertext image with the best encryption effect from initial population. A crossover operator is introduced in the ABC algorithm. This method considerably increases the population's diversity throughout the optimization phase. Compared with other optimization algorithms, the ABC algorithm has its own special mechanisms—role switching, and positive and negative feedback mechanism and has a minimal number of parameters; it limits the influence of artificial parameter setting as much as possible and has significant robustness, which increases optimization efficiency and the final result. In the encryption phase, compared with other research studies, the algorithm improves the algorithm's link with plaintext and its capacity to resist plaintext attack. The scrambling and diffusion encryption operations are intertwined, making the technique more safe. The experimental simulation results indicated that the encryption algorithm proposed in this

article could efficiently cut down the correlation between adjacent pixels and improve the ciphertext information entropy, and the ciphertext image has high randomness and dispersion. Simultaneously, the encryption algorithm had eminent security and could oppose general representative attacks.

In future work, when moving algorithms to hardware systems, we have to deal with time consumption and storage issues, and there are three aspects that can be further improved. Firstly, different heuristic optimization algorithms can be combined to form a more efficient optimization algorithm applied in the field of image encryption; secondly, in the selection of fitness function, multiple evaluation indexes can be used for mixed calculation, which can make the optimization more perfect; finally, the optimization algorithm can be used to optimize the parameters or initial values of the chaotic system, which can make the obtained chaotic sequence more random, and the obtained chaotic sequence can be used to encrypt the image more secure.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Erfu Wang conceived the study; Yanqi Zhou and Miaomeng Song helped with the methodology; Yanqi Zhou helped with software; Yanqi Zhou, Miaomeng Song, and Mengna Shi validated the study; Miaomeng Song and Mengna Shi curated the data and reviewed the literature; Yanqi Zhou prepared the original draft; Yanqi Zhou and Erfu Wang reviewed and edited the manuscript; Erfu Wang helped with the project administration; and Erfu Wang and Yanqi Zhou carried out the funding acquisition. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

This work was supported by the Natural Science Foundation of Heilongjiang Province, China (No. LH2019F048), the Outstanding Youth Fund Project of Heilongjiang University: The Research on parallel compressed sensing encryption Algorithm based on sequence Signal Generator, Heilongjiang University (No. YJSCX2020-062HLJU), and the Natural Science Foundation of China (No. 61801173).

References

[1] M. Kaur, D. Singh, and K. Sun, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[2] A. Biryukov and C. De Cannière, "Data encryption standard (DES)," *Encyclopedia of Cryptography and Security*, vol. 28, no. 2, pp. 295–301, 2011.

[3] M. Dawood, A. R. Khan, and S. Akhter, "Advanced Encryption Standard," *Encyclopedia of Cryptography & Security*, 2011.

[4] J. Yu, S. Guo, X. Song, Y. Xie, and E. Wang, "Image parallel encryption technology based on sequence generator and chaotic measurement matrix," *Entropy*, vol. 22, no. 1, p. 76, 2020.

[5] G. Cheng, C. Wang, and C. Xu, "A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 29243–29263, 2020.

[6] R. Premkumar and S. Anand, "Secured and Compound 3-D Chaos Image Encryption Using Hybrid Mutation and Crossover Operator," *Multimedia Tools and Applications*, vol. 78, 2018.

[7] X. Wu, "A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 99, p. 1, 2017.

[8] M. Farajallah, S. E. Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," *International Journal of Bifurcation & Chaos*, vol. 26, no. 2, pp. 1650021–1650023, 2016.

[9] L. Wenhao, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[10] X.-Y. Wang, S.-X. Gu, and Y.-Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering*, vol. 68, no. may, pp. 126–134, 2015.

[11] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, Complete, 2017.

[12] L. Xiang, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Optik*, vol. 127, no. 5, pp. 2558–2565, 2016.

[13] X.-y. Wang, H.-l. Zhang, and X.-m. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, 2016.

[14] H. Pan, Y. Lei, and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, p. 142, 2018.

[15] J. Liu, Y. Ma, S. Li, L. Jing, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 1–22, 2018.

[16] Y. Peng, S. He, and K. Sun, "A higher dimensional chaotic map with discrete memristor," *AEU - International Journal of Electronics and Communications*, vol. 129, Article ID 153539, 2020.

[17] C. Li, K. Tan, B. Feng, and J. Lu, "The graph structure of the generalized discrete arnold's Cat map," *IEEE Transactions on Computers*, vol. 99, p. 1, 2021.

[18] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications*, vol. 54, no. 5, Article ID 102566, 2020.

[19] R. Ponuma and R. Amutha, "Compressive Sensing Based Image Compression-Encryption Using Novel 1D-Chaotic

Map," *Multimedia Tools and Applications*, vol. 77, pp. 19209–19234, 2017.

[20] L. Cui, Q. Ou, and L. Xu, "Fractional order Lorenz hyper-chaotic system and its circuit simulation (In Chinese)," *Electronic Measurement Technology*, vol. 33, no. 5, pp. 13–16, 2010.

[21] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition," *Optics Communications*, vol. 285, no. 5, pp. 594–608, 2012.

[22] V. Rathore and A. K. Pal, "An image encryption scheme in bit plane content using Henon map based generated edge map," *Multimedia Tools and Applications*, vol. 80, pp. 22275–22300, 2021.

[23] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, 2012.

[24] M. Ghazvin, M. Mirzadi, and N. Parvar, "A modified method for image encryption based on chaotic map and genetic algorithm," *Multimedia Tools and Applications*, vol. 79, no. 10, p. 5, 2020.

[25] S. Mozaffari, "Parallel image encryption with bitplane decomposition and genetic algorithm," *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 1–21, 2018.

[26] M. Dua, A. Wesanekar, V. Gupta, M. Bhola, and S. Dua, "Differential evolution optimization of intertwining logistic map-dna based image encryption technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 10, 2020.

[27] S. Saravanan and M. Sivabalakrishnan, "DA hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption," *Soft Computing*, vol. 6-7, 2021.

[28] J. Liu, J. Zhang, and S. Yin, "Hybrid Chaotic System-Oriented Artificial Fish Swarm Neural Network for Image Encryption," *Evolutionary Intelligence*, 2021.

[29] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption scheme based on fractional Hartley transform and chaotic substitution–permutation," *The Visual Computer*, vol. 3, pp. 1–24, 2021.

[30] G. Kaur, R. Agarwal, and V. Patidar, "Chaos based multiple order optical transform for 2D image encryption," *Engineering Science and Technology, an International Journal*, vol. 23, no. 5, pp. 998–1014, 2020.

[31] D. Karaboga, "An idea based on honey bee swarm for numerical optimization," *Tech. Rep TR06 Erciyes University, Engineering Faculty, Computer Engineering Department*, vol. Jan, 2005.

[32] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, no. May, pp. 1–11, 2016.

[33] K. Patro and B. Acharya, "Secure multi-level permutation operation based multiple colour image encryption," *Journal of Information Security and Applications*, vol. 40, no. JUN, pp. 111–133, 2020.

[34] N. Hossein, R. Enayatifar, H. Motameni, F. G. Guimares, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering*, vol. 110, no. 2018, pp. 24–32, 2018.

[35] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Scientific Reports*, vol. 10, p. 9784, 2020.

[36] X. Wang, H. Zhao, and M. Wang, "A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices," *Optics & Laser Technology*, vol. 115, pp. 42–57, 2019.

[37] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, no. JUL, pp. 45–58, 2019.

[38] H. Liu, B. Zhao, and L. Huang, "A Novel Quantum Image Encryption Algorithm Based on Crossover Operation and Mutation Operation," *Multimedia Tools and Applications*, vol. 78, 2019.

[39] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Optics and Lasers in Engineering*, vol. 125, no. 2, Article ID 105851, 2020.

[40] K. Patro, B. Acharya, and V. Nath, "A secure multi-stage one-round bit-plane permutation operation based chaotic image encryption," *Microsystem Technologies*, vol. 25, pp. 2331–2338, 2018.

[41] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, no. SEP, pp. 129–137, 2017.

[42] G. Pashakolaee, H. S. Shahhoseini, and M. Mollajafari, "Hyper-chaotic Feeded GA (HFGA): A Reversible Optimization Technique for Robust and Sensitive Image Encryption," *Multimedia Tools and Applications*, vol. 77, no. 16, 2017.

[43] M. Kaur and V. Kumar, "Beta chaotic map based image encryption using genetic algorithm," *International Journal of Bifurcation & Chaos*, vol. 28, no. 11, 2018.

[44] X. Wang and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[45] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Optics and Lasers in Engineering*, vol. 137, no. 11, Article ID 106393, 2021.

[46] A. u. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-or with dna complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, 2018.

[47] W. Wen, Y. Hong, Y. Fang, and L. Meng, "A visually secure image encryption scheme based on semi-tensor product compressed sensing," *Signal Processing*, vol. 173, no. 6, Article ID 107580, 2020.

[48] Y. Yang, L. Wang, S. Duan, and L. Luo, "Dynamical analysis and image encryption application of a novel memristive hyperchaotic system," *Optics & Laser Technology*, vol. 133, Article ID 106553, 2021.