IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 September 2022, accepted 2 October 2022, date of publication 1 November 2022, date of current version 8 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3218668

RESEARCH ARTICLE

A Fast Image Encryption Algorithm Based on Improved 6-D Hyper-Chaotic System

HAIPING CHEN, ENJIAN BAI, XUEQING JIANG, (Senior Member, IEEE), AND YUN WU
School of Information Science and Technology, Donghua University, Shanghai 201620, China

Corresponding author: Enjian Bai (baiej@dhu.edu.cn)

This work was supported in part by the National Natural Science Foundation of Shanghai under Grant 20ZR1400700, and in part by the Shanghai Municipal Science and Technology Major Project under Grant 2019SHZDZX01.

ABSTRACT Aiming at the security and efficiency of image transmission, a fast image encryption algorithm based on an improved 6-D chaotic system is proposed. Firstly, we design a hyper-chaotic system with more complex chaotic behavior, analyze the Lyapunov exponential spectrum, chaotic attractor and randomness of the system, and generate random sequences through randomness enhancement operation. Secondly, image preprocessing is used to select pixels from the original image to form a thumbnail, the size of the key space can be changed by adjusting the thumbnail. Thirdly, the hash value of the original image is used as the initial values of the hyper-chaotic system to realize the uniqueness of the key. The row encryption matrix and column encryption matrix are generated according to the maximum and minimum values of row and column pixels in the thumbnail. These two encryption matrices are composed of the full arrangement of random sequences, which refers to the random combination of random sequences in a certain order. Before the encryption, the Arnold transformation is performed on the original image and then the cipher image is obtained by row encryption and column encryption respectively. The experimental results illustrate that the proposed algorithm has excellent security performance, robustness and the speed of encryption and decryption is very fast.

INDEX TERMS Image encryption, hyper-chaotic system, Lyapunov exponential spectrum, chaotic attractor, full permutation.

I. INTRODUCTION

The current image encryption algorithms can be roughly divided into the following four categories: image encryption based on matrix transformation or pixels replacement [1], [2], [3], [4], encryption based on secret segmentation or sharing [5], [6], [7], [8], encryption based on modern cryptosystems [9], [10], [11], [12] and chaos-based image encryption [13], [14], [15], [16], [17], [18], [19]. So far, there are many algorithms for the four types of image encryption. For example, magic squares transformation [20], [21], one of the most classical matrix transform encryption algorithms, mainly realizes encryption by changing the position of pixels. However, the histogram of the original image after the magic square transformation does not change, and the displacement of the magic square is cyclical, so the encrypted image can be cracked by exhaustive attack. Compared with the magic squares, the image encryption algorithm based on key sharing [22] retains higher security, but it may inflate the data of images. Therefore, the key sharing-based encryption scheme is not a suitable algorithm for images with large amount of data. In contrast, chaotic signals not only have natural concealment but also possess larger key space [23], [24]. In addition, the unpredictability of chaotic signals also makes it applicable to secret communication, and the chaos-based image encryption algorithms have become a popular trend in encryption [25], [26], [27].

Since Matthews first took chaotic systems for encryption [28], many encryption algorithms based on chaotic systems have been developed [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40]. However, there are significant problems in some encryption algorithms based

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

on chaotic systems. Low-dimensional chaotic systems have simpler structures and fewer system parameters, which makes encryption algorithms based on low-dimensional chaotic systems have a smaller key space and lower security [41]. The encryption algorithm introduced by Hua et al. [42] contains poor correlation with the original image, which is prone to the problem that the algorithm cannot resist differential attack. The encryption algorithm based on chaotic system [43], [44], [45], [46], [47] can resist common malicious attacks, such as plaintext attack and noise attack, but the disadvantage is high computational complexity. Therefore, encryption algorithms using low-dimensional chaotic systems and inefficient algorithm cannot take advantage in practical applications. Besides, when high-dimensional chaotic systems are used for image encryption, the common practice is to use chaotic sequences of different dimensions to control different security operations, such as DNA coding, scrambling and diffusion operations at block level, pixel level or bit level [15], [26], [32], [34], [36], [38], [48]. The corresponding algorithm is very complex and the efficiency of encryption and decryption is not high. Therefore, this paper proposes a different way to use the high-dimensional chaotic sequences.

In the paper, the proposed hyper-chaotic system is used for encryption after chaotic verification. Firstly, SHA-256 is used to get the hash value of the original image and convert it into the initial values of the 6-D chaotic system. Meanwhile, pixels are selected from the original image at interval of n to form a thumbnail. For improving the reliability of the algorithm, the reinforcement operation is used to enhance the randomness of the chaotic sequences. In the process of generating encryption matrix, modulo operation is carried out between the result of full arrangement of chaotic sequences and the maximum or minimum gray value of each row and column in thumbnail. And the result of the modulo operation is used as the basis for generating the row encryption matrix and column encryption matrix. Considering the problem of data loss during transmission, Arnold transformation is performed on the image before encryption. When encrypting an image, the image obtained by Arnold transformation is XOR-ed with the row encryption matrix and the column encryption matrix respectively to generate the cipher image. After receiving the encrypted image and the key, the receiver can reconstruct the plaintext image according to the information in the key by reverse operation. The main contributions of our work are summarized as follows:

1. We designed a 6-D chaotic system, which can ameliorate the problem of weak security caused by taking low-dimensional chaotic system for image encryption.
2. The proposed image encryption scheme does not involve complex method such as DNA encoding, but only the simple arrangement and XOR operation are applied, so it can complete the encryption of the image in a short time.
3. The size of the key space can be controlled by the parameters in image preprocessing, and any dimension (no more than six dimensions) can be selected from the 6-D system according to the security requirement for image encryption.

The rest of this paper is arranged as follows. In Section 2, the hyper-chaotic system is designed and the analysis of dynamic behavior and randomness of the system is given. In Section 3, the image encryption and decryption based on proposed hyper-chaotic system is described. The proposed algorithm is simulated and its performance is analyzed in Section 4. Finally, a brief conclusion is drawn in Section 5.

II. 6-D CHAOTIC SYSTEM

Chaotic system is a nonlinear dynamical system. It can generate chaotic sequences with good randomness and non-correlation, and it is very suitable for encryption because of its sensitivity to initial values and parameters.

Liu et al. [49] proposed a 5-dimensional hyper-chaotic system, and the equation is shown in (1). Meanwhile, the related parameters are set as $a = 11.5, b = 43, c = -1$, $d = 16, e = 4, h = 4.9, r = -0.07$, and $k = -1$.

$$\begin{cases} \dot{x} = a(y - x) + eyz \\ \dot{y} = cx + dy - xz - w + u \\ \dot{z} = xy - bz \\ \dot{w} = rw + hy \\ \dot{u} = ky \end{cases} \tag{1}$$

In order to further improve the complexity of the chaotic system, an improved 6-D system is proposed based on the above 5-dimensional hyper-chaotic system. The specific equations are as follows:

$$\begin{cases} \dot{x} = a(y - x) + eyz \\ \dot{y} = cx + dy - xz - w + u \\ \dot{z} = xy - bz \\ \dot{w} = rw + hy \\ \dot{u} = ky + v \\ \dot{v} = \sin v + x \end{cases}, \tag{2}$$

where $a = 25, b = 53, c = -5, d = 16, e = 10$, $h = 4.9, r = -0.07$, and $k = -1$.

A. VERIFICATION OF CHAOS FEATURES

The Lyapunov exponent and Kolmogorov entropy are often used to verify the state of the system. In this paper, we take the Lyapunov exponential spectrum to analyze the dynamic characteristic of the 6-D system, which represents the separation velocity of trajectory. When a nonlinear dynamic system retains a positive Lyapunov exponent, it shows that the system is in a state of chaos, and the larger the Lyapunov exponent, the more obvious the chaotic characteristics and the higher the degree of chaos [50]. Meanwhile, a nonlinear dynamic system can be regarded as a hyper-chaotic system if it has at least two positive Lyapunov exponents [50].

Under the above parameters of the 6-D system, the Lyapunov exponential spectrum is shown in Fig 1. There are two positive Lyapunov exponent, it means the 6-D system

is a hyper-chaotic system. Meanwhile, the trajectories of the system in the phase space (x, y), (x, z), (x, w), (x, u), (x, v), (y, v) are shown in Fig 2 after experimental simulation. As can be seen from the figure, there are chaotic attractors in every phase space of the system, which confirms that the proposed system is hyper-chaotic. In order to further analyze the dynamics of chaotic systems, the bifurcation diagram of the chaotic system in the $x = y(y > 0)$ plane when the parameter $r \in (0, 80)$ is shown in Fig 3.

B. RANDOM REINFORCEMENT OPERATION

For the image encryption algorithm in this paper, the encryption matrix is generated by the chaotic sequences, so the randomness of chaotic sequences greatly affects the reliability of the encryption algorithm.

In order to enhance the randomness of the chaotic sequences, we carried out a randomness reinforcement operation on the chaotic sequences. The specific operation are as follows:

Step 1: Finding the maximum and minimum values of each chaotic sequence and denoting them by p_1 and p_2.

Step 2: Setting the parameters p_0, ε and e, where $p_1 < p_0 < p_2, \varepsilon \in (0, 0.5)$ and $e \in (0, 0.5)$. We select the sequence value that satisfies (3) from the chaotic sequence, and take the result of $(x_n(i) - p_0)$ as the element $S(i)$ in the new set $\mathbf{S}$.

$$|x_n(i) - p_0| < e \tag{3}$$

Step 3: After completing the operation in step 2, take the following formula to update the value of p_0,

$$p_0' = p_0 + \varepsilon. \tag{4}$$

Step 4: Repeating the above steps until p_0 is greater than p_2.

Step 5: Considering the subsequent operations, the elements in $\mathbf{S}$ are converted into the range of [0, 255] by

$$S(i) = \left\lceil mod(S(i) * 10^{15}, 256) \right\rceil, \tag{5}$$

where $S(i)$ represents the elements in $\mathbf{S}$.

Since the size of the encryption matrix in the subsequent operation is the same as that of the original image, and the encryption matrix is composed of the chaotic sequence after the randomness enhancement operation, the length of the chaotic sequence should be larger than the length and width of the original image. In fact, the number of elements in the set $\mathbf{S}$ determines the length of the chaotic sequence, and there are $(p_2 - p_0)/\varepsilon$ elements in the set $\mathbf{S}$. Hence, when the parameters are set to satisfy (6), the length of the chaotic sequence can be guaranteed to meet the requirements.

$$\frac{p_2 - p_0}{\varepsilon} > \max(L1, W1), \tag{6}$$

where L_1 represents the length of the original image, W_1 represents the width of the image.

C. RANDOMNESS OF CHAOTIC SEQUENCES

The randomness of chaotic sequences generated by hyper-chaotic system is analyzed with NIST SP800-22 standard. The NIST SP800-22 standard contains fifteen tests such as frequency detection, the $P-$value and pass rates are regarded as criteria of each test. When P value is larger than 0.01, the sequence is regard as random, and the sequences that pass all the test have good randomness [51]. The results of 100 groups different chaotic sequences obtained after random reinforcement operation are shown in Table 1.

As shown in Table 1, the chaotic sequences pass all the fifteen tests. Therefore, the randomness reinforcement operation proposed in this scheme makes the chaotic sequences have good randomness, and enhances the reliability of chaotic systems.

TABLE 1. Test results of NIST test.

Test	P-value	Pass rate
Frequency	0.224661	1
Block Frequency	0.271090	1
Cumutative Sums	0.769299	0.99
Runs	0.895086	0.99
Longest Run	0.154026	1
Rank	0.463127	0.99
FFT	0.393768	0.98
Non Overlapping Template	0.946245	0.99
Overlapping Template	0.974902	1
Universal	0.981371	1
Approximate Entropy	0.926358	0.99
Random Excursions	0.340527	0.98
Random Excursions Variant	0.429374	0.98
Serial	0.920038	0.99
Linear Complexity	0.137149	0.99

III. IMAGE ENCRYPTION ALGORITHM BASED ON 6-D CHAOTIC SYSTEM

The flowchart of encryption algorithm proposed in this paper is shown in Fig 4(a). The SHA-256 function is used to get the hash value of the original image and take the result as the initial values of hyper-chaotic system. At the same time, pixels are selected from the original image to form a thumbnail by image preprocessing, and then combine the thumbnail with chaotic sequences after random reinforcement operation to generate row encryption matrix and column encryption matrix. Considering that the image may lose part of its data during the transmission, an Arnold transformation is performed on the original image before the encryption. once the encryption matrix is determined, the XOR operation is performed on the image obtained after Arnold transformation and the column encryption matrix to generate the column encrypted image. In order to improve the security of the encryption algorithm, a second encryption is performed on the basis of the column encrypted image, and the second encryption result is transmitted in the channel as a cipher image.

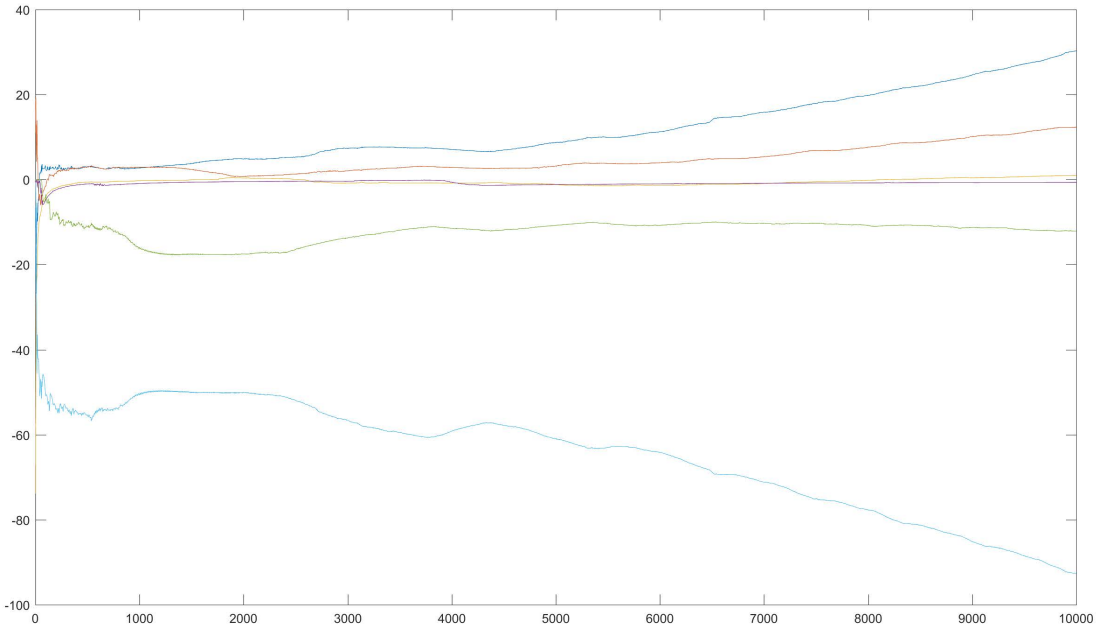
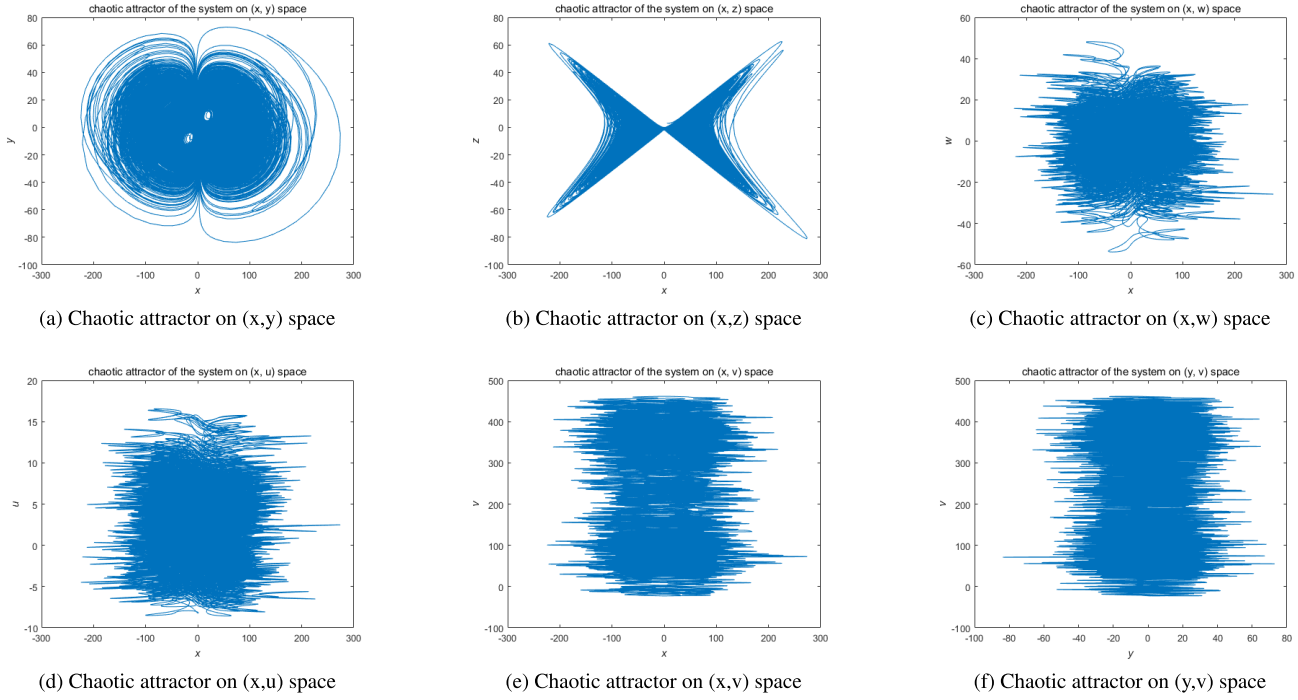


FIGURE 1. Lyapunov exponential spectrum.



(a) Chaotic attractor on (x,y) space (b) Chaotic attractor on (x,z) space (c) Chaotic attractor on (x,w) space

(d) Chaotic attractor on (x,u) space (e) Chaotic attractor on (x,v) space (f) Chaotic attractor on (y,v) space

FIGURE 2. Attractor phase diagram of 6-D chaotic system.

A. IMAGE PREPROCESSING

Assuming an original image G with size of $M_1 \times M_2$ is in uncompressed format. Selecting pixels from each row and column of pixels in the image G at an interval of n to generate the thumbnail H sized $H_1 \times H_2$. The number of rows and columns in H are

$$H_1 = round(M_1/n)$$
$$H_2 = round(M_2/n), \quad (7)$$

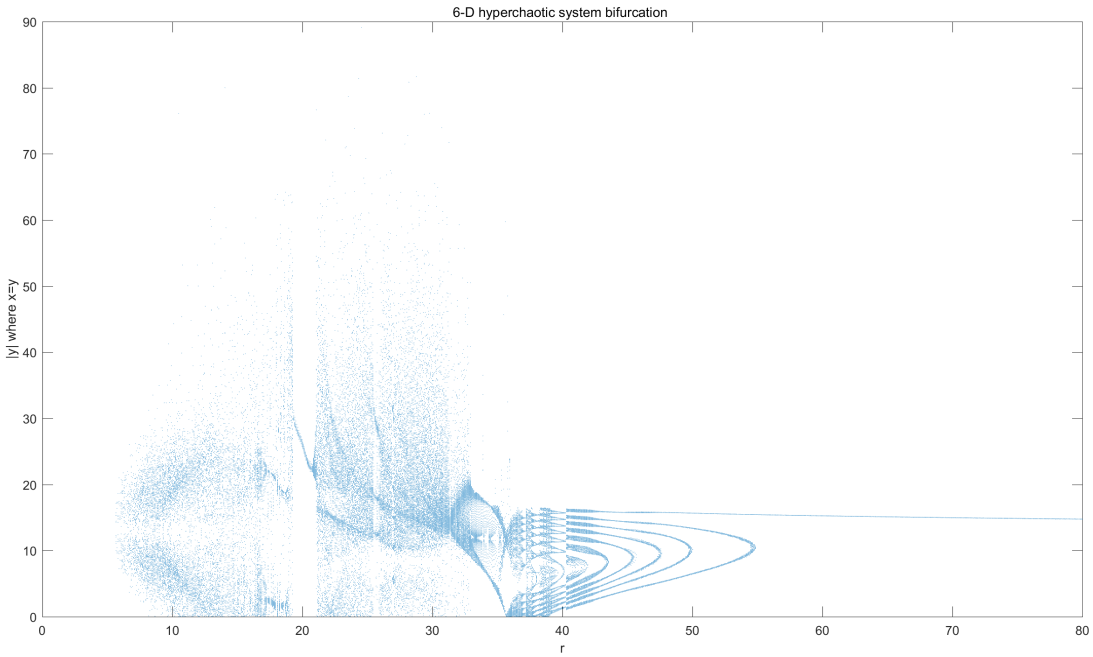


FIGURE 3. Bifurcation of 6-D chaotic system where $r \in (0, 80)$ and $x = y (y > 0)$.

and the pixel value in H are

$$H(h_1, h_2) = G(h_1 \times n, h_2 \times n), \tag{8}$$

where $1 \leq h_1 \leq H_1, 1 \leq h_2 \leq H_2$.

B. HASH VALUE CONVERSION

The hash value of original image obtained by SHA-256 is regarded as the initial values of the hyper-chaotic system. However, the system only enters a hyper-chaotic state within a specific range of initial values. Hence, it is reasonable to convert the hash value to a suitable range.

SHA-256 generates 64 hexadecimal hash values and then convert it by the following steps:

Step 1: Binarizing the hexadecimal hash values.

Step 2: Dividing the binary sequence into six groups of D_1, D_2, D_3, D_4, D_5, D_6.

Step 3: Since 256 can not be divided by 6, the number of binary elements in $D_1, D_2, \cdots, D_5$ is $round(256/6)$, and there are $(256 - round(256/6) \times 5)$ elements in D_6.

Step 4: After grouping, $D_1, D_2, \cdots, D_6$ are summed respectively to obtain $data_1, data_2, \cdots, data_6$. Taking the $data_1$ as a demonstration,

$$data_1 = \sum_{i=1}^{43} D_1(i), \tag{9}$$

where $D_1(i)$ represents the elements in D_1.

Step 5: As different chaotic systems, the range of initial values is different. So, $data_1, data_2, \cdots, data_6$ need to be converted to the corresponding range. For example, the initial values of the hyper-chaotic system proposed in this paper need to satisfy $x(0) \in [-10, 50]$, $y(0) \in [0, 60]$, $z(0) \in [0, 100]$, $w(0) \in [-10, 50]$, $u(0) \in [0, 20]$, $v(0) \in [-10, 20]$, so the hash value can be converted as follows

$$\begin{cases} x(0) = data_1 - 7 \\ y(0) = \frac{1}{2} data_2 + 13 \\ z(0) = \frac{1}{3} data_3 + 9 \\ w(0) = data_4 - 7 \\ u(0) = \frac{2}{5} data_5 \\ v(0) = \frac{1}{2}(data_6 - 1) \end{cases}. \tag{10}$$

C. ENCRYPTION MATRIX

Before encrypting the original image, the encryption matrix is first generated by thumbnail H and chaotic sequences. Due to the generality of the encryption scheme proposed in this paper, the N dimensional chaotic system refers to the chaotic system of any dimension. The following part describes the specific steps of generating encryption matrix.

Step 1: Firstly, performing full permutation on N groups chaotic sequences, and there are totally $N!$ arrangements.

Step 2: Getting an array $R = [r_1, r_2, \cdots, r_{h1}]$ consisted of the maximum gray value of each row in the thumbnail H, where r_i represents the maximum gray value in the ith row of pixels in H.

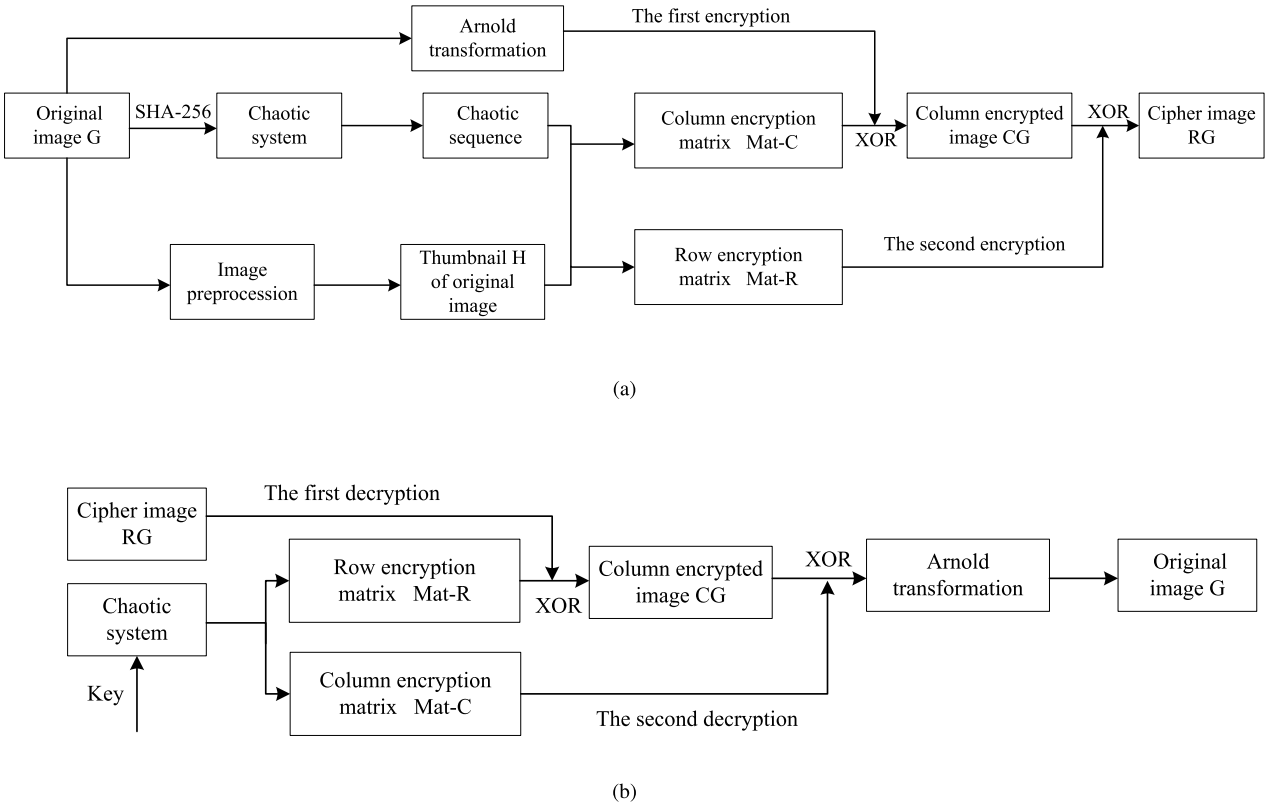


FIGURE 4. The flow chart of proposed algorithm. (a) encryption process; (b) decryption process.

Step 3: Copying and expanding R to get $R' = [r_1, r_2, \cdots, r_{h1}, r_1, r_2, \cdots, r_{h1}, r_1, r_2, \cdots]$, and the number of elements in R' is M_1.

Step 4: In order to avoid obvious distribution rules of elements in R', bitxor operation is carried out on the hash value $data_1, data_2, \cdots, data_6$ of original image and the result is used as the seed of Randperm function. Then, scramble the elements in R'according to the obtained random number and R'' represents the scrambled R'.

Step 5: Elements in R'' are processed according to the following two formulas

$$\begin{aligned} a &= \max(R''(i), N!) \\ b &= \min(R''(i), N!), \end{aligned} \tag{11}$$

where $1 \leq i \leq M_1$. The resulting full permutation number is

$$\begin{cases} K = mod(a, b) & if \quad b > 0 \\ K = mod(a, b+1) & otherwise, \end{cases} \tag{12}$$

by which we can avoid the situation where the value of K corresponding to each row is equal to R'' when $N!$ is greater than 256.

Step 6: The Kth permutation is selected as the arrangement of the N groups chaotic sequences after gaining the K of each row in the original image.

For example, the four-dimensional Lorenz system is adopted for image encryption and four groups chaotic sequences can generate 4!, 24 permutations. Table 2 displays the 24 permutations and from left to right, the indices corresponding to the permutations increases by 1 successively, among which the index of the leftmost permutation is 0.

Assuming that the first element in R'' is r_3 and the value of r_3 is 123, that is $R''(1) = 123$, then we can figure out that K is equal to 3. Then, the fourth arrangement, that is, the arrangement of $x_1(i)$, $x_3(i)$, $x_4(i)$, $x_2(i)$ should be selected from the 24 permutations as the composition of the encryption sequence for the first row in the original image. Therefore, the encryption sequence corresponding to the first row of the original image is $[x_1(1), x_3(1), x_4(1), x_2(1), x_1(2), x_3(2), x_4(2), x_2(2), x_1(3), x_3(3), \cdots]$.

Step 7: According to the above steps, each row in the original image selects sequence values from the N sets chaotic sequences based on the corresponding arrangement to form encryption sequences. When the encryption sequences of all rows are obtained, the row encryption matrix $Mat - R$ is determined.

The column encryption matrix $Mat - C$ is constructed in a similar way, except that the array R is composed of the minimum gray value of each column in the thumbnail H.

TABLE 2. The full permutation of four groups chaotic sequences.

x_1, x_2, x_3, x_4	x_1, x_2, x_4, x_3	x_1, x_3, x_2, x_4	x_1, x_3, x_4, x_2
x_1, x_4, x_2, x_3	x_1, x_4, x_3, x_2	x_2, x_1, x_3, x_4	x_2, x_1, x_4, x_3
x_2, x_3, x_1, x_4	x_2, x_3, x_4, x_1	x_2, x_4, x_1, x_3	x_2, x_4, x_3, x_1
x_3, x_1, x_2, x_4	x_3, x_1, x_4, x_2	x_3, x_2, x_1, x_4	x_3, x_2, x_4, x_1
x_3, x_4, x_1, x_2	x_3, x_4, x_2, x_1	x_4, x_1, x_2, x_3	x_4, x_1, x_3, x_2
x_4, x_2, x_1, x_3	x_4, x_2, x_3, x_1	x_4, x_3, x_1, x_2	x_4, x_3, x_2, x_1

D. ENCRYPTED OPERATIONS

After completing all the above operations, the column encryption matrix and row encryption matrix for image encryption can be received, and then encrypt the image G' after Arnold transformation by

$$\begin{aligned} CG &= G' \oplus Mat - C \\ RG &= CG \oplus Mat - R, \end{aligned} \tag{13}$$

where CG represents the column encrypted image and the result of the second encryption operation is the cipher image, represented by RG. In order to enable the receiver to recover the original image from the cipher image, the key needs to be sent together with the cipher image.

In the scheme, the encryption matrix is jointly determined by the maximum or minimum gray value of each row and column in thumbnail H and chaotic sequences. Moreover, the chaotic sequences are depended on the relevant parameters and the hash value of the original image. Hence, the parameters p_0, ε, e, the maximum gray value and the minimum gray value of each row and column in the thumbnail are selected as key to be transmitted to the receiver.

E. IMAGE DECRYPTION

The decryption process is shown in Fig 4(b). After receiving the cipher image and the key, the receiver can get the same encryption matrix according to the information in the key, and then perform the following inverse operations on the cipher image and Arnold transformation to reconstruct the plain image G,

$$\begin{aligned} CG &= RG \oplus Mat - R \\ G' &= CG \oplus Mat - C. \end{aligned} \tag{14}$$

IV. PERFORMANCE ANALYSIS

In this part, we analyse the performance of the proposed encryption algorithm. When taking Lena as the original image, according to the respective maximum and minimum values of the six groups chaotic sequences generated by the 6-D chaotic system, let $p_0 = [-114, -71, -69, -24, 7, 4]$, $\varepsilon = [0.2, 0.2, 0.2, 0.2, 0.2, 0.2]$, $e = [0.5, 0.5, 0.5, 0.5, 0.5, 0.5]$, respectively. Using Peppers, Man and Girl as the original images, we set the parameters $p_0 = [-195, -42, -56, -1, 6, -19]$, $p_0 = [-160, -50, -45, -32, 6, -11]$, $p_0 = [-161, -58, -55, -10, 4, -14]$, and the values of ε and e are the same as those of the original image Lena. The original images, cipher images and decrypted images are shown in Fig 5.

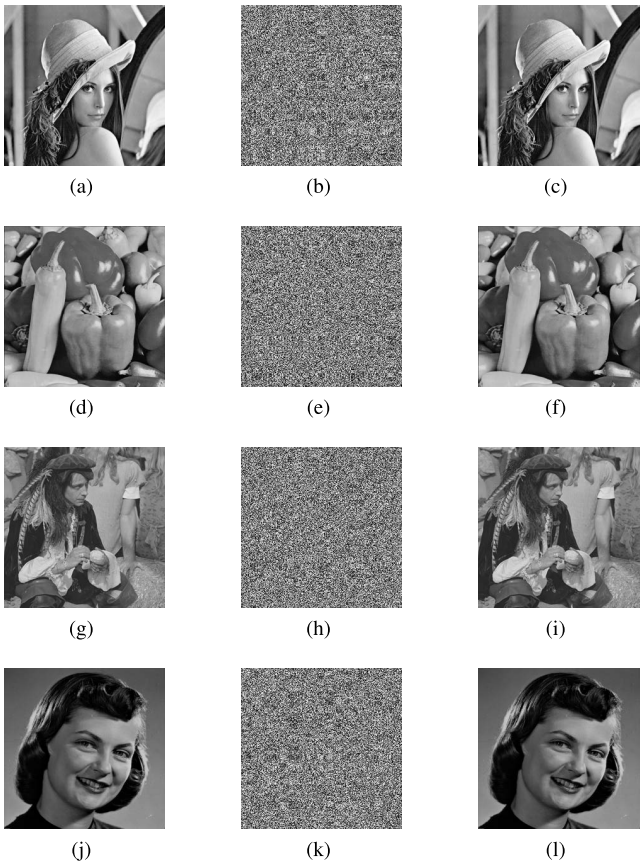


FIGURE 5. Experimental results: (a), (d), (g), (j) are the plain images of "Lena", "Peppers", "Man" and "Girl" (b), (e), (h), (k) are the cipher images, (c), (f), (i), (l) are the decrypted images.

A. ADJACENT PIXEL CORRELATION ANALYSIS

Due to the high correlation between adjacent pixels in the unprocessed plain image, a pixel tends to leak the information of its surrounding pixels. In this case, the attacker can roughly infer the information of the plain image by using the known pixels, so the encryption algorithm must be able to break the strong correlation between the adjacent pixels to protect the information of the plain image.

In order to intuitively represent the relationship between adjacent pixels, we utilize the correlation coefficients in the horizontal, vertical and diagonal directions of the plaintext images and ciphertext images. The smaller the correlation coefficient, the worse the correlation between adjacent pixels, that is, the more uniform the image distribution is. We calculate the correlation coefficients of the original image as well as adjacent pixels in the encrypted image and compared them with that of other encryption algorithms. The experimental result are shown in Table 3 and Table 4. In addition, we also select the Lena and Peppers from the above four experimental images to briefly show the adjacent pixel correlation of original images and encrypted images. And the results are shown in Fig 6.

It is clear from tables that the adjacent pixel coefficients in the encrypted image are much smaller than those in the

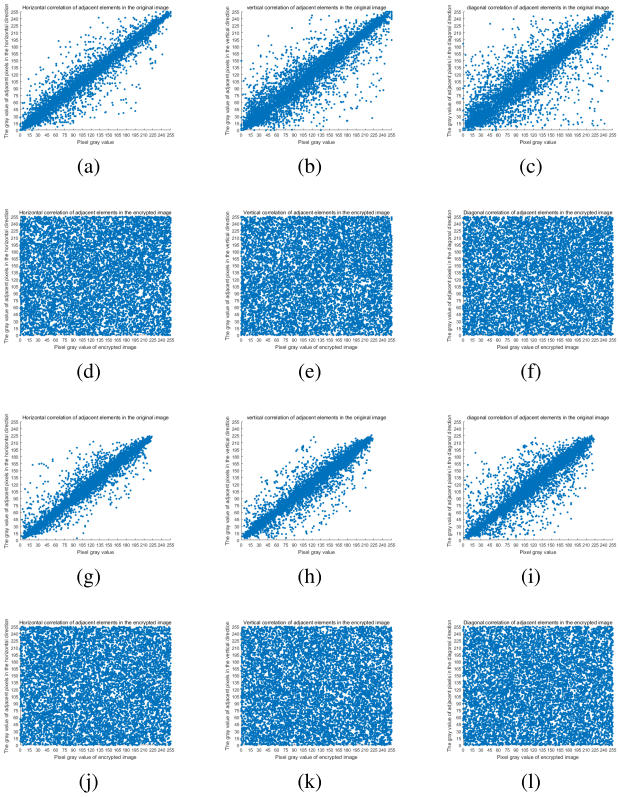


FIGURE 6. Pixel correlation coefficient analysis: (a), (b), (c) Horizontal, Vertical and Diagonal direction of original Lena image, (d), (e), (f) Horizontal, Vertical and Diagonal direction of encrypted Lena image; (g), (h), (i) Horizontal, Vertical and Diagonal direction of original Peppers image, (j), (k), (l) Horizontal, Vertical and Diagonal direction of encrypted Peppers image.

original image and the correlation coefficients of our algorithm is generally smaller than that of other algorithms. Meanwhile, the graphs show that the original image has a strong linear correlation in the three directions and the adjacent pixels of the cipher image are uniformly distributed. Therefore the results mean that the proposed encryption algorithm breaks the strong correlation between adjacent pixels in the original image.

B. HISTOGRAM STATISTICS

The histogram shows the statistical information of the image, which intuitively reflects the distribution of pixel values in the image. The histogram of plaintext images has obvious statistical rule, and attacks against images with statistical rule are called statistical analysis attack. In a statistical analysis attack, the attacker analyzes the intercepted cipher images, summarizes the statistical rules, and compares them with those in plaintext to extract the transformation relationship between the plain images and cipher images to decrypt the encryption scheme. To resist statistical analysis attacks, the histogram of an encrypted image must be uniform and completely different from the plain image.

To more objectively represent the distribution of the pixels in the image, we utilize the variance of the histogram and chi-square test to analysis the distribution of pixels. In fact, chi-square values between 0 and 1 are better at judging the distribution, so we normalize the image before performing the chi-square test. Then, compare them with that of other encryption algorithms. The smaller the variance and chi-square values, the more uniform the image distribution is. At the same time, we select Lena and Peppers from the experimental images as examples for presentation.

The variances of the histogram and chi-square values of four images are shown in Table 5,Table 6 and the histograms of the original and encrypted images are shown in Fig 7. As can be seen from the results, all the encryption scheme enable even distribution of pixels in encrypted images, the encryption scheme [54] and our algorithm enable a more uniform distribution of pixels because they leads to a smaller variance of the histogram. The evenly distributed histograms of cipher images mean that the images after encryption cannot provide effective information, which also confirms that the encryption algorithm proposed in this paper can effectively resist statistical analysis attacks.

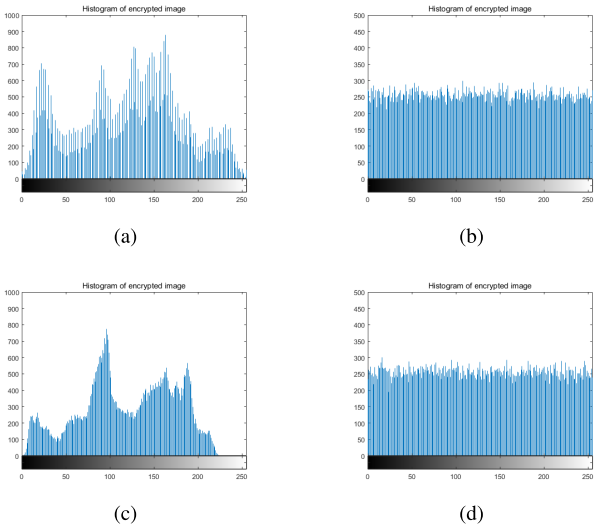


FIGURE 7. Histograms of the plaintext and cipher image. (a) is histogram of "Lena"; (b) is histogram of encrypted "Lena"; (c) is histogram of "Peppers"; (d) is histogram of encrypted "Peppers".

C. INFORMATION ENTROPY ANALYSIS

The information entropy can reflect the randomness of the image. The calculation formula of image information entropy is shown as

$$H(x) = -\sum_{i=1}^{l-1} p(x_i) \log_2 p(x_i), \tag{15}$$

where $p(x_i)$ represents the probability of x_i appearing in the image.

For gray-scale images, the ideal value of information entropy is 8 and the larger the information entropy, the higher the complexity of the cipher image. Under the same preconditions, the proposed encryption algorithm and

TABLE 3. The correlation coefficient of adjacent pixels.

Correlation coefficient	Original images				Encrypted images			
	Lena	Peppers	Man	Girl	Lena	Peppers	Man	Girl
Horizontal correlation coefficients	0.9684	0.9625	0.9459	0.9695	0.0110	0.0101	-0.0012	0.0013
Vertical correlation coefficients	0.9751	0.9721	0.9577	0.9767	-0.0032	0.0196	0.0000	-0.0143
Diagonal correlation coefficients	0.9487	0.9357	0.9149	0.9493	-0.0001	-0.0013	0.0032	0.0193

TABLE 4. The correlation coefficients of the encrypted Lena image with different algorithms.

direction	original images	[52]	[53]	[54]	[55]	[56]	Ours
Horizontal correlation coefficients	0.9684	0.0056	0.0036	0.0068	0.0113	0.0224	0.0110
Vertical correlation coefficients	0.9751	0.0037	0.0027	0.0258	0.0033	-0.0008	-0.0032
Diagonal correlation coefficients	0.9487	0.0032	0.0021	-0.0047	0.0002	0.0007	-0.0001

TABLE 5. The variance of histogram with different algorithms.

	original images	[52]	[53]	[54]	[55]	[56]	Ours
Lena	96589	1027.59	765.32	502.96	841.17	511.22	493.39
Peppers	63259	946.67	734.75	529.63	952.83	539.24	512.63
Man	111088	941.06	653.92	577.21	952.30	541.88	593.36
Girl	1410789	957.16	627.81	501.38	830.87	525.49	579.27

TABLE 6. The chi-square values with different algorithms.

	original images	[52]	[53]	[54]	[55]	[56]	Ours
Lena	0.1613	0.0217	0.0112	0.0049	0.0183	0.0057	0.0044
Peppers	0.1887	0.0205	0.0106	0.0061	0.0197	0.0064	0.0051
Man	0.1091	0.0203	0.0104	0.0063	0.0182	0.0069	0.0064
Girl	0.1465	0.0216	0.0099	0.0050	0.0178	0.0057	0.0068

schemes [52], [53], [54], [55], [56] are used to encrypt image and the information entropy of cipher images are show in Table 7. In order to further verify the randomness of encrypted images, the NIST tests are performed on 100 encrypted images obtained by our encryption scheme and the results for Lena, Peppers, Man and Girl are shown as examples in Table 8.

The experimental results in Table 7 show that the information entropy obtained by the five encryption algorithms are close to 8 and the differences are not significant. That is, all the five algorithms can resist entropy attacks. And as the data in the Table 8 shows, most of the encrypted images can pass all test items, which means that our encryption algorithm can make the encrypted images more random and more resistant to exhaustive attacks.

D. NOISE ATTACK

The transmission of images in the channel is inevitably affected by various factors, such as distortion, degradation, and pollution caused by communication noise. These adverse effects will increase the difficulty for the receiver to decrypt the cipher image, because it is difficult to recover the image from the encrypted image containing noise. So encryption algorithms must be robust enough to resist noise attacks in practical scenarios.

TABLE 7. Information entropy for the encryption.

plain image	[52]	[53]	[54]	[55]	[56]	Ours
Lena	7.9832	7.9952	7.9969	7.9976	7.9971	7.9973
Peppers	7.9856	7.9947	7.9971	7.9974	7.9973	7.9973
Man	7.9834	7.9935	7.9954	7.9967	7.9969	7.9967
Girl	7.9871	7.9961	7.9963	7.9971	7.9970	7.9968

To evaluate the robustness of the encryption algorithm proposed in this paper, we add 0.002 salt and pepper noise to the cipher images. The decrypted images obtained from the encrypted images with noise are shown in Fig 8, and the experimental results show that only some pixels of the decrypted images are changed, but the approximate information of the original image is still preserved. Therefore, the encryption algorithm proposed in this paper can overcome some adverse effects of cipher images caused normal noise in the channel.

E. CUTTING ATTACK

In the process of image transmission, lawbreakers usually carry out cutting attacks on the image. The traditional algorithm can only hide the details, and the range of pixel value moving is small, so it is difficult to resist cutting attacks. To be

TABLE 8. NIST test results of encrypted images.

test name	P-value				pass rate(minimum pass rate)
	Lena	Peppers	Man	Girl	
Frequency	0.9992	0.9995	0.9999	0.9986	1
Block Frequency	0.7261	0.6515	0.4193	0.2824	0.99
Cumulative Sums	0.4193	0.8931	0.4503	0.2398	0.98
Runs	0.7299	0.6135	0.9585	0.8126	0.99
Longest Run	0.7697	0.5723	0.6897	0.1728	1
Rank	0.9985	0.9731	0.9943	0.8796	0.99
FFT	0.2276	0.6684	0.4193	0.2824	0.99
Non Overlapping Template	1	1	1	1	1
Overlapping Template	0.1041	0.3247	0.0974	0.2748	0.94
Universal	0.9995	0.9992	0.9986	0.9999	1
Approximate Entropy	0.5625	0.7153	0.6715	0.2918	0.98
Random Excursions	0.2336	0.5084	0.6426	0.8972	0.99
Random Excursions Variant	0.0984	0.2409	0.5673	0.3921	0.98
Serial	0.6135	0.7299	0.9585	0.8126	0.99
Linear Complexity	0.1750	0.2411	0.3636	0.1105	1

TABLE 9. Performance analysis of different size of thumbnails.

Performance indices	Original image		n=2		n=5		n=10	
	Lena	Peppers	Lena	Peppers	Lena	Peppers	Lena	Peppers
information entropy	7.2419	7.3009	7.9973	7.9972	7.9976	7.9968	7.9973	7.9973
Variance of histogram	96589	63259	490.70	514.02	577.23	434.58	493.39	512.63
Horizontal correlation coefficients	0.9421	0.9627	0.0051	0.0036	0.0128	0.0114	0.0110	0.0101
Vertical correlation coefficients	0.9705	0.9698	-0.0022	-0.0124	-0.0027	-0.0157	-0.0032	0.0196
Diagonal correlation coefficients	0.9191	0.9358	-0.0029	-0.0046	-0.0013	-0.0054	-0.0001	-0.0013

able to defend against cropping attacks, Arnold transformation have been introduced into our encryption scheme, and the encrypted image that has undergone the cutting attack and the corresponding decrypted image are shown in the Fig 9. From the figure, it can be concluded that the encrypted images after cutting attack can still recover the approximate contents of the original images after decryption in our scheme.

F. KEY SPACE

One of the most important factors that determine the performance of an image encryption algorithm is the size of the key space. In the encryption algorithm proposed in the paper, the key consists of the maximum gray values, and the minimum gray values of each row and column in the thumbnail. Besides, the hash value of the original image and the parameters p_0, ε and e are also parts of the key.

The hash value of the original image has 256 bits which means that the size of the key is not less than 256 bits. Actually, only encryption algorithms with keys smaller than 100 bits can be easily decrypted by computer through exhaustive attack, so the proposed encryption algorithm can resist the brute force attacks.

In addition to a large key space, our proposed encryption scheme can also adjust the key space as required. When the parameter $n = 2$, the size of the key space is 2448 bits, and when $n = 10$, there are 800 bits. With different values of n, the size of the key space varies greatly. That is, the size of the key space can be controlled by the value of n.

G. THE EFFECT OF THUMBNAIL SIZE

Image preprocessing can change the size of the thumbnails in the encryption algorithm by setting different values of parameter n. In order to assess whether the size of the thumbnail has an impact on the performance of the encryption algorithm, the cipher images obtained by using thumbnails of different sizes are tested for information entropy, adjacent pixel correlation and histogram analysis.

The experimental results are shown in Table 9. As the results show, the size of the thumbnail has little effect on the information entropy of the cipher image, and the influence of the cipher image on the correlation of adjacent pixels and histogram statistics is also negligible.

H. SENSITIVITY ANALYSIS

The degree of sensitivity to the key is one of the criteria for evaluating the security of an encryption algorithm. For the encryption algorithm, when the ciphertext image obtained before and after the slight change of the key is not much different, it means that the algorithm is not sensitive to the key and the security of the algorithm is insufficient.

To assess the key sensitivity of the proposed encryption algorithm, we take the Lena image as an example and the change of the key is 10^{-14}. Fig 10 shows the result of

TABLE 10. Comparison of performance against differential attacks.

Original image	NPCR						UACI					
	Our	[52]	[53]	[54]	[55]	[56]	Ours	[52]	[53]	[54]	[55]	[56]
Lena	99.5720	99.5601	99.3149	99.1547	99.5267	99.5837	33.3724	33.3675	33.1526	33.2072	33.3005	33.2749
Peppers	99.5881	99.5493	99.3408	99.2739	99.5120	99.5923	33.3952	33.3607	33.1957	33.2349	33.3118	33.3997
Man	99.5834	99.4718	99.3218	99.2572	99.5186	99.5901	33.3562	33.3596	33.1603	33.2533	33.3378	33.3869
Girl	99.5956	99.4692	99.3507	99.2691	99.5274	99.5874	33.3798	33.3587	33.1792	33.2617	33.3285	33.3903

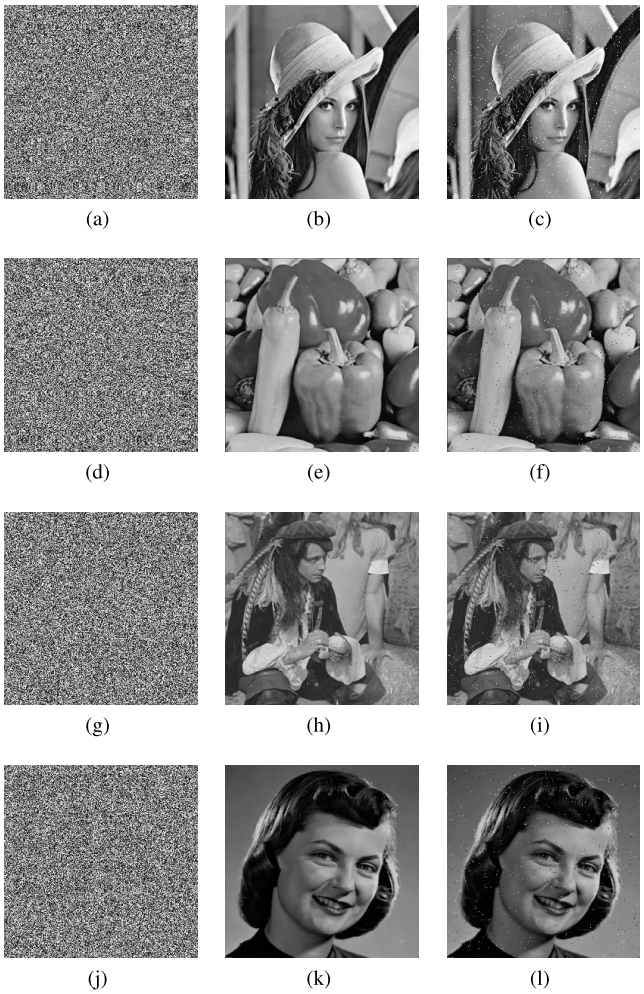


FIGURE 8. Noise attack test: (a), (d), (g), (h) Encrypted images with noise, (b), (e), (h), (k) Decryption by images without noise, (c), (f), (i), (l) Decryption by image with noise.

decrypting the ciphertext image obtained by changing the key with the original key. The experimental results show that the original image can no longer be reconstructed from the ciphertext image based on the original key, which means that the proposed encryption algorithm is highly sensitive to the key.

I. DIFFERENTIAL ATTACK

Differential attack is an important analysis method to test the plaintext sensitivity of algorithms. If the ciphertext image obtained by slight change of plaintext is very different from that obtained by original plaintext, the algorithm is sensitive to plaintext, and it can resist differential attack and has high security. To quantify the differences between images, we introduce two variables, the number of pixels change rate (NPCR) and the uniform average change intensity (UACI). NPCR reflects the ratio of the number of unequal pixels in the same position of the two images to the total number of pixels in the image, and UACI represents the average change intensity of the image. Meanwhile, the theoretical value of NPCR, UACI are 99.6094% and 33.4653% [57].

The NPCR and UACI of Lena, Peppers, Man and Girl are shown in Table 10. AS can be seen from the tables, the NPCR and UACI of the proposed encryption algorithm are closer to the theoretical values than those of the encryption algorithms [52], [53] and not much different than in [56].

J. TIME CONSUMPTION

For encryption algorithms, the time spent in encryption is one of the indicators to measure whether the algorithm can be widely used. So, we made statistics on the time spent by the proposed encryption algorithm and schemes [52], [53], [54], [55], [56], and the results are shown in Table 11. Obviously, compared with the other five encryption schemes, the encryption scheme [54] and our proposed encryption algorithm take less time and are more efficient.

In the encryption algorithm [52], after using 2D-HSM to generate four sets chaotic sequences and permutation matrices, the author mainly uses DNA encoding and decoding, pixels replacement and XOR operation to generate cipher images. The complexity of DNA encoding and decoding operations and replacement operations is higher than that of the full permutation operation used in the encryption algorithm proposed in this paper, so the encryption scheme [52] takes more time. The encryption algorithm [53] is theoretically simpler than algorithm proposed in this paper. In the encryption scheme [53], the Logistic map is combined with an 8-stage Linear Feed Back Shift register to generate the encryption sequences, and then XOR the plain images and the encryption sequences to get the cipher images. In practice, this encryption algorithm takes a lot of time to generate the encryption sequence because it needs to recycle the shift register for many times.

The encryption scheme [54] initially divides the plaintext image into blocks, calculates the correlation coefficient of blocks, and then uses the correlation coefficient, skew tent

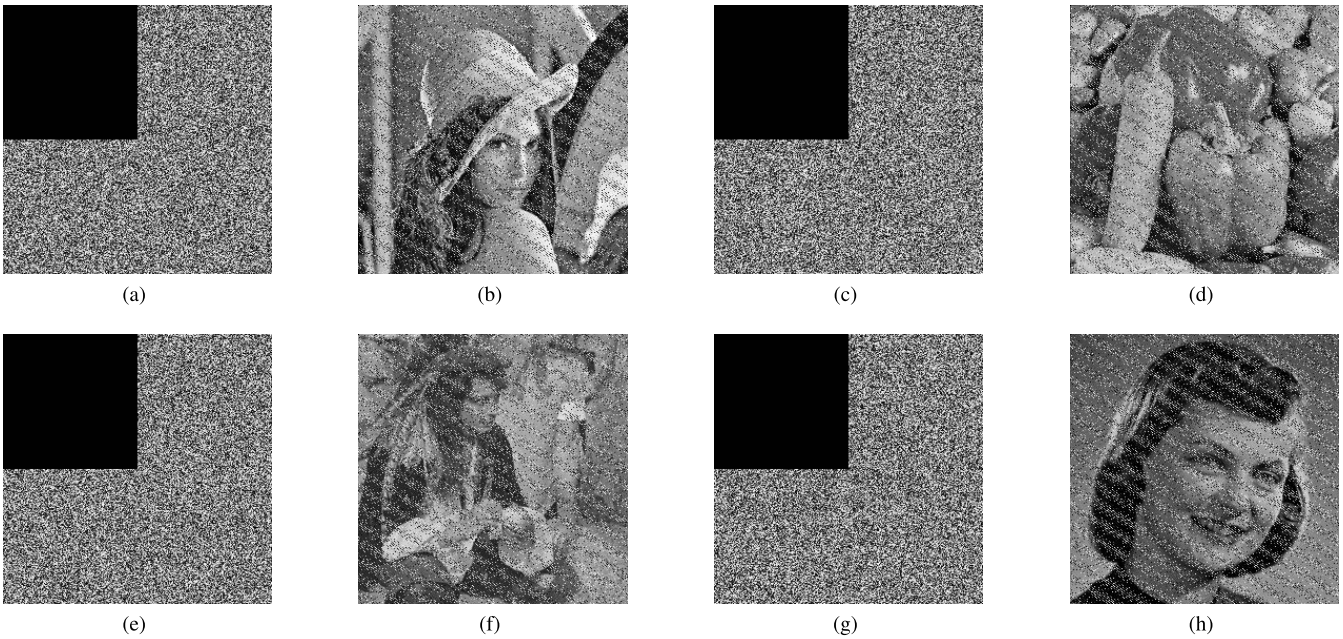


FIGURE 9. Cutting attack test: (a), (c), (e), (g) are encrypted images with cutting, (b), (d), (f), (h) are decryption of images with cutting.

TABLE 11. Comparison of time consumption.

Original image	[52](s)	[53](s)	[54](s)	[55](s)	[56](s)	Ours(s)
Lena (256×256)	2.310	14.005	0.179	0.312	0.304	0.168
Lena (512×512)	3.471	37.297	0.295	0.474	0.523	0.283
Peppers (256×256)	3.191	15.247	0.183	0.275	0.321	0.194
Peppers (512×512)	5.764	40.178	0.228	0.397	0.618	0.231

FIGURE 10. Key sensitivity test. (a) cipher image with original key; (b) decryption by original key; (c) decryption by incorrect key.

map, and XOR operation to generate a scrambled matrix. Finally, the matrix obtained by the TD-ERCS Map and the above-mentioned scrambled matrix are used to scramble the original image. Finally, the result of scrambling is the encrypted image. Only low-dimensional discrete chaotic systems and scrambled operations are used to generate the encrypted images, so the computational complexity of the encryption algorithms is also relatively low. In addition, the encryption algorithms [55], [56] also use low-dimensional chaotic systems and scramble method to generate encrypted images. However, the linear-delay-modulation introduced in [55] makes it take more time, and the encryption algorithms [56] spend more time by requiring multiple scrambling and pixel replacement operations on the original image.

V. CONCLUSION

In this paper, a fast image encryption algorithm based on an improved 6-D chaotic system is proposed. In order to improve the complexity of the chaotic system, we design a six-dimensional chaotic system and perform random enhancement operations on the chaotic sequences. The hash value of original image is used as the initial value of chaotic system to realize the purpose of one graph one key. In addition, we take the hash value of the original image as the seed of the Randperm function, which can further strengthen the association between the plain image and the encryption algorithm. Meanwhile, scrambling the encryption matrix based on the random numbers can avoid the obvious distribution of elements in the encryption matrix caused by replication and expansion. The security of the image encryption algorithm proposed in this paper is to generate the encryption matrix based on the full arrangement of high-dimensional chaotic sequences, which is completely different from the existing image encryption algorithm based on high-dimensional chaotic system. Because the encryption process is very simple, the encryption speed is very fast. Moreover, the algorithm can also meet the needs of different security levels from another aspect. For example, when constructing encryption matrix, $N!$ or $M!(M < N)$ full permutations can be selected.

Another reason why the algorithm uses thumbnails is that when some application scenarios need to preview the picture, through some pixel arrangement scheme, the algorithm in this paper can be simply modified, and only the thumbnail can be decrypted firstly without decrypting the whole picture. At the same time, the algorithm can be further combined with information hiding technology to realize information hiding in plaintext domain or ciphertext domain in thumbnail.

REFERENCES

[1] B. Acharya, S. K. Patra, and G. Panda, "Image encryption by novel cryptosystem using matrix transformation," in *Proc. 1st Int. Conf. Emerg. Trends Eng. Technol.*, Nagpur, India, Jul. 2008, pp. 77–81.

[2] H. Ye, S. Huang, and W. Liu, "Research on image scrambling method based on combination of Arnold transform and exclusive-or operation," in *Proc. IEEE 4th Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Chongqing, China, Jun. 2020, pp. 151–154.

[3] W. Zhang, H. Yu, Y.-L. Zhao, and Z.-L. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Process.*, vol. 118, pp. 36–50, Jan. 2016, doi: 10.1016/j.sigpro.2015.06.008.

[4] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018, doi: 10.1016/j.sigpro.2017.10.004.

[5] P. R. Kamble and S. Patil, "Exploring secret image sharing with embedding of shares," in *Proc. 2nd Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2018, pp. 1090–1093.

[6] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3848–3858, 2020, doi: 10.1109/TIFS.2020.3001735.

[7] Y. Jain, R. Bansal, G. Sharma, B. Kumar, and S. Gupta, "Image encryption schemes: A complete survey," *Int. J. Signal Process., Image Process. Pattern Recognit.*, vol. 9, no. 7, pp. 157–192, Jul. 2016, doi: 10.14257/ijsip.2016.9.7.15.

[8] H. Wadekar, A. Babu, V. Bharvadia, and P. N. Tatwadarshi, "A new approach to video steganography using pixel pattern matching and key segmentation," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Coimbatore, India, Mar. 2017, pp. 1–5.

[9] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *Proc. Int. Conf. Eng. Technol. (ICET)*, Antalya, Turkey, Aug. 2017, pp. 1–7.

[10] A. Murtaza, S. J. Hussain Pirzada, and L. Jianwei, "A new symmetric key encryption algorithm with higher performance," in *Proc. 2nd Int. Conf. Comput., Math. Eng. Technol. (iCoMET)*, Sukkur, Pakistan, Jan. 2019, pp. 1–7.

[11] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Opt. Laser Eng.*, vol. 121, pp. 169–180, Oct. 2019, doi: 10.1016/j.optlaseng.2019.03.006.

[12] B. Mahalakshmi, G. Deshmukh, and V. N. L. N. Murthy, "Image encryption method using differential expansion technique, AES and RSA algorithm," in *Proc. 5th Int. Conf. Image Inf. Process. (ICIIP)*, Solan, India, Nov. 2019, pp. 363–366.

[13] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018, doi: 10.1109/ACCESS.2018.2817600.

[14] Y. Luo, X. Ouyang, J.-X. Liu, and L.-C. Cao, "An image encryption method based on elliptic curve ElGamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[15] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1319–1333, 2018, doi: 10.1007/s11071-018-4426-4.

[16] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," *Opt. Exp.*, vol. 18, no. 11, pp. 12033–12043, May 2010, doi: 10.1364/OE.18.012033.

[17] S. Sun and Y. Guo, "A new hyperchaotic image encryption algorithm based on stochastic signals," *IEEE Access*, vol. 9, pp. 144035–144045, 2021, doi: 10.1109/ACCESS.2021.3121588.

[18] M. Kaur and V. Kumar, "Efficient image encryption method based on improved Lorenz chaotic system," *Electron. Lett.*, vol. 54, no. 9, pp. 562–564, 2018, doi: 10.1049/el.2017.4426.

[19] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Opt. Lasers Eng.*, vol. 82, pp. 95–103, Jul. 2016, doi: 10.1016/j.optlaseng.2016.02.002.

[20] S. Sowmiya, I. M. Tresa, and A. P. Chakkaravarthy, "Pixel based image encryption using magic square," in *Proc. Int. Conf. Algorithms, Methodol., Models Appl. Emerg. Technol. (ICAMMAET)*, Chennai, India, Feb. 2017, pp. 1–4.

[21] W. Zhong, Y. Hui Deng, and K.-T. Fang, "Image encryption by using magic squares," in *Proc. 9th Int. Congr. Image Signal Process., Biomed. Eng. Informat. (CISP-BMEI)*, Datong, China, Oct. 2016, pp. 771–775.

[22] S. Ochiai, K. Iwamura, and A. A. A. M. Kamal, "Secure pairwise key sharing using geometric group key sharing method," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2020, pp. 1–2.

[23] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019, doi: 10.1016/j.ins.2018.12.048.

[24] C.-Q. Li, D.-D. Li, B.-B. Feng, J.-H. Lu, and H. Feng, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75843, 2018, doi: 10.1109/ACCESS.2018.2883690.

[25] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018, doi: 10.1016/j.optlastec.2017.10.024.

[26] Z. Man, J. Li, X. Di, and O. Bai, "An image segmentation encryption algorithm based on hybrid chaotic system," *IEEE Access*, vol. 7, pp. 103047–103058, 2019, doi: 10.1109/ACCESS.2019.2931732.

[27] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014, doi: 10.1016/j.sigpro.2013.10.034.

[28] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989.

[29] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020, doi: 10.1109/ACCESS.2020.2965740.

[30] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–15, Jun. 2018, doi: 10.1109/JPHOT.2018.2827165.

[31] F. Yang, J. Mou, H. Yan, and J. Hu, "Dynamical analysis of a novel complex chaotic system and application in image diffusion," *IEEE Access*, vol. 7, pp. 118188–118202, 2019, doi: 10.1109/ACCESS.2019.2937126.

[32] L. Liu, D. Wang, and Y. Lei, "An image encryption scheme based on hyper chaotic system and DNA with fixed secret keys," *IEEE Access*, vol. 8, pp. 46400–46416, 2020, doi: 10.1109/ACCESS.2020.2978492.

[33] C. Zou, Q. Zhang, X. Wei, and C. Liu, "Image encryption based on improved Lorenz system," *IEEE Access*, vol. 8, pp. 75728–75740, 2020, doi: 10.1109/ACCESS.2020.2988880.

[34] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," *IEEE Access*, vol. 7, pp. 147106–147118, 2019, doi: 10.1109/ACCESS.2019.2946208.

[35] J. Sun, C. Li, T. Lu, A. Akgul, and F. Min, "A memristive chaotic system with hypermultistability and its application in image encryption," *IEEE Access*, vol. 8, pp. 139289–139298, 2020, doi: 10.1109/ACCESS.2020.3012455.

[36] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107484, doi: 10.1016/j.sigpro.2020.107484.

[37] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[38] S. Sun, Y. Guo, and R. Wu, "A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping," *IEEE Access*, vol. 7, pp. 28539–28547, 2019, doi: 10.1109/ACCESS.2019.2901870.

[39] J.-Z. Liu, Y.-D. Ma, S.-L. Li, J. Lian, and X.-G. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools Appl.*, vol. 77, no. 17, pp. 22787–22802, Sep. 2018, doi: 10.1007/s11042-017-5534-8.

[40] Z. Yong, "The unified image encryption algorithm based on chaos and cubic S-box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018, doi: 10.1016/j.ins.2018.03.055.
[41] C. Pak, K. An, and P. Jang, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019, doi: 10.1007/s11042-018-6739-1.
[42] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018, doi: 10.1016/j.sigpro.2018.03.010.
[43] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik*, vol. 181, pp. 779–785, Mar. 2019, doi: 10.1016/j.ijleo.2018.12.178.
[44] Y. Aydin and F. Ozkaynak, "A provable secure image encryption schema based on fractional order chaotic systems," in *Proc. 23rd Int. Conf. Electron.*, Palanga, Lithuania, Jun. 2019, pp. 1–5.
[45] W. Le-Le and L. Guo-Dong, "Double chaotic image encryption algorithm based on run-length," in *Proc. Int. Conf. Eng. Simulation Intell. Control (ESAIC)*, Changsha, China, Aug. 2018, pp. 35–38.
[46] J. Xu, P. Li, F. Yang, and H. Yan, "High intensity image encryption scheme based on quantum logistic chaotic map and complex hyper-chaotic system," *IEEE Access*, vol. 7, pp. 167904–167918, 2019, doi: 10.1109/ACCESS.2019.2952140.
[47] X. Sun, D. Liu, Y. Ji, S. Yan, C. Li, and B. Du, "A new image block encryption method based on chaotic map and DNA encoding," in *Proc. 7th Int. Conf. Digit. Home (ICDH)*, Guilin, China, Nov. 2018, pp. 37–41.
[48] H. Dong, E. Bai, X.-Q. Jiang, and Y. Wu, "Color image compression-encryption using fractional-order hyperchaotic system and DNA coding," *IEEE Access*, vol. 8, pp. 163524–163540, 2020, doi: 10.1109/ACCESS.2020.3022398.
[49] J. Liu, M. Zhang, X. Tong, and Z. Wang, "Image compression and encryption algorithm based on 2D compressive sensing and hyperchaotic system," *Multimedia Syst.*, vol. 28, no. 2, pp. 595–610, Apr. 2022, doi: 10.1007/s00530-021-00859-6.
[50] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, Jan. 2008, doi: 10.1016/j.physleta.2007.07.040.
[51] F. Pareschi, R. Rovatti, and G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 491–505, Apr. 2012, doi: 10.1109/TIFS.2012.2185227.
[52] M. Li, M. Xu, J. Luo, and H. Fan, "Cryptanalysis of an image encryption using 2D Hénon-Sine map and DNA approach," *IEEE Access*, vol. 7, pp. 63336–63345, 2019, doi: 10.1109/ACCESS.2019.2916402.
[53] S. Rohith, K. N. H. Bhat, and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of linear feedback shift register," in *Proc. Int. Conf. Adv. Electron. Comput. Commun.*, Rukmini Knowledge Park, India, Oct. 2014, pp. 1–6.
[54] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019, doi: 10.1007/s11045-018-0589-x.
[55] P. He, K. Sun, and C. Zhu, "A novel image encryption algorithm based on the delayed maps and permutation-confusion-diffusion architecture," *Secur. Commun. Netw.*, vol. 2021, pp. 1–16, Mar. 2021, doi: 10.1155/2021/6679288.
[56] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, and W. J. Buchanan, "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Pers. Commun.*, vol. 2021, pp. 1–28 May 2021, doi: 10.1007/s11277-021-08584-z.
[57] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Opt. Laser Technol.*, vol. 121, Jan. 2020, Art. no. 105777, doi: 10.1016/j.optlastec.2019.105777.

HAIPING CHEN received the B.E. degree in electronic information engineering from the Jiangxi Normal University of Science and Technology, in 2020. She is currently pursuing the M.E. degree in communication engineering with Donghua University, China. Her research interests include information security, chaotic systems, and image security.

ENJIAN BAI received the B.S. degree in mathematics from Qufu Normal University and the M.S. and Ph.D. degrees in cryptography from Xidian University. He is currently an Associate Professor with the College of Information Science and Technology, Donghua University, Shanghai, China. His mainly research interests include applied mathematics, cryptography, and fuzzy systems.

XUEQING JIANG (Senior Member, IEEE) received the B.S. degree in computer science from the Nanjing Institute of Technology, Nanjing, China, and the M.S. and Ph.D. degrees in electronics engineering from Chonbuk National University, Jeonju, South Korea. He is currently an Associate Professor with the School of Information Science and Technology, Donghua University, Shanghai, China. His main research interests include wireless communication and coding theory.

YUN WU received the B.S. and M.S. degrees in electrical engineering from the Harbin Institute of Technology, Harbin, China, in 1999 and 2001, respectively, and the Ph.D. degree from Shanghai Jiaotong University, Shanghai, China, in 2006. She is currently an Associate Professor with the School of Information Science and Technology, Donghua University. Her research interests include channel estimation and synchronization, cognitive radio technology, MIMO, and compressive sensing.