IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 25, 2020, accepted December 7, 2020, date of publication December 16, 2020,
date of current version December 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3045101

Image Encryption Algorithm Based on Block Scrambling and Finite State Machine

SHENGTAO GENG, TAO WU, SHIDA WANG, XUNCAI ZHANG, (Member, IEEE), AND YANFENG WANG

School of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

Corresponding author: Xuncai Zhang (zhangxuncai@pku.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62072417 and Grant U1804262, and in part by the Key Research and Development Program of Henan Province under Grant 202102210177 and Grant 192102210134.

ABSTRACT To better protect the image information, an image encryption algorithm based on block scrambling and finite state machine is proposed. The method uses discrete wavelet transform (DWT) to divide the original image into four frequency bands. Secondly, chaotic sequences and zigzag scanning curve are used to construct a scrambling matrix to scramble the four frequency bands. Then combine the chaotic sequence, DNA coding, and automata to transform the state of the scrambled image. Finally, the key stream is used to diffuse the sequence to improve the security of cipher images further. Experimental results and security analysis show that the proposed encryption scheme can resist various attacks and ensure the secure transmission of images.

INDEX TERMS Image encryption, Zigzag scanning curve, DNA coding, finite state machine, discrete wavelet transform.

I. INTRODUCTION

With the development of communication technology, information security has been paid more and more attention. As a carrier carrying a lot of information, it is very important to prevent digital images from being stolen in network transmission. Using image encryption technology can improve the security of digital images in network transmission to some extent. Although text encryption technology has sufficient security, for example, the methods represented by DES [1], AES [2], and SM4 algorithm [3] have been widely used. However, the digital image has a large amount of data, high redundancy, and strong correlation between adjacent pixels, so text encryption technology is not suitable for digital image encryption.

Chaotic systems are characterized by periodicity, ergodic, pseudo-randomness, and high sensitivity to initial conditions and parameters. Since Fridrich [4] proposed a scrambling-diffusion encryption architecture, chaotic systems have received more and more attention. The security of chaotic encryption algorithm is closely related to chaotic system. For example, Logistic map-based encryption algorithm, with simple structure and low computational complexity, has been widely used in early image encryption. Luo *et al.* [5] proposed an image encryption algorithm that uses two-dimensional discrete wavelet transform and chaotic system to carry out adaptive replacement of pixels. This method enhances encrypted images' security, but Logistic mapping's encryption structure is often relatively simple and has weak resistance to violent attacks and statistical analysis attacks [6]. Zhou *et al.* [7] proposed a new chaotic system combining two one-dimensional chaotic systems and then used the system to encrypt the image. Sam *et al.* [8] used Logistic mapping to design a lossless symmetric image encryption algorithm for pixel replacement diffusion structure. However, one-dimensional chaotic systems have the fundamental defects of small keyspace and low chaos. High-dimensional chaotic systems, especially hyperchaotic systems, have many variables and parameters, more complex dynamic characteristics, and larger key space [9], [10], [11]. Therefore, using hyperchaotic system to encrypt images is a better choice. Peng *et al.* [12] proposed a new image encryption algorithm based on a multi-dimensional multi-wing hyperchaos system with two Lyapunov exponents greater than zero. In 2015, Guan *et al.* [13] improved the classical Lorentz system and constructed a Lorentz chaotic system with a relatively large positive Lyapunov index and size by increasing control parameters and changing nonlinear terms.

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

Although the hyperchaotic system has a good effect on image encryption, it still has some shortcomings. Gao and Chen [14] proposed an image encryption algorithm based on hyperchaos using pixel-level permutation. The algorithm has the advantage of large key space, but it cannot resist the plaintext and ciphertext attack. Compressive sensing (CS) theory can be regarded as a symmetric cryptosystem. Some scholars combine this theory with chaotic system and propose image encryption algorithm based on CS theory [15], [16]. Chai *et al.* [17] proposed a color image compression and encryption scheme based on compressed sensing and double random encryption strategy. This algorithm improved its ability to resist KPA and CPA, but the algorithm complexity was high.

Image encryption algorithms based on chaos are generally divided into pixel scrambling and diffusion [18]. Image pixel scrambling mainly uses curves to scan pixels and rearrange them [19], [20], or rearrange pixels through chaotic sequences [21], [22]. The image scrambling method based on chaotic sequence is widely used, and the scrambling effect is better. By sorting the pseudo-random sequence generated by the chaotic system, the image pixels are scrambled by the sorting result. However, sorting of big data often takes a lot of time, and chaotic systems may have chaotic degradation. A single algorithm for encrypting images using chaotic sequences is not reliable, so chaotic systems and other methods are often used for encryption. Unlike the scrambling operation, the diffusion process is generally to perform bit XOR between the encrypted image and the generated chaotic sequence to change the image pixels. The latest trend in image encryption is the application of DNA theory [23]. Based on DNA encryption technology involves two main steps. First, the original image is converted into DNA coding sequence through DNA coding rules. Secondly, the DNA coding sequence created from the chaotic sequence and converted with the original image is used to perform base-pair operations. Zhang and Luo [24] proposed a typical DNA encryption method. First, the hyperchaotic system is used to scramble the image pixels, then the scrambled pixels are DNA-encoded and the base-pair exclusive XOR is performed, and finally, the DNA is decoded to convert it into an image. Wu *et al.* [25] applied it to color image encryption, and diffusion between image pixels is carried out by combining DNA addition, subtraction, and XOR operations. However, these algorithms have some security risks. If an attacker encrypts an image with all pixel values of zeros, it is likely to crack the generated chaotic sequence and thus lead to information leakage.

To solve the above problems, this paper proposes a hyperchaotic image encryption algorithm based on block scrambling and finite automata machine. First, discrete wavelet transform (DWT) is used to divide the original image into four frequency bands: low-frequency part (LL1), horizontal detail (HL1), vertical detail (LH1), and diagonal detail (HH1). Secondly, construct a pixel position scrambling matrix through the zigzag curve and chaotic sequence to scramble the elements of four frequency bands respectively. Four frequency bands after scrambling are subjected to discrete wavelet inverse transform (IDWT), generate the scrambled image, and use the zigzag curve to scramble the image again. Third, DNA encoding rules are used to encode the scrambled image, and the key stream generated by the deterministic state automata (DFA) and hyperchaotic system is used to transform the DNA encoding sequence. Finally, the key stream generated by the chaotic sequence is used to diffuse the image pixels to enhance the security of cipher image. The algorithm complies with the one-time password system and can effectively resist choice known attacks.

We organize the rest of this paper as follows. Section 2 introduces the principle of the method used, Section 3 presents the encryption process of the algorithm in detail, Section 4 conducts an experimental analysis on the algorithm proposed in this paper to prove its security. The conclusion is given in Section 5.

II. BASIC THEORY

A. NEW FOUR-WING 4D CHAOTIC SYSTEM

Yu *et al.* [26] modified the three-dimensional (3D) smooth quadrat-ic autonomous chaotic system proposed by Liu *et al.* [27], and add-ed a linear term to the system to obtain a new 4D smooth quadratic autonomous chaotic system. As shown in equation (1):

$$\begin{cases} \dot{x} = -ax + yz + bu \\ \dot{y} = -xz + cy \\ \dot{z} = \text{xy-dz} \\ \dot{u} = xy - eu, \end{cases} \tag{1}$$

where *a, b, c, d* and *e* are system parameters. x, y and z are state variables and u are nonlinear state feedback controllers. As shown in Figure 1, set the control parameters $a = 10$, $b = 2$, $c = 12$, $d = 50$ and $e = 5$. The phase diagram of the chaotic system is shown in Fig. 1. It can be seen from Fig. 1 that the chaotic attractor of the system can show the four-wing type, whether in the 3D space or the 2D plane, so it is a real four-wing attractor. The chaos system has a large positive Lyapunov index, it can show complex and rich chaotic dynamics behavior.

B. DISCRETE WAVELET TRANSFORM

DWT is a kind of orthogonal wave with very concentrated energy in the time domain. It can display spatial and frequency views simultaneously, so it has the capability of multi-scale analysis. Suppose an image $f(x, y)$ with a size of $M \times N$, its 2D-DWT is defined as:

$$W_{\Phi}(j_0, m, n) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)\, \Phi_{j_0,m,n}(x, y) \tag{2}$$

$$W_{\Psi}^{i}(j, m, n) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)\, \Psi_{j,m,n}^{i}(x, y) \tag{3}$$

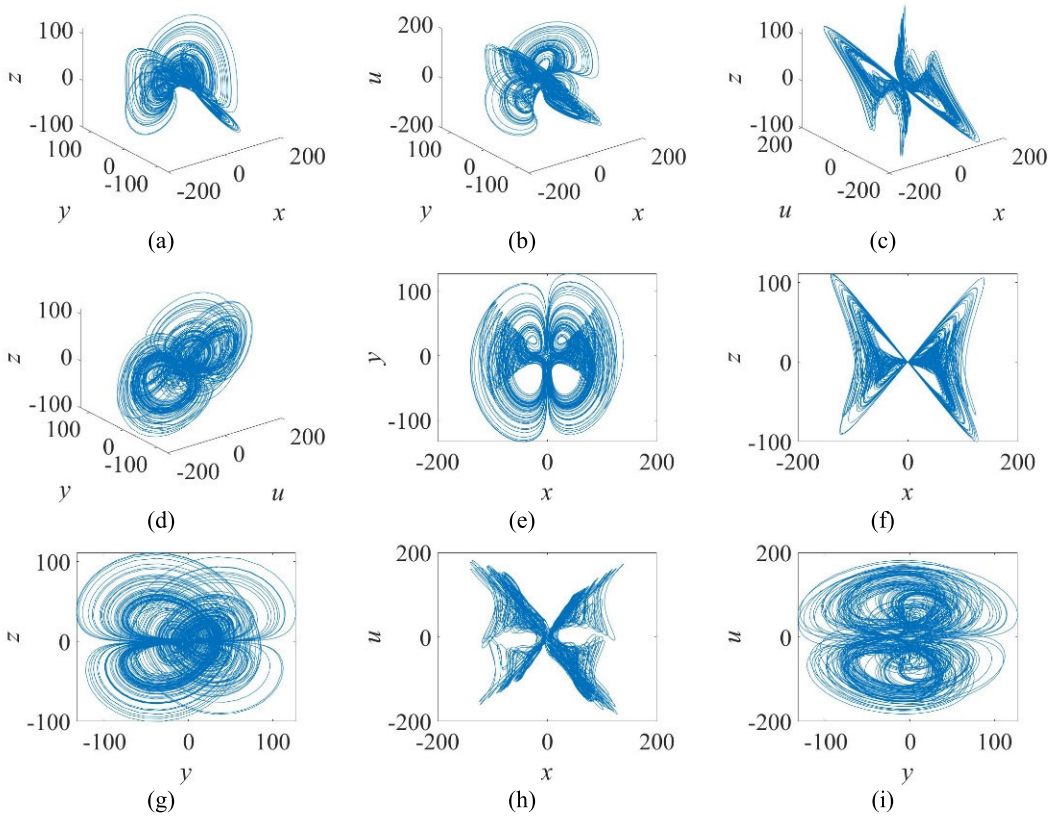


FIGURE 1. The new four-wing 4D chaotic system phase portraits. (a) *x-y-z* space, (b) *x-y-u* space, (c) *x-u-z* space, (d) *u-y-z* space, (e) *x-y* space, (f) *x-z* space, (g) *y-z* space, (h) *x-u* space,(I) *y-u* space.

where $W_\Phi(j_0, m, n)$ represents the approximate part of the image, and $W^i_\Psi(j, m, n)$ represents the horizontal, vertical and diagonal parts of the image. $\Phi_{j_0,m,n}(x, y)$ represents the scaling function, $\Psi^i_{j,m,n}(x, y)$ represents the wavelet function. The 2D-IDWT is defined as:

$$\begin{aligned} & f(x, y) \\ &= \frac{1}{M \times N} \sum_m \sum_n W_\Phi(j_0, m, n)\, \Phi_{j_0,m,n}(x, y) \\ &\quad + \frac{1}{M \times N} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_m \sum_n W_\Phi(j_0, m, n) \Psi^i_{j,m,n}(x, y) \end{aligned} \tag{4}$$

C. DNA CODING

As an important genetic information storage carrier in organisms, DNA has massive parallelism and information density characteristics [28]. Through performing DNA encoding processing on the pixels of the image, the complexity of the encryption algorithm can be enhanced. DNA sequence has four types of nucleic acid bases, namely adenine (A), thymine (T), cytosine (C) and guanine (G). According to the base pair complementation rule, A and T are complementary, G and C are complementary. This complementary rule is similar to binary numbers. For example, 0 and 1 are complementary, so 00 and 11, 01 and 10 are also complementary. Encoding the four bases A, T, C, G to binary 00, 01, 10, 11, there are 24 encoding combinations, but only eight kinds of rules satisfy the Watson-Crick complement rule [29], such as Table 1 shows.

TABLE 1. 8 kinds of DNA map rules.

Rules	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
C	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
T	10	01	11	00	11	00	10	01

According to DNA coding rules, the pixels of the image are coded. For example, if the original image's pixel value is 147, the converted binary sequence is [10010011]. Use DNA coding rule 1 to encode to obtain DNA sequence [TGAC]. The DNA decoding rule is the inverse operation of the DNA encoding rule, and the pixel value can be restored through the corresponding DNA decoding rule. If the DNA sequence is [TGAC], the binary sequence decoded according to DNA coding rule 1 is [01111101], and the decimal value is 147. If decoding is performed according to DNA coding rule 3, the decoded decimal is 198.

III. ENCRYPTION SCHEME

A. GENERATE KEYS AND CHAOTIC SEQUENCES

Input the image into the SHA-384 algorithm to generate a 384-bit long hash value, it is divided into 48 sequences with a length of 8 bit, and obtain k_1, k_2, k_3, …, k_{48}. The initial iterative parameters of the new four-wing 4D chaotic system x_0, y_0, z_0 and u_0 are calculated from equations (5) and (6):

Input the generated initial iteration parameters x_0, y_0, z_0 and u_0 into four-wing 4D chaotic system iteration $999 + 4 \times M \times N$ times, remove the first 999 times, generate chaotic sequences $\boldsymbol{XY}$, $\boldsymbol{D}$, $\boldsymbol{U}$ and $\boldsymbol{W}$ are used in the encryption scheme proposed in this paper.

$$\begin{cases} Q_1 = k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_8 \\ Q_2 = k_9 \oplus k_{10} \oplus k_{11} \oplus k_{12} \oplus k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{16} \\ Q_3 = k_{17} \oplus k_{18} \oplus k_{19} \oplus k_{20} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{24} \\ Q_4 = k_{25} \oplus k_{26} \oplus k_{27} \oplus k_{28} \oplus k_{29} \oplus k_{30} \oplus k_{31} \oplus k_{32} \\ Q_5 = k_{33} \oplus k_{34} \oplus k_{35} \oplus k_{36} \oplus k_{37} \oplus k_{38} \oplus k_{39} \oplus k_{40} \\ Q_6 = k_{41} \oplus k_{42} \oplus k_{43} \oplus k_{44} \oplus k_{45} \oplus k_{46} \oplus k_{47} \oplus k_{48} \end{cases} \tag{5}$$

$$\begin{cases} x_0 = \dfrac{1}{256} mod\ (Q_1 + Q_2 + Q_3, 256) \\ y_0 = \dfrac{1}{256} mod\ (Q_2 + Q_3 + Q_4, 256) \\ z_0 = \dfrac{1}{256} mod\ (Q_3 + Q_4 + Q_5, 256) \\ u_0 = \dfrac{1}{256} mod\ (Q_4 + Q_5 + Q_6, 256) \end{cases} \tag{6}$$

B. SCRAMBLING SCHEME

By scrambling image pixels, the correlation between adjacent pixels can be broken, and differential attacks can be effectively resisted. The Space Filling Curve (SFC) is a continuous scanning method that can scan each pixel accurately and effectively scramble the image pixels. However, it requires multiple repeated scans to achieve a better scrambling effect. Using the index value generated by the pseudo-random sequence to scramble the image pixels is better, but it takes a long time to sort big data. This paper combines the SFC scrambling method and the chaotic sequence scrambling method to design a block scrambling scheme.

Assuming that the size of the original image matrix $\boldsymbol{P}$ is $M \times N$, First, use DWT to divide the original image into four frequency bands, LL1, HL1, LH1 and HH1. From the generated chaotic sequence $\boldsymbol{XY}$, let $\boldsymbol{X} = \boldsymbol{XY}(1{:}\ M/2)$, $\boldsymbol{Y} = \boldsymbol{XY}(M/2 + 1{:}\ M/2 + N/2)$, obtain a chaotic sequence $\boldsymbol{X}$ of length $M/2$ and a chaotic sequence $\boldsymbol{Y}$ of length $N/2$ respectively. Then arrange them in descending order to obtain their position index vector $\boldsymbol{IX}$ and vector $\boldsymbol{IY}$, $\boldsymbol{IX}$ and $\boldsymbol{IY}$ are respectively used as row coordinate index and column coordinate index, and the corresponding positions of row coordinate and column coordinate are combined to generate a scrambling matrix $\boldsymbol{S}$. The scrambling matrix $\boldsymbol{S}$ is shown in Fig. 2(a). Through the zigzag curve to scan the matrix $\boldsymbol{S}$ to get the scrambling matrix $\boldsymbol{W}$. Finally, use the scrambling matrix $\boldsymbol{W}$ to scramble the four frequency bands of LL1, HL1, LH1 and HH1, respectively. Perform IDWT transformation on the four frequency bands after scrambling, and use zigzag scanning curve to scrambling the image after inverse transformation to obtain the scrambling image matrix $\boldsymbol{P'}$. The scrambling process is shown in Fig. 2.

C. STATE TRANSITION

Finite state machines can be divided into deterministic finite automata (DFA) and uncertain finite automata (NFA). Given the current state and input characters, DFA can determine the transition to a certain state, and NFA can transition to multiple states simultaneously. To ensure the algorithm's reversibility, the encryption scheme proposed in this paper uses DFA for state transition. The DFA is defined as:

$$M = (Q, \Omega, f, s, Z) \tag{7}$$

where M represents DFA, Q is a finite state set. Ω is a set of input characters, f is a state transition function, $s \subseteq Q$ is the only initial state, $Z \subseteq Q$ is a final state set.

The state transition of the image can effectively hide the original information of the image. In the state transition scheme proposed in this paper, the pixel value of the input image is encoded by DNA rules (in this paper, use rule 1 is for coding), and the DNA coding sequence SQ is obtained as input for state transition. Define $Q = \{A, C, G, T\}$, $\Omega = \{0, 1, 2, 3\}$, $s = A$, $Z = \{A, C, G, T\}$, f is defined by state transition table 2.

TABLE 2. State transition table.

Rules	0	1	2	3
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

For example, $f(A, 0) = A, f(A, 1) = C, f(A, 2) = G$. Use formula (8) to process the generated chaotic sequence $\boldsymbol{D}$ to obtain sequence $\boldsymbol{D'}$, and make the value range between 0 and 3 as input characters:

$$\boldsymbol{D}'(j) = floor(mod(\boldsymbol{D}(j) * \mathbf{2}^{32}, 4)) \tag{8}$$

where $j = 1, 2, 3, \ldots, 4 \times M \times N$. The corresponding elements in the DNA coding sequence $\boldsymbol{SQ}$ and the sequence $\boldsymbol{D'}$ sequentially input into the state transition machine for state transition, and the state transition sequence $\boldsymbol{SQ'}$ is obtained. That is, $f(\boldsymbol{SQ}(i), \boldsymbol{D}'(i)) = \boldsymbol{SQ}'(i)$, where $i = 1, 2, 3, \ldots, 4 \times M \times N$. The sequence $\boldsymbol{SQ'}$ is DNA-decoded according to rule 1, converted to decimal, and a state transition sequence $\boldsymbol{E}$ is generated, where $j = 1, 2, 3, \ldots, 4 \times M \times N$.

D. DIFFUSION SCHEME

Diffusing the encrypted image pixels can effectively make the original image pixels produce different cipher images when minor changes occur. The first $M \times N$ elements of

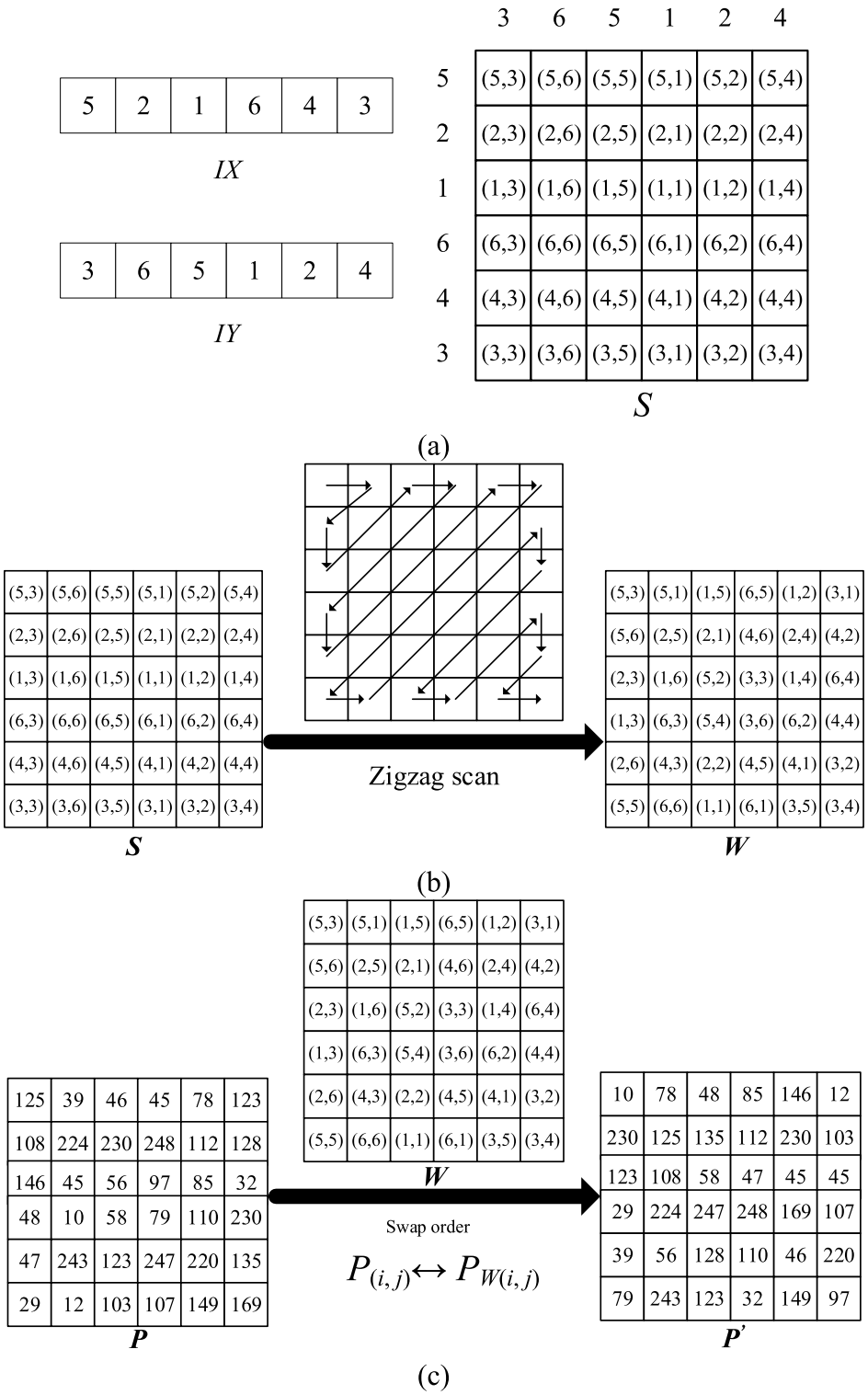


FIGURE 2. Scrambling scheme. (a). Generate scrambling matrix ***S***, (b). Zigzag curve scan scrambling matrix ***S*** to generate scrambling matrix ***W***, (c) Scrambling process.

the generated chaotic sequence $\boldsymbol{U}$ and chaotic sequence $\boldsymbol{V}$ are respectively intercepted, and the chaotic sequence $\boldsymbol{U_1}$ and the chaotic sequence $\boldsymbol{V_1}$ are processed according to equations (9) and (10) to obtain the sequence $\boldsymbol{U'}$ and the sequence $\boldsymbol{V'}$:

$$\boldsymbol{U}'(j) = floor(mod(\boldsymbol{U_1}(j) \times 2^{32}, 256)) \quad (9)$$

$$\boldsymbol{V}'(j) = floor(mod(\boldsymbol{V_1}(j) \times 2^{32}, 256)) \quad (10)$$

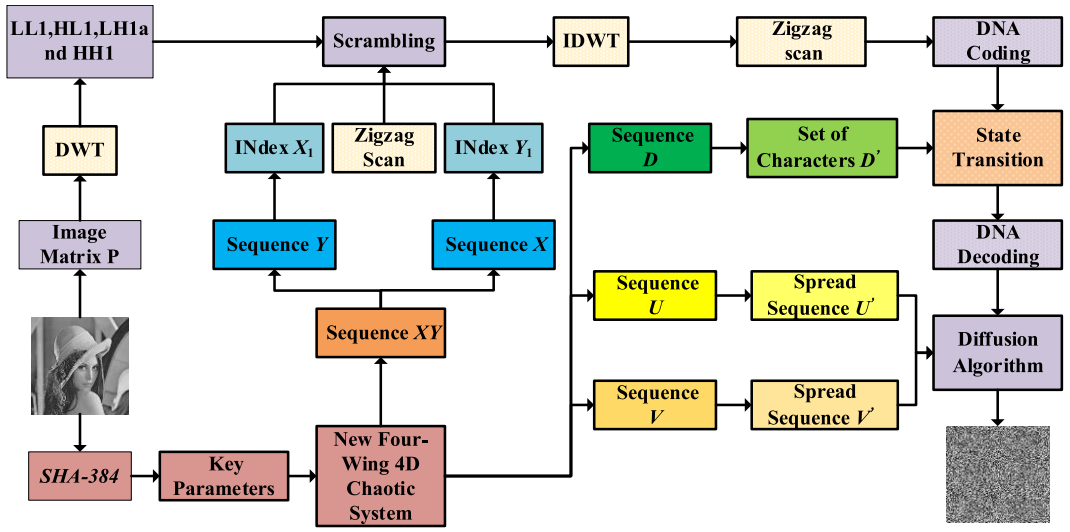


FIGURE 3. Flowchart of the encryption algorithm.

where $j = 1, 2, 3, \ldots, M \times N$, the encrypted image is transformed into a one-dimensional sequence $\boldsymbol{E}$, the diffusion algorithm is shown in formula (11), as shown at the bottom of the page.

E. ENCRYPTION PROCESS

The complete encryption algorithm includes four parts: key generation, block scrambling, state transition and diffusion plan. Steps are as follows:

Step 1: Input the original image matrix $\boldsymbol{P}$ of size $M \times N$, and use the key generation system to generate initial parameters x_0, y_0, z_0 and u_0. Input the generated initial iteration parameters x_0, y_0, z_0 and u_0 into the iterative four-wing 4D chaotic system iteration $999 + 4 \times M \times N$ times, remove the first 999 times, and generate four chaotic sequences, denoted as sequence $\boldsymbol{XY}$, sequence $\boldsymbol{D}$, sequence $\boldsymbol{U}$ and sequence $\boldsymbol{W}$ respectively.

Step 2: Intercept the chaotic sequence $\boldsymbol{XY}$ to obtain a chaotic sequence $\boldsymbol{X}$ with a length of $M/2$ and a chaotic sequence $\boldsymbol{Y}$ with a length of $N/2$ and two chaotic sequences are arranged in descending order, respectively. The position index value of the chaotic sequence $\boldsymbol{X}$ as the row scrambling vector $\boldsymbol{IX}$ and the position index value of the chaotic sequence $\boldsymbol{Y}$ as the column scrambling vector $\boldsymbol{IY}$ to generate a scrambling matrix $\boldsymbol{S}$. Use the zigzag scan curve to scramble the scrambling matrix $\boldsymbol{S}$ again to obtain the scrambling matrix $\boldsymbol{W}$. The image matrix P is scrambled according to the scheme in section 3.2 to get the pixel value scrambled matrix $\boldsymbol{P'}$.

Step 3: Perform DNA coding on the pixel scrambling matrix $\boldsymbol{P'}$ to obtain the DNA coding sequence $\boldsymbol{SQ}$, and use formula (8) to process the chaotic sequence $\boldsymbol{D}$ to get the sequence $\boldsymbol{D'}$. The corresponding elements in the sequence $\boldsymbol{SQ}$ and the sequence $\boldsymbol{D'}$ sequentially input into the automaton for state transition, and the state transition sequence $\boldsymbol{SQ'}$ is obtained. Perform DNA decoding on the sequence $\boldsymbol{SQ'}$ and convert it to decimal to get the state transition sequence E;

Step 4: Let $\boldsymbol{U} = \boldsymbol{U}(1{:}\ M \times N)$, $\boldsymbol{V} = \boldsymbol{V}(1{:}\ M \times N)$, use formula (9) and formula (10) to obtain the sequence $\boldsymbol{U'}$ and the sequence $\boldsymbol{V'}$. Proceed according to formula (11) diffusion and transform it into a ciphertext matrix of $M \times N$ size to generate an encrypted image $\boldsymbol{P_1}$.

The flowchart of the encryption algorithm is shown in Fig. 3.

IV. SAFETY ANALYSIS

This paper uses Matlab 2019a to simulate the encryption algorithm. The computer configuration environment is Windows 10, 8.00 GB RAM, Intel(R) Core(TM) i7-4510 CPU @ 2.00GHz. Fig. 4 shows the original image, cipher image and decrypted image of Lena, Boat, Hill, Peppers. By directly observing the cipher image, no valid information can be identified. To verify the performance of the algorithm, the encryption scheme is analyzed experimentally in this section.

A. KEY SPACE

According to research, even in powerful computer capabilities, if the key space is greater than 2^{100}, the encryption scheme cannot be cracked by brute force attacks. Therefore, the key space of the encryption scheme should be large enough to resist brute force attacks. In the encryption scheme proposed in this article, SHA-384 generates the initial parameters of the encryption algorithm x_0, y_0, z_0 and u_0. The key

$$\begin{cases} E'(k) = mod(E(k) + E(M \times N) + U'(k), 256) \oplus V'(k) & k = 1 \\ E'(k) = mod(E(k) + E'(k-1) + U'(k), 256) \oplus V'(k) & k = 2, 3, \ldots, M \times N \end{cases} \tag{11}$$

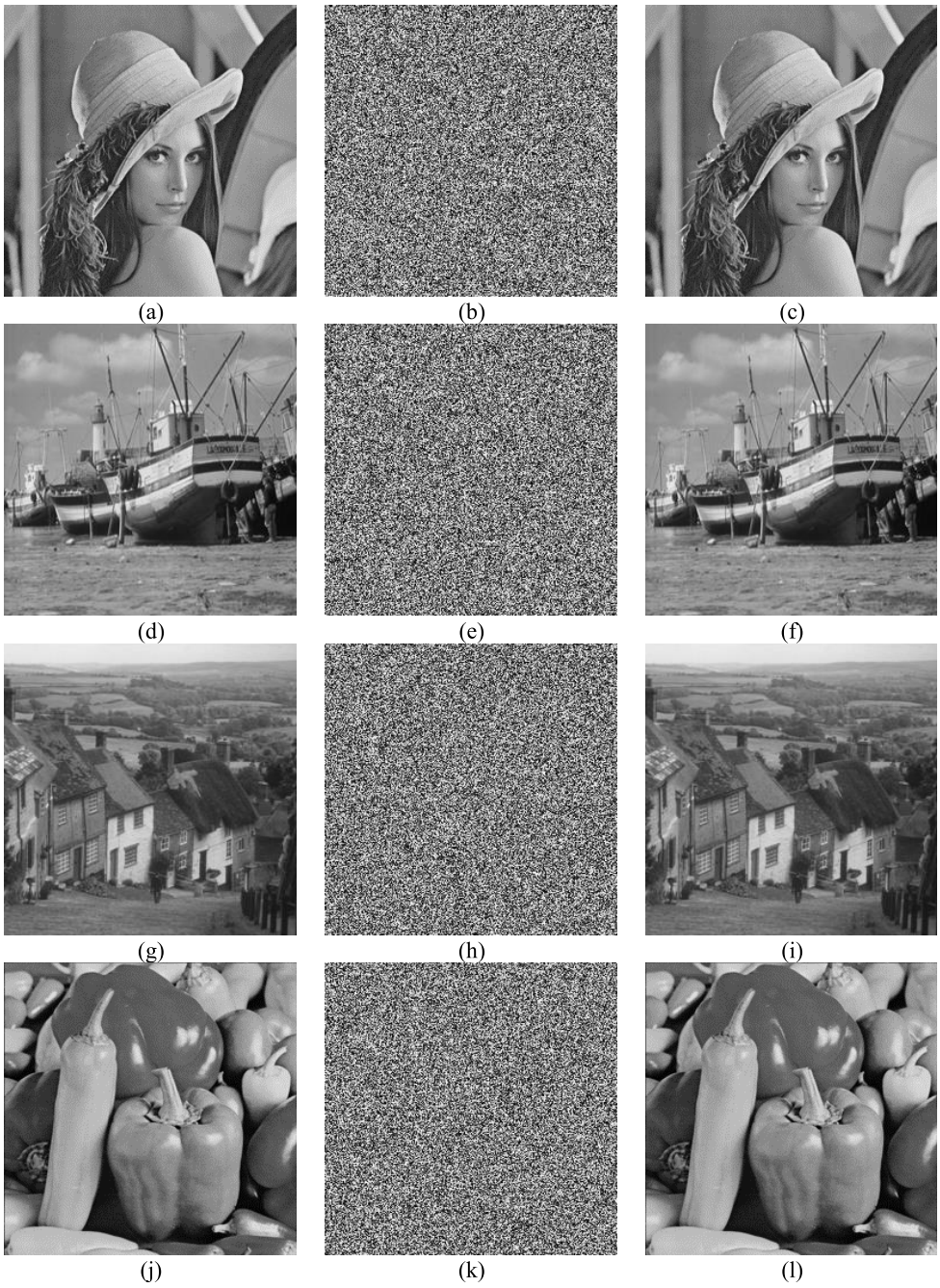


FIGURE 4. The original images, cipher images and decrypted images. (a) The original Lena image. (b) The encrypted Lena image. (c) The decrypted Lena image. (d) The original Boat image. (e) The encrypted Boat image. (f) The decrypted Boat image. (g) The original Hill image. (h) The encrypted Hill image. (i) The decrypted Hill image. (j) The original Peppers image. (k) The encrypted Peppers image. (l) The decrypted Peppers image.

space of SHA-384 is 2^{192}, and the calculation precision of x_0, y_0, z_0 and u_0 is 10^{15}, so the total key space is about 10^{117}. Therefore, the key space of the encryption scheme proposed in this paper is large enough to resist brute force attacks effectively.

B. DIFFERENTIAL ATTACK ANALYSIS

A good encryption algorithm can be highly sensitive to subtle changes in the original image to resist differential attacks. NPCR and UACI are generally used to measure the resistance to differential attacks. The calculation method is as follows:

$$\begin{cases} NPCR = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} D_{(i,j)}}{M \times N} \times 100\% \\ UACI = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} |P_1(i,j) - P_2(i,j)|}{255 \times M \times N} \times 100\% \end{cases} \tag{12}$$

Among them, $\boldsymbol{P_1}$ is generated by encrypting the selected original image through the encryption scheme proposed in

TABLE 3. NPCR test scores and comparison.

Image name	Size	Liu's [30]	Hua's [31]	Wang's[32]	Tang's [33]	Our method
5.1.09	256×256	99.5773%	99.6064%	99.6185%	99.5956%	99.5972%
5.1.10	256×256	99.6353%	99.6154%	99.5803%	99.6459%	99.6078%
5.1.11	256×256	99.6277%	99.6244%	99.6215%	99.5803%	99.6146%
5.1.12	256×256	99.5351%	99.5703%	99.6231%	99.6154%	99.6123%
5.1.13	256×256	99.6170%	99.6109%	99.5971%	99.4400%	99.6323%
5.1.14	256×256	99.6109%	99.6364%	99.6353%	99.5803%	99.6140%
5.2.08	512×512	99.6212%	99.5870%	99.6242%	99.5937%	99.5937%
5.2.09	512×512	99.6147%	99.6260%	99.6044%	99.5975%	99.5975%
5.2.10	512×512	99.6151%	99.6124%	99.6086%	99.6051%	99.6071%
7.1.01	512×512	99.6105%	99.5992%	99.6166%	99.5784%	99.6123%
7.1.02	512×512	99.6124%	99.6075%	99.6097%	99.5544%	99.6284%
7.1.03	512×512	99.6216%	99.6079%	99.5983%	99.5754%	99.6233%
7.1.04	512×512	99.6124%	99.5988%	99.6089%	99.6009%	99.5918%
7.1.05	512×512	99.6342%	99.6170%	99.6025%	99.5956%	99.6254%
7.1.06	512×512	99.6078%	99.6272%	99.6086%	99.5925%	99.6323%
7.1.07	512×512	99.6307%	99.5931%	99.5780%	99.5937%	99.6075%
7.1.08	512×512	99.6014%	99.6094%	99.5891%	99.9369%	99.5924%
7.1.09	512×512	99.6010%	99.6162%	99.5941%	99.5601%	99.5997%
7.1.10	512×512	99.5960%	99.6045%	99.5948%	99.6173%	99.6170%

TABLE 4. UACI test scores and comparison.

Image name	Size	Liu's [30]	Hua's [31]	Wang's [32]	Tang's [33]	Our method
5.1.09	256×256	33.3368%	33.4197%	33.3785%	32.0157%	33.4197%
5.1.10	256×256	33.4478%	33.3640%	33.6559%	32.4913%	33.3461%
5.1.11	256×256	33.5105%	33.5293%	33.2149%	32.9639%	33.4096%
5.1.12	256×256	33.4483%	33.3835%	33.3513%	33.4799%	33.4529%
5.1.13	256×256	33.5006%	33.4355%	33.4222%	33.5458%	33.4529%
5.1.14	256×256	33.4946%	33.4754%	33.5030%	32.6501%	33.4542%
5.2.08	512×512	33.4636%	33.4872%	33.4537%	32.4536%	33.4049%
5.2.09	512×512	33.4771%	33.4367%	33.4846%	32.9213%	33.4300%
5.2.10	512×512	33.4771%	33.4868%	33.4307%	33.0080%	33.4206%
7.1.01	512×512	33.5637%	33.4727%	33.5603%	31.9474%	33.4126%
7.1.02	512×512	33.5150%	33.5432%	33.4345%	31.9622%	33.4804%
7.1.03	512×512	33.4519%	33.4693%	33.3733%	31.9399%	33.4954%
7.1.04	512×512	33.4687%	33.4592%	33.5170%	32.2346%	33.4414%
7.1.05	512×512	33.5009%	33.4538%	33.4265%	32.3752%	33.5104%
7.1.06	512×512	33.3860%	33.5144%	33.4610%	32.3346%	33.4361%
7.1.07	512×512	33.4519%	33.5327%	33.5384%	31.9997%	33.4601%
7.1.08	512×512	33.4635%	33.4605%	33.4659%	31.9369%	33.4618%
7.1.09	512×512	33.4398%	33.4479%	33.4501%	32.3606%	33.4267%
7.1.10	512×512	33.4680%	33.4447%	33.4550%	32.1019%	33.4423%

this paper, and P_2 is the cipher image generated by encrypting the selected original image by changing a pixel value and then using the same encryption scheme again. If $\boldsymbol{P_1}(i,j) = \boldsymbol{P_2}(i,j)$, $\mathbf{D}(i,j) = 1$, otherwise $\mathbf{D}(i,j) = 0$. Calculate the values of UACI and NPCR using the images provided In the USC-SIPI image database and the encryption scheme proposed in this paper, and compare them with the literature [30], [31], [32], [33]. The results are shown in Table 3 and Table 4. The theoretical values of NPCR and UACI are close to 99.6093% and 33.4635%. We set the significance level

TABLE 5. Shannon entropy of original image and cipher image.

Shannon entropy	Lena	Boat	Hill	Peppers
Original image	7.4532	7.1572	7.4460	7.5797
Cipher image	7.9976	7.9975	7.9972	7.9973

$\alpha = 0.05$, when the NPCR $>$NPCR$^*_\alpha$, stands for NPCR pass the test. When the value of UACI is in the interval [UACI$^{*-}_\alpha$, UACI$^{*+}_\alpha$], it means UACI passes the randomness test. If the input image size is 256×256, $NPCR^*_\alpha = 99.5693\%$ and [UACI$^{*-}_\alpha$, UACI$^{*+}_\alpha$] = [33.2824%, 33.6447%], if the input image size is 526×526, $NPCR^*_\alpha = 99.5893\%$ and [UACI$^{*-}_\alpha$, UACI$^{*+}_\alpha$] = [33.3730%, 33.5541%], if the input image size is 1024×1024, $NPCR^*_\alpha = 99.5994\%$ and [UACI$^{*-}_\alpha$, UACI$^{*+}_\alpha$] = [33.4183%, 33.5088%]. It can be seen from table 3 and table 4 that the encryption scheme proposed in this paper is more resistant to differential attacks.

C. SHANNON ENTROPY AND LOCAL SHANNON ENTROPY

Shannon entropy entropy represents the randomness in the image and the average amount of information carried in the image. Let $\boldsymbol{P}$ be an encrypted image, then the entropy value calculation method of image $\boldsymbol{P}$ is as shown in formula (13):

$$H(m) = -\sum_{i=0}^{256} P(m_i) log_2 \boldsymbol{P}(m_i) \tag{13}$$

where m_i represents the ith message source and $\boldsymbol{P}(m_i)$ is the probability of m_i, the ideal entropy for an 8-bit grayscale image is 8. If the cipher image's entropy value is much lower than 8, the original image has the possibility of predictability, and the security of the image encryption algorithm is not high. Table 5 shows the Shannon entropy obtained by encrypting the image using the encryption scheme proposed in this paper.

However, there are some shortcomings in calculating the information entropy of the cipher image. For example, the uneven distribution of pixel values may appear in the part of the cipher image. Therefore, calculating the local Shannon entropy (LSE) of cipher image is more effective and more accurate than the global Shannon entropy measure [34]. The calculation method of LSE is: randomly select non-overlapping image blocks $S_1, S_2, \ldots, S_k$ with T_B pixels in the test image $\boldsymbol{P}$. the LSE can be defined as:

$$\overline{H_{k,T_B}}(\mathbf{P}) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{14}$$

Obtain the information entropy of each image block according to formula (14), and calculating the average value of the information entropy of these k image blocks is the local information entropy of the image. k represents the number of selected image blocks, and T_B is the number of pixels in the selected image block. Set the parameters (k, T_B) to (30, 1936), and the significance $\alpha = 0.05$, then the ideal local information entropy is 7.902469317. If the obtained

TABLE 6. Comparison of LSE scores of encrypted images obtained by different encryption schemes.

Image name	Size	Hua's [31]	Wang's [32]	Our method
5.1.09	256×256	**7.902281**	**7.902682**	7.892487
5.1.10	256×256	**7.902198**	7.903397	**7.903005**
5.1.11	256×256	7.899982	7.904131	7.899556
5.1.12	256×256	**7.902827**	**7.902789**	**7.902242**
5.1.13	256×256	**7.902281**	7.903841	**7.902367**
5.1.14	256×256	7.903117	**7.901668**	**7.901856**
5.2.08	512×512	**7.902304**	7.903854	7.903167
5.2.09	512×512	**7.902022**	7.905012	**7.902994**
5.2.10	512×512	7.906701	**7.902882**	**7.902304**
7.1.01	512×512	**7.902191**	**7.902966**	**7.902683**
7.1.02	512×512	**7.902047**	7.906349	**7.902050**
7.1.03	512×512	**7.902584**	7.900470	**7.902305**
7.1.04	512×512	**7.901913**	7.900964	**7.903028**
7.1.05	512×512	**7.902392**	**7.901991**	**7.901995**
7.1.06	512×512	**7.902565**	**7.902182**	**7.902890**
7.1.07	512×512	7.904015	7.900828	7.901541
7.1.08	512×512	7.901096	7.901676	**7.902741**
7.1.09	512×512	**7.902933**	7.901032	**7.902240**
7.1.10	512×512	**7.902534**	**7.903549**	**7.902959**
Pass/all	---	14/19	8/19	15/19

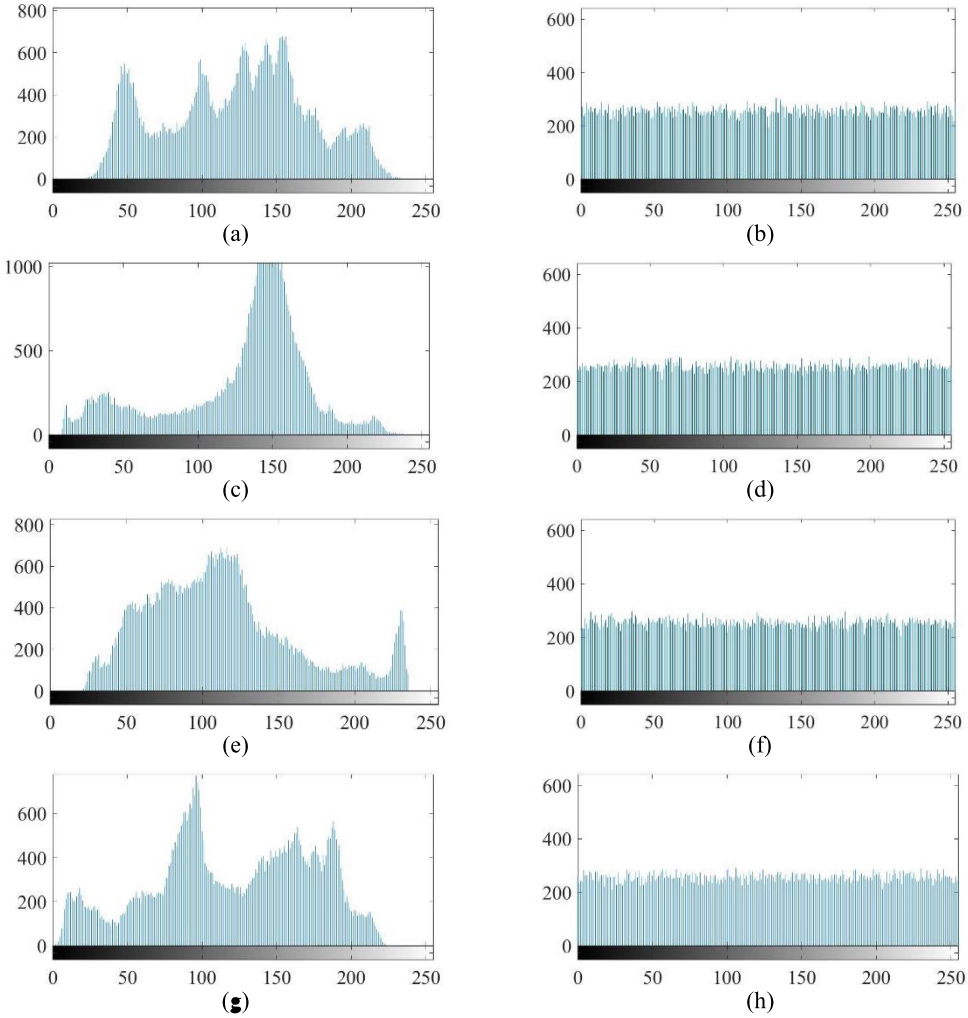


FIGURE 5. The histograms of original images and corresponding ciphered images: (a) Histogram of original Lena image. (b) Histogram of ciphered Lena image. (c) Histogram of original Boat image. (d) Histogram of ciphered Boat image. (e) Histogram of original Hill image. (f) Histogram of ciphered Hill image. (g) Histogram of original Peppers image. (h) Histogram of ciphered Peppers image.

TABLE 7. Chi-square test of histogram.

Images	Lena	Boat	Hill	Peppers
Original image	3.951×10^4	1.0085×10^5	4.3854×10^4	3.1630×10^4
Cipher image	220.8047	231.0703	260.5234	264.8828

local information entropy is in the interval (7.901901305, 7.903037329), the image is considered to pass the test. Use the encryption algorithm proposed in this paper and the encryption algorithm proposed in [31] and [32] to encrypt the image provided in the USC-SIPI image database and calculate its local information entropy. As shown in Table 6, it can be seen that the encryption algorithm proposed in this paper has a better encryption effect.

D. HISTOGRAM ANALYSIS

Through the histogram of the image, it can be seen intuitively whether the pixel distribution is uniform. Fig. 5 shows the histograms of original images and cipher images. It can be seen that the pixel value of the password image is evenly distributed in the interval [0,255], which is completely different from the pixel value of the original image. The Chi-square test is used to measure the uniformity of the histogram [35], [36]. It is defined as:

$$X^2 = \sum_{i=0}^{255} \frac{(f_i - g_i)^2}{g_i} \tag{15}$$

where f_i represents the actual pixel frequency of the gray level and g_i represent the expected frequency of each gray level. The commonly used significance level is $\alpha = 0.05$,

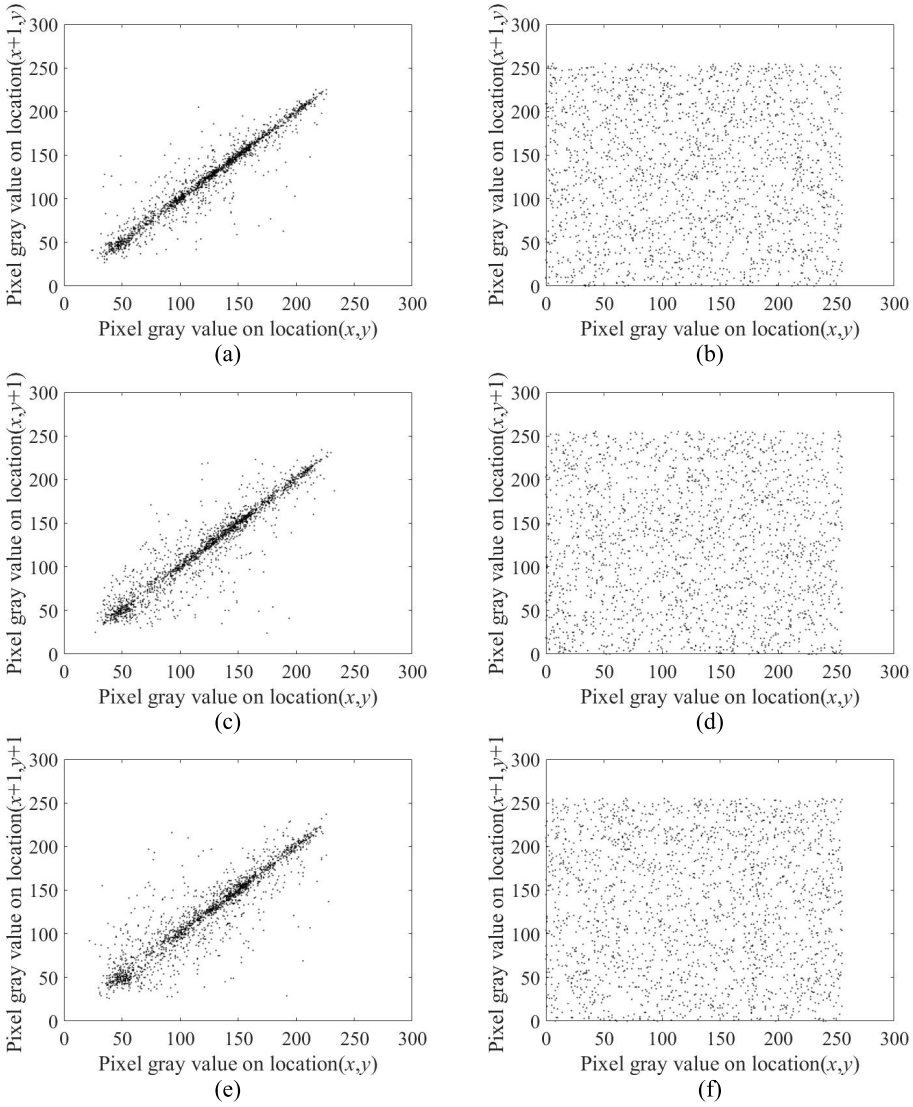


FIGURE 6. Distribution of adjacent pixels in the original Lena image and corresponding ciphered image: (a), (c), (e) are horizontal, vertical and diagonal direction of original image, and (b), (d), (f) are horizontal, vertical and diagonal direction of corresponding ciphered image.

$X^2_{0.05} = 293.24783$, that is, when X^2_{test} is lower than this value, it can be considered that the histogram is approximately uniform. The Chi-square test of histogram are shown in Table 7. It can be seen that the algorithm encrypts the original image and can obtains a cipher image with evenly distributed pixels.

E. CORRELATION ANALYSIS

The adjacent pixels of the original image have a high correlation in the horizontal, vertical, and diagonal directions, which is undesirable for encrypted images. An ideal encryption algorithm can reduce the correlation of adjacent pixels and effectively resist statistical attacks. The Pearson Product Moment Correlation Coefficient (PMCC) is used to measure the correlation between adjacent pixels of the original image and the encrypted image. It is defined as:

$$\begin{cases} E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\ cov(x, y) = \dfrac{1}{N}\sum_{i=1}^{N} ((x_i - E(x))(y_i - E(y))) \\ \rho_{xy} = \dfrac{cov(x, y)}{\sqrt{D_x} \times \sqrt{D_y}} \end{cases} \tag{16}$$

Among them, the $E(x)$ and $D(x)$ to represent the expectation and variance of the variable x respectively, $cov(x, y)$ represents the covariance, and ρ_{xy} is the correlation coefficient of adjacent pixels. Randomly select 2000 pairs of pixels, and then use equation (16) to calculate the correlation of the original image and the cipher image of Lena adjacent pixels

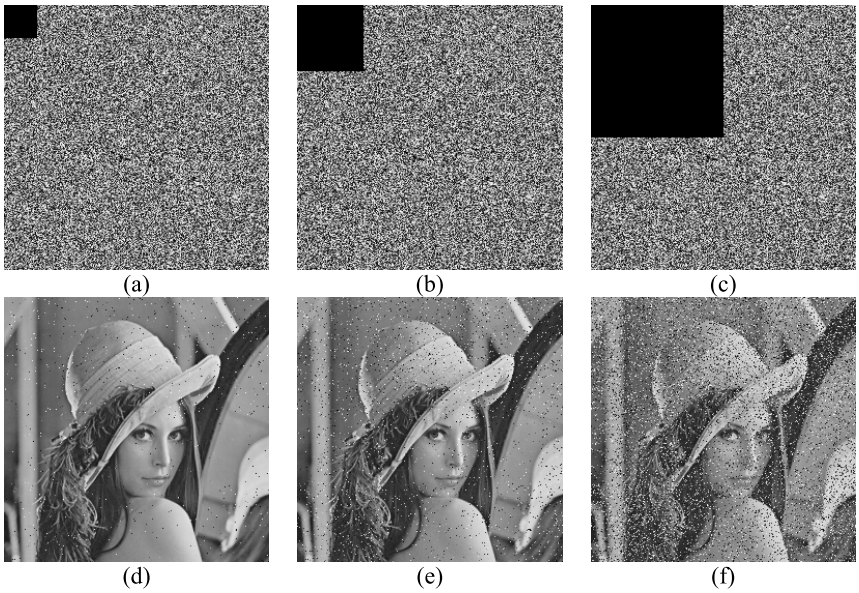


FIGURE 7. Robustness against occlusion attack under low computing precision. (a) Encrypted image with 1/64 data loss. (b) Encrypted image with 1/16 data loss. (c) Encrypted image with 1/4 data loss. (d) Decrypted image with 1/64 data loss. (e) Decrypted image with 1/16 data loss. (f) Decrypted image with 1/4 data loss.

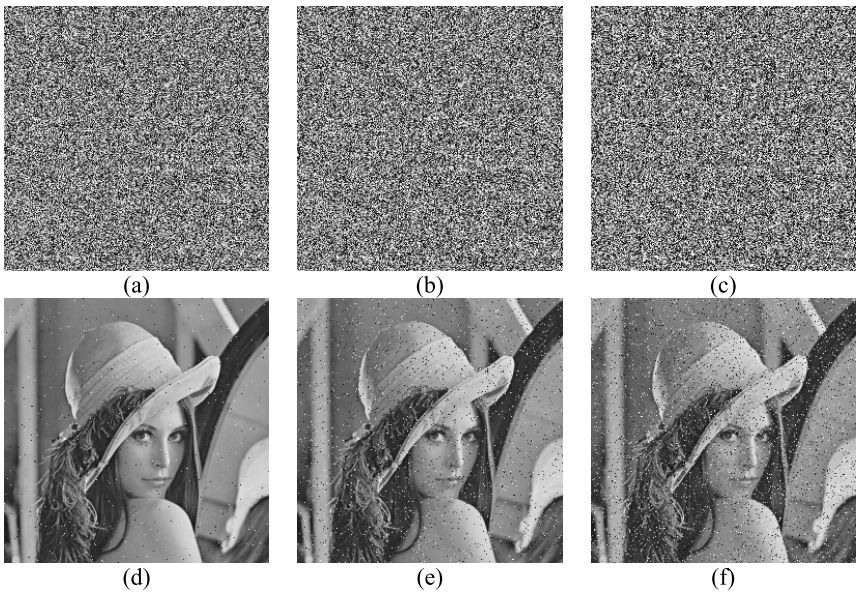


FIGURE 8. Robustness against noise attack under low computing precision. (a) Encrypted image with 0.01 salt and pepper noise. (b) Encrypted image with 0.05 salt and pepper noise. (c) Encrypted image with 0.1 salt and pepper noise. (d) Decrypted image with 0.01 salt and pepper noise. (e) Decrypted image with 0.05 salt and pepper noise. (f) Decrypted image with 0.1 salt and pepper noise.

respectively. It can be seen from Table 6 that after encryption, the cipher image effectively reduces the correlation between adjacent pixels.From Figure 6 shows that the distribution of adjacent pixels in the original Lena image is highly concentrated, indicating that the original image of Lena is highly correlated. The distribution of adjacent pixels in the cipher image of Lena is randomly distributed, indicating that the correlation of Lena cipher image is very low.

F. DATA LOSS ANALYSIS

When images are transmitted over the network, data may be lost due to various reasons. It uses cropping a part of the cipher image to test the ability of cipher image to be restored to the original image when data is lost and analyzes the encryption algorithm's performance against the cropping attack. Fig. 7 shows the decrypted image of the cipher image after it has been cropped. It is obvious that even if the data

TABLE 8. Correlation test analysis.

	Horizontal (%)	Vertical (%)	Diagonal (%)
Plain image Lena	0.9618	0.9854	0.9618
Our method	-0.0175	0.0080	0.0131
Liu's [30]	0.0287	−0.0322	−0.0113
Hua's [31]	−0.0353	0.0286	−0.0249
Wang's [32]	−0.0059	−0.0146	0.0211
Tang's [33]	0.0335	−0.0174	−0.0295

is lost, the image can still identify the corresponding information after decryption. Therefore, the encryption algorithm proposed in this paper is highly robust to cropping attacks.

G. NOISE ATTACK ANALYSIS

When the image is transmitted on the transmission channel, it is usually affected by noise. Noise attacks on transmitted images are also a way to verify the robustness of encryption algorithms. The noise includes Gaussian noise, uniform noise and salt and pepper noise. In this section, the encryption algorithm is tested by using salt and pepper noise analysis.

Fig. 8 shows the experimental results of Lena's plain image and decrypted image with noise intensity of 0.01, 0.05, and 0.1. It can be seen from Fig. 8 that even if the noise intensity reaches 0.1, the decrypted image can still be identified. This shows that the encryption algorithm proposed in this paper can effectively resist noise attacks.

V. CONCLUSION

In this paper, an image encryption scheme based on block scrambling and state transformation is proposed. Firstly, through discrete wavelet transform (DWT) to divide the original image into four frequency bands, and use chaotic sequence and zigzag curve to scramble the image pixels. Secondly, through DNA coding rules to perform DNA coding on the scrambled pixels to obtain DNA coding sequence. Third, use the state machine to convert the state of the DNA coding sequence and then decode the DNA to restore it to decimal. Finally, the key stream generated by the chaotic system is used to diffuse the sequence after the state transition to generate cipher images. Experimental analysis shows that the scheme is highly secure and suitable for image encryption.

REFERENCES

[1] J. Kim, Y. Lee, and S. Lee, "DES with any reduced masked rounds is not secure against side-channel attacks," *Comput. Math. Appl.*, vol. 60, no. 2, pp. 347–354, Jul. 2010.

[2] E. Tromer, D. A. Osvik, and A. Shamir, "Efficient cache attacks on AES, and countermeasures," *J. Cryptol.*, vol. 23, no. 1, pp. 37–71, Jan. 2010.

[3] J. T. Liu, K. Liang, J. Wang, X. W. Chen, H. C. Xu, and G. F. Li, "Cuttable structure design and hardware implementation of SM4 encryption algorithm," *Acta Scientiarum Naturalium Universitatis Nankaiensis*, vol. 52, no. 4, pp. 41–45, 2019.

[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998.

[5] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 447–460, Feb. 2015.

[6] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[7] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, Apr. 2014.

[8] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "A novel image cipher based on mixed transformed logistic maps," *Multimedia Tools Appl.*, vol. 56, no. 2, pp. 315–330, Jan. 2012.

[9] L. Zhou, C. Wang, and L. Zhou, "A novel no-equilibrium hyperchaotic multi-wing system via introducing memristor," *Int. J. Circuit Theory Appl.*, vol. 46, no. 1, pp. 84–98, Jan. 2018.

[10] X. Zhang and C. Wang, "Multiscroll hyperchaotic system with hidden attractors and its circuit implementation," *Int. J. Bifurcation Chaos*, vol. 29, no. 9, Aug. 2019, Art. no. 1950117.

[11] X. Zhang and C. Wang, "A novel multi-attractor period multi-scroll chaotic integrated circuit based on CMOS wide adjustable CCCII," *IEEE Access*, vol. 7, pp. 16336–16350, 2019.

[12] Z. Peng, C. Wang, Y. Lin, and X. Luo, "A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption," *Acta Phys. Sinica*, vol. 63, no. 24, pp. 97–106, Dec. 2014.

[13] G. Guan, C. Wu, and Q. Jia, "An improved high performance Lorenz system and its application," *Acta Phys. Sinica*, vol. 64, no. 2, pp. 35–48, Jan. 2015.

[14] 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.

[15] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, to be published, doi: 10.1016/j.ins.2020.10.007.

[16] R. Ponuma and R. Amutha, "Compressive sensing based image compression-encryption using novel 1D-chaotic map," *Multimedia Tools Appl.*, vol. 77, no. 15, pp. 19209–19234, Aug. 2018.

[17] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, Nov. 2020, Art. no. 107684.

[18] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, p. 749, Jul. 2004.

[19] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns," *Pattern Recognit.*, vol. 25, no. 6, pp. 567–581, Jun. 1992.

[20] N. Bourbakis and A. Dollas, "SCAN-based compression-encryption-hiding for video on demand," *IEEE MultimediaMag.*, vol. 10, no. 3, pp. 79–87, Jul. 2003.

[21] Y. V. S. Rao, A. Mitra, and S. R. M. Prasanna, "A partial image encryption method with pseudo random sequences," in *Proc. Int. Conf. Inf. Syst. Secur.*, vol. 4432, 2006, pp. 315–325.

[22] B. Zhang and C. H. Jin, "Breaking method for composite chaotic pseudo-random sequence encryption algorithm," *Comput. Eng.*, vol. 33, no. 19, pp. 164–167, 2007.

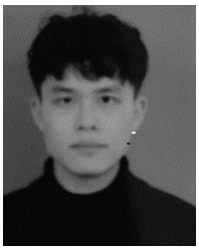
[23] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 51–66, Jan. 2017.

[24] Q. Zhang, L. Guo, and X. Wei, "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik - Int. J. Light Electron Opt.*, vol. 124, no. 18, pp. 3596–3600, Sep. 2013.

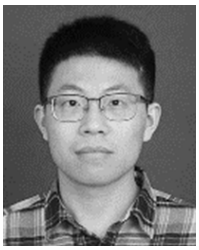
[25] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.

[26] F. Yu, L. Gao, K. Gu, B. Yin, Q. Wan, and Z. Zhou, "A fully qualified four-wing four-dimensional autonomous chaotic system and its synchronization," *Optik*, vol. 131, pp. 79–88, Feb. 2017.
[27] W. Liu and G. Chen, "Can a three-dimensional smooth autonomous quadratic chaotic system generate a single four-scroll attractor," *Int. J. Bifurcation Chaos*, vol. 14, no. 04, pp. 1395–1403, Apr. 2004.
[28] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.
[29] J. D. Watson and F. H. C. Crick, "A structure for deoxyribose Nucleic Acid," *Nature*, vol. 421, no. 6921, pp. 141–143, Aug. 2003.
[30] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21445–21462, Aug. 2018.
[31] 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.
[32] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dyn.*, vol. 95, no. 4, pp. 2797–2824, Jan. 2019.
[33] J. Tang, Z. Yu, and L. Liu, "A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24765–24788, May 2019.
[34] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[35] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[36] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.

SHENGTAO GENG received the M.S. degree in detection technology and automatic equipment from Jiangnan University, in 2010. He has been with the Zhengzhou University of Light Industry, Zhengzhou, China, since 2010. His research interests include the area of image processing and information security.



TAO WU received the bachelor's degree from the Henan Agricultural University, in 2018. He is currently pursuing the master's degree in control engineering with the Zhengzhou University of Light Technology. His research interest includes information security.



SHIDA WANG received the bachelor's degree from the Zhengzhou University of Light Industry, in 2020, where he is currently pursuing the master's degree in electrical engineering. His research interests include the areas of DNA computing and information security.

XUNCAI ZHANG (Member, IEEE) was born in Zhoukou, China, in 1981. He received the Ph.D. degree from the Huazhong University of Science and Technology, in 2009. From 2010 to 2012, he accomplished his postdoctoral research at Peking University. He is currently an Associate Professor with the School of Electrical and Information Engineering, Zhengzhou University of Light Industry. His research interests include the area of DNA computing and information security.

YANFENG WANG received the M.S. and Ph.D. degrees from the Huazhong University of Science and Technology, Wuhan, China, in 2004 and 2007, respectively. He is currently a Professor with the School of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou, China. He has published more than 80 SCI journal articles in the fields of dynamic modeling, memristor, data-driven modeling, and control and synchronization control. His research interests include bioinformatics computing and intelligent computing.