IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 March 2024, accepted 13 April 2024, date of publication 16 April 2024, date of current version 23 April 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3389975*

RESEARCH ARTICLE

# Double Image Encryption Algorithm Based on Parallel Compressed Sensing and Chaotic System

**CHAOXIA ZHANG, SHANGZHOU ZHANG, KAIQI LIANG, AND ZHIHAO CHEN**
School of Mechanical and Electrical Engineering and Automation, Foshan University, Foshan 528225, China

Corresponding author: Shangzhou Zhang (2112202038@stu.fosu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61403143, in part by the Natural Science Foundation of Guangdong Province under Grant 2014A030313739, in part by the Research on Common Technologies of Intelligent Factories for Discrete Manufacturing Industry Chain under Grant X220931UZ230, and in part by Guangdong Province Postgraduate Joint Training Base (Foshan) Joint Training Support Project.

**ABSTRACT** We propose a double image encryption scheme combining DNA, parallel compressed sensing, enhanced Zigzag confusion, chaotic sparse basis matrix, and chaotic permutation. Firstly, use the logistic map to scramble a Discrete Wavelet Transformation (DWT) matrix to obtain a chaotic DWT matrix. Next, 2D-LICM generates the measurement matrix. Parallel compressed sensing is then performed separately on the two images. Then, enhanced Zigzag confusion and DNA encryption are performed on the new matrix using chaotic sequences to obtain an encrypted image. The chaotic system's initial value is generated using SHA-256, which has a strong sensitivity to the plain image. We improve on the third-order Colpitts chaotic circuit to construct a more general higher-order Colpitts chaotic oscillator and propose a new fourth-order Colpitts chaotic system. The performance analysis indicates that our encryption algorithm provides excellent security and performance while saving storage space.

**INDEX TERMS** Parallel compressed sensing, image encryption, chaotic systems, image compression.

## I. INTRODUCTION

With the rapid development of Internet communication technology, anyone can publish information through the Internet anytime and anywhere. Then, while facing a large amount of information sharing and convenience, we also face massive data leakage, tampering and forgery. Information privacy has developed into a key issue. Digital images have contents that cannot be expressed by words and can convey information more intuitively and effectively, so digital images are more popular. Therefore, information protection of digital images has become a popular research topic. Image encryption, as an effective method to protect image information, involves several subject areas such as mathematics, information theory and cryptography [1], [2], [3]. For this reason, various communication security mechanisms have been gaining attention to secure the privacy of image information.

Arnold transform [4] encryption is vulnerable to cracking by exhaustive attacks and XOR operation encryption [5] is not resistant to plaintext attacks. Chaotic systems are deterministic nonlinear dynamical systems. Its motion is unpredictable, restricted, repetitive and sensitive to initial conditions and is widely used in the field of image encryption. Matthews first proposed the application of chaos in cryptography in 1989 [6]. It has higher encryption efficiency compared to traditional image encryption algorithm schemes. Liu et al. [7] proposed a cluster of 1D quadratic chaotic maps and its applications in image encryption. Wang et al. [8] presented a random scrambling image cryptography method to use a 1D logical self-embedding chaotic map. Due to the uncertainty of the quantum mechanics and the principle of measurement collapse, Hao et al. [9] studied an encryption system. They were using two-dimensional quantum walks

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

and quantum encoding. Images are encrypted by combining adaptive parameters with the proposed obfuscation method based on quantum position encoding. Saljoughi and Mirvaziri [10] used three-dimensional Logistic mapping to arrange and diffuse images. There needs to be more security when using low-dimensional chaotic systems [11], [12], [13]. Chaotic systems in low dimensions have a certain fragility in their algorithms due to their limited critical space. Thus, high-dimensional chaotic systems have become a better choice in image cryptography because of their more complex and unpredictable system. Detecting the information encrypted by hyperchaos with general low-dimensional deciphering methods is difficult. Using a 4D memristive hyperchaos, Vijayakumar and Ahilan [14] proposed a new encryption technology based on chaotic map substitution boxes (S-box) and cellular automata (CA). Naim et al. [15] proposed an encryption algorithm using hyperchaotic systems and the Josephus problem. In this paper, we propose a new chaotic system that improves on the third-order Colpitts chaotic oscillator and constructs a fourth-order Colpitts chaotic oscillator, which presents more complex bifurcation and chaotic properties.

Integrating chaotic systems in biogenetics with DNA encoding and decoding operations can further increase the performance of the encryption algorithm. Signing et al. [16] proposed to perturb the pixel distribution of images with dynamic DNA coding. Hu et al. [17] proposed a DNA pseudo-operation of DNA deletion and DNA insertion type DNA manipulation. Combining the pseudo-random sequence generated by chaos to scramble and diffuse the image to complete image encryption. Based on DNA image encryption the algorithm also has shortcomings and cannot resist plaintext attacks.

Images have a high degree of redundancy and strong correlation between neighboring pixels, which can lead to increased costs during transmission. Therefore, it is vital to compress the image properly when performing encryption. In this way, not only can the transmission speed be increased, but also can ensure that the image quality is not affected. In image compression, both deep learning-based [18], [19] and compressed sensing (CS) [20], [21], [22], [23] techniques are hot research topics. Fu et al. [24] proposed a discretized Gaussian-Laplacian-Logistic Mixture Model (GLLMM) that can adapt more accurately and efficiently to the different contents of different images and different regions of the same image. Zou et al. [25] proposed a new Symmetric Transform (STF) framework that uses absolute transform blocks in downsampling encoder and upsampling decoder. Fu et al. [26] proposed an effective asymmetric learning image compression method. In CS theory [20], [21], [22], [23], unlike the traditional Nyquist sampling theorem, compressed sensing completes both sampling and compression of the signal simultaneously. It avoids the generation of redundant data in the signal sampling stage. Some encryption algorithms combined with CS have gradually emerged, mainly through the encryption key to control a measurement matrix. For example, Gong et al. [27] proposed an effective image compression and encryption algorithm based on chaotic system and compressive sensing. Lu et al. [28] proposed a digital image encryption method based on CS combined with double random-phase encoding(DRPE) technology. Wang et al. [29] proposed an efficient double-image encryption and hiding algorithm using a newly designed chaotic system and parallel compressive sensing. Brahim et al. [30] proposed using a three-dimensional chaotic system to create measurement matrices. One-dimensional chaotic systems apply pixel scrambling to generate scrambling vectors to encrypt further. In the above scheme, the design of the security measurement matrix is mainly studied, while the security of the sparse base matrix is ignored. In this paper, We propose the use of chaotic DWT to enhance the security of sparse basis matrices.

In order to improve security against plaintext attacks and to save storage space, this paper proposes a double image encryption scheme combining Parallel Compressed Sensing(PCS), DNA, Zigzag chaos, chaotic sparse base matrix, and chaotic scrambling.

The main contributions of this article are: (1) PCS is more suitable for image processing and replacing traditional DWT with chaotic DWT can improve security. (2) A fourth-order Colpitts chaotic oscillator is constructed by improving on the third-order Colpitts chaotic oscillator, which presents more complex bifurcation and chaos characteristics. The fourth-order Colpitts confusion system is utilized to generate chaotic sequences. (3) The traditional zigzag chaos is improved to make up for the shortcomings of the traditional zigzag chaos, and the zigzag chaos is simple to realize with low time complexity. (4) The chaotic system's initial value is generated using SHA-256, strongly sensitive to the plain image. The encryption algorithm could effectively defend against the chosen plaintext attack. (5) Two images can be encrypted simultaneously by an encryption algorithm without multiple encryption transmissions for each image, saving data storage space and improving efficiency.

The organization of the rest of the paper is as follows. Parallel compression sensing, the construction of the measurement matrix, chaotic systems, and zigzag confusion are briefly described in Section II. Algorithms for image encryption and decryption are described in Section III. Performance analysis in Section IV. Conclusion in Section V.

## II. RELATED WORK

### A. PARALLEL COMPRESSED SENSING

In 2004, based on functional analysis and approximation theory, Candes and Donoho et al. proposed an efficient signal sampling technique based on functional analysis and approximation theory, namely compressed sensing theory [20], [21], [22], [23]. Compressed sensing uses the sparsity of the signal and a linear projection of the converted high-dimensional signal to low-latitude space using a measurement matrix independent of the transformation base to obtain the measured signal. The low-dimensional signal contains all the information of the high-dimensional measurement signal. It can recover the original signal by solving the sparse optimization problem.

Given an N-dimensional signal $x \in R^N$, it can be sparsely represented as follows:

$$\mathrm{x} = \Psi\theta \tag{1}$$

where $\theta$ represents the sparse coefficient and satisfies $\|\theta\|_0 = K(K \ll N)$, then the signal $x$ is considered to be k-sparse. $\Psi$ is an $N \times N$ sparse basis matrix. There are many sparse basis transform methods commonly used, such as discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transforms (DWT), etc.

After a signal is sparse, CS can be performed to obtain a measurement value $y$.

$$y = \Phi_X = \Phi\Psi\theta = A\theta \tag{2}$$

where $\Phi$ is measurement matrix of size $M \times N(M < N)$, $A$ is a sensing matrix of size $M \times N$. Equation (2) transforms an N-dimensional original signal $X$ into an M-dimensional vector $y$ after compressed sensing, and realizes the compressed sampling of the signal.

However, not all matrices can be used as measurement matrices. The measurement matrix must be independent of the sparse basis matrix. If sparse reconstruction conditions such as Restricted Isometry Property (RIP) are satisfied, the sparse signal can be reconstructed with a very high probability using the $l_0$ norm minimization problem. However, the $l_0$ norm problem is an NP-hard problem, and the $l_1$ norm minimization problem is equivalent to the $l_0$ norm minimization problem under certain conditions; the same solution can be obtained. Therefore, the $l_0$ norm minimization problem is usually transformed into an $l_1$ norm minimization problem.

$$\min \|\theta\|_1 \text{ s. t. } \mathrm{y} = \Phi\Psi\theta \tag{3}$$

where $\|\cdot\|_1$ denotes the $l_0$-norm of a vector. Signal $x$ could be reconstructed by the following method. For example, iterative reweighted least-Squares (IRLS) [31], smoothed $l_0$ norm (Sl$_0$) [32], orthogonal matching pursuit (OMP) [8], basis pursuit (BP) [33], etc. We use the smoothed $l_0$ norm Sl$_0$ in this paper.

Traditional compressed sensing usually directly samples one-dimensional signals or converts multi-dimensional signals into one-dimensional vectors before sampling. However, when a one-dimensional signal or a multi-dimensional signal is converted into a one-dimensional vector, a large measurement matrix is required. It will increase storage space and computational complexity. In order to solve this problem, a 2D signal is transformed into a sampled and reconstructed column-by-column signal using a measurement matrix. This approach is called parallel compressed sensing [34].

### B. MEASUREMENT MATRIX BASED ON TWO-DIMENSIONAL CHAOS

Constructing a suitable measurement matrix is the core of compressed sensing. In Ref. [35], a new two-dimensional Logistic iterative chaotic map with infinite collapse (ICMIC) concatenated graph (2D-LICM) was proposed based on the cascaded modulation coupling (CMC) model. Performance evaluation shows it has hyperchaotic behavior, a wide chaotic range and high complexity. In this article, the measurement matrix is generated by 2D-LICM to improve the security of the encryption algorithm, described as [36]:

$$\begin{cases} A_{i+1} = \sin\left(21/\left(a\left(B_i + 3\right)kx_i\left(1 - kA_i\right)\right)\right) \\ B_{i+1} = \sin\left(21/\left(a\left(kA_{i+1} + 3\right)yi\left(1 - B_i\right)\right)\right) \end{cases} \tag{4}$$

where system parameter $a \in (0, \infty), k \in (0, \infty)$, In this paper, $a = 0.5, k = 0.8$, initial values $A_0$ and $B_0$ are set as keys. In order to avoid transient effects, set $n_0$ as the chaotic sequence initial position. The sampling step is $d_0$. In this case, two pseudo-random chaotic sequences are obtained by iterating the chaotic system. $A = \left\{A_1, A_2 \ldots A_{n_0+\left(N\times\frac{N}{2}\right)\times d_0}\right\}$, $B = \left\{B_1, B_2 \ldots B_{n_0+\left(N\times\frac{N}{2}\right)\times d_0}\right\}$, The measurement matrix is generated by the following formula:

$$\Phi_A = \sqrt{\frac{4}{N}}\begin{pmatrix} A_1 & A_{\frac{N}{2}+1} & \cdots & A_{\frac{N}{2}(N-1)+1} \\ A_2 & A_{\frac{N}{2}+2} & \cdots & A_{\frac{N}{2}(N-1)+2} \\ \ddots & \ddots & \ddots & \ddots \\ A_{\frac{N}{2}} & A_N & \cdots & A_{\frac{N}{2}N} \end{pmatrix} \tag{5}$$

$$\Phi_B = \sqrt{\frac{4}{N}}\begin{pmatrix} B_1 & B_{\frac{N}{2}+1} & \cdots & B_{\frac{N}{2}(N-1)+1} \\ B_2 & B_{\frac{N}{2}+2} & \cdots & B_{\frac{N}{2}(N-1)+2} \\ \ddots & \ddots & \ddots & \ddots \\ B_{\frac{N}{2}} & B_N & \cdots & B_{\frac{N}{2}N} \end{pmatrix} \tag{6}$$

where $\sqrt{\frac{4}{N}}$ is used for normalization.

### C. THE FOURTH-ORDER COLPITTS CHAOS

The high-dimensional hyperchaotic sequence has good random characteristics; the critical space is big enough, dynamic behavior is more difficult to predict, and high security. A new higher-order chaotic system based on a fourth-order Colpitts oscillator. Kennedy proposed a third-order Colpitts chaotic oscillator based on a capacitive three-point sinusoidal oscillator based on nonlinear oscillation theory. In order to construct a more general higher-order Colpitts chaotic oscillator from the basis of the third-order Colpitts chaotic circuit, we connect a capacitor $C_3$ in parallel with the two ends of the inductor $L$ in the existing Colpitts chaotic circuit and construct a kind of fourth-order Colpitts chaotic oscillator consisting of four dynamic elements, which enters into the chaotic state by a periodic bifurcation and exhibits complex. The circuit enters the chaotic state after a period of bifurcation and exhibits complex bifurcation and chaos characteristics. The state equation of the fourth-order Colpitts chaos is as follows:

$$\begin{cases} \dfrac{dx}{dt} = \alpha_1(-x+y-z) - \beta_F f(y) + \alpha_2 \\ \dfrac{dy}{dt} = \beta_1(x+z) - \beta_2 f(y) - \beta_4 \\ \dfrac{dz}{dt} = \gamma_1(-x+y-z) - \gamma_2\omega + \gamma_3 \\ \dfrac{dw}{dt} = \delta z \end{cases} \tag{7}$$

where $f(y0 = 0.5(y - 1 + |y + 1|)$, $\alpha_1 = 2.86$, $\alpha_2 = 19$, $\beta_F = 200$, $\beta_1 = 2.86$, $\beta_2 = 3.11$, $\beta_3 = 1$, $\beta_4 = 17.38$, $\gamma_1 = 57.14$, $\gamma_2 = 20.0$, $\gamma_3 = 381$, $\delta = 5.48$. The Lyapunov exponents of the system are LE1 $= 1.23$, LE2 $= 0.08646$, LE3 $= 0$, LE4 $= -4.15$. Because it has two positive Lyapunov exponents, its chaotic system is more complex. Its phase diagram is presented in Fig.1.

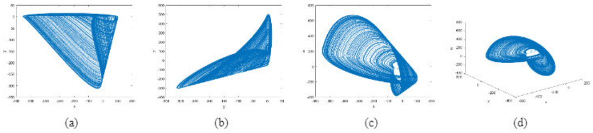


**FIGURE 1.** Attractor diagrams of this 4D hyperchaotic system. (a) the plane $x - y$; (b) the $y - z$ plane; (c) the $x - w$ plane; (c) the $x - y - w$ plane.

### D. ENHANCED ZIGZAG CONFUSION

Zigzag confusion is a scrambling method that replaces data by scanning the elements of a matrix from the top left corner in the zigzag order [37]. For zigzag confusion, different positions will produce different confusion effects. Fig. 2 shows that if the selected initial position is (1, 1), the element is traversed from position (1,1). Fig. 2 shows that in the traditional zigzag confusion transformation, 1, 2, 15, and 16 positions remain unchanged regardless of the number of iterations. This stands as a significant limitation of the standard zigzag chaotic approach. The enhanced zigzag confusion algorithm effectively addresses this limitation. The specific steps are outlined as follows: We define the starting point of the scan as the bottom-right corner of the matrix and subsequently perform a sequential zigzag transformation. This approach ensures that each element's position can undergo alteration during the iterative process. The enhanced zigzag confusion is shown in Fig. 3. Zigzag confusion is characterized by simple algorithm implementation and low time complexity, which can disrupt the high correlation between pixels and improve encryption security.

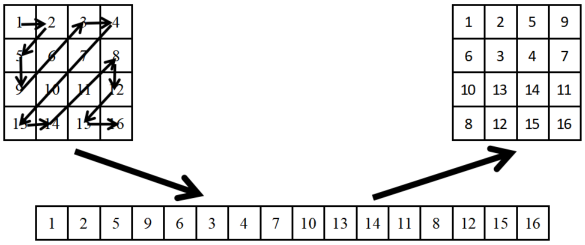


**FIGURE 2.** The matrices before and after zigzag confusion with the starting pixel (1, 1).

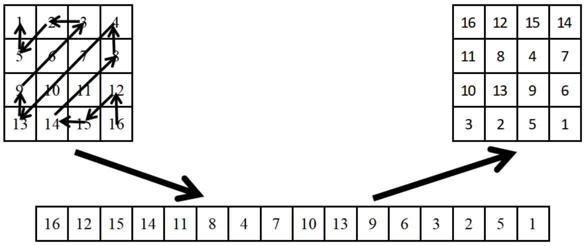


**FIGURE 3.** The enhanced zigzag scan path.

## III. IMAGE ENCRYPTION AND DECRYPTION PROCESS

### A. ENCRYPTION PROCESS

Fig. 4 shows the encryption process. Assuming the size of two plain images $X_1$ and $X_2$ is $N \times N$, the compression encryption process is as follows:

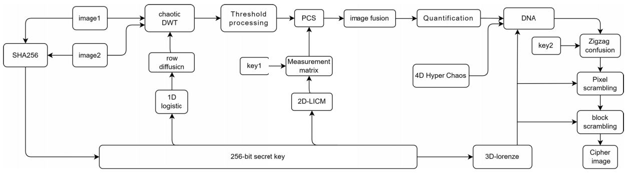


**FIGURE 4.** The flowchart of the proposed image encryption algorithm.

#### 1) SECRET KEY STRUCTURE

In this paper, the original image of the 256 hash function to generate 256 - bit hash value, the 256 - bit hash value into 64 - bit hexadecimal number as the key $K = k_1, k_2, \cdots k_{64}$ [38]. The initial value of the chaotic system is calculated using the key $K$. Therefore, for different plain image, the generated chaotic systems are different. Calculate initial values by Equation (8).

$$\begin{aligned} x_{0i} = 1/125(&k_{8i-7} \oplus k_{8i} \oplus k_{8i-6} \oplus k_{8i-1} + k_{8i-5} \oplus k_{8i-2} \\ &\oplus k_{8i-4} \oplus k_{8i-3}, i = 1, 2, 3, 4, 5, 6, 7, 8 \end{aligned} \tag{8}$$

#### 2) THE PROCESS OF PCS

Step 1: According to the generated initial value $x_{01}$ substituted into the logistics system iteration,set the sampling step to $d_0$, discard the first $n_0$ times to get the sequence $Z$. A position sequence is derived from a sequence of $Z$ sorted ascendingly. The conventional DWT is scrambled to get the chaotic sparse base matrix $\Psi$, which is used to sparse the two original images to get the sparse matrix $X_3$, $X_4$; $X_3 \in R^{N\times N}$, $X_4 \in R^{N\times N}$

Step 2: Threshold processing; Set the threshold $Qu$. Modify the elements of $X_3$, $X_4$, change the element whose absolute value are less than $Qu$ to zero. Then get the matrix $X_5$, $X_6$.

Step 3: Based on the generated initial value $x_{02} + key_1 * i$, $x_{03} + key_1 * i$, creat the measurement matrix of column

$i$-th ($i = 1, 2 \cdots N$) [39]. $Key_1$ is the perturbation after each measurement matrix is generated. Substituting it into 2-D LICM system to iterate and discarding the former $n_0$ times, we can obtain chaotic sequences Ai and Bi with length $(N/2) \times N$. Set $CR = 0.5$. Generate measurement matrix $\Phi_{Ai}$ and $\Phi_{Bi}$. $\Phi_{Ai} \in R^{(N/2)\times N}$, $\Phi_{Bi} \in R^{(N/2)\times N}$. The obtained measurement matrix $\Phi_{Ai}$ is used to calculate the measured values of each column of matrix $X_5$, and all the measured values are combined into matrix Y1. The obtained measurement matrix $\Phi_{Bi}$ is used to calculate the measured values of each column of matrix $X_6$, and all the measured values are combined into matrix Y2. Y1 $\in R^{(N/2)\times N}$, Y2 $\in R^{(N/2)\times N}$.

Step 4: image fusion; Combine the matrices Y1 and Y2 into one matrix Y3. Y3 $\in R^{N\times N}$.

### 3) THE PROCESS OF CHAOTIC ENCRYPTION

Step 1: Convert the value of matrix Y3 into the range of 0 to 255 for DNA operation.

$$\mathrm{Y4} = round\left[\frac{255 \times (\mathrm{Y3} - \mathrm{Y3}_{\min})}{(\mathrm{Y3}_{\max} - \mathrm{Y3}_{\min})}\right] \tag{9}$$

Step 2: Using $x_{08}, x_{01}, x_{04}$, 3-D Lorenze system is iterated to generate three chaotic sequences $\{U\}, \{V\}, \{W\}$;

By Equation (10), convert the elements in $\{U\}$ to the range zero to 255.

$$U = \mathrm{mod}\left(\mathrm{round}\left(U * 10^6\right), 256\right) \tag{10}$$

The sequence $\{U\}$ is transformed into a matrix $R$ of the same size $N \times N$ as Y3;

$$R = \mathrm{reshape}(U, N, N) \tag{11}$$

Step 3: Using $x_{04}$, $x_{05}$, $x_{06}$, $x_{07}$, iterate the 4-D hyperchaotic system to generate four chaotic sequences $E = \{E_1, E_2, \cdots E_{N\times N}\}$, $L = \{L_1, L_2, \cdots L_{N\times N}\}$, $M = \{M_1, M_2, \cdots M_{N\times N}\}$, $N = \{N_1, N_2, \cdots N_{N\times N}\}$.

DNA encoding method of matrix Y3 is defined in terms of the chaotic sequence $\{E\}$; DNA encoding method of $R$ is defined in terms of the chaotic sequence $\{L\}$. Because DNA has 8 encoding methods, the values of chaotic sequence $\{E\}$ and $\{L\}$ need to be converted to integers between 1 and 8. Transform the values of the chaotic sequence $\{E\}$ and the chaotic sequence $\{L\}$.

$$\begin{cases} E = \mathrm{mod}\left(\mathrm{round}\left(E \times 10^6\right), 8\right) + 1 \\ L = \mathrm{mod}\left(\mathrm{round}\left(L \times 10^6\right), 8\right) + 1 \end{cases} \tag{12}$$

The DNA operation of matrix Y3 and matrix $R$ is determined by the chaotic sequence $\{M\}$. Because this algorithm uses four DNA algorithms, it is necessary to transform $\{M\}$ into an integer ranging from 0 to 3 according to Equation (13).

$$M = \mathrm{mod}\left( round\left(M \times 10^6\right), 4\right) + 1 \tag{13}$$

The chaotic sequence $\{N\}$ determines the DNA decoding rules after calculation. DNA decoding is the reverse process of DNA encoding, and there are 8 decoding methods. Transform the values of the chaotic sequence $\{N\}$ in accordance with Equation (14).

$$M = \mathrm{mod}\left(\mathrm{round}\left(M \times 10^6\right), 4\right) + 1 \tag{14}$$

Step 4: DNA encoding method of matrix Y4(i) is E(i). DNA encoding method of chaotic R(i) is L(i). According to M(i), the DNA operation is performed on the encoded Y4(i) and the encoded R(i) to obtain Y5(i).

Perform DNA decoding the matrix Y5(i) after DNA operation to obtain a matrix $P_1$(i). The sequence N(i) determines the DNA decoding rules after calculation. $P_1 \in R^{N\times N}$.

Step 5: Generated $1 \sim N \times N$ random numbers $key_2$, The matrix $P_2$ is obtained by zigzag confusion of matrix $P_1$ according to $key_2$.

Step 6: Pixel scrambling; Chaotic sequence $V = \{V_1, V_2, \cdots V_{N\times 8}\}$. Block the matrix $P_2$ by column and convert each pixel to binary. The index is obtained by chaotic $V$ sorting, and each pixel is scrambled. Finally, In order to obtain the matrix $P_3$, the pixel values are converted to decimal values; $P_3 \in R^{N\times N}$.

Step 7: Block scrambling; Divide the matrix $P_3$ into blocks of size $t \times t$. The index is obtained by sorting the chaotic sequence $W = \left\{W_1, W_2, \cdots W_{(N\times N)(txt)}\right\}$, and the matrix $P_3$ is scrambled to obtain the final encrypted image $P_4$; $P_4 \in R^{N\times N}$

## B. DECRYPTION PROCESS

The decryption process is shown in Fig. 5. The decryption process is opposite to the encryption process. Before decryption, $x_{01}$, $x_{02}$, $x_{03}$, $x_{04}$, $x_{05}$, $x_{06}$, $x_{07}$, $x_{08}$, $\mathrm{Y3}_{\min}$ and $\mathrm{Y3}_{\max}$, sampling period $d_0$ and initial sampling position $n_0$ are transmitted to the receiver as keys. Firstly, the corresponding chaotic sequence is calculated and generated, which is substituted into the logistics system iteration to generate the confusion sequence $Z$; Substitute into the 2D-LICM system, iteratively generate obfuscation sequences $Ai$ and $Bi$; Substitute into the 3-D Lorenze system to generate chaotic sequences $U$, $V$, $W$; Substituting into 4-D hyperchaotic system, chaotic sequences $E, L, M, N$ are generated.

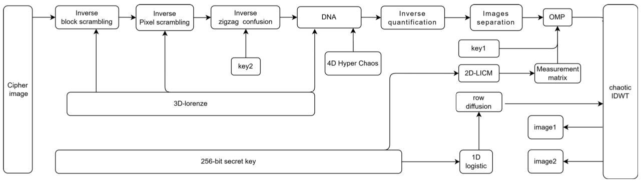


**FIGURE 5.** The flowchart of the proposed image decryption scheme.

Step 1: Inverse block scrambling; The matrix $P_4$ is divided into blocks of $t \times t$. Then use the chaotic sequence $W$ to inverse block scrambling of the matrix to obtain $P_3$.

Step 2: Inverse pixel scrambling; The matrix $P_2$ is obtained by using the pixel chaos of matrix $P_3$ inversed by chaotic sequence $V$.

Step 3: Inverse zigzag confusion; The matrix $P_1$ can be obtained by reversing the zigzag chaos of matrix $P_2$ with the $key_2$.

Step 4: DNA decryption; Matrix $P_1$ is DNA coded by chaotic sequence $N$ and matrix $R$ is coded by chaotic sequence $L$. Different from DNA encryption, if subtraction is applied in encryption, addition is applied here, and vice versa. The encoded matrix $R$ and the encoded matrix $P_1$ are subjected to DNA inverse operation to obtain the matrix Y5. The matrix Y5 is decoded by DNA using $E$ to obtain the matrix Y4.

Step 5: Inverse quantization; Matrix Y4 is inversely quantized according to keys $Y3_{\min}$ and $Y3_{\max}$ to obtain matrix Y3.

$$Y3 = \frac{Y4 \times (Y3_{\max} - Y3_{\min})}{255} + Y3_{\min} \tag{15}$$

Step 6: Image separation; Divide matrix Y3 into two matrices Y1 and Y2.

Step 7: Reconstruct; According to the corresponding measurement matrices $\Phi_{Ai}$ and $\Phi_{Bi}$ generated by chaotic sequences Ai and Bi, matrix X3 is obtained from matrix Y1 and matrix X4 is obtained from matrix Y2 by using a certain reconstruction algorithm.

Step 8: Restore images; Use inverse chaotic DWT on matrix X3 and matrix X4 to get original images X1 and X2.

## IV. PERFORMANCE ANALYSES

An operating system of Windows 11 was used for the simulation experiment. The simulation experiment is implemented in Matlab 2016b.

### A. ENCRYPTION AND DECRYPTION RESULTS

The experimental simulation selected the classic ‘‘House’’, ‘‘Peppers’’, ‘‘Cameraman’’, ‘‘Woman’’, ‘‘DICOM1’’ and ‘‘DICOM2’’ grayscale images, the size of which is 512×512. Set the following parameters: $x_{01} = 0.0313$, $x_{02} = 0.0898$, $x_{03} = 0.0234$, $x_{04} = 0.0625$, $x_{05} = 0.0977$, $x_{06} = 0.0195$, $x_{07} = 0.1016$, $x_{08} = 0.0898$, $key_1 = 0.001$, $key_2 = 2$, $d_0 = 3$, $n_0 = 1000$. Fig. 6 shows the plain images and the encrypted images. From the visual point of view, the encrypted image has no connection to the plain image. Fig. 7 shows the correctly decrypted image. Two plain images are compressed into one encrypted image, saving half the storage space. The encryption, as well as the decryption of our proposed algorithm, is excellent.

The encryption algorithm in this paper can also be used for color images. The color digital image is divided into three two-dimensional matrices, R, G, and B, significantly reducing the time and space resources required. The encryption operation is performed on each 2D matrix, and finally, the three channels are merged to get the color-encrypted image. The decryption process is the inverse operation of the encrypted image opposite to the encryption. The result of encryption and decryption of the color image is shown in Fig. 8.

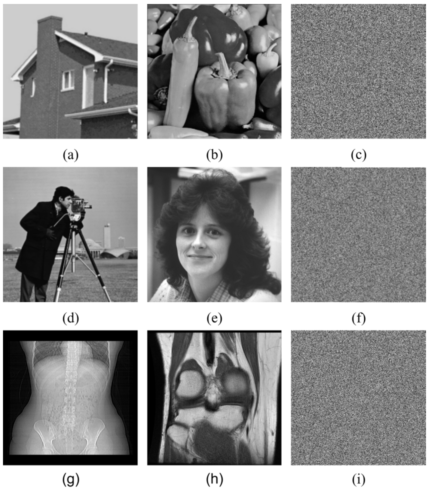


**FIGURE 6.** Encryption: (a) “House”, (b) “Peppers”, (c) encryption “House” and “Peppers”, (d) “Cameraman”, (e) “Woman”, (f) encryption “Cameraman” and “Woman”, (g) “DICOM1”, (h) “DICOM2”, (i) “encryption “DICOM1” and “DICOM2”.

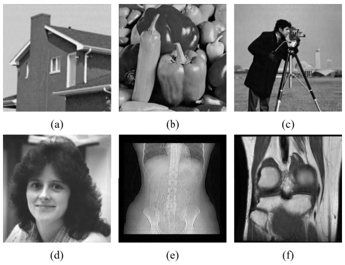


**FIGURE 7.** Decryption: (a) “House”, (b) “Peppers”, (c) “Cameraman”, (d) “Woman”, (e) “DICOM1”, (f) “DICOM2”.

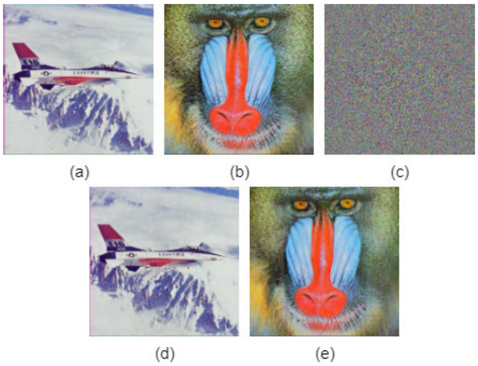


**FIGURE 8.** Encryption: (a) “Plane”, (b) “Baboon”, (c) encryption “Plane” and “Baboon”; Decryption: (d) “Plane”, (e)“Baboon”.

### B. EVALUATION OF THE RECONSTRUCTION

Peak signal-to-noise ratio (PSNR) is a commonly used image evaluation criterion. The more significant the PSNR value, the smaller the difference. PSNR is defined by Equation (16) [40].

$$PSNR = 10\lg \frac{255^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[P(i,j) - Q(i,j)]^2} \tag{16}$$

where $P(i, j)$ represents the pixel value of the plain image. $Q(i, j)$ represents the pixel value of the reconstructed image.

Structural similarity (SSIM) is an index to measure the similarity between two images [41]. It is evaluated by calculating the SSIM of the plain and reconstructed image. Its range is between [0, 1]. The closer the test value is to 1, the higher the similarity between two images. SSIM is defined as follows [42]:

$$\mathrm{SSIM} = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{PQ} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{17}$$

where $k_1 = 0.01$ and $k_2 = 0.03$, $c_1 = (k_1 \times L)^2$, $c_2 = (k_2 \times L)^2$, $L = 255$, $c_1 = (k_1 \times L)^2$ and $c_2 = (k_2 \times L)^2$. $\mu_x$ and $\mu_y$ are the means of images $X$ and $Y$ respectively. $\sigma_x^2$ and $\sigma_y^2$ are the variances of images $X$ and $Y$ respectively. $\sigma_{xy}$ is the covariance of images $X$ and $Y$.

Table 1 shows the peak signal-to-noise ratio (PSNR) between the decrypted image and the original image. Table 2 shows the structural similarity index (SSIM) between the decrypted image and the original image. The algorithm performs satisfactorily in PSNR and SSIM tests. Therefore, the algorithm has good reconstruction quality.

**TABLE 1.** PSNRs (dB) comparison of decrypted image and original image.

| Image | PSNR(dB) |
|---|---|
| Peppers | 33.9745 |
| House | 34.3330 |
| Cameraman | 33.7221 |
| Woman | 35.8089 |
| DICOM1 | 33.9346 |
| DICOM2 | 33.5619 |

**TABLE 2.** SSIM comparison of decrypted image and original image.

| Image | SSIM |
|---|---|
| Peppers | 0.8994 |
| House | 0.9122 |
| Cameraman | 0.8924 |
| Woman | 0.9246 |
| DICOM1 | 0.8934 |
| DIICOM2 | 0.9070 |

### C. KEY SPACE

As a good image encryption algorithm, it should have a substantial key space to resist brute force attacks effectively. The algorithm has sufficiently high security if the key space is more significant than $2^{100}$ [43]. Calculation accuracy of $10^{-14}$ is taken into account. Key space consists of the following main components: (1) The 256-bit hash value. (2) Given numerical parameters $key_1$, $key_2$. (3) $Y3_{\max}$ and $Y3_{\min}$. (4) Sampling period $d_0$ and initial sampling position $n_0$. The total key space is $2^{256} + \left(10^{14}\right)^2 + \left(10^{14}\right)^2 + \left(10^{14}\right)^2 = 2^{256} + 10^{84} > 2^{256} + 2^{279} \approx 2^{279}$. Thus, the sum key space in our algorithm is much bigger than $2^{100}$ [43]. Therefore, the key can resist brute force attacks. Table 3 shows that compared with other encryption schemes [44], [45], [46].

**TABLE 3.** Comparison of key space.

| Algorithm | Ours | Ref.[44] | Ref.[45] | Ref.[46] |
|---|---|---|---|---|
| Key space | $\mathbf{2^{279}}$ | $2^{123}$ | $2^{148}$ | $2^{256}$ |

We can see that our algorithm is more secure than other encryption schemes.

### D. CORRELATION ANALYSIS

For an ideal encrypted image, there should not exist a correlation between adjacent pixels. The correlation coefficient of the adjacent pixels is an essential statistical feature of the images. If the correlation between adjacent pixels of an encrypted image is close to zero, the better performance of the algorithm. In the plain image and the encrypted image, 5000 pairs of adjacent pixels in the image's horizontal, vertical and diagonal directions are randomly selected for analysis. The formula for calculating the correlation coefficient is as follows [47]:

$$R_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{18}$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{19}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{20}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \tag{21}$$

where $x$ and $y$ respectively represent the pixel values of two adjacent pixel points in the image. $N$ is the logarithm of the selected pixels. E(x) and D(x) are the expectation and variance of variable $x$, respectively. $\operatorname{cov}(x, y)$ is the co-variance of $x$ and $y$, $R_{xy}$ is the correlation coefficient $x$ and $y$.

Fig. 9 is a dot diagram of the correlation coefficient of adjacent position data values. It can be seen from Fig. 9 that the pixels of the plain image are concentrated near the diagonal, indicating that the correlation between the pixels of the plain images are strong. However, the pixels of the encrypted image are scattered, showing that the correlation of the pixels of the ciphertext image has been destroyed.

Table 4 shows the correlation coefficients between the adjacent positions of the plain images and the encrypted image. The correlation coefficients of the plain images in horizontal, vertical, and diagonal directions are all near 1, indicating that the data values of its adjacent positions are highly correlated. However, the correlation coefficients of the cipher image are close to 0, indicating that the correlations of the encrypted image have been broken.

It shows that the algorithm proposed in this paper is good at reducing the strong correlation between adjacent pixels of the image.

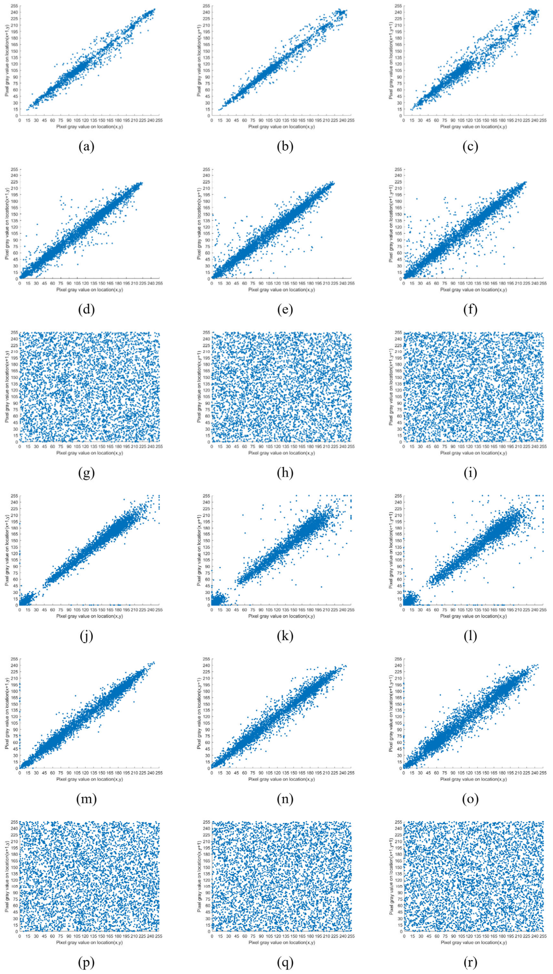


**FIGURE 9.** Correlation analysis: (a) - (c) "House" horizontal, vertical, diagonal correlation. (d) - (f) "Peppers" horizontal, vertical, diagonal correlation. (g) - (i) encryption "House" and "Peppers" horizontal, vertical, diagonal correlation. (j) - (l) "DICOM1" horizontal, vertical, diagonal correlation. (m) - (o) "DICOM2" horizontal, vertical, diagonal correlation. (p) - (r) encryption "DICOM1" and "DICOM2" horizontal, vertical, diagonal correlation.

**TABLE 4.** Images with different correlation coefficients.

| Image | Horizontally | vertically | Diagonally |
|---|---|---|---|
| House | 0.9951 | 0.9946 | 0.9898 |
| Peppers | 0.9777 | 0.9847 | 0.9673 |
| Cipher image of House and Peppers | 0.0028 | -0.0027 | 0.0003 |
| Cameraman | 0.9832 | 0.9898 | 0.9729 |
| Woman | 0.9964 | 0.9970 | 0.9948 |
| Cipher image of Cameraman and Woman | -0.0037 | 0.0185 | -0.0196 |
| DICOM1 | 0.9858 | 0.9854 | 0.9751 |
| DICOM1 | 0.9894 | 0.9915 | 0.9828 |
| Cipher image of DICOM1 and DICOM2 | 0.9858 | 0.9854 | 0.9751 |

### E. HISTOGRAM

The image's histogram counts the distribution of gray levels in the image, visually showing the frequency of different gray levels. A histogram can represent the distribution of pixel values in an image. A flatter histogram generally indicates a more uniform distribution of pixel values. Fig. 10 shows the histograms of the plain image and the encrypted image. The histogram distribution of the encrypted image is flat, and it can hide the statistical characteristics of the plain image. As a result, the encryption algorithm proposed in this paper can effectively resist statistical attacks based on histograms.

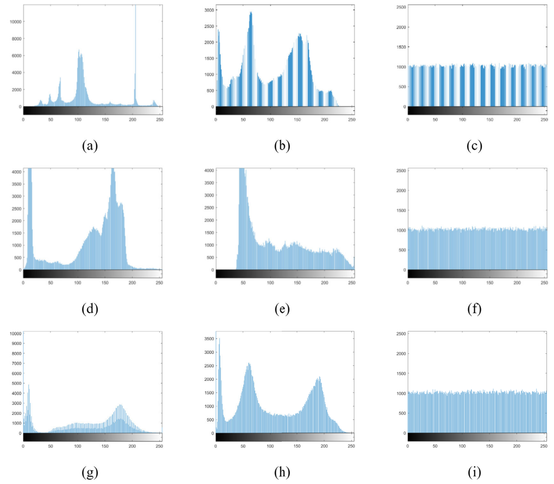


**FIGURE 10.** Histogram: (a) "House", (b) "Peppers", (c) encrypted images of "House" and "Peppers", (d) "Cameraman", (e) "Woman", (f) encrypted images of "Cameraman" and "Woman", (g) "DICOM1", (h) "DICOM2", (i) encrypted images of "DICOM1" and "DICOM2".

### F. ENTROPY OF INFORMATION

The one-dimensional entropy of an image can represent the aggregation characteristics of the gray-scale distribution of the image, but cannot reflect the spatial characteristics of the gray-scale distribution of the image, in order to characterize such spatial characteristics, the feature quantity that can reflect the spatial characteristics of the gray-scale distribution can be introduced on the basis of the one-dimensional entropy of the information to form the two-dimensional entropy of the information of the image. The mean gray value of the neighborhood of the image is chosen as the spatial feature quantity of gray scale distribution, and the pixel gray scale of the image is composed of the feature binary, denoted as $(i, j)$; where $i$ denotes the gray value of the pixel $0 \leq i \leq 255$ and $j$ denotes the mean gray value of the neighborhood $0 \leq j \leq 255$. Meanwhile, in order to reflect the combined characteristics of the gray value at the position of a pixel with the gray distribution of its surrounding pixels, the probability of the occurrence of $f(i, j)$ in the image is defined as $P(i, j)$.

$$P(i, j) = \frac{f(i, j)}{MN} \tag{22}$$

The above equation can reflect the combined characteristics of the gray value at a pixel location with its surrounding pixel gray distribution, where $f(i, j)$ is the number of times the feature binary appears [48].

$$H = -\sum_{i=0}^{255}\sum_{j=0}^{255} Pij \log_2 Pij \tag{23}$$

The greater the second-order information entropy of an image, the more chaotic the image is, which contains more information and complexity. The second-order information entropy before and after image encryption is shown in Table 5, which shows that the second-order information entropy of encrypted image is greater than that of the original image, and the encrypted image is more chaotic.

**TABLE 5. Second order information entropy.**

| Image | second order information entropy |
|---|---|
| House | 2.6067 |
| Peppers | 3.6133 |
| Cipher image of House and Peppers | 5.9999 |
| Cameraman | 3.0159 |
| Woman | 2.9487 |
| Cipher image of Cameraman and Woman | 5.9998 |
| DICOM1 | 3.1796 |
| DICOM2 | 3.6289 |
| Cipher image of DICOM1 and DICOM2 | 5.9999 |

### G. DIFFERENTIAL ATTACK ANALYSIS

Differential attack analysis is slightly modifying the plaintext to obtain the corresponding cipher and decipher the cryptographic system through the difference between the modified ciphertext and the original ciphertext. A good encryption scheme shall have the power to resist differential attacks effectively. Unified Average Change in Intensity (UACI) and Number of Pixels Change Rate (NPCR) are generally suitable measures of how minor changes in a plain image can influence an encryption image. The calculation formulas as follows [49]:

$$NPCR = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N} D(x, y) \times 100\% \tag{24}$$

$$UACI = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N} \frac{|P_1(x, y) - P_2(x, y)|}{255} \times 100\% \tag{25}$$

$$D(x, y) = \begin{cases} 0, P_1(x, y) = P_2(x, y) \\ 1, P_1(x, y) \neq P_2(x, y) \end{cases} \tag{26}$$

where $M$, $N$ are the size of the image. $P_1(i, j)$ is the pixel value of encrypted image $P_1$. $P_2(i, j)$ is the pixel value of encrypted image $P_2$. The expected value of NPCR is approximately $255/256 \approx 0.9960$. The expected value of UACI is approximately 0.3346. A pixel value at (1, 1), (256, 256) and (512, 512) is changed and then encrypted.

**TABLE 6. NPCR of changing the pixels of different positions.**

| Image | Pixel Change Position | | |
|---|---|---|---|
| | (1, 1) | (256, 256) | (512, 512) |
| House | 99.5991 | 99.6143 | 99.6212 |
| Peppers | 99.5979 | 99.6284 | 99.6227 |
| Cameraman | 99.6017 | 99.5850 | 99.6105 |
| Woman | 99.5975 | 99.6197 | 99.6132 |
| DICOM1 | 99.6003 | 99.6124 | 99.5921 |
| DICOM2 | 99.5995 | 99.6028 | 99.6148 |

**TABLE 7. UACI of changing the pixels of different positions.**

| Image | Pixel Change Position | | |
|---|---|---|---|
| | (1, 1) | (256, 256) | (512, 512) |
| House | 33.3446 | 33.4186 | 33.4822 |
| Peppers | 33.4717 | 33.4119 | 33.4718 |
| Cameraman | 33.4376 | 33.5087 | 33.5074 |
| Woman | 33.4676 | 33.4648 | 33.4291 |
| DICOM1 | 33.4159 | 33.3563 | 33.4058 |
| DICOM2 | 33.4267 | 33.4356 | 33.4674 |

Table 6 shows the results of NPCR tests. Table 7 shows the results of UACI tests. It can be seen that the values of NPCR and UACI are close to the ideal value of the index. It shows that the algorithm proposed in this paper can resist differential attacks very well.

### H. NOISE ATTACK

Noise often occurs when password images are transmitted on the Internet. Salt & pepper noise and Gaussian noise are common in images. $10^{-3}$ or $10^{-2}$ salt & pepper noise is added to the encrypted image to decrypt the encrypted image affected by the noise. Gaussian noise with zero mean and variance $10^{-4}$ is added to the encrypted image to decrypt the noise-affected encrypted image. It is evident that the pixel values at some points have changed, but the information of the plain images could nevertheless remain decryptable. The results show the proposed encryption algorithm in this paper has good robustness.

### I. CROPPING ATTACK

In the process of image transfer, data loss will inevitably occur. A high-quality security encryption algorithm should have the ability to resist data loss. Even if part of the data in the encrypted images is missing, decrypted images can be distinguished by eye observation. Fig. 12 shows the encrypted image and the corresponding decrypted image with 0.95% and 3.8% of the pixels missing. It can be seen that the decrypted image contains most of the information of the plain image. As such, this shows that the algorithm has a strong performance against cropping attacks.

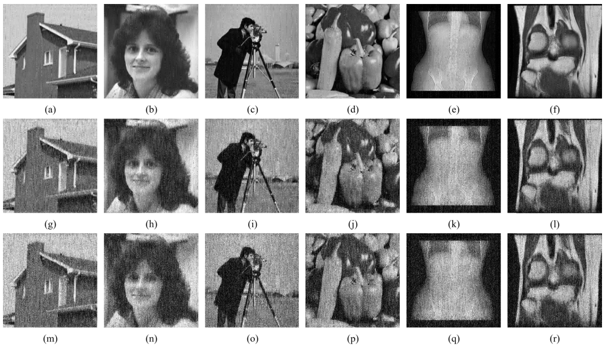


**FIGURE 11.** Noise attack: (a)-(d) the decrypt images with $10^{-3}$ salt & pepper noise. (e)-(h) the decrypt images with $10^{-2}$ salt & pepper noise. (m)-(r) the decrypt images with $10^{-4}$ Gaussian noise.

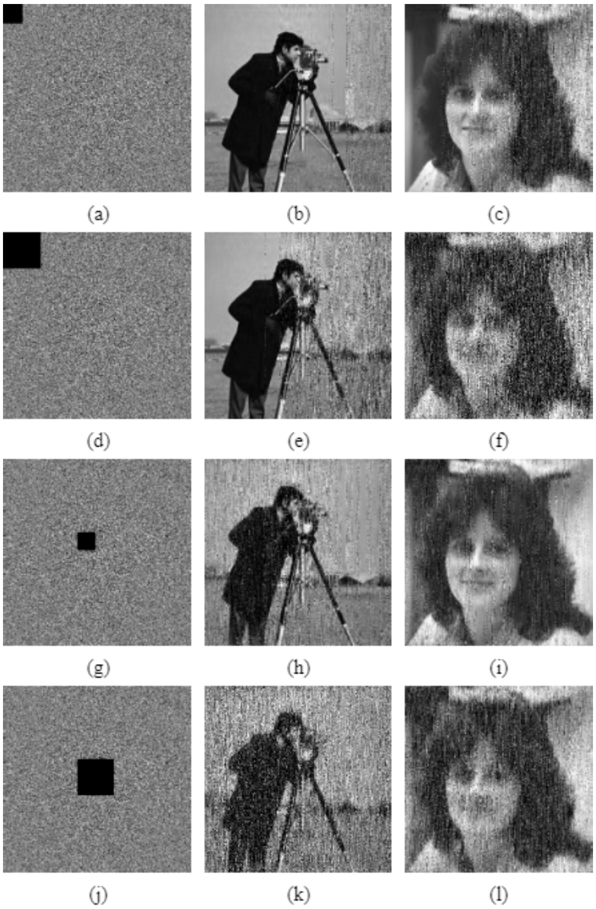


**FIGURE 12.** (a)(g) are the encrypted images with 0.95% data loss, (d)(j) are the encrypted images with 3.8% data loss, (b)(c)(e)(f)(h) (i)(k)(l) are the decrypted images.

### J. KEY SENSITIVITY

A secure cryptosystem must be highly sensitive to keys during encryption and decryption. For testing the sensitivity of the algorithm to the key, we use images "House" and "Peppers" and change the values of $x_{01}$, $x_{02}$, $x_{03}$, $key_1$ by adding $10^{-15}$ respectively. The experimental results are shown in Fig. 13. Experimental results show that even though there is only a slight difference in the key, it also leads to a complete decryption failure. Therefore, the algorithm possesses extreme sensitivity to the key.

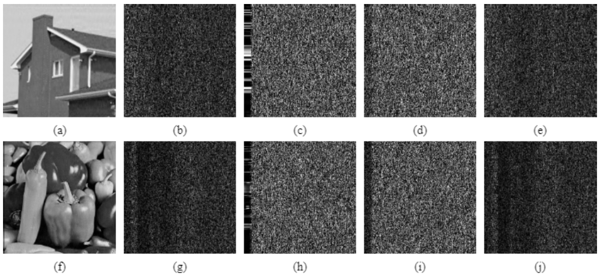


**FIGURE 13.** Key sensitivity analysis. (a) decrypt image House with correct keys, (b) decrypt image House $x_{01} + 10^{-15}$, (c) decrypt image House $x_{02} + 10^{-15}$, (d) decrypt image House $x_{03} + 10^{-15}$, (e) decrypt image House $key_2 + 10^{-15}$, (f) decrypt image Peppers with correct keys, (g) decrypt image Peppers $x_{01} + 10^{-15}$, (h) decrypt image Peppers $x_{02} + 10^{-15}$, (i) decrypt image Peppers $x_{03} + 10^{-15}$, (j) decrypt image Peppers $key_2 + 10^{-15}$.

### K. CLASSICAL ATTACKS

There are four types of classical attacks in which an attacker uses a password to find a plain image.

(1) Ciphertext-Only attack (COA) refers to a cryptanalysis method that analyzes only the ciphertext and solves the plaintext or key.

(2) Known Plaintext attack (KPA) means that the attacker has mastered part of the plaintext and the corresponding ciphertext, thus solving or breaking the corresponding key or the plaintext corresponding to the desired ciphertext.

(3) Chosen plaintext attack (CPA) means that as much as the attacker knows the encryption algorithm, he can also obtain the encrypted ciphertext by choosing the plaintext message, i.e., he knows the chosen plaintext and the encrypted ciphertext, but cannot directly crack the key.

(4) Chosen ciphertext attack (CCA) is one in which an attacker can select ciphertexts to decrypt. As well as knowing the known plaintext attacks, an attacker can create or chose some ciphertext at will and obtain the decrypted plaintext.

The CPA is the most potent attack [50]. This paper uses some methods to improve the algorithm's resistance to CPA. Initial values of SHA-256 are applied to create chaotic systems. Plain image is related to chaotic sequence generation. The sparse base matrix and the measurement matrix must be known if one wants to obtain a correct decrypted image from a compressed sensing and encryption algorithm. Measurement matrix, as well as sparse basis matrix, are associated with chaotic system. As a result of the unpredictability of chaotic systems, measurement matrix $\Phi$ and sparse basis matrix $\Psi$ are also unknown and unpredictable. In the encryption stage, DNA encoding, operation and decoding are related to chaotic sequences, and pixel scrambling is also related to chaos. The generated information depends on the plain image. Therefore, the proposed image compression and encryption algorithm can resist chosen plain-text attacks well.

### L. THE NIST SP800-22 TEST

The NIST SP 800-22 test consists of 15 tests for the randomness of binary sequences generated by cryptographic random numbers or pseudo-random number generators. Each sub-test produces a corresponding p-value. When the P-value exceeds 0.01, the chaotic system is proven to pass the NIST test. In the encryption algorithm of this paper, we have performed the NIST SP 800-22 test on the encrypted image, and the test results are shown in Table 8. Table 8 show that the encrypted image can pass NIST SP 800-22 test, which indicates that the encrypted image in this paper has a high level of chaos.

**TABLE 8. NIST test results.**

| Test name | P-value | Result |
|---|---|---|
| Approximate Entropy | 0.350485 | Pass |
| Block Frequency | 0.739918 | Pass |
| Cumulative Sums(forward) | 0.017912 | Pass |
| Cumulative Sums(reverse) | 0.534146 | Pass |
| FFT | 0.534146 | Pass |
| Frequency | 0.739918 | Pass |
| Linear Complexity | 0.534146 | Pass |
| Longest Run of Ones | 0.350485 | Pass |
| Non-Overlapping Template | 0.534146 | Pass |
| Overlapping Template | 0.122325 | Pass |
| Random Excursions | 0.215658 | Pass |
| Random Excursions Variant | 0.358458 | Pass |
| Rank | 0.911413 | Pass |
| Runs | 0.350485 | Pass |
| Serial Test 1 | 0.213309 | Pass |
| Serial Test 2 | 0.534146 | Pass |
| Universal | 0.256842 | Pass |

### M. COMPLEXITY AND TIME EFFICIENCY ANALYSIS

A competent algorithm needs to minimize the time complexity while considering security. The complexity of the encryption scheme proposed in this paper is calculated as chaotic sequence generation, compression sensing, DNA encryption and disruption operations. Assume that the size of both original images is $N \times N$. The time complexity required to generate the chaotic sequence is $\theta(N + \frac{1}{2} \times N \times N + \frac{1}{2} \times N \times N + 3 \times N \times N + 4 \times N \times N)$. The time complexity for disambiguating the sparse matrix in the compression perception and generating the measurement matrix is $\theta(N \times N)$ and $\theta(N \times N)$. The time complexity of DNA encoding, DNA manipulation, and DNA decoding is $\theta(12 \times N \times N)$. The time complexity of disambiguation is $\theta(2 \times N \times N)$. Therefore, the total time complexity of the scheme is $\theta(12 \times N \times N)$.

We tested the encryption time for two test images of size $512 \times 512$. The results are shown in Table 9. Our encryption time is shorter than that of [51]] and slightly longer than that of [52], but the algorithm in this paper is more secure and this time cost is acceptable.

**TABLE 9. Time test results (s).**

| Algorithm | second order information entropy |
|---|---|
| Ref. [51] | 114.7362 |
| Ref. [52] | 19.1744 |
| The proposed algorithm | **24.437078** |

**TABLE 10. PSNRs (dB) for the different methods.**

| Algorithm | PSNR(dB) |
|---|---|
| Ref. [42] | 29.96 |
| Ref. [53] | 31.3812 |
| Ref. [54] | 32.9960 |
| The proposed algorithm | **33.8674** |

**TABLE 11. SSIMs for the different methods.**

| Algorithm | SSIM |
|---|---|
| Ref. [42] | 0.8235 |
| Ref. [53] | 0.8436 |
| Ref. [54] | 0.8547 |
| The proposed algorithm | **0.8694** |

**TABLE 12. Correlation coefficients for the different method.**

| Algorithm | correlation coefficients | | |
|---|---|---|---|
| | Horizontally | vertically | Diagonally |
| The proposed algorithm | 0.0114 | 0.0052 | -0.0141 |
| Ref. [53] | **0.0004** | **0.0043** | -0.0003 |
| Ref. [55] | -0.0139 | 0.0177 | **6.79e − 04** |
| Ref. [56] | -0.0065 | 0.0071 | -0.0165 |

### N. COMPARISON WITH OTHER ALGORITHMS

The image "Peppers" with size $512 \times 512$ is a test image. Set the compression ratio to 0.5. Compared with other image encryption algorithms with the same compression ratio. Table 10 shows the PSNR of the decrypted image for different algorithms. We could see that our proposed image encryption algorithm has a large PSNR value. Table 11 shows the SSIMs of the decrypted image for different algorithms. It can be seen that the SSIMs value of the proposed algorithm is higher than the other algorithms. So our encryption algorithm has a better recovery effect. Table 12 shows the Correlation coefficients of the encrypted image for different algorithms. It can be seen that the pixel correlation of the encrypted images in this paper and in other literatures are very close to the same as 0. Table 13 shows the Second order information entropy of the encrypted image for different algorithms. Compared to

**TABLE 13.** Second order information entropy for the different methods.

| Algorithm | second order information entropy |
|---|---|
| Ref. [42] | 4.5921 |
| Ref. [53] | 4.8935 |
| The proposed algorithm | **5.9998** |

other algorithms, the encryption algorithm proposed in this paper has higher second-order information entropy. So the encrypted images in this paper are much more confusing.

## V. CONCLUSION

This paper proposes a double image encryption algorithm based on parallel compressed sensing and chaotic systems. The plain image is compressed by parallel compressive sensing, and 2D-LICM generates measurement matrices. Sparsification using chaotic DWT. Chaos sequence is used to control DNA encryption. Zigzag chaos is used to improve the PSNR of the reconstructed images. Finally, pixel scrambling and block scrambling are used to reduce the correlation. The chaotic system's initial value is generated using SHA-256, which has a strong sensitivity to the plain image. This scheme can reduce the data from multi-image encryption and save storage space. Experimental results show that the algorithm proposed in this paper has the advantages of high reconstruction quality, sizeable key space and high key sensitivity. The password image histogram is evenly distributed and has excellent robustness to noise as well as occlusion attacks. The algorithm can resist common attacks, such as brute force attacks, cropping attacks, noise attacks, differential attacks, statistical attacks, and chosen plaintext attacks.

## ACKNOWLEDGMENT

The code is publicly available at: https://github.com/Zhangshangzhou/image-encryption-algorithm.git.

## REFERENCES

[1] W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, and Y. He, "Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform," *Mathematics*, vol. 10, no. 15, p. 2751, Aug. 2022.

[2] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008.

[3] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Proc. Comput. Sci.*, vol. 54, pp. 472–481, Jan. 2015.

[4] P. Singh, A. K. Yadav, and K. Singh, "Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition," *Opt. Lasers Eng.*, vol. 91, pp. 187–195, Apr. 2017.

[5] X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme," *Opt. Lasers Eng.*, vol. 102, pp. 106–111, Mar. 2018.

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

[7] L. Liu and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," *Math. Comput. Simul.*, vol. 204, pp. 89–114, Feb. 2023.

[8] X. Wang, N. Guan, and J. Yang, "Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map," *Chaos, Solitons Fractals*, vol. 150, Sep. 2021, Art. no. 111117.

[9] W. Hao, T. Zhang, X. Chen, and X. Zhou, "A hybrid NEQR image encryption cryptosystem using two-dimensional quantum walks and quantum coding," *Signal Process.*, vol. 205, Apr. 2023, Art. no. 108890.

[10] A. S. Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," *Pattern Anal. Appl.*, vol. 22, no. 1, pp. 243–257, Feb. 2019.

[11] T. Yang, L.-B. Yang, and C.-M. Yang, "Breaking chaotic switching using generalized synchronization: Examples," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 45, no. 10, pp. 1062–1067, Oct. 1998.

[12] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, Dec. 2012.

[13] B. Wang, X. Wei, and Q. Zhang, "Cryptanalysis of an image cryptosystem based on logistic map," *Optik*, vol. 124, no. 14, pp. 1773–1776, Jul. 2013.

[14] M. Vijayakumar and A. Ahilan, "An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map," *Ain Shams Eng. J.*, vol. 15, no. 4, Apr. 2024, Art. no. 102620.

[15] M. Naim, A. Ali Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem," *Adv. Space Res.*, vol. 67, no. 7, pp. 2077–2103, Apr. 2021.

[16] V. R. F. Signing, G. A. G. Tegue, M. Kountchou, Z. T. Njitacke, N. Tsafack, J. D. D. Nkapkop, C. M. L. Etoundi, and J. Kengne, "A cryptosystem based on a chameleon chaotic system and dynamic DNA coding," *Chaos, Solitons Fractals*, vol. 155, Feb. 2022, Art. no. 111777.

[17] T. Hu, Y. Liu, L.-H. Gong, S.-F. Guo, and H.-M. Yuan, "Chaotic image cryptosystem using DNA deletion and DNA insertion," *Signal Process.*, vol. 134, pp. 234–243, May 2017.

[18] D. He, Z. Yang, W. Peng, R. Ma, H. Qin, and Y. Wang, "ELIC: Efficient learned image compression with unevenly grouped space-channel contextual adaptive coding," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 5708–5717.

[19] D. He, Y. Zheng, B. Sun, Y. Wang, and H. Qin, "Checkerboard context model for efficient learned image compression," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2021, pp. 14766–14775.

[20] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[21] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[22] R. Baraniuk, "A lecture on compressive sensing," *IEEE Signal Process. Mag.*, vol. 24, no. 4, pp. 118–121, Jul. 2007.

[23] Y. Tsaig and D. L. Donoho, "Extensions of compressed sensing," *Signal Process.*, vol. 86, no. 3, pp. 549–571, Mar. 2006.

[24] H. Fu, F. Liang, J. Lin, B. Li, M. Akbari, J. Liang, G. Zhang, D. Liu, C. Tu, and J. Han, "Learned image compression with Gaussian–Laplacian-logistic mixture model and concatenated residual modules," *IEEE Trans. Image Process.*, vol. 32, pp. 2063–2076, 2023.

[25] R. Zou, C. Song, and Z. Zhang, "The devil is in the details: Window-based attention for image compression," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 17471–17480.

[26] H. Fu, F. Liang, J. Liang, B. Li, G. Zhang, and J. Han, "Asymmetric learned image compression with multi-scale residual block, importance scaling, and post-quantization filtering," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 8, pp. 4309–4321, Aug. 2023.

[27] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.

[28] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik*, vol. 124, no. 16, pp. 2514–2518, Aug. 2013.

[29] X. Wang, C. Liu, and D. Jiang, "An efficient double-image encryption and hiding algorithm using a newly designed chaotic system and parallel compressive sensing," *Inf. Sci.*, vol. 610, pp. 300–325, Sep. 2022.

[30] A. H. Brahim, A. A. Pacha, and N. H. Said, "Image encryption based on compressive sensing and chaos systems," *Opt. Laser Technol.*, vol. 132, Dec. 2020, Art. no. 106489.

[31] R. Chartrand and W. Yin, "Iteratively reweighted algorithms for compressive sensing," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2008, pp. 3869–3872.

[32] M. R. Abuturab and A. Alfalou, "Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional Fourier transform," *Opt. Laser Technol.*, vol. 151, Jul. 2022, Art. no. 108071.

[33] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Rev.*, vol. 43, no. 1, pp. 129–159, Jan. 2001.

[34] H. Fang, S. A. Vorobyov, H. Jiang, and O. Taheri, "Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals," *IEEE Trans. Signal Process.*, vol. 62, no. 1, pp. 196–210, Jan. 2014.

[35] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

[36] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Opt. Lasers Eng.*, vol. 121, pp. 169–180, Oct. 2019.

[37] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, May 2017.

[38] Z. Bashir, M. G. A. Malik, M. Hussain, and N. Iqbal, "Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol," *Multimedia Tools Appl.*, vol. 81, no. 3, pp. 3867–3897, Jan. 2022.

[39] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Process.*, vol. 155, pp. 218–232, Feb. 2019.

[40] Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map," *Phys. Scripta*, vol. 95, no. 3, Mar. 2020, Art. no. 035223.

[41] Z. Gan, J. Bi, W. Ding, and X. Chai, "Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption," *Neural Comput. Appl.*, vol. 33, no. 19, pp. 12845–12867, Oct. 2021.

[42] X. Lv, X. Liao, and B. Yang, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28633–28663, Nov. 2018.

[43] Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Process., Image Commun.*, vol. 28, no. 3, pp. 292–300, Mar. 2013.

[44] J. Deng, S. Zhao, Y. Wang, L. Wang, H. Wang, and H. Sha, "Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 10097–10117, Apr. 2017.

[45] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform," *Opt. Commun.*, vol. 343, pp. 10–21, May 2015.

[46] H. Liu, Y. Xu, and C. Ma, "Chaos-based image hybrid encryption algorithm using key stretching and hash feedback," *Optik*, vol. 216, Aug. 2020, Art. no. 164925.

[47] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Comput. Appl.*, vol. 32, no. 9, pp. 4961–4988, May 2020.

[48] H. Zhu, C. Zhao, X. Zhang, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," *Optik*, vol. 125, no. 22, pp. 6672–6677, Nov. 2014.

[49] G. Ye, K. Jiao, and X. Huang, "Quantum logistic image encryption algorithm based on SHA-3 and RSA," *Nonlinear Dyn.*, vol. 104, no. 3, pp. 2807–2827, May 2021.

[50] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.

[51] Q. Liang and C. Zhu, "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding," *Opt. Laser Technol.*, vol. 160, May 2023, Art. no. 109033.

[52] Q. Zhang, J. Han, and Y. Ye, "Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding," *IET Image Process.*, vol. 15, no. 4, pp. 885–896, Mar. 2021.

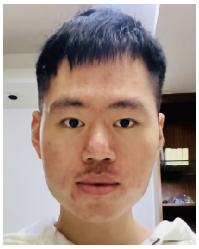
[53] Z. Chen and G. Ye, "An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing," *Optik*, vol. 267, Oct. 2022, Art. no. 169676.

[54] Z. Gan, X. Chai, J. Zhang, Y. Zhang, and Y. Chen, "An effective image compression–encryption scheme based on compressive sensing (CS) and game of life (GOL)," *Neural Comput. Appl.*, vol. 32, no. 17, pp. 14113–14141, Sep. 2020.

[55] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Jan. 2019.

[56] F. Musanna and S. Kumar, "A novel image encryption algorithm using chaotic compressive sensing and nonlinear exponential function," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102560.

**CHAOXIA ZHANG** received the Ph.D. degree in control theory and control engineering from Guangdong University of Technology, in 2011. In 2015, she was with the Information and Communication Engineering Postdoctoral Mobile Station, South China University of Technology. She is currently an Associate Professor with the School of Mechanical and Electrical Engineering and Automation, Foshan University. Her current research interests include ARM/DSP embedded system development, robot control, autonomous driving control, and image processing.



**SHANGZHOU ZHANG** received the bachelor's degree from the School of Mechanical and Electrical Engineering and Automation, Foshan University, in 2022, where he is currently pursuing the master's degree.

**KAIQI LIANG** received the bachelor's degree from the School of Mechanical and Electrical Engineering and Automation, Foshan University, in 2022, where he is currently pursuing the master's degree.

**ZHIHAO CHEN** is currently pursuing the master's degree with Foshan University of Science and Technology.