Security of Encrypted Images in Network Transmission Based on an Improved Chaos Algorithm

Gaili Du

Public Foundation Department of Henan Medical College, Zhengzhou, Henan, 451191, China
E-mail: hndgl1981@yeah.net

Received 08 April 2023; Accepted 08 May 2023;
Publication 12 August 2023

Abstract

With the wide application of 5G networks, many digital images must rely on networks for transmission. Traditional image encryption algorithms can no longer meet modern security requirements, and it is important to protect digital images in network transmission more securely. To address the shortcomings of traditional chaotic algorithms in image encryption, such as the strong randomness of image pixel replacement and time-consuming computations of image pixel iteration, we use a fractional-order Fourier transform to replace the image pixel matrix, a one-dimensional logistic chaos algorithm to reduce the problem of strong randomness of image pixels, and a sine chaos-based idea to optimize the diffusion algorithm to reduce the computational complexity. After encrypting a digital image in simulation experiments, we achieved better results through statistical analysis, adjacent pixel correlation, and resistance to differential attack performance analysis index tests, and verified the protection effect of this algorithm in digital images during network attacks.

Keywords: Network, encryption, image.

Journal of Cyber Security and Mobility, Vol. 12_5, 675–696.
doi: 10.13052/jcsm2245-1439.1253

1 Introduction

5G networks are now being used more extensively by people around the world. Thus, how to transmit text, voice, image and other information on such networks more quickly and more securely has become a popular topic in research. Digital images have become a type of multimedia information that is widely transmitted on networks due to their large amounts of information, easy storage and vivid expression of information [1]. For digital image information, there are primarily two more effective protection measures. First, digital watermarking technology emerged in recent years and protects images by embedding digital watermark information in digital images; however, this approach does not hide the visible information of images and cannot effectively protect confidential images from being transmitted securely over the network. Second, image encryption technology transforms the original image information into random noise information by encrypting an image so that a network eavesdropper cannot recognize the noise information without knowing the key, protecting the image data during transmission.

In recent years, research on image encryption algorithms has progressed, and various schemes with good performance have been proposed. However, due to the rapid development of image processing technology, the amount of data contained in an image has gradually increased; thus, there is a need to design encryption algorithms that can meet the diverse characteristics of current image information. The basic principle of so-called image encryption is to use some reversible operation under the control of key parameters to transform a valuable image into a noise-like image that cannot visually express the original information. Image encryption can be divided into space-domain image encryption and frequency-domain image encryption according to whether the encryption operation is performed in the space domain or in the frequency domain. Spatial domain image encryption processes the image in pixel units, which can take full advantage of the matrix storage of image information, and the algorithm is faster to implement. The common methods are pixel-based scrambling and diffusion, where scrambling does not change the pixel value, and using some method to transform the position of pixel points can reduce the similarity of adjacent pixel values in the image. The common methods of random dislocation, Arnold transform, phantom square transform, affine transform, etc., are used in space domain encryption. The object of frequency-domain encryption is the transform-domain coefficients of the image. Before encryption, the image matrix is transformed into the frequency domain by some linear orthogonal transform,

such as the discrete cosine transform (DCT), discrete wavelet transform (DWT) or discrete Fourier transform (DFT), into frequency domain data before encryption. The cryptographic strength of this method is relatively low.

In this study, based on the existing chaos theory research, we use the fractional-order Fourier transform to replace the matrix of image pixels; the one-dimensional logistic chaos algorithm to solve the problem of reducing the randomness of image pixels; and the sine chaos-based idea to optimize the diffusion algorithm to reduce computational complexity.

2 Related Research

Image encryption using chaos is a popular topic in research currently, and different scholars have attempted different degrees of research. [2] proposed a multi-image encryption algorithm based on a single-channel scrambled called a diffuse chaotic system, which uses the initial value of the chaotic system as the key for each group of image encryption; the performance of simulation experiments showed that the algorithm achieves both good encryption speed and security performance. [3] proposed a new chaotic encryption image strategy, which is derived from sinusoidal graphs, tangent functions and Chebyshev polynomials of the first class. Simulation experiments showed that the algorithm achieved good results in terms of encryption performance and algorithm complexity. [4] proposed a colour image encryption strategy using block scrambling and chaos, which changes the arrangement of pixels in subimages and blocks and scrambles them in subimages. The scrambled images are then diffused using logic graphs to obtain the encrypted images. Experimental results show that the proposed algorithm achieved good performance in encrypting colour images. [5] propose a multi-image encryption algorithm based on chaos and gene fusion, which uses chaotic sequences to scramble the pixel positions in k pure images, and then uses chaotic images generated by chaotic systems to control the cyclic movement of pixels in multiple images. and plaintext attacks. [6] proposed a block cipher-based medical image encryption for multiple map interest areas. The proposed encryption algorithm has better security performance, particularly in the face of data loss attacks, differential attacks, statistical attacks and brute-force attacks. [7] proposed a chaos-based image encryption method, which uses a single replacement box of substitution and replacement to solve problems. The efficiency of the proposed encryption technique is verified using different measures and benchmarks. [8] proposed a noise-resistant image encryption scheme that uses cubic logic map, discrete wavelet transform and bit-plane

extraction methods, and simulation experiments show that the proposed algorithm can decrypt plaintext images with little information loss. [9] proposed a random encryption method for finger vein images using chaotic systems, and simulation experiments show good results in terms of NPCR, UACI and other indicators. [10] proposed a new method of global pixel diffusion with two chaotic sequences, which has good security and high encryption efficiency in the test of resistance to differential attacks. Results were similar to theoretical values, data fluctuation was small, and the image obtained during cropping and noise attacks was also clearer. [10] proposed a new method of global pixel diffusion with two chaotic sequences, and the method achieved good security and high encryption efficiency. In [11], a new grayscale image encryption scheme based on a hybrid chaotic map was proposed and used a confusion phase to disrupt the pixel position and a diffusion phase to continuously change the pixel content. [12] proposed a fractional 1D chaotic map with a large chaotic space that combined substitution and replacement phases to modify the pixel positions and values simultaneously, and simulations and experiments showed that the scheme achieved high encryption performance. [14] proposed a fast and efficient multi-image encryption method based on a chaotic system, which replaces the subblocks of the merged image as a chaotic sequence generated using a combined chaotic system, and results showed that it can effectively resist various attacks. [15] proposed an image encryption algorithm based on the PWLCM chaotic map and hash algorithm, and simulation experiments showed that the algorithm provides rapid encryption and decryption. [16] proposed a multi-image encryption algorithm based on bit-plane and chaos, and achieved good encryption, high encryption efficiency, a large key space, key sensitivity, resistance to statistical attacks, and strong capability of brute force attacks. [17] proposed an image encryption strategy using particle swarm algorithm, and simulation results showed that the encrypted image achieved low adjacent pixel high correlation and better results.

These studies summarized the chaos algorithm for image encryption to different degrees, and scholars have proposed good solutions, which can be roughly divided into the following categories: (1) using chaotic sequences instead of general pseudorandom sequences for encryption, an algorithm is closely related to the computed accuracy and the selection of chaotic mapping; if the parameters are not selected properly, it is easy to show periodicity; and (2) infiltrating the encryption key or plaintext information into the chaotic system. (3) The encryption key or plaintext information is infiltrated into the chaotic system, and some known algorithms are faster and

can achieve a better encryption effect without iterating too many times. Based on these research results, we perform an in-depth study of image encryption based on chaotic ideas.

3 Improved Chaotic Image Encryption Algorithm

3.1 Chaotic Image Encryption Analysis

Most images are encrypted using chaos theory to obtain better results. Chaos theory has the characteristics of sensitivity to initial conditions, control parameters, and ergodicity, and these characteristics are similar to the current cryptographic system of dislocation and diffusion; thus, the introduction of chaos theory in images can provide better encryption results. However, the following two problems must be considered:

(1) The strength of image pixel dislocation depends on the sensitivity of the initial value of the chaotic mapping and its traversal because the higher the sensitivity of the initial value of the chaotic mapping, the smaller the correlation between the adjacent pixels of the dislocated image, and vice versa. Thus, the randomness of the dislocation is stronger.
(2) The higher the number of iterations of the chaotic mapping in the process of pixel dislocation and substitution, the higher the encryption strength, which increases the computational complexity of the encryption process.

To consider these two problems in more detail, we use a fractional-order Fourier transform based on the image pixel replacement matrix, a one-dimensional logistic chaos algorithm to reduce the randomness of the image pixels, and a sine chaos-based optimization diffusion algorithm to reduce the computational complexity.

3.2 Image Pixel Scrambling Based on Fractional-order Fourier Transform

The permutation of image pixels in the image encryption process is a common approach that is faster, easier to implement in the encryption method, and has a larger key space and can mask the information of the plaintext image well but is less resistant to statistical characteristic attacks and noise attacks. The first use of the fractional-order Fourier transform in image encryption in [18] achieved better results because the fractional-order Fourier transform provides additional key information to the image encryption system due to

the additional parameter of fractional order, and the number of orders and their additivity can provide more degrees of freedom to the image encryption scheme and expand the key space. In this paper, we use the first-order Fourier transform combined with chaotic encryption ideas to encrypt images.

(1) Fractional-order Fourier transform

The expression for the p-order fractional-order Fourier transform of function $x(t)$ defined in the t-domain is shown in (1):

$$X_p(t) = \int_{-\infty}^{+\infty} x(t) K_p(u,t) du \tag{1}$$

where $K(u,t) = \sqrt{\frac{1-j\cot\alpha}{2\pi}} \exp[j(\frac{\mu^2+t^2}{2}\cot\alpha - \frac{ut}{\sin\alpha})]$ is the kernel function of the fractional-order Fourier transform. In the kernel function, α is the angle of rotation. We use $X_\alpha(u)$ to denote the fractional-order Fourier transform of order p of $x(t)$. The one-dimensional fractional-order Fourier expression (2):

$$x(t) = \int_{-\infty}^{+\infty} X_p(u) K_{-p}(u,t) du \tag{2}$$

Equation (2) shows that $x(t)$ is the manifestation characteristic of a set of orthogonal basis functions $K_{-p}(u,t)$ with weight coefficients $X_p(\mu)$. When p is 1, the fractional-order Fourier expression is (3):

$$X(u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-jut} x(t) dt \tag{3}$$

The inverse of this fractional-order Fourier is the expression (4):

$$x(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{jut} X(u) du \tag{4}$$

The image pixel coordinates are transformed using the two-dimensional discretization algorithm in fractional-order Fourier, and the results are described by shown in Equation (5):

$$F(u) = \int_{-\infty}^{+\infty} K_a(u,t) f(t) dt \tag{5}$$

We discretize Equation (5) to obtain the expression shown in Equation (6):

$$F(u) = \int_{t=0}^{N-1} K_a(u,t) f(t) \tag{6}$$

Converting Equation (6) into matrix form is shown in Equation (7):

$$\begin{bmatrix} F(0) \\ F(1) \\ \vdots \\ F(N-1) \end{bmatrix} = \begin{bmatrix} K_a(0,0) & K_a(0,1) & \cdots & K_a(0,N-1) \\ K_a(1,0) & K_a(1,1) & \cdots & K_a(1,N-1) \\ \vdots & \vdots & & \vdots \\ K_a(N-1,0) & K_a(N-1,1) & \cdots & K_a(N-1,N-1) \end{bmatrix} \times \begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(N-1) \end{bmatrix} \tag{7}$$

We set F_a to denote the transformation matrix as shown in Equation (8):

$$F_a = \begin{bmatrix} K_a(0,0) & K_a(0,1) & \cdots & K_a(0,N-1) \\ K_a(1,0) & K_a(1,1) & \cdots & K_a(1,N-1) \\ \vdots & \vdots & & \vdots \\ K_a(N-1,0) & K_a(N-1,1) & \cdots & K_a(N-1,N-1) \end{bmatrix} \tag{8}$$

Thus, the fractional-order Fourier representation of the discrete form is shown in Equation (9):

$$F = F_a X \tag{9}$$

In this study, we use the method of eigenmatrix decomposition to construct the F_a matrix, as shown in Equation (10):

$$F_a = V \Lambda V^T \tag{10}$$

Substituting Equation (10) into Equation (7) expands to obtain the expression shown in Equation (11):

$$\begin{bmatrix} F_a(0,0) & F_a(0,1) & \cdots & F_a(0,N-1) \\ F_a(1,0) & F_a(1,1) & \cdots & F_a(1,N-1) \\ \vdots & \vdots & & \vdots \\ F_a(N-1,0) & F_a(N-1,1) & \cdots & F_a(N-1,N-1) \end{bmatrix}$$

$$
\begin{aligned}
&= \begin{bmatrix} p_0[0] & p_1[0] & \cdots & p_{N-1}[0] \\ p_0[1] & p_1[1] & \cdots & p_{N-1}[1] \\ \vdots & \vdots & & \vdots \\ p_0[N-1] & p_1[N-1] & \cdots & p_{N-1}[N-1] \end{bmatrix} \\
&\quad \times \begin{bmatrix} \lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{N-1} \end{bmatrix} \times \begin{bmatrix} p_0[0] & p_1[1] & \cdots & p_{N-1}[N-1] \\ p_0[0] & p_1[1] & \cdots & p_{N-1}[N-1] \\ \vdots & \vdots & & \vdots \\ p_0[0] & p_1[1] & \cdots & p_{N-1}[N-1] \end{bmatrix} \\
&= \begin{bmatrix} \sum_{k=0}^{N-1} p_k[0] & \sum_{k=0}^{N-1} p_k[0] & \cdots & \sum_{k=0}^{N-1} p_k[0] \\ \lambda_k p_k[0] & \lambda_k p_k[1] & & \lambda_k p_k[N-1] \\ \sum_{k=0}^{N-1} p_k[1] & \sum_{k=0}^{N-1} p_k[1] & \cdots & \sum_{k=0}^{N-1} p_k[1] \\ \lambda_k p_k[0] & \lambda_k p_k[1] & & \lambda_k p_k[N-1] \\ \vdots & \vdots & & \vdots \\ \sum_{k=0}^{N-1} p_k[N-1] & \sum_{k=0}^{N-1} p_k[N-1] & \cdots & \sum_{k=0}^{N-1} p_k[N-1] \\ \lambda_k p_k[0] & \lambda_k p_k[1] & & \lambda_k p_k[N-1] \end{bmatrix}
\end{aligned} \tag{11}
$$

We simplify Equation (11) to obtain the following Equation (12):

$$F_a[m,n] = \sum_{k=0}^{N-1} p_k[m] \lambda_k p_k[n] \tag{12}$$

The corresponding expressions for the coordinates of the converted pixels are therefore as follows:

$$F_a[x',y'] = \sum_{k=0}^{N-1} p_k[x] \lambda_k p_k[y] \tag{13}$$

(2) Improvement of the Logistic Chaos-based Displacement Algorithm

Currently, chaos-based image encryption is only related to chaotic sequences in terms of the improved disruption key sequence; thus, we improve each encryption by introducing the sum of the ciphertext pixel values into the parameters of the chaotic system used to generate the disruption sequence. We set the size of the plaintext image P to S and convert the pixels of the plaintext into a one-dimensional sequence of pixels $P = \{P(1), P(2), \ldots P(S)\}$ of length S in left-to-right, top-to-bottom order. The sequence of pixels is mapped to a length S using logistic chaos to obtain an ordered sequence $nx(i)$, and a new sequence $t(i)$ is generated to record the positions of the elements of $nx(i)$ in the original sequence $x(i)$. The sequence $t(i)$ is then used to globally disorder the sequence P of plaintext images, resulting in the final disorder effect.

3.3 Improvements to the Diffusion Algorithm

The size of the plaintext image P is set to S ($S = m \times n$), and the plaintext pixels are converted into a one-dimensional pixel sequence $P = \{P(1), P(2), \ldots P(S)\}$ of length S in the order of top to bottom and left to right, and we accumulate all the plaintext pixel values as shown in the expression of Formula (14). The key sequence $K(i)$, $key(i)$ of the diffusion is computed from the first pixel to the first pixel according to Equations (15)–(16), which represents the image pixel key processed based on the idea of the sine chaos algorithm, to encrypt the plaintext sequentially using Equation (17), where $A, B \in [0, 255]$:

$$Sum = \sum_{i=1}^{S} P(i) \tag{14}$$

$$Sum = Sum - P(i) \tag{15}$$

$$K(i) = (key(i) + Sum) \mathrm{mod} 256 \tag{16}$$

$$C(i) = (P(i) + A * K(i)) \mathrm{mod} 256 \oplus (P(i) + B * K(i)) \mathrm{mod} 256 \tag{17}$$

3.4 Decryption Operations

We use C to denote the decrypted image matrix and initialize the one-dimensional pixel sequence $C(i)$ in image C with the sum of pixel values as $Sum = 0$, starting from the last pixel in pixel $C(i)$ and cycling to the second pixel point for decryption according to Equations (18)–(19). For the

first pixel, decryption is performed according to $P(1)$:

$$K(i) = (key(i) + Sum)\mathrm{mod}256 \tag{18}$$

$$P(i) = ((C(i-1) + B * K(i))\mathrm{mod}256 \oplus C(i) - A * K(i))\mathrm{mod}256 \tag{19}$$

$$Sum = Sum + P(i) \tag{20}$$

4 Improved Encryption and Decryption of Chaotic Images

4.1 An Improved and Complete Image Encryption Process

Step 1: A plaintext image pixel of size $S = m \times n$ is transformed according to the Fourier transform of the image and then transformed into a sequence of two pixels of length $S/2$, $P_1(i), P_2(i)$. When the length of the image sequence is odd, we add all 0 pixels at the end of the plaintext image; otherwise, it remains unchanged.

Step 2: We set the key start value and the number of encryptions, perform $S/2$ times *Logistic* chaos with the initial values μ_0 and x_0, and process the resulting chaotic sequence E according to Equation (21):

$$x(i) = \lfloor x(i) * 10^5 \rfloor \tag{21}$$

Step 3: Using $x(i)$ from step 2 instead of Equation (15), the ciphertext sequence $C_1(i)$ is obtained by diffusing P_1 according to the improved diffusion method, and the encrypted image matrix E_1 is obtained after converting $C_1(i)$ into the matrix form of $m \times n$;

Step 4: The sum Sum of all pixel values of $C_1(i)$ is introduced into the positive integer N, the initial value x_0' of the *Logistic* map of the resulting permutation matrix is calculated according to Equation (22), and the permutation sequence $H(i)$ is obtained by permuting $C_1(i)$ according to the improved permutation algorithm under the action of parameter μ_0':

$$x_0' = \lfloor (Sum + N) \times 10^3 / S \rfloor - \lfloor (Sum + N) \times 10^3 / S \rfloor \tag{22}$$

Step 5: $H(i)$ is used to replace the key in Equation (16), and the ciphertext sequence $C_2(i)$ is obtained by diffusing another part of the plaintext P_2 according to the diffusion method in Section 3.3 and transformed into $m \times n/2$ to obtain the encrypted image matrix E_2.

Step 6: We combine the two halves of the ciphertext into one $m \times n$ matrix to obtain the entire ciphertext image.

Step 7: According to the number of encryptions, the ciphertext obtained from the previous encryption is used as the plaintext P to be encrypted in the current round, and the above steps are iterated to obtain the final ciphertext.

4.2 Image Decryption Process

Step 1: The decrypted ciphertext must be divided in half in the middle and converted into a sequence of pixels $E_1(i)$ and $E_2(i)$C of length $S/2$;

Step 2: We set the initial key value and the number of encryption iterations, perform $S/2$ iterations according to $Logistic$ under the initial values x_0' and μ_0', and process the generated sequence according to Section 3.3 to obtain the sequence $H(i)$;

Step 3: We use $H(i)$ instead of $key(i)$ in Equations (18)–(20) to decrypt the ciphertext E_1 according to Section 3.4 and finally decrypt the matrix P_2 that converts the plaintext to $m \times n/2$;

Step 4: Iteration $S/2$ of the chaotic mapping $Logistic$ is performed under the action of parameters x_0' and μ_0' to generate a chaotic sequence $x(i)$, which is processed according to Equation (21);

Step 5: We decrypt E_2 by replacing $key(i)$ in Equations (18)–(20) with $x(i)$ in Step 4, and the decrypted plaintext is converted to $m \times n/2$ in the form of matrix P_1;

Step 6: We combine the images obtained in steps 3 and 5 after decryption to obtain the entire plaintext image;

Step 7: According to the number of encryption iterations, the decrypted plaintext in the previous iteration is used as the ciphertext to be decrypted this time, and the process is repeated to obtain the final plaintext.

5 Simulation Experiments

To demonstrate the effect of the algorithm after the improved chaotic encryption, we chose a plane image as the object of analysis. The hardware platform includes a Core i7 processor, 16 GB of DDR3 RAM, a hard disk capacity of 1 T, the Windows 10 operating system, and MATLAB 2012. The image after encryption results are shown in Figure 2. In this study, the effect of

Figure 1 Original image.

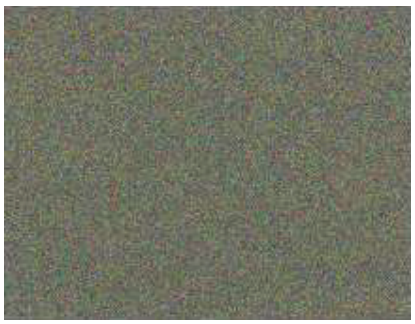

Figure 2 Encrypted image.

image encryption is verified from three aspects (statistical analysis, statistical histogram analysis and anti-differential performance analysis), and the effect of image encryption under a network transmission attack is simulated.

5.1 Statistical Analysis

Figure 3 shows the histogram of the algorithm before and after encryption. Figure 3(a) shows the image before encryption, and Figure 3(b) shows the image after encryption. The distribution of the grayscale histogram of the image before encryption is not uniform, while the distribution of the image after encryption is very uniform, which shows that the algorithm is effective at resisting aggressiveness.

5.2 Adjacent Pixel Correlation

To describe the effect of encryption, 100 sets of adjacent pixels are selected from Figures 1 and 2, and the pixel correlation is calculated in the horizontal,

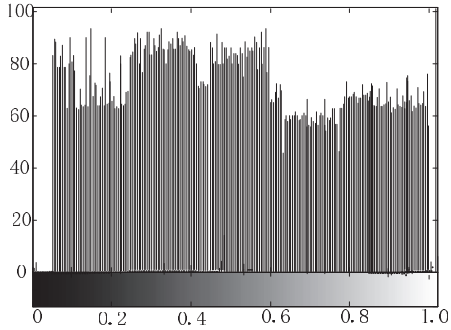

Figure 3(a) Histogram of unencrypted images.

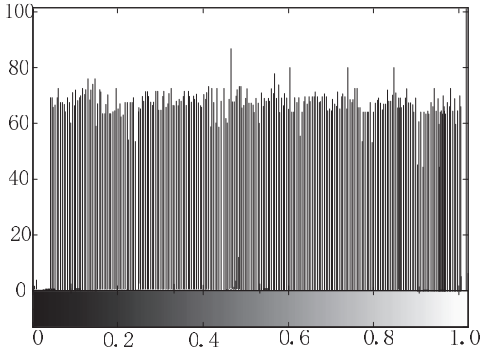

Figure 3(b) Histogram of encrypted images.

vertical and diagonal directions according to Equations (23)–(26):

$$E(x) = \frac{1}{N}\sum_{k=1}^{N} x_k \tag{23}$$

$$D(x) = \frac{1}{N}\sum_{k=1}^{N}(x_k - E(x)) \tag{24}$$

$$Cov(x,y) = \frac{1}{N}\sum_{k=1}^{N}(x_k - E(x))(y_k - E(y)) \tag{25}$$

$$r(x,y) = \frac{|Cov(x,y)|}{\sqrt{D(x)\sqrt{D(y)}}} \tag{26}$$

Table 1 Correlation of two adjacent pixels for Figures 1 and 2

Direction	Figure 1	Figure 2
Horizontal	0.8921	0.0082
Vertical	0.8403	0.0089
Diagonal	0.8816	0.0081

Table 2 Comparison of the time complexity of Figures 1 and 2

Direction	Figure 1(%)	Figure 2(%)
Horizontal	82.13	32.15
Vertical	81.62	42.35
Diagonal	92.35	44.18

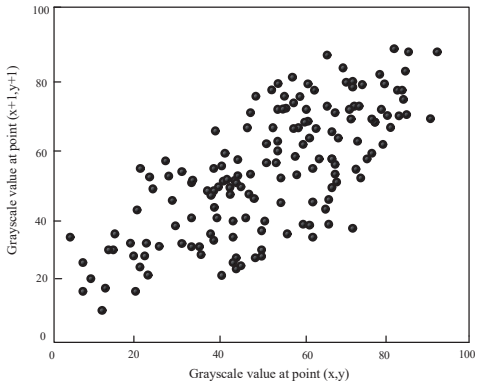

Figure 4(a) Diagonal orientation of Figure 1.

where Cov in Equation (25) is the covariance, (x, y) is the grayscale value of neighbouring pixel points in the image, and N is the number of pixels selected. Table 1 shows the results of the correlation of neighbouring elements in three directions for Figures 1 and 2. The results of the comparative data in the three directions for Figures 1 and 2 are shown to be different, indicating that Figure 2 retains the primary pixel features of Figure 1 after encryption. Table 2 shows the results of the time complexity comparison between Figures 1 and 2 in the three directions, and the encrypted image is shown to have a clear advantage. Figures 4–6 show the results of the comparison between the two images in the diagonal, horizontal and vertical directions. Neighbouring pixel values of the original image in each direction are roughly concentrated around y=x, but the pixel distribution of the encrypted image is randomly distributed, which enables the encryption of the image to be completed.

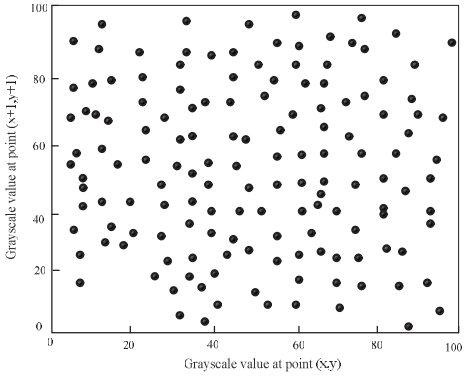

Figure 4(b) Diagonal orientation of Figure 2.

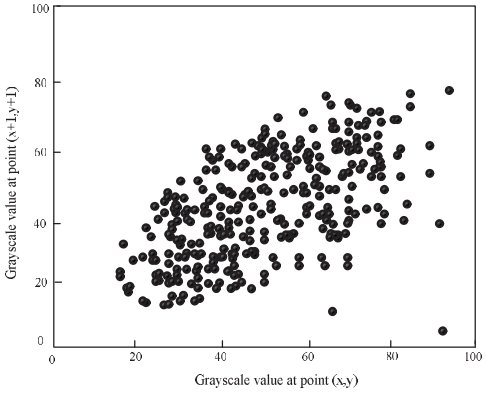

Figure 5(a) Horizontal orientation of Figure 1.

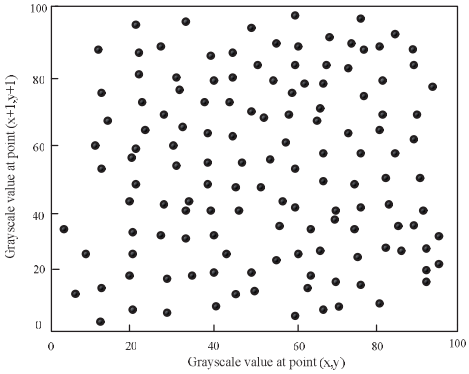

Figure 5(b) Horizontal orientation of Figure 2.

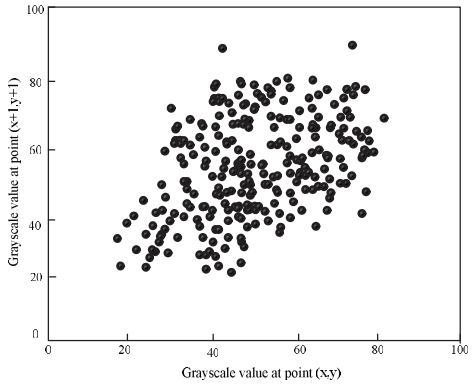

Figure 6(a) Vertical orientation of Figure 1.

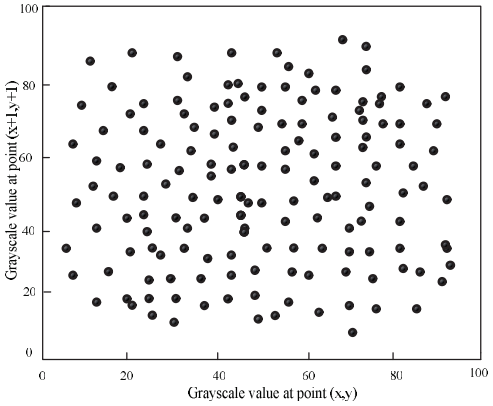

Figure 6(b) Vertical orientation of Figure 2.

5.3 Analysis of Performance Against Differential Attacks

The resistance to differential attacks primarily consists of two components, the pixel change rate (NP) and the normalized average change intensity (UA), which describe the extent to which a change in the details of the plaintext can cause a transformation of the ciphertext. The pixel change rate is calculated as the percentage of the total number of pixels occupied by the number of different pixels in the two images, while the normalized average intensity primarily describes the difference between the grey value of all pixels at the corresponding position in the two images and the average of the maximum values. The ideal value of the pixel change rate for the two random images is 97.194%, and the normalized mean intensity is 37.732%.

Two images with different pixel values, P_1 and P_2, are selected from the plane image, and C_1 and C_2F are the encrypted images of the corresponding images. We then set the existence of a certain pixel point (i, j), $i \in m, j \in n$; if the grey value of the ciphertext exists $C_1(i, j) = C_2(i, j)$, we set $D(i, j) = 0$; otherwise, $D(i, j) = 1$. The pixel change rate is shown in Equation (27), and the normalized mean change intensity is shown in Equation (27):

$$NP = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} D(i,j)}{m \times n} \times 100\% \tag{27}$$

$$UA = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |C_1(i,j) - C_2(i,j)|}{255 \times m \times n} \times 100\% \tag{28}$$

One hundred sets of plane images were selected for testing, and one pixel was randomly selected from one of the images at a time to add 1 to its value and then encrypted using this algorithm. The final NP is 96.142%, and the UA is 38.181%, which shows that both are near the ideal value and that the algorithm is sensitive to plaintext.

5.4 Network Transmission Effect

To verify the effectiveness of the encryption algorithm of digital images proposed in this paper, we decrypted the images in the network using software that simulates Distributed Denial of Service(DDoS) attacks. In network transmission, encryption time is one of the keys to measure the effectiveness of an encryption, and it is related to the security efficiency, in order to verify this index, this we choose 10 images of size 256 × 256 from the University of Granada standard test gallery as objects, and choose literature [11], literature [12], literature [19], literature [20] The algorithms of literature [11], literature [12], literature [19], literature [20] are selected for comparison with the algorithm of this paper, and from the comparison results in Table 3, the algorithm of this paper has certain advantages in terms of time compared with the other four algorithms, especially the current newer encryption algorithms of literature [19] and literature [20] are reduced by 8.9% and 8.1% respectively, which shows that the algorithm of this paper has better encryption effect. Meanwhile, in order to further test the encryption effect of this paper's algorithm in the three directions of the image, we designed 50 different angles of Plane images with 512 × 512 pixels and encrypted them, and the results are shown in Table 4. From these data results, the correlation result values of this paper's algorithm in the three directions are more close to 0 compared

Table 3 Five algorithms to encrypt time(S)

Name	Literature [11]	Literature [12]	Literature [19]	Literature [20]	Algorithm in This Paper
cameraman	0.2322	0.2298	0.1793	0.1732	0.1589
peppers	0.2301	0.2328	0.1784	0.1783	0.1585
clock	0.2981	0.2275	0.1696	0.1794	0.1572
einstein	0.2103	0.2183	0.1632	0.1632	0.1573
house	0.2281	0.2281	0.1721	0.1723	0.1568
galaxia	0.2383	0.2271	0.1739	0.1695	0.1569
barche	0.2412	0.2219	0.1732	0.1632	0.1576
leopard	0.2982	0.2341	0.1792	0.1693	0.1575
portofino	0.2218	0.2301	0.1635	0.1722	0.1572
pallon	0.2128	0.2289	0.1632	0.1627	0.1573
Average	0.2411	0.2279	0.1716	0.1703	0.1575

Table 4 Average adjacent pixel correlation results for the three algorithms

Direction	Literature [11]	Literature [12]	Literature [19]	Literature [20]	Algorithm in This Paper
Horizontal	0.0038	0.0023	0.0016	0.0017	0.0015
Vertical	0.0065	0.0043	0.0015	0.0016	0.0012
Diagonal	0.0063	0.0024	0.0011	0.0009	0.0008

with the other four algorithms, which are reduced by 6.7%, 8.3%, 25% and 6.7%, 16.7,%12.5% compared with the literature [19] and literature [20], respectively, indicating that the encryption effect of this paper's algorithm is obviously better than the other four algorithms.

We transmit the images encrypted by the five algorithms in the network, with 0 indicating "completely decrypted successfully" and 1 indicating "complete decryption failure". The comparative results are shown in Figure 7. From the data statistics, only three images of the algorithm in this paper were corrupted, but the overall values were between 0.7 and 1, which shows that although they were attacked, they were not completely decrypted, and the original image information was still retained. The algorithm of literature [11] has 5 images corrupted, and these images were decrypted to different degrees, although they were not decrypted completely, but the encryption was strongly affected. Four images in [12] were corrupted, and although these results were better than those of [11]. The algorithm of literature [19] and literature [20] have 4 images corrupted, they were markedly weaker than the proposed algorithm. Thus, this experiment shows that the proposed algorithm achieves good encryption performance.

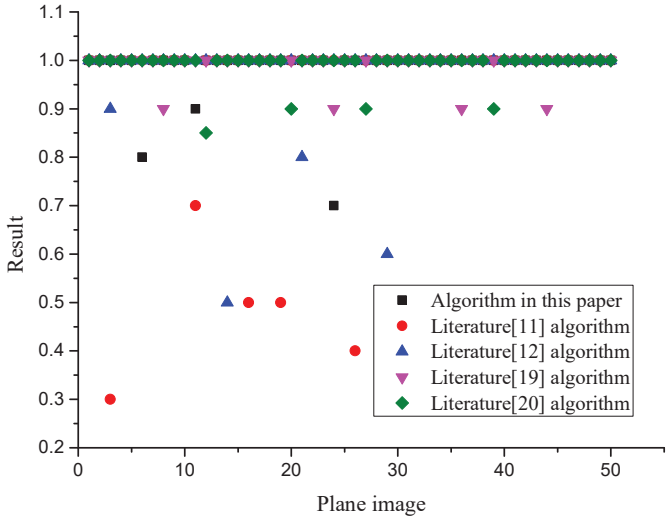

Figure 7 Encryption effect of the five algorithms.

6 Conclusions

To address the problems of strong randomness of image pixel replacement and large computation of image pixel iteration in the current use of encrypted images, we use a fractional-order Fourier transform to replace the image pixel matrix, use a one-dimensional logistic chaos algorithm to reduce the problem of strong randomness of image pixels, and use a sine chaos-based idea to optimize the diffusion algorithm to reduce computational complexity. Simulation experiments show that the proposed algorithm achieves better results in statistical analysis, adjacent pixel correlation, and resistance to differential attack performance analysis indices, and that the algorithm can protect image information better than other algorithms in network transmission.

References

[1] M. Singh, A.K. Singh, 'A comprehensive survey on encryption techniques for digital images', Multimedia Tools and Applications, Vol. 82, No. 8, pp. 11155–11187. March, 2022.

[2] X. Gao, J. Mou, L. Xiong, et al., 'A fast and efficient multiple images encryption based on single-channel encryption and chaotic system', Nonlinear Dynamics, Vol. 108, No. 1, pp. 613–636. March, 2022.

[3] A. Belazi, S. Kharbech, M.N. Aslam, et al., 'Improved Sine-Tangent chaotic map with application in medical images encryption', Journal of Information Security and Applications, Vol. 66, pp. 103131. May, 2022.
[4] K.M. Hosny, S.T. Kamal, M.M. Darwish, 'A color image encryption technique using block scrambling and chaos', Multimedia Tools and Applications, Vol. 81, pp. 501–525, January, 2022.
[5] X. Zhang, L. Zhang, 'Multiple-image encryption algorithm based on chaos and gene fusion', Multimedia Tools and Applications, Vol. 81, No. 14, pp. 20021–20042. June, 2022.
[6] P. Kiran, B.D. Parameshachari, 'Resource optimized selective image encryption of medical images using multiple chaotic systems', Microprocessors and Microsystems, Vol. 91, pp. 104546. June, 2022.
[7] J. Arif, M.A. Khan, B. Ghaleb, et al., 'A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution', IEEE Access, Vol. 10, pp. 12966–12982. January, 2022.
[8] A. Shafique, J. Ahmed, M.U. Rehman, et al., 'Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain', IEEE Access, Vol. 9, pp. 59108–59130. April, 2021.
[9] Ö. F. Boyraz, M.E. Çimen, E. Güleryüz, et al., 'A chaos-based encryption application for wrist vein images', Chaos Theory and Applications, Vol. 3, No. 1, pp. 3–10. June, 2021.
[10] Y. Xian, X. Wang, 'Fractal sorting matrix and its application on chaotic image encryption', Information Sciences, Vol. 547, pp. 1154–1169. February, 2021.
[11] K.A. Pourjabbar, N.A. Habibizad, A.M. Bidgoli, et al., 'A new image encryption scheme based on hybrid chaotic maps', Multimedia Tools and Applications, Vol. 80, pp. 2753–2772. January, 2021.
[12] M.Z. Talhaoui, X. Wang, 'A new fractional one dimensional chaotic map and its application in high-speed image encryption', Information Sciences, Vol. 550, pp. 13–26. March, 2021.
[13] X. Liu, X. Tong, Z. Wang, et al., 'Uniform non-degeneracy discrete chaotic system and its application in image encryption', Nonlinear Dynamics, Vol. 108, No. 1, pp. 653–682. January, 2022.
[14] M. Zarebnia, H. Pakmanesh, R. Parvaz, 'A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images', Optik, Vol. 179: 761–773. February, 2019.
[15] A. Bisht, M. Dua, S. Dua, 'A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random

transform', Journal of Ambient Intelligence and Humanized Computing, Vol. 10, pp. 3519–3531. September, 2019.
[16] L. Zhang, X. Zhang, 'Multiple-image encryption algorithm based on bit planes and chaos', Multimedia Tools and Applications, Vol. 79, pp. 20753–20771, August, 2020.
[17] M. Ahmad, M.Z. Alam, Z. Umayya, et al., 'An image encryption approach using particle swarm optimization and chaotic map', International Journal of Information Technology, Vol. 10, pp. 247–255. January, 2018.
[18] G. Unnikrishnan, J. Joseph, K. Singh, 'Optical encryption by double-random phase encoding in the fractional Fourier domain', Optical Letters, Vol. 225, No. 12, pp. 887–889. June, 2000.
[19] S. Shao, J. Li, P. Shao, et al., 'Chaotic Image Encryption Using Piecewise-Logistic-Sine Map', IEEE Access, Vol. 11, pp. 27477–27488, March, 2023.
[20] X. Wang, X. Chen, M. Zhao, 'A new two-dimensional sine-coupled-logistic map and its application in image encryption', Multimedia Tools and Applications, Vol. 10, pp. 1–37. March, 2023.

Biography

Gaili Du received the bachelor's degree in Electronic information engineering from First Aeronautical College in 2003, the master's degree in Circuit system from Sichuan University in 2009, respectively. She is currently working as an Assistant Professor at the He Nan Medical College. Her research area is Computer application.