

CHAOS IMAGE ENCRYPTION BASED ON JOSEPHUS SCRAMBLING AND DNA DIFFUSION

RUIBIN XUE¹, JIANENG TANG^{2,*} AND ZEZONG ZHANG²

¹Fujian Torch Electron Technology Company Ltd.
No. 4, Zihua Road, Jiangnan Park of Hi-Tech Industrial Park, Quanzhou 362000, P. R. China
rbx_torch@163.com

²College of Engineering
Huaqiao University
No. 269, Chenghua North Road, Quanzhou 362021, P. R. China
zz_zhang@stu.hqu.edu.cn

*Corresponding author: jn_tang@hqu.edu.cn

Received September 2025; revised January 2026

ABSTRACT. *One-dimensional (1D) chaotic maps are broadly utilized for image encryption owing to their simple structure and the short time to generate chaotic sequences. However, in most of the existing 1D chaotic systems, there are some drawbacks, such as discrete chaotic intervals and narrow chaotic ranges. Therefore, to solve the key deficiency of these 1D chaotic maps, a novel 1D Chebyshev-Sine coupled map (1D-CSCM) with two parameters is developed in this paper. The 1D-CSCM couples the traditional Chebyshev map and Sine map, exhibiting superior chaotic performance compared to traditional chaotic maps. Performance evaluation of the 1D-CSCM shows that it exhibits more complex chaotic behaviors and wider continuous chaotic ranges. In addition, using the 1D-CSCM, we further design a novel chaos-based image encryption algorithm by combining Josephus scrambling and DNA diffusion. The Josephus scrambling approach originates from the classical Josephus problem, which is able to efficiently disrupt the target image's pixel positions. In addition, based on the proposed 1D-CSCM, we design a novel chaos-based image encryption algorithm that combines Josephus scrambling and DNA diffusion. Both processes are dynamically controlled by chaotic sequences, which significantly enhances the security and randomness of the encryption process. Experimental simulation results demonstrate that the designed encryption algorithm is able to effectively convert the target image into an unidentifiable noise-like image. The security test results suggest that the presented encryption algorithm can defend against common cryptanalytic attacks, including brute-force attacks, differential attacks, cropping attacks, and noise attacks, etc.*

Keywords: 1D-CSCM, Image encryption, Josephus scrambling, DNA diffusion

1. Introduction. With the fast development of network technology, it has become handier for people to use Internet technology to store and transmit information. Due to the richer and more intuitive characteristics of image information, digital images have become one of the most common information formats [16, 17]. However, it is because of the image information widely stored and transmitted on the Internet that more and more researchers are becoming concerned about the security of digital images. There are many characteristics about digital images, including large amounts of data, high correlation among neighbouring pixels, and strong redundancy [53]. Therefore, classical text-oriented

encryption methods, like advanced encryption standard (AES) and data encryption standard (DES), are less efficient when applied directly to image encryption [11]. Thus, it is necessary to design efficient image-oriented encryption methods.

Recently, a large number of image-oriented encryption methods using different techniques including DNA coding [35, 39, 41, 42], meta-cellular automata [15, 37], bit-plane decomposition [8, 33], compressive sensing [24, 45], elliptic curves [3, 13], P-Fibonacci transform [55], Fourier transform [7, 48], and chaotic systems [30, 46, 52], have been proposed by researchers. Chaotic systems have unpredictability, ergodicity, and initial sensitivity, which makes them very suitable for the design of cryptosystems [51]. Thus, among these techniques, the design of image encryption algorithms using chaotic systems has attracted the most extensive attention from researchers. Chaotic systems can be broadly divided into two categories: one-dimensional (1D) map and high-dimensional (HD) map. Due to the low implementation cost of 1D chaos, a quantity of image encryption algorithms using 1D chaos have been designed by researchers [1, 31]. However, traditional 1D chaotic maps, like Logistic map [21], Sine map [46], and Gaussian map [49], only exhibit chaotic behaviors within a small parameter range, and their chaotic intervals are discrete as the parameters change. Therefore, when using these chaotic maps to design encryption algorithms, the key space of the entire algorithm will be subject to certain constraints, which may affect the security of the whole algorithm [19]. Therefore, to enhance the performance of the encryption algorithm, it is essential to design some 1D chaotic maps with wider chaotic intervals.

As far as we know, many image encryption schemes designed by combining chaotic maps and other techniques have shown better encryption performances than those using only chaotic systems. For example, Xian et al. designed an image encryption algorithm with a permutation-diffusion structure. The permutation part of the algorithm uses the double parameters fractal sorting matrix (DPFSM) technique, and the diffusion operation is performed using chaotic sequences created by the Logistic map [44]. Singh et al. used DNA technology and chaotic maps to design an encryption algorithm for protecting Industrial Internet of Things (IIoT) digital images. In this algorithm, the chaotic sequences are used for image scrambling and selecting the DNA encoding rules involved in the diffusion module [27]. Jithin and Sankar devised a colour image encryption scheme that combines chaotic maps, DNA technology, and Mandelbrot sets [14]. Although experimental simulations and security tests have shown that the above algorithms show favorable encryption performance, they still have certain drawbacks. In [44], due to the periodicity of the DPFSM scrambling, it may affect the encryption effect under certain circumstances. In [14, 27], only the XOR operation about DNA technology is used in the algorithms, so the encryption performance of algorithms can be enhanced by introducing some other DNA operations.

The main contributions of this paper are summarized as follows.

- 1) A novel 1D Chebyshev-Sine chaotic map (1D-CSCM) is proposed. The 1D-CSCM is inspired by the investigation of the Chebyshev map and the Sine map. In order to enhance the key space of our designed encryption algorithm, two system parameters are designed in the newly proposed chaotic map. Chaotic performance analyses show that the 1D-CSCM exhibits more complex chaotic behaviors and wider control parameter intervals than some advanced 1D chaos.
- 2) A novel image encryption scheme based on the 1D-CSCM is proposed, which integrates multiple techniques, including Josephus scrambling and DNA diffusion. In the proposed algorithm, the sequences created by the 1D-CSCM are first used to determine the parameters related to Josephus scrambling in the scrambling module.

Then, some chaotic sequences are utilized to determine the DNA coding rules and the type of DNA operations in the DNA diffusion module.

- 3) We add the Hash function for updating the key of the algorithm by combining the target image information to resist the selective plaintext analysis attack. Simulation experiments and security analyses suggest that the presented image encryption scheme exhibits ideal performance and can withstand prevalent cryptanalysis attacks.

The remainder of the paper is structured as below. Section 2 presents the basic structure of the 1D-CSCM and its chaotic performance analysis results. Section 3 introduces the knowledge of the Josephus scrambling and the DNA coding technology. Section 4 provides a detailed explanation of the designed encryption algorithm. Section 5 performs simulation experiments and security analyses of the designed algorithm. Section 6 gives a brief conclusion.

2. 1D-CSCM. The Chebyshev map and Sine map are traditional chaotic maps. They exhibit limitations such as low Lyapunov exponent and discontinuous chaotic intervals, which restrict their applicability in practical scenarios. The Chebyshev map and Sine map are shown below:

$$x_{n+1} = \cos(\alpha \arccos(x_n)) \quad (1)$$

$$x_{n+1} = \alpha \sin(\pi x_n) \quad (2)$$

Thus, to address the above issues, we develop the 1D-CSCM by integrating the nonlinear structures of these maps and introducing two control parameters to regulate its performance. It can be represented by a simple mathematical equation as

$$x_{n+1} = a |\sin(\pi \arccos(bx_n))| \bmod 1 \quad (3)$$

where $a > 0$ and $b > 0$ are the two control parameters.

2.1. Bifurcation diagram. The bifurcation diagram reveals the variation in the number of stable points of the system as the system parameters change [22]. Scientific researcher can analyze chaotic behaviors of a nonlinear system by observing its bifurcation diagram [30]. The bifurcation diagrams of the Sine map and Chebyshev map are shown in Figures 1(a) and 1(b). It can be observed that the chaotic interval is discontinuous. In contrast, the bifurcation diagram of the 1D-CSCM with $b = 20$ is illustrated in Figure 1(c). As can be seen, the outputs are uniformly distributed in $[0, 1]$ for all intervals of the parameter a , indicating that the system exhibits good chaotic performance. The bifurcation diagram of the 1D-CSCM with $a = 20$ is displayed in Figure 1(d). As observed from the figure, when $b \in (0, 0.17)$, the system outputs are periodic, indicating that the system does not have chaotic behavior under this condition. However, when $b \geq 0.17$, the output of the system is randomly distributed within $[0, 1]$, which means that the 1D-CSCM has chaotic behaviors. The analysis results of bifurcation diagrams demonstrate that the 1D-CSCM has a wider chaotic interval.

2.2. Sensitivity analysis. One of the most significant features of chaotic systems is the initial value sensitivity. In other words, when a chaotic map is given two subtly different initial input values, the iterative outputs of the system will be distinctly different [20]. Generally, Lyapunov exponent (LE) can be applied to quantitatively evaluating chaotic behaviors of dynamical systems. Its calculation expression for a differentiable nonlinear system $x_{i+1} = f(x_i)$ is

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n |f'(x_i)| \quad (4)$$

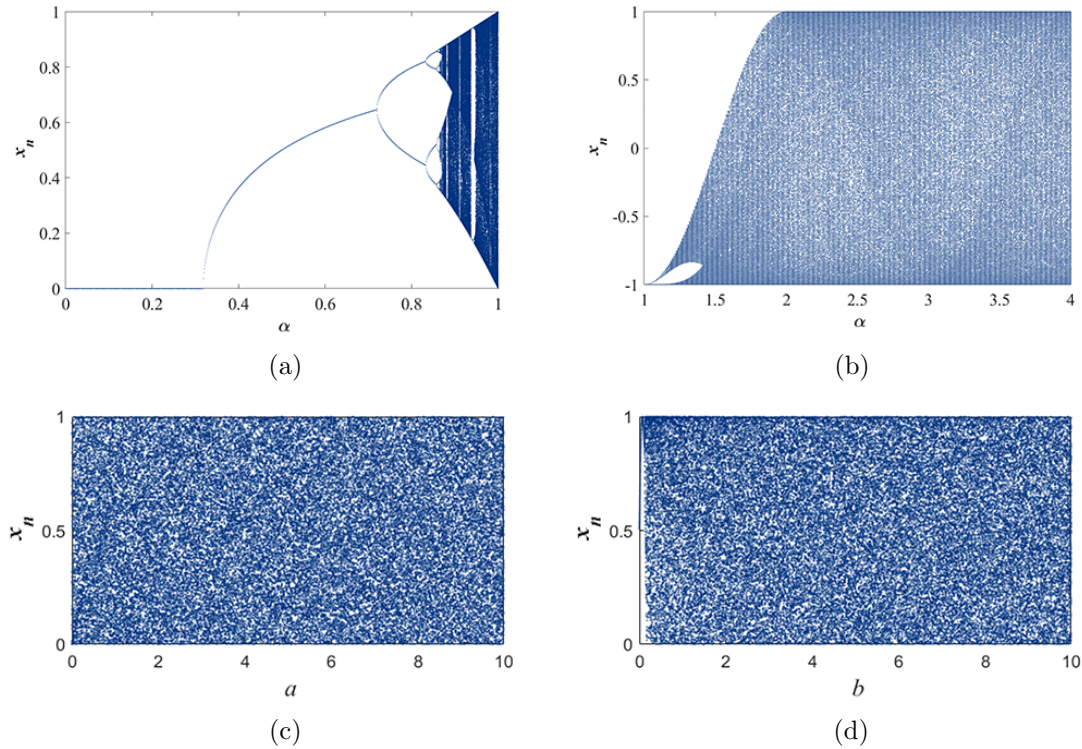


FIGURE 1. Bifurcation diagrams: (a) Sine map; (b) Chebyshev map; (c) 1D-CSCM with a ($b = 20$); (d) 1D-CSCM with b ($a = 20$)

A positive LE means that the adjacent trajectories of the system diverge exponentially during each iteration, gradually becoming two completely different trajectories as the number of iterations increases [12]. And a larger LE indicates a faster separation rate of the adjacent trajectories of the system, which also means that it has a stronger initial sensitivity. Therefore, when there is a positive LE for a nonlinear system, it can be regarded as a chaotic system. Meanwhile, a larger LE denotes the more complex chaotic behaviors of a system. Figure 2(a) and Figure 2(b) show the results of LE spectrum calculations for the 1D-CSCM. The results display that the system has positive LE values under the condition of $a > 0$ ($b = 20$) or $b \geq 0.17$ ($a = 20$), indicating that the 1D-CSCM has a wider range of chaotic intervals. In addition, to better investigate the chaotic performance of the 1D-CSCM, we calculated the LE spectra of different 1D maps. The mathematical expressions of the different chaotic maps, the 1D-DFCS [23], the 1D-DSP [20], and C-P map [56] are shown in Equations (5)-(7).

$$x_{n+1} = \frac{\cos((ax_n + 1)^2 + 1)}{\sin((ax_n + 1)^2 + 1) + 2} \quad (5)$$

$$x_{n+1} = (x_n(\alpha + 1))^{\sin(\beta\pi + x_n)} \quad (6)$$

$$x_{n+1} = \cos(b(x_n^3 + \pi x_n + \pi)) \quad (7)$$

Figure 2(a) and Figure 2(b) are comparison results of LE spectra. The results show that compared to the other 1D chaotic maps, the 1D-CSCM has larger LE values within most parameter ranges. In other words, the 1D-CSCM has more complex chaotic behaviors. In a word, the 1D-CSCM not only has wider chaotic intervals but also has more complex chaotic behaviors.

Furthermore, in Figure 3(a), we plot the difference in the system output sequences under different initial conditions with a difference of 10^{-5} . When $\{x_0, a, b\} = \{0.2, 30, 30\}$, the

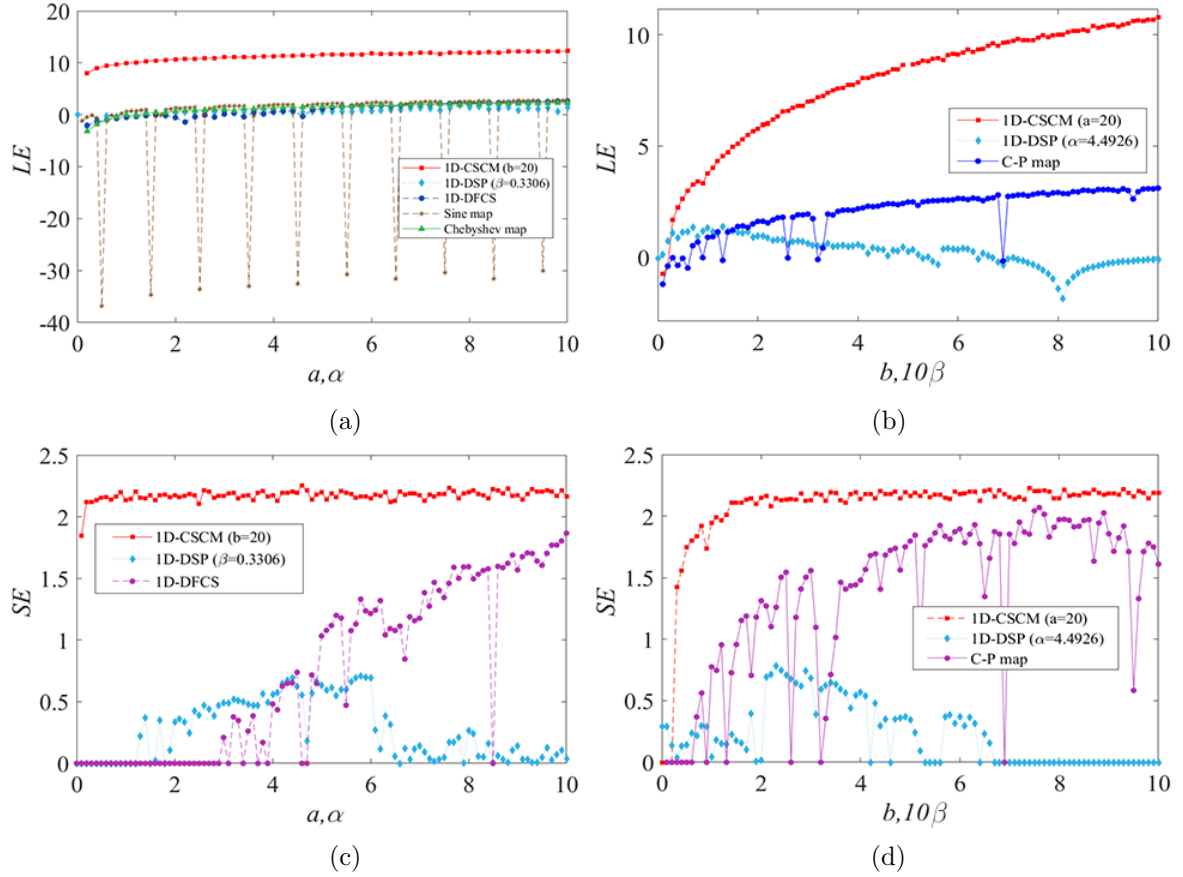


FIGURE 2. Comparison of LEs and SEs for different chaotic maps

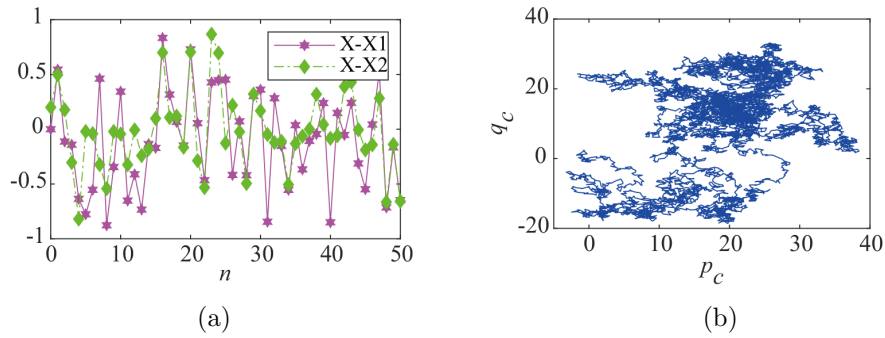


FIGURE 3. (a) Sensitivity test results; (b) 0-1 test results

output trajectory of the system is X . The output trajectory of the system is $X1$ when $\{x_0, a, b\} = \{0.2 + 10^{-5}, 30, 30\}$. And the output trajectory of the system is $X2$ when $\{x_0, a, b\} = \{0.2, 30 + 10^{-5}, 30 + 10^{-5}\}$. The results show that even if the initial conditions of the 1D-CSCM are slightly altered, the system output trajectory will become completely different. It is further indicated that the 1D-CSCM is supremely responsive to the initial condition.

2.3. Sample entropy analysis. Sample entropy (SE) is available to assess the complexity and regularity of time sequences data [26]. When a time series has a large SE, it indicates that the regularity of the time sequences is low. Therefore, if the SE is used to evaluate the complexity and regularity of time sequences generated by chaotic maps, larger SEs show that chaotic systems have more complex behaviors [12].

The SEs of the 1D-CSCM and the other three 1D chaotic maps are illustrated in Figures 2(c) and 2(d). It can be shown that the 1D-CSCM always has a larger SE value compared to the other chaotic maps when $a > 0$ ($\alpha > 0$) or $b > 0.6$ ($10\beta > 0.6$). Therefore, the results suggest that the 1D-CSCM exhibits more complex chaotic behaviors than the other chaotic maps.

2.4. 0-1 test analysis. The 0-1 test can determine whether a deterministic dynamic system is periodic or chaotic dynamics [9]. It is different from analyzing the maximum LE of the system. It does not need a phase space reconstruction of the system but directly analyzes the time sequences produced by the system. Therefore, it can be used for almost all deterministic dynamic systems [25]. For regular dynamic systems, the 0-1 test results are always bounded. However, the 0-1 test outcomes of chaotic dynamic systems are similar to Brownian motion and unbounded [9, 53]. In the 0-1 test experiment, we set the initial condition as $\{x_0, a, b\} = \{0.4, 20, 20\}$, and the detailed calculation approach is presented in [9]. Figure 3(b) illustrates the 0-1 test results of the 1D-CSCM. As we can see, trajectories obtained from the 0-1 test are unbounded and resemble Brownian motion, suggesting that the 1D-CSCM is a chaotic system.

3. Josephus and DNA. This section introduces the Josephus scrambling and the DNA encoding techniques, and explains their application in image encryption algorithms.

3.1. Josephus scrambling. The Josephus scrambling comes from a Josephus sequence generated by the classical Josephus problem [10]. The process of generating the Josephus sequence can be simply described as the following process. Suppose a ring has some elements placed on it. First, a specified element is selected and removed from the ring as the first removed element. Then, the position of the first removed element in the ring is used as the next start position, and then the next specified element is selected as the second removed element after a preset step value. Repeat the above operation until all elements on the ring are removed. Finally, all the elements taken down are arranged sequentially to generate a Josephus sequence. In the Josephus scrambling, the elements of a target sequence are taken as elements in the ring. Then the obtained Josephus sequence is the scrambled target sequence. The mathematical expression for the scrambling can be expressed as

$$S = Jos(T, m, n) \quad (8)$$

where T is a target sequence and S is the scrambled target sequence. The first specified element starting position is $m + n - 1$ and n is the preset step value. To better illustrate the entire scrambling process, a simple Josephus scrambling example is shown in Figure 4.

3.2. DNA encoding technology. DNA-based image encryption technology is to encode pixels with nucleic acid bases. Then new encoded nucleic acid bases are obtained by various DNA operations. Finally, these newly encoded nucleic acid bases are decoded to obtain the pixels of encrypted images [47]. There are four different nucleic acid bases in DNA, namely Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) [32]. In general, DNA coding is the use of two binary, such as 00, 01, 10, and 11, to represent each base. Therefore, there are 24 coding rules for DNA. However, only eight coding rules meet the Watson-Crick basic pairing rules [40], as listed in Table 1. Thus, we only consider these eight DNA encoding rules to design DNA-based image encryption algorithms. For example, the binary encoding of pixel value 198 is $(11000110)_2$, which can be encoded as 'TACG' using rule 1 in Table 1. Furthermore, we use three different DNA operations, including the DNA XOR, the DNA addition, and the DNA subtraction, to devise an image encryption

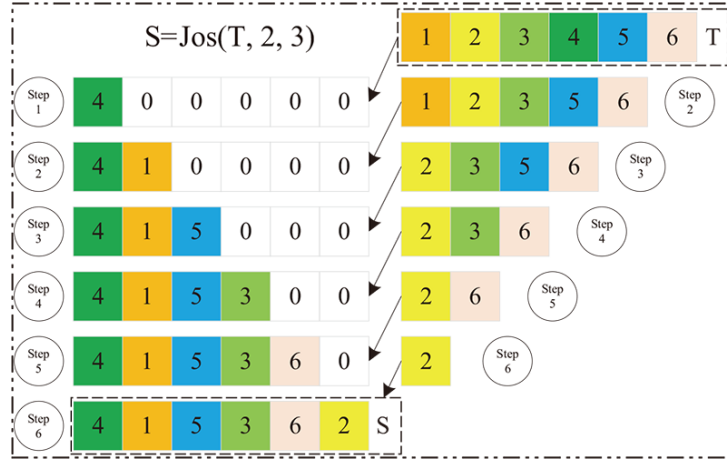


FIGURE 4. A simple example of the Josephus scrambling

TABLE 1. DNA encoding rules

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

TABLE 2. Different DNA operations with rule 1

$\oplus$	A	T	C	G	+	A	T	C	G	-	A	T	C	G
A	A	T	C	G	A	A	T	C	G	A	A	T	C	G
T	T	A	G	C	T	T	G	A	C	T	C	A	G	T
C	C	G	A	T	C	C	A	G	T	C	T	G	A	C
G	G	C	T	A	G	G	C	T	A	G	G	C	T	A

scheme. Since the result of each operation is different under different coding rules, we take rule 1 as an example and list the results of the corresponding operations in Table 2.

4. Designed Encryption Algorithm. In this part, we will elaborate on the image encryption algorithm. There are four modules in the algorithm, including the Key sequence generation module, the Josephus scrambling module, and the DNA row (column) diffusion module. Figure 5 illustrates the flowsheet of the algorithm. To explain the whole encryption process in detail, we consider that the size of the original target image is $M \times N$. The detailed steps for each module are as follows.

4.1. Key sequence generation. To enhance the algorithm's immunity to selective plaintext analysis attacks, the Hash (SHA-512) function is introduced for updating the initial key. The target image is taken as the input of the SHA-512 to generate a 512-bit hash string H , and then every 4-bit hash value is sequentially converted to a decimal number h_i .

$$h_i = \text{bin2dec}(H(4i - 3 : 4i)), \quad i = 1, 2, \dots, 128 \quad (9)$$

where $\text{bin2dec}(x)$ represents the transformation of a binary number x to a decimal number and $H(v : w)$ means to take the v -th to w -th bit of H as a new binary number.

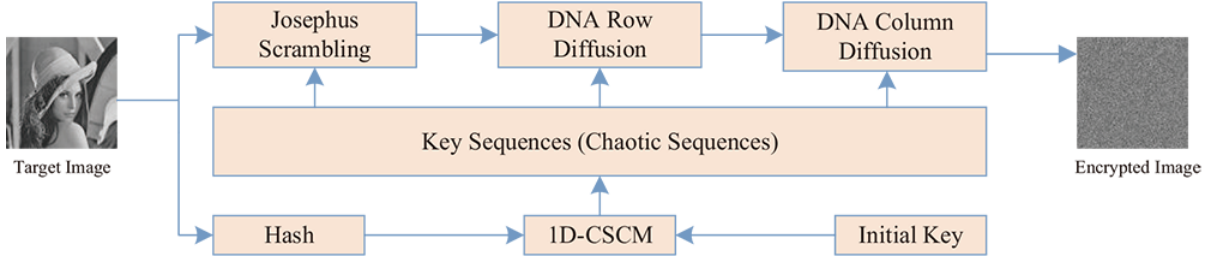


FIGURE 5. The encryption structure of the proposed image encryption algorithm

Here, we set the initial key of the encryption algorithm to $\{x_0 = 0.4, a_0 = 20, b_0 = 20\}$. And the key updated with the hash value is $\{x_1, a, b\}$, as shown in Equation (10).

$$\left\{ \begin{array}{l} x_1 = \text{mod}(\text{sum}(h_1, h_2, \dots, h_{32})/480 + x_0, 1) \\ a = \begin{cases} \text{if } \text{sum}(h_{65}, h_{66}, \dots, h_{96}) = 0 \\ \frac{\text{sum}(h_{33}, h_{34}, \dots, h_{64})}{\text{sum}(h_{65}, h_{66}, \dots, h_{96}) + 1} + a_0 \\ \text{else} \\ \frac{\text{sum}(h_{33}, h_{34}, \dots, h_{64})}{\text{sum}(h_{65}, h_{66}, \dots, h_{96})} + a_0 \end{cases} \\ b = \begin{cases} \text{if } \text{sum}(h_1, h_2, \dots, h_{32}) = 0 \\ \frac{\text{sum}(h_{97}, h_{98}, \dots, h_{128})}{\text{sum}(h_1, h_2, \dots, h_{32}) + 1} + b_0 \\ \text{else} \\ \frac{\text{sum}(h_{97}, h_{98}, \dots, h_{128})}{\text{sum}(h_1, h_2, \dots, h_{32})} + b_0 \end{cases} \\ Q = \text{sum}(h_1, h_2, \dots, h_{128}) + 100 \end{array} \right. \quad (10)$$

where $\text{sum}(h_1, h_2)$ denotes the sum of h_1 and h_2 and $\text{mod}()$ means the modulo operation. Q is the number of elements in a chaotic sequence, which are discarded to prevent transient effects [25].

To obtain the Key sequences, we first use the updated key as the initial condition of the 1D-CSCM. Then we iterate the 1D-CSCM $Q + 4q$ times and discard the first Q elements to obtain the sequence $X = \{x_{Q+1}, x_{Q+2}, \dots, x_{Q+4q}\}$, where $q = \max\{M, N\}$. Here, M and N represent the size of the target image. Finally, the Key sequences are obtained based on the sequence X as shown in Algorithm 1. The $\text{floor}(\bullet)$ means that each element of the $\bullet$ is rounded to the closest integer smaller than or equal to that element.

4.2. Josephus scrambling. An image encryption algorithm should have the ability to reduce the correlation between neighbouring pixels of the target image. Here, we use the Josephus scrambling to achieve the goal of breaking the correlation among neighboring pixels of the target image. According to the discussion in Section 3, the Josephus scrambling is mainly used for the change of element positions of 1D arrays. Therefore, it is necessary to convert the 2D image matrix into a 1D array before performing the Josephus scrambling. Here, we turn the image into a 1D array using the order of values taken from the outermost circle to the innermost circle of the image I . The following are the detailed steps.

Algorithm 1 Key sequences generation**Input:** X **Output:** $A, B, D, A1, C1, D1, E1$

- 1: $n1 = \min\{M, N\}$
- 2: $A = \text{mod}(\text{floor}(X(1 : 2) \times 10^9), 10) + 1$
- 3: $B = \text{mod}(\text{floor}(X(1 : \text{floor}(n1/2)) \times 10^{10}), 2n1) + 1$
- 4: $D = \text{mod}(\text{floor}(X(1 : \text{floor}(n1/2)) \times 10^{12}), 2n1) + 1$
- 5: $A1 = \text{mod}(\text{floor}(X(1 : 4N) \times 10^9), 8) + 1$
- 6: $C1 = \text{mod}(\text{floor}(X(1 : M) \times 10^{10}), 8) + 1$
- 7: $D1 = \text{mod}(\text{floor}(X(1 : N) \times 10^{12}), 256)$
- 8: $E1 = \text{mod}(\text{floor}(X(1 : M) \times 10^{10}), 256)$

Step 1: For the i -th circle of the image matrix I , the direction of taking pixels is determined according to the Key sequence value $B(i)$. When $B(i)$ is an even number, the pixel values are taken in a clockwise direction. Otherwise, the pixel values are taken in a counterclockwise direction. Finally, arrange the extracted pixel values into a 1D array $I1$.

Step 2: Josephus scrambling is performed on the 1D array $I1$ to obtain a new 1D sequence $I11$, where the scrambling parameters m and n are determined by the sequences B and A , respectively. Finally, $I11$ is transformed into a 2D matrix in row-first order to get the first permuted image matrix $Z1$. The simple procedure is denoted as Equations (11) and (12).

$$I11 = \text{Jos}(I1, B(\text{floor}(n1/2)), A(1)) \quad (11)$$

$$Z1 = \text{reshape}(I11, [M, N]) \quad (12)$$

Step 3: Perform Josephus scrambling again in a similar way as in steps 1 and 2. For the i -th circle of the matrix $Z1$, the direction of taking pixel values is determined according to the Key sequence value $D(i)$. When $D(i)$ is an even number, the pixel values are taken in a clockwise direction. Otherwise, the pixel values are taken in a counterclockwise direction. Finally, arrange the extracted pixel values into a 1D array $I2$.

Step 4: Josephus scrambling is performed on the 1D array $I2$ to obtain a new 1D sequence $I22$, where the scrambling parameters m and n are determined by the sequences D and A , respectively. Finally, $I22$ is converted into a 2D matrix in row-first order to obtain the first permuted image matrix Z . The simple procedure is expressed as Equations (13) and (14).

$$I22 = \text{Jos}(I2, D(\text{floor}(n1/2)), A(2)) \quad (13)$$

$$Z = \text{reshape}(I22, [M, N]) \quad (14)$$

To better illustrate the Josephus scrambling process, a simple example is displayed in Figure 6.

4.3. DNA diffusion. Josephus scrambling merely changes the pixel positions and does not modify the statistical properties of the image pixels. Thus, to enhance the capability of the encryption algorithm to withstand statistical analysis attacks, DNA-based diffusion operations are introduced into the designed encryption algorithm. Here, DNA diffusion is separated into two main parts: row diffusion and column diffusion.

4.3.1. Row diffusion.

Step 1: Following the discussion of DNA encoding technology in Section 3, the image

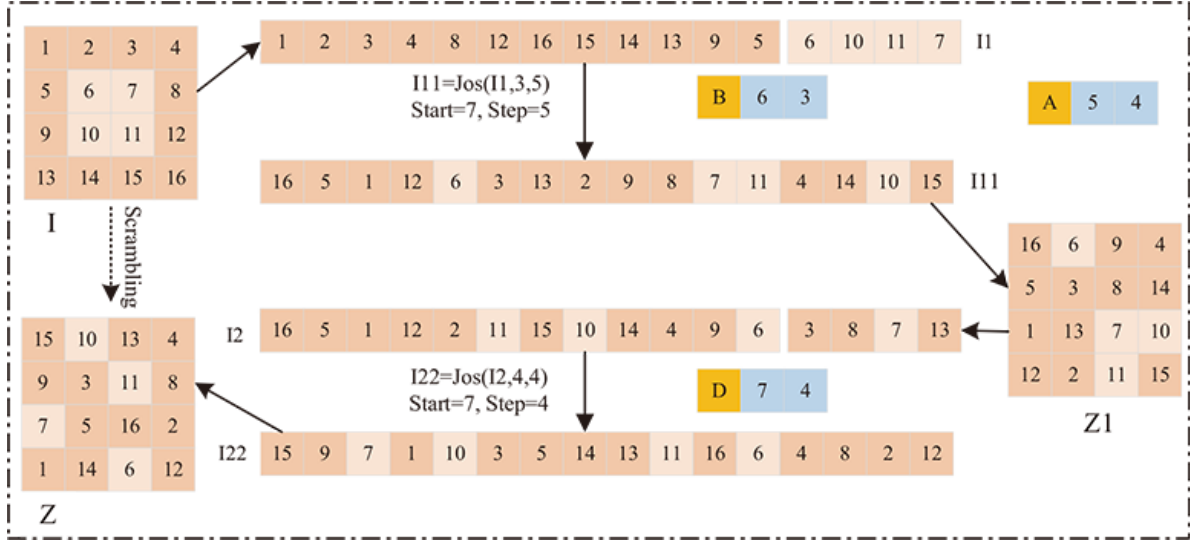


FIGURE 6. An example of the Josephus scrambling

matrix Z is encoded as a DNA matrix DZ , where the encoding rule for each row is decided by the Key sequence $A1$, as shown in Equation (15).

$$DZ(i, :) = DNACode(Z(i, :), A1(i)), \quad i = 1, 2, \dots, M \quad (15)$$

The $DNACode(V, c)$ denotes that the elements in V are encoded as DNA sequences by the encoding rule c .

Step 2: Use encoding rule $A1(1)$ to perform DNA encoding operation on the Key sequence $D1$, as in Equation (16).

$$DD1 = DNACode(D1, A1(1)) \quad (16)$$

Step 3: The row diffusion operation is implemented on DZ using the DNA XOR operation combined with $DD1$. The detailed operation process is given in Algorithm 2 and a simple example is shown in Figure 7. The $optx(V, W, c)$ means that the DNA XOR operations are performed on elements in V and W by rule c .

Algorithm 2 Row diffusion

Input: $DZ, DD1$

Output: $DZ1$

- 1: $DZ1(1, :) = optx(DZ(1, :), DD1, C1(1))$
 - 2: **for** $i = 2 : M$ **do**
 - 3: $DZ1(i, :) = optx(DZ(i, :), DZ1(i - 1, :), C1(i))$
 - 4: **end for**
-

4.3.2. *Column diffusion.* In the subsection, column diffusion is performed to increase the security of the algorithm.

Step 1: Use encoding rule $A1(4N)$ to perform DNA encoding operation on the Key sequence $E1$, as in Equation (17).

$$DE1 = DNACode(E1, A1(4N)) \quad (17)$$

Step 2: The column diffusion operation is performed on $DZ1$ using DNA addition and subtraction operations combined with $DE1$ and $A1$. Here $A1$ is used for the dynamic selection of DNA operations. When $A1(i)$ is even, we perform the DNA addition operation on the i -th column. Otherwise, the DNA subtraction operation is performed. Algorithm 3

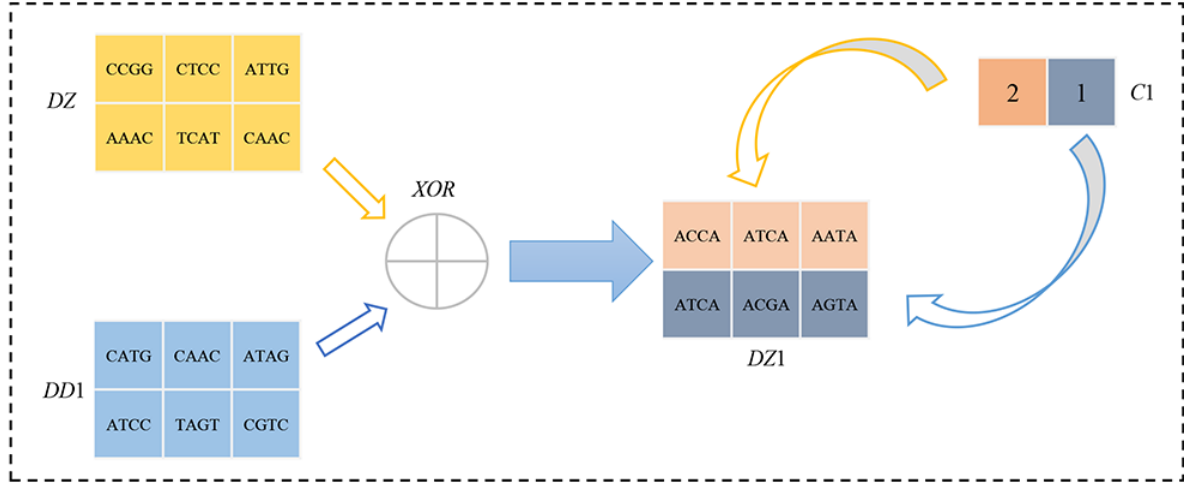


FIGURE 7. An example of the row diffusion operation

Algorithm 3 Column diffusion

Input: $DZ1, DE1$
Output: $DZ2$

```

1: if mod( $A1(1), 2$ ) == 0 then
2:    $DZ2(:, 1) = opta(DZ1(:, 1), DE1(1 : M), A1(1))$ 
3: else
4:    $DZ2(:, 1) = opts(DZ1(:, 1), DE1(1 : M), A1(1))$ 
5: end if
6: for  $j = 2 : 4N$  do
7:   if mod( $A1(j), 2$ ) == 0 then
8:      $DZ2(:, j) = opta(DZ1(:, j), DZ2(:, j - 1), A1(j))$ 
9:   else
10:     $DZ2(:, j) = opts(DZ1(:, j), DZ2(:, j - 1), A1(j))$ 
11:   end if
12: end for

```

provides a specific operational procedure. Figure 8 shows a simple procedure of the column diffusion. And the $opta(V, W, c)$ indicates that DNA addition is performed on the elements in V and W , and the addition operation under coding rule c is selected. Meanwhile, $opts(V, W, c)$ denotes the DNA subtraction operation under rule c , where the element in V is the minuend and the element in W is the subtrahend.

Step 3: The DNA matrix $DZ2$ is decoded to get the final encrypted image ENC , as in Equation (18).

$$\begin{cases} ENC(i, :) = DNAdcode(DZ2(i, :), C1(i)) \\ i = 1, 2, \dots, M \end{cases} \quad (18)$$

The $DNAdcode(V, c)$ denotes that the elements in V are decoded into numerical sequences by the decoding (encoding) rule c .

4.4. Decryption algorithm. Due to the fact that the designed image encryption algorithm belongs to a symmetric cryptographic algorithm, the decryption procedure and encryption procedure are reciprocal operations. Therefore, the decryption algorithm is not explained in detail.

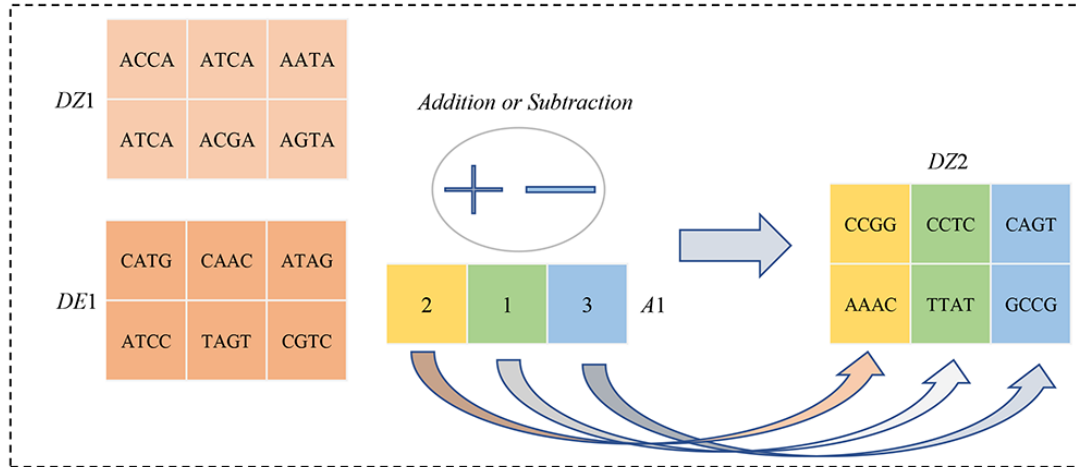


FIGURE 8. An example of the column diffusion operation

5. Simulation Experiments and Safety Analyses. In this chapter, we have performed simulation experiments and safety analysis experiments on the designed image encryption algorithm using the MATLAB R2022b software platform with Windows 10 environment. The processor used for the experiments is Intel (R) Core (TM) i5-7200 CPU @ 2.50 GHz. The images used in the experiments include 512×512 Lena, $256 \times 256 \times 3$ Lena, and a few images from the USC-SIPI database¹.

5.1. Simulation experiments. The simulation experimental results of the designed algorithm are depicted in Figure 9. As can be seen from the figure, the encrypted images are noise-like images from which no information about the plain image can be acquired. At the same time, the decrypted images are the same as the plain images, suggesting that the designed encryption algorithm is able to reach the desired visual encryption effect.

5.2. Safety analyses.

5.2.1. Key analysis. An optimal encryption scheme is supposed to have a larger key space for better withstanding brute force analysis attacks [2]. According to Equation (9), the key of the designed algorithm mainly consists of four parts, namely x_1 , a , b , and Q . Based on the discussion of chaotic systems in Section 2, we can conclude that the a can be taken in the range $(0, \infty)$ and the b can be taken in the range $(0.17, \infty)$. Thus, the key space is sufficiently large [36], which implies that the algorithm can well withstand brute-force analysis attacks.

Moreover, the key sensitivity is also one of the significant factors that affect encryption algorithms' ability to withstand various key analysis attacks. Therefore, we explain the key sensitivity in the encryption procedure by comparing the encryption results of different keys (with a slight difference) encrypting the same target image. First, we encrypt the target Lena image utilizing the key K . Figure 10(a) illustrates the encrypted image. Then, the target Lena image is encrypted utilizing the key $K1 = \{x_0 = 0.4 + 10^{-10}, a_0 = 20, b_0 = 20\}$, as shown in Figure 10(b). Finally, Figures 10(c) and 10(f) show the differences between Figure 10(a) and Figure 10(b). The results show that the two encrypted images are completely different, implying that the key of the proposed algorithm exhibits strong encryption sensitivity. In addition, similar test approaches are used to evaluate the key sensitivity in the decryption process. Figures 10(d) and 10(e) are the analysis results, where only the correct key can generate the original target image, and a minor variation

¹<http://sipi.usc.edu/database/>

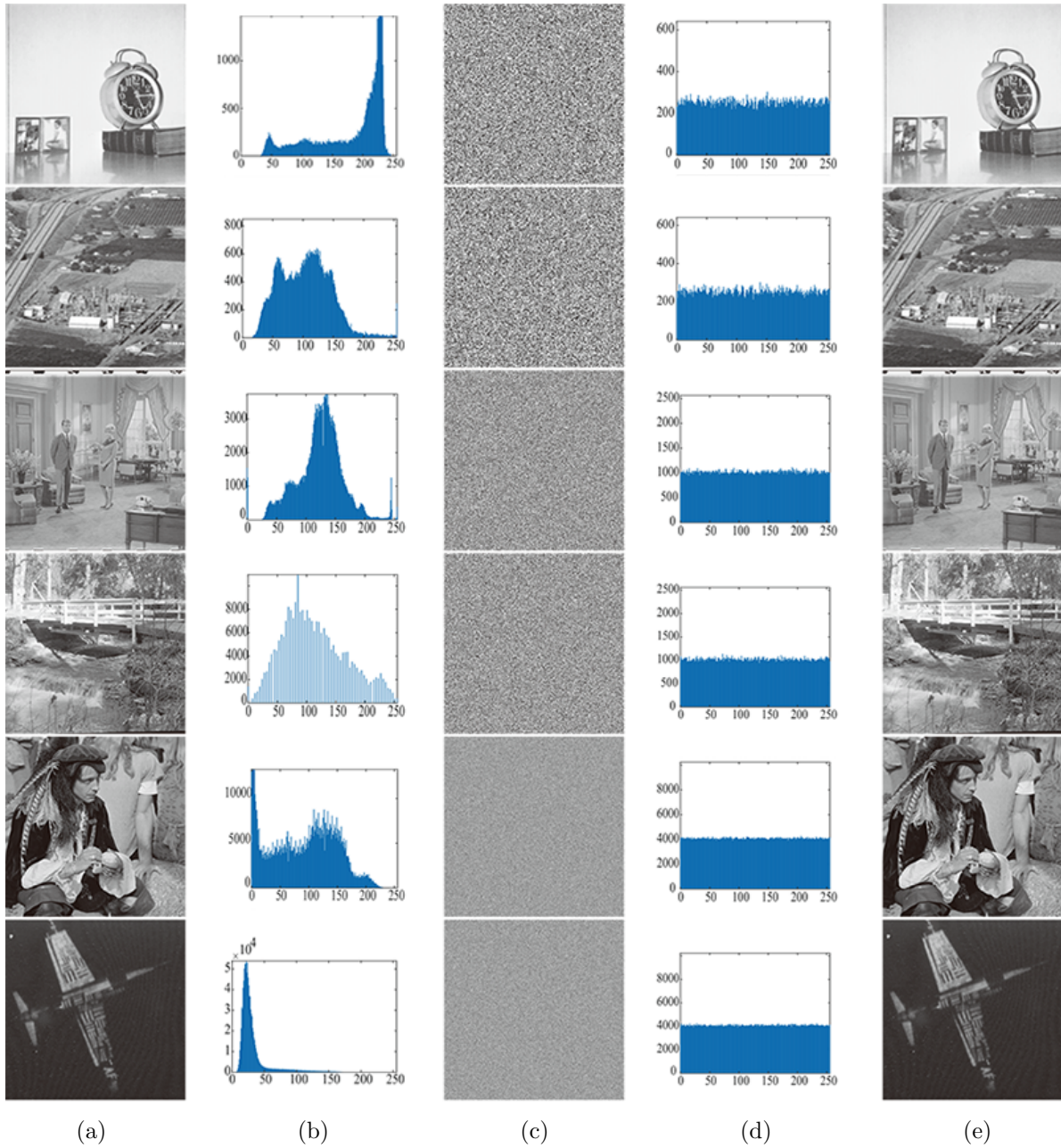


FIGURE 9. Simulation experimental results: (a) Target images; (b) histograms of the target images; (c) encryption images; (d) histograms of the encryption images; (e) decryption images

in the key will result in decryption failure. Thus, the proposed algorithm is extremely sensitive to the key.

5.2.2. Histogram analysis. The histogram gives statistical information about all pixels in an image. In other words, hackers can obtain information about the pixel distribution from the histogram [46]. Therefore, to prevent hackers from getting any relevant information about a target image, the histogram of an encrypted image acquired by an excellent encryption algorithm ought to be as flat as possible. Figure 9(b) displays the histograms of the original target images. Meanwhile, Figure 9(d) shows the histograms of the encryption images. The results show that the histograms of the encrypted images are flat, demonstrating that the hacker cannot get any relevant information about the original target

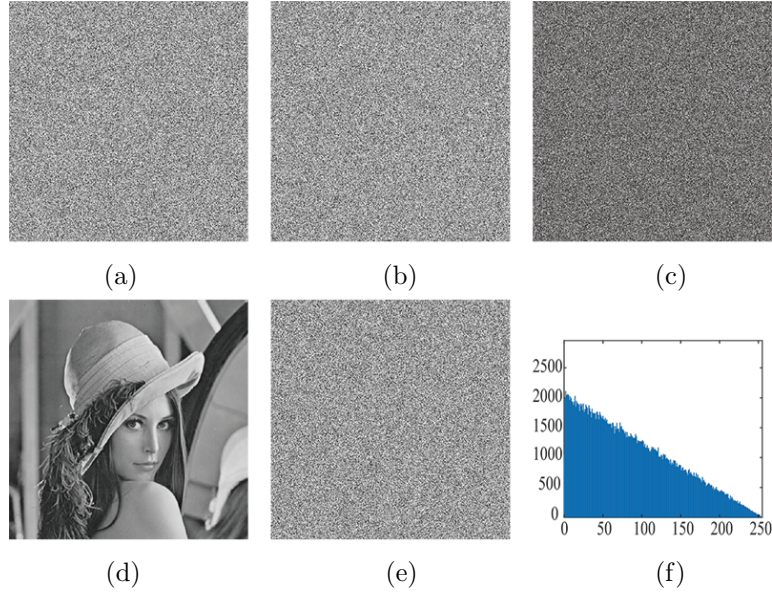


FIGURE 10. Key sensitivity testing: (a) Encryption image by K ; (b) encryption image by $K1$; (c) $|\text{Figure 10(a)} - \text{Figure 10(b)}|$; (d) decryption image of Figure 10(a) by K ; (e) decryption image of Figure 10(a) by $K1$; (f) histogram of Figure 10(c)

images from the histograms. In addition, to observe the pixel distribution of the images more rigorously, the chi-square (χ^2) test is used for quantitatively evaluating whether the histograms of the images are flat [34]. The formula of the χ^2 test is

$$\chi^2 = \sum_{r=0}^{255} \frac{(p_r - p)^2}{p} \quad (19)$$

where p_r denotes the occurrence's frequency of pixel value r and $p = MN/256$. When $\chi^2_{0.05} \leq 293.2478$, it indicates that the histogram is uniform. The χ^2 test results for different images are listed in Table 3. As can be seen, the χ^2 values are less than 263, indicating that the histograms of the encrypted images are flat. As a result, the experimental results demonstrate that our encryption algorithm exhibits the desired encryption performance.

TABLE 3. The results of the chi-square tests

Size	Image	χ^2
256×256	5.1.12	247.1641
	5.1.14	248.6875
512×512	5.2.08	238.8906
	5.2.10	262.1328
1024×1024	5.3.01	244.3179
	7.2.01	260.0942

5.2.3. *Information entropy analysis.* Information entropy (IE) can represent the degree of image pixels confusion [34]. Its mathematical formula is

$$IE = - \sum_{i=0}^{2^k-1} f(x_i) \log_2 f(x_i) \quad (20)$$

where $f(x_i)$ denotes the probability that the image pixel value x_i appears in an image, and k is the pixel depth of an image. IE has a maximum value k when each pixel has an equal probability of appearance in an image. The greater IE of an image, the more uniform distribution of image pixels. For an encryption algorithm, a larger IE suggests a higher degree of image pixels confusion, which also means that the encrypted image is more secure [11]. For a digital image with an 8-bit pixel depth, the maximum IE value is eight. Table 4 enumerates the IE calculation results of the original target image and the corresponding encrypted image. It can be noted that the IEs of the encrypted images are all approach to the maximum value, demonstrating that the designed encryption algorithm has a desirable encryption effect.

TABLE 4. The results of the information entropy analysis

Size	Image	Information entropy	
		Plain	Cipher
256×256	5.1.12	6.7057	7.99727
	5.1.14	7.3424	7.99726
512×512	5.2.08	7.2010	7.99934
	5.2.10	5.7056	7.99928
1024×1024	5.3.01	7.5237	7.99983
	7.2.01	5.6415	7.99982

5.2.4. Correlation analysis. A natural image has a significant correlation among adjacent pixels [6]. To prevent hackers from analyzing image pixel information by this property, breaking the correlation among adjacent pixels is a necessary capability for encryption algorithms. To observe the change of correlation among adjacent pixels of the Lena image before and after encryption, we randomly select 5000 pairs of pixel values in three directions of the Lena image, and their distributions are illustrated in Figure 11. The results show that among the pixels of the Lena image have a significant correlation, while there is little correlation among the pixels of the encrypted Lena image. Moreover, using the correlation coefficient (CC) quantifies the correlation among adjacent pixels, and its calculation formula is shown in Equation (21).

$$CC_{GU} = \frac{1/L \sum_{i=1}^L (g_i - E(G))(u_i - E(U))}{\sqrt{1/L \sum_{i=1}^L (g_i - E(G))^2} \sqrt{1/L \sum_{i=1}^L (u_i - E(U))^2}} \quad (21)$$

$E(\Phi)$ denotes the mathematical expectation of the sequence Φ . A lower CC_{GU} indicates a weaker correlation between sequences G and U . Table 5 lists the CCs among neighbouring pixels before and after encryption of different target images. As we can see, the CCs of the encrypted images are all approaching 0, indicating that the pixels of the encrypted images are uniformly distributed with little correlation. Thus, the designed encryption scheme can significantly reduce the correlation among the target image pixels.

5.2.5. Differential attack analysis. The differential attack is a popular method of cryptanalysis used by attackers. The hacker first encrypts two target images with very minor differences to obtain two encrypted images. Then, they hope to break the encryption algorithm by analyzing the connection and difference between the two encrypted images. Therefore, a superior encryption algorithm should be highly sensitive to the target image for withstanding differential attacks.

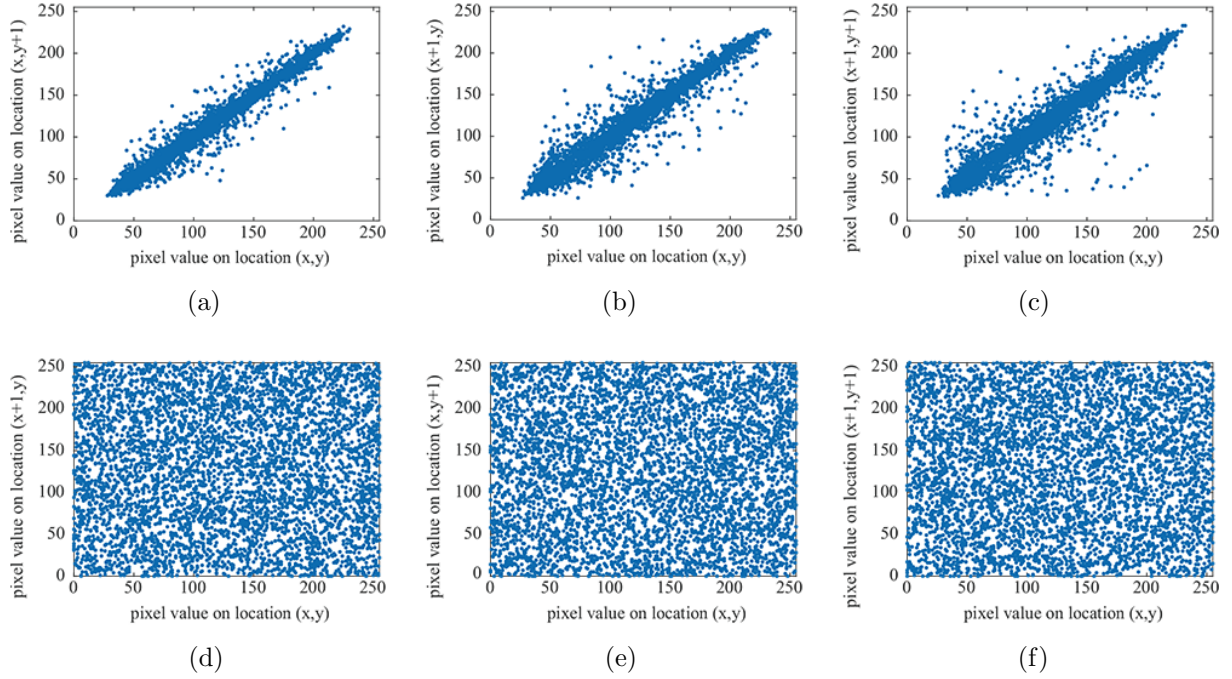


FIGURE 11. Correlation analysis (512×512 Lena image): (a) Horizontal, (b) vertical, (c) diagonal; Correlation analysis (encrypted 512×512 Lena image): (d) horizontal, (e) vertical, (f) diagonal

TABLE 5. The results of the correlation analysis

Size	Image	Plain image			Encrypted image		
		H	V	D	H	V	D
256×256	5.1.12	0.9540	0.9734	0.9376	0.0011	-0.0034	-0.0029
	5.1.14	0.9441	0.8900	0.8691	-0.0005	-0.0020	0.00007
512×512	5.2.08	0.9355	0.8780	0.8550	-0.0030	-0.0019	0.0009
	5.2.10	0.9388	0.9217	0.8988	0.0041	0.0001	-0.0024
1024×1024	5.3.01	0.9769	0.9804	0.9669	0.0004	-0.0015	0.00005
	7.2.01	0.9674	0.9458	0.9442	-0.0007	0.0011	-0.0016

Here, we use two indicators, the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) [43], to quantitatively assess the capacity of the proposed algorithm to withstand differential attacks. Their formulae are as follows:

$$\begin{cases} H(i, j) = \begin{cases} 1, & H_1(i, j) \neq H_2(i, j) \\ 0, & H_1(i, j) = H_2(i, j) \end{cases} \\ NPCR = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N H(i, j) \times 100\% \end{cases} \quad (22)$$

$$UACI = \frac{\sum_{i=1}^M \sum_{j=1}^N |H_1(i, j) - H_2(i, j)|}{255 \times M \times N} \times 100\% \quad (23)$$

where H_1 and H_2 are two digital images of size $M \times N$, and they are derived from encrypting two target images that differ by only one bit. According to the discussion in [43], the pass criteria for the NPCR and the UACI of different-size images are shown

TABLE 6. The pass criteria for NPCR and UACI

Size	NPCR (%)			UACI (%)		
	$N_{0.05}^*$	$N_{0.01}^*$	$N_{0.001}^*$	$(U_{0.05}^{*-}, U_{0.05}^{*+})$	$(U_{0.01}^{*-}, U_{0.01}^{*+})$	$(U_{0.001}^{*-}, U_{0.001}^{*+})$
256×256	99.5693	99.5527	99.5341	(33.2824, 33.6447)	(33.2255, 33.7016)	(33.1594, 33.7677)
512×512	99.5893	99.5810	99.5717	(33.3730, 33.5541)	(33.3445, 33.5826)	(33.3115, 33.6156)
1024×1024	99.5994	99.5952	99.5906	(33.4183, 33.5088)	(33.4040, 33.5231)	(33.3875, 33.5396)

TABLE 7. The test results for NPCR and UACI

Size	Image	NPCR (%)	UACI (%)
256×256	5.1.12	99.6126709	33.4829744
	5.1.14	99.6108398	33.4534760
512×512	5.2.08	99.6080208	33.4565632
	5.2.10	99.6085968	33.4629929
1024×1024	5.3.01	99.6104088	33.4639839
	7.2.01	99.6101332	33.4639422

in Table 6. An image encryption algorithm is able to resist differential attacks when $NPCR > N^*$ and $UACI \in (U^{*-}, U^{*+})$.

The test results of the NPCR and the UACI for different images are listed in Table 7. To avoid accidental results, the data in Table 7 are the average results of 100 randomly conducted experiments. The results suggest that the NPCR (UACI) of all images is within the acceptable criteria and is very approaching the theoretical value of 99.6094% (33.4635%) [34]. Thus, the results suggest that the designed encryption scheme can withstand differential attacks.

5.2.6. Analysis of noise attacks and cropping attacks. Encrypted images are susceptible to noise pollution in the channel when they are transmitted over the Internet [28]. To appraise the capacity of the designed algorithm to withstand noise pollution, we have added different levels of salt & pepper noise to the encrypted images. Figure 12 displays decrypted images of different noisy encrypted images. As we can see, the decrypted image can show the general information of the original image, suggesting that the designed algorithm has a certain ability to withstand noise pollution.

In addition, there is occasionally a partial loss of image information during network transmission. Therefore, to appraise the capacity of the designed algorithm to withstand partial data loss, we first set some pixel values of encrypted images to 0 to imitate data loss. Then, the incomplete encrypted images are decrypted using the correct key, as illustrated in Figure 12. The outcomes demonstrate that even though half of the encrypted image pixel information is lost, its decrypted image remains recognizable. Additionally, to better evaluate the resistance of the proposed algorithm against noise attacks and cropping attacks, we select peak signal-to-noise ratio (PSNR) to measure the quality of the original image and the decrypted image. The PSNR is as follows:

$$\text{PSNR} = 10 \lg \frac{M \times N \times 255^2}{\sum_{i=1}^M \sum_{j=1}^N (V_1(i, j) - V_2(i, j))^2} \quad (24)$$

where V_1 and V_2 respectively represent the decrypted image and the original image. Tables 8 and 9 present the PSNR results for different images and algorithms, respectively. It

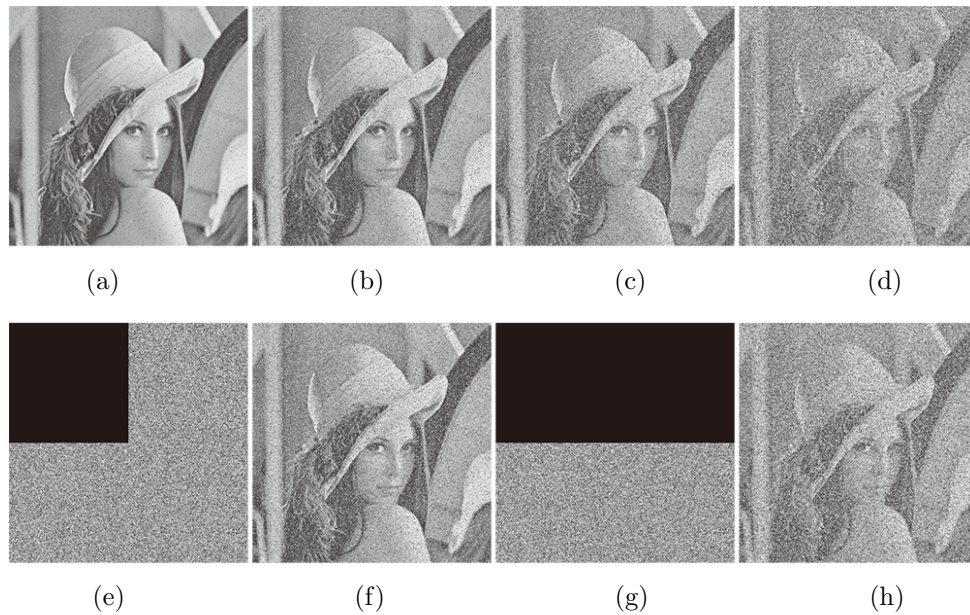


FIGURE 12. Noise attacks analysis: (a) Decrypted image (noise density = 0.01), (b) decrypted image (noise density = 0.05), (c) decrypted image (noise density = 0.1), (d) decrypted image (noise density = 0.2); Cropping attacks analysis (encrypted Lena image): (e) 1/4 data loss, (f) decrypted image of Figure 12(e), (g) 1/2 data loss, (h) decrypted image of Figure 12(g)

TABLE 8. PSNRs under cropping attack and noise attack

Size	Images	1/16 data loss	1/4 data loss	1/2 data loss	0.01 noise density
256×256	5.1.12	20.0629	15.0610	13.8645	9.1974
	5.1.14	20.2888	15.2326	13.9614	10.3472
512×512	5.2.08	20.8576	15.8450	15.7601	10.4996
	5.2.10	20.6072	15.8479	14.7205	10.1607
1024×1024	5.3.01	21.0022	16.9823	16.9034	10.2409
	7.2.01	21.1926	16.1108	15.0023	10.3609

TABLE 9. Comparison of the PSNR (Lena)

Ref.	1/16 data loss	1/4 data loss	1/2 data loss
[50]	20.3469	14.3600	11.3754
[4]	20.3745	14.4533	11.4365
[29]	21.2912	15.2288	12.2028
Ours	20.3794	15.2786	12.0513

can be observed that under various levels of cropping attacks and noise attacks, the proposed algorithm achieves a favorable level of PSNR values. This demonstrates the strong robustness of the proposed algorithm in resisting cropping attacks and noise attack. Therefore, the proposed algorithm can resist noise attacks and cropping attacks.

5.2.7. Time complexity analysis. A prime image encryption algorithm should not only have high security but also low time complexity. Here, we consider that the target image's

size is $M \times N$ for analyzing time complexity [38]. The whole algorithm can be simply divided into four parts: 1) The time complexity of generating the key sequence part can be expressed approximately as $O(4 \times N)$; 2) The time complexity of the two Josephus permutations is $O(2 \times M \times N)$; 3) The total time complexity of DNA encoding and decoding is $O(2 \times 4 \times M \times N)$; 4) The computational complexity of DNA row and column diffusion is $O(4N + M)$. To sum up, the total time complexity is $O(8N + M + 10MN)$.

5.2.8. Comparative analysis. To display the performance of the designed algorithm more objectively, we compare the performance indicators of our encryption algorithm with some state-of-the-art image encryption algorithms by taking the Lena image as an example. The comparison result is listed in Table 10. For the grayscale 512×512 Lena image, our encryption algorithm has the highest information entropy and a lower chi-square value. It shows that our algorithm can achieve a higher degree of pixel confusion than the other algorithms. In terms of resisting differential attacks, the UACI of our encryption algorithm is closer to the theoretical value of 33.4635% than most of the other algorithms. The NPCR is also nearer to the theoretical value of 99.6094% compared to most of the other algorithms. As a result, our encryption scheme is relatively more robust to resist differential attacks. From the correlation coefficient comparison results, it is clear that our algorithm can produce encrypted images with lower correlation compared to most of advanced encryption algorithms. For the color $256 \times 256 \times 3$ Lena image, although the encryption algorithm in [14] can achieve relatively greater information entropy, our algorithm performs better in the other aspects. Overall, our encryption algorithm exhibits better encryption performance than the image encryption algorithm in [14]. To sum up, the designed encryption algorithm integrally has relatively more outstanding encryption performance compared with most advanced image encryption algorithms.

TABLE 10. The comparison result of different encryption schemes (Lena)

Size	Ref.	CC				IE	NPCR	UACI	χ^2
		H	V	D	Ave				
512×512	[41]	0.0032	0.0016	0.0023	0.00236	7.9994	99.6002%	33.5079%	/
	[44]	0.0009	-0.0003	-0.0026	0.00127	7.9991	99.6132%	33.4540%	/
	[36]	0.0020	-0.0060	-0.0003	0.00276	7.9993	/	/	247.40
	[4]	-0.0139	0.0177	0.0006	0.01073	7.9993	99.58%	33.43%	262.83
	[50]	-0.0004	0.0037	-0.0378	0.01396	7.9993	99.61%	33.50%	/
	[5]	0.0015	0.0003	-0.0038	0.00186	7.9994	99.6124%	33.4474%	/
	[54]	0.0005	-0.0025	0.0028	0.00193	7.9993	99.60%	33.48%	/
	[18]	0.0010	0.0010	0.0003	0.00076	7.9993	99.6051%	33.5033%	246.29
	Ours	-0.0020	-0.0015	-0.0006	0.00136	7.9994	99.6090%	33.4578%	227.75
$*256 \times 256 \times 3$	[14]	0.0026	0.0036	0.0044	0.00353	7.99924	99.57%	33.33%	261.86
	Ours	0.0023	0.0037	0.0036	0.00325	7.99914	99.6103%	33.4429%	236.42

*The CC and χ^2 are the average of the three image components.

6. Conclusion. In this paper, a novel 1D chaotic map is proposed, named the 1D Chebyshev-Sine coupled map (1D-CSCM). The 1D-CSCM has wider chaotic ranges and more complex chaotic behaviors than some new 1D chaotic maps. Then, using the 1D-CSCM, we designed an image encryption algorithm using the Josephus permutation and the DNA diffusion. The algorithm updates the initial key by the SHA-512 Hash function combined with the target image information so that the Key sequence generated by the 1D-CSCM

is associated with the plaintext. Then a Josephus sequence-based scrambling approach is used for image pixels perturbations. A new DNA row (column) parallel computing technology is used for image pixels diffusion, and the scheme can diffuse a minor modification in the target image pixel into the whole encrypted image. The simulation experimental results suggest that the algorithm achieves the desired effect of encrypting the target images to noise-like images. Furthermore, various security analyses, such as the chi-square analysis, the information entropy analysis, the differential attack analysis, and the robustness analysis, demonstrate that the designed algorithm exhibits excellent encryption performance. In future work, we will seek a reasonable balance among computational complexity, encryption performance, and encryption speed to design a secure encryption algorithm that is better suited for protecting color image content. Meanwhile, the robustness of the algorithm against noise will be further enhanced to improve its applicability and reliability in practical application scenarios.

Acknowledgment. This work was supported in part by the National Natural Science Foundation of China under Grant 61573004, in part by the Pilot Project of Fujian Province under Grant No. 2022H0017, in part by the innovation Fund Project of Fujian Province of China under Grant No. 2022C0037, and in part by the Quanzhou City Science & Technology Major Special Pilot Project of China under Grant No. 2022GZ1. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

- [1] M. Alawida, A. Samsudin, J. S. Teh and R. S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, *Signal Process.*, vol.160, pp.45-58, 2019.
- [2] G. Álvarez and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifurcation Chaos*, vol.16, no.8, pp.2129-2151, 2006.
- [3] N. A. Azam, I. Ullah and U. Hayat, A fast and secure public-key image encryption scheme based on mordell elliptic curves, *Opt. Lasers Eng.*, vol.137, 106371, 2021.
- [4] 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, 2019.
- [5] Q. Cun, X. Tong, Z. Wang and M. Zhang, A new chaotic image encryption algorithm based on dynamic DNA coding and RNA computing, *Vis. Comput.*, 2023.
- [6] U. Erkan, A. Toktas and Q. Lai, 2D hyperchaotic system based on Schaffer function for image encryption, *Expert Syst. Appl.*, vol.213, 119076, 2023.
- [7] O. S. Faragallah, H. S. El-Sayed, A. Afifi and W. El-Shafai, Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform, *Opt. Lasers Eng.*, vol.137, 106333, 2021.
- [8] Z. Gan, X. Chai, D. Han and Y. Chen, A chaotic image encryption algorithm based on 3-D bit-plane permutation, *Neural Comput. Appl.*, vol.31, no.11, pp.7111-7130, 2019.
- [9] G. A. Gottwald and I. Melbourne, *The 0-1 Test for Chaos: A Review*, Springer Berlin Heidelberg, 2016.
- [10] L. Halbeisen and N. Hungerbühler, The Josephus problem, *Journal de Théorie des Nombres de Bordeaux*, vol.9, no.2, pp.303-318, 1997.
- [11] Z. Hua, Z. Zhu, Y. Chen and Y. Li, Color image encryption using orthogonal Latin squares and a new 2D chaotic system, *Nonlinear Dyn.*, vol.104, no.4, pp.4505-4522, 2021.
- [12] Z. Hua, Z. Zhu, S. Yi, Z. Zhang and H. Huang, Cross-plane colour image encryption using a two-dimensional logistic tent modular map, *Inf. Sci.*, vol.546, pp.1063-1083, 2021.
- [13] S. Ibrahim and A. M. Abbas, Efficient key-dependent dynamic S-boxes based on permuted elliptic curves, *Inf. Sci.*, vol.558, pp.246-264, 2021.
- [14] K. C. Jithin and S. Sankar, Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set, *J. Inf. Secur. Appl.*, vol.50, 102428, 2020.
- [15] Y. Khedmati, R. Parvaz and Y. Behroo, 2D hybrid chaos map for image security transform based on framelet and cellular automata, *Inf. Sci.*, vol.512, pp.855-879, 2020.

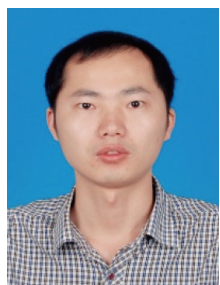
- [16] M. Li, M. Wang, H. Fan, K. An and G. Liu, A novel plaintext-related chaotic image encryption scheme with no additional plaintext information, *Chaos, Solitons & Fractals*, vol.158, 111989, 2022.
- [17] S. Li, J. Lin, Y. Lv and T. Li, Deep learning-based algorithm for complex small target detection in UAV aerial images, *International Journal of Innovative Computing, Information and Control*, vol.21, no.1, pp.135-152, 2025.
- [18] 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, 109033, 2023.
- [19] X. Liu, K. Sun and H. Wang, A novel image encryption scheme based on 2D SILM and improved permutation-confusion-diffusion operations, *Multimed. Tools Appl.*, 2022.
- [20] A. Mansouri and X. Wang, A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme, *Inf. Sci.*, vol.520, pp.46-62, 2020.
- [21] R. M. May, Simple mathematical models with very complicated dynamics, *Nature*, vol.261, no.5560, pp.459-467, 1976.
- [22] X. Meng, J. Li, X. Di, Y. Sheng and D. Jiang, An encryption algorithm for region of interest in medical DICOM based on one-dimensional e^λ -cos-cot map, *Entropy*, vol.24, no.7, 2022.
- [23] M. A. Midoun, X. Wang and M. Z. Talhaoui, A sensitive dynamic mutual encryption system based on a new 1D chaotic map, *Opt. Lasers Eng.*, vol.139, 106485, 2021.
- [24] T. Pan, X. Tong, M. Zhang and Z. Wang, A joint image compression and encryption algorithm based on compression sensing and bit-plane embedding, *Phys. Scr.*, vol.97, no.9, 095209, 2022.
- [25] H. Qiu, X. Xu, Z. Jiang, K. Sun and C. Xiao, A color image encryption algorithm based on hyper-chaotic map and Rubik's Cube scrambling, *Nonlinear Dyn.*, vol.110, no.3, pp.2869-2887, 2022.
- [26] J. S. Richman and J. R. Moorman, Physiological time-series analysis using approximate entropy and sample entropy, *Am. J. Physiol. Heart Circ. Physiol.*, vol.278, no.6, H2039, 2000.
- [27] A. K. Singh, K. Chatterjee and A. Singh, An image security model based on chaos and DNA cryptography for IIoT images, *IEEE Trans. Ind. Informat.*, vol.19, no.2, pp.1957-1964, 2023.
- [28] J. Tang, Z. Zhang, P. Chen, F. Zhang, H. Ni and Z. Huang, An image layered scrambling encryption algorithm based on a novel discrete chaotic map, *IET Image Proc.*, vol.17, no.2, pp.518-532, 2022.
- [29] J. Tang, W. Song, H. Ni, S. Pan and Y. Zhao, A novel memristor-coupled 3D hyperchaotic system and its application in image encryption, *Phys. Scr.*, vol.100, no.12, 125207, 2025.
- [30] J. Tang, F. Zhang and H. Ni, A novel fast image encryption scheme based on a new one-dimensional compound sine chaotic system, *Vis. Comput.*, 2022.
- [31] J. S. Teh, K. Tan and M. Alawida, A chaos-based keyed Hash function based on fixed point representation, *Clust. Comput.*, vol.22, no.2, pp.649-660, 2019.
- [32] M. Uddin, F. Jahan, M. K. Islam and M. R. Hassan, A novel DNA-based key scrambling technique for image encryption, *Complex Intell. Syst.*, vol.7, no.6, pp.3241-3258, 2021.
- [33] Y. Wan, S. Wang and B. Du, A bit plane image encryption algorithm based on compound chaos, *Multimed. Tools Appl.*, 2022.
- [34] S. Wang, Q. Peng and B. Du, Chaotic color image encryption based on 4D chaotic maps and DNA sequence, *Opt. Laser Technol.*, vol.148, 107753, 2022.
- [35] X. Wang and Y. Li, Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence, *Opt. Lasers Eng.*, vol.137, 106393, 2021.
- [36] X. Wang and P. Liu, A new full chaos coupled mapping lattice and its application in privacy image encryption, *IEEE Trans. Circuits Syst. I*, vol.69, no.3, pp.1291-1301, 2022.
- [37] X. Wang and D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, *Commun. Nonlinear Sci. Numer. Simul.*, vol.18, no.11, pp.3075-3085, 2013.
- [38] X. Wang, Y. Zhang and X. Bao, A novel chaotic image encryption scheme using DNA sequence operations, *Opt. Lasers Eng.*, vol.73, pp.53-61, 2015.
- [39] Y. Wang, X. Li and Q. Wang, Integral imaging based optical image encryption using CA-DNA algorithm, *IEEE Photon. J.*, vol.13, no.2, pp.1-12, 2021.
- [40] J. D. Watson and F. H. C. Crick, Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid, *Nature*, vol.171, no.4356, pp.737-738, 1953.
- [41] J. Wu, X. Liao and B. Yang, Image encryption using 2D Hénon-Sine map and DNA approach, *Signal Process.*, vol.153, pp.11-23, 2018.
- [42] Y. Wu, L. Zhang, S. Berretti and S. Wan, Medical image encryption by content-aware DNA computing for secure healthcare, *IEEE Trans. Ind. Informat.*, vol.19, no.2, pp.2089-2098, 2023.
- [43] Y. Wu, J. P. Noonan and S. S. Agaian, NPCR and UACI randomness tests for image encryption, *Cyber J. Multidisciplinary J. Sci. Technol. J. Sel. Areas Telecommun.*, vol.1, no.2, pp.31-38, 2011.

- [44] Y. Xian, X. Wang and L. Teng, Double parameters fractal sorting matrix and its application in image encryption, *IEEE Trans. Circuits Syst. Video Technol.*, vol.32, no.6, pp.4028-4037, 2022.
- [45] J. Xu, J. Mou, J. Liu and J. Hao, The image compression-encryption algorithm based on the compression sensing and fractional-order chaotic system, *Vis. Comput.*, vol.38, no.5, pp.1509-1526, 2022.
- [46] J. Yu, K. Peng, L. Zhang and W. Xie, Image encryption algorithm based on DNA network and hyperchaotic system, *Vis. Comput.*, vol.40, pp.8001-8021, 2024.
- [47] J. Yu, W. Xie, Z. Zhong and H. Wang, Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation, *Chaos, Solitons & Fractals*, vol.162, 112456, 2022.
- [48] S. Yu, N. Zhou, L. Gong and Z. Nie, Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system, *Opt. Lasers Eng.*, vol.124, 105816, 2020.
- [49] Y. Yu, S. Gao, S. Cheng, Y. Wang, S. Song and F. Yuan, CBSO: A memetic brain storm optimization with chaotic local search, *Memetic Comput.*, vol.10, no.4, pp.353-367, 2018.
- [50] E. Z. Zefreh, An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and Hash functions, *Multimed. Tools Appl.*, vol.79, no.33, pp.24993-25022, 2020.
- [51] S. Zhang and L. Liu, A novel image encryption algorithm based on SPWLCM and DNA coding, *Math. Comput. Simulation*, vol.190, pp.723-744, 2021.
- [52] X. Zhang, Z. Liu and X. Yang, Fast image encryption algorithm based on 2D-FCSM and pseudo-wavelet transform, *Nonlinear Dyn.*, vol.111, no.7, pp.6839-6853, 2023.
- [53] Z. Zhang, J. Tang, H. Ni and T. Huang, Image adaptive encryption algorithm using a novel 2D chaotic system, *Nonlinear Dyn.*, vol.111, no.11, pp.10629-10652, 2023.
- [54] W. Zhou, X. Wang, M. Wang and D. Li, A new combination chaotic system and its application in a new Bit-level image encryption scheme, *Opt. Lasers Eng.*, vol.149, 106782, 2022.
- [55] Y. Zhou, K. Panetta, S. Agaian and C. L. P. Chen, Image encryption using P-Fibonacci transform and decomposition, *Opt. Commun.*, vol.285, no.5, pp.594-608, 2012.
- [56] H. Zhu, W. Qi, J. Ge and Y. Liu, Analyzing Devaney chaos of a sine-cosine compound function system, *Int. J. Bifurcation Chaos*, vol.28, no.14, 1850176, 2018.

Author Biography



Ruibin Xue received the bachelor's degree from Beijing University of Science and Technology, China, in 2012. Currently, he serves as the vice president of operations at Fujian Torch Electron Technology Company Ltd. He is leading a number of scientific research projects on intelligent manufacturing. His research interests include image encryption and artificial intelligence.



Jianeng Tang received the M.Sc. degree in Circuits and Systems from Ningxia University, China, in 2009; the Ph.D. degree in Information and Communication Engineering from Southeast University, China, in 2012. He is currently an associate professor at College of Engineering, Huaqiao University, China. His research interests include image encryption, RF circuit design, complex network synchronization, and chaos synchronization and control. He has published over 30 papers in journals and conferences.



Zezong Zhang received the M.Sc. degree in the College of Information Science and Engineering, Huaqiao University, China, in 2024. He is pursuing a Ph.D. degree at the National University of Defense Technology, China. His research interests include nonlinear dynamics and control, information security, cryptanalysis, and the application of chaotic cryptography in image processing.