



A color image encryption algorithm based on hyperchaotic map and Rubik's Cube scrambling

Haojie Qiu · Xuemei Xu · Zhaohui Jiang · Kehui Sun · Chuwen Xiao

Received: 25 February 2022 / Accepted: 20 July 2022 / Published online: 25 August 2022
© The Author(s), under exclusive licence to Springer Nature B.V. 2022

Abstract At present, many encryption algorithms for color images either decompose color images into three gray images and encrypt them, respectively, or combine R, G, B channels into a two-dimensional image matrix before encryption. These methods break the internal link between the three colors and reduce the efficiency of encryption. Here, to address these shortcomings, a new hyperchaotic system two-dimension Chebyshev–Sine coupling map (2D-CSCM) is proposed to improve the security of the encryption algorithm, and the dynamic behaviors of the system are analyzed by phase diagram, bifurcation diagram, Lyapunov exponent spectra information entropy and 0–1 test. We propose a Rubik's Cube scrambling method to scramble a three-dimensional bit-level matrix of the color image directly. Then the pixel values of the scrambled image matrix are diffused by two rounds of different operations based on chaotic sequences. The parameters and initial values of the chaotic system are derived from the secret key generated by the hash function SHA-512. Simulation results and security analysis demonstrate that the

proposed algorithm has high efficiency and security to resist various common attacks.

Keywords Color image encryption · Hyperchaotic system · Rubik's Cube scrambling · Security analysis

1 Introduction

With the rapid development of artificial intelligence, multimedia communication and Internet technology, information security has become a serious problem in modern society. Image is one of the main carriers of multimedia information, which conveys more information than sound and text. Image contains information related to personal privacy, trade secrets, national security and other aspects. Therefore, it is essential to adopt an encryption technology to prevent images from being leaked and attacked in the process of storage and transmission [1–9].

Several traditional encryption algorithms are gradually replaced in the field of image encryption with a large amount of data, such as data encryption standard (DES) [10], advanced encryption standard (AES) [11], RSA [12] and so on. With the continuing research, DNA coding [13, 14], cellular automata [15, 16], Fourier transform [17, 18], chaos [19, 20] and other new image encryption technologies have emerged [21–23]. Among them, taking chaos as the core of the

H. Qiu · X. Xu (✉) · K. Sun · C. Xiao
School of Physics and Electronics, Central South University, Changsha 410083, China
e-mail: xxm999@csu.edu.cn

Z. Jiang
School of Automation, Central South University,
Changsha 410083, China

cryptosystem can greatly improve the performance of the encryption algorithm.

Chaos is a long-term unpredictable behavior produced by deterministic nonlinear systems, and its unpredictability comes from the instability of the internal motion of the system [24–26]. Chaotic system has the characteristics of sensitivity to the initial value, ergodicity, internal stochastic [27–31], so it has a favorable prospect in the field of cryptography. In recent years, many scholars have proposed image encryption technology based on chaos theory [32–35]. For instance, Liu et al. [36] proposed a new two-dimensional Sine ICMIC (iterative chaotic map with infinite collapse) modulation map based on the close-loop modulation coupling model and a chaotic shift transform for image encryption. Hu et al. [37] established a fractional-order chaotic circuit with different coupled memristors and applied it to image encryption. Wang et al. [38] used the chaotic sequences generated by Chen hyperchaotic system to perform inter-block index scrambling and intra-block Fisher-Yates scrambling. Chen et al. [39] generalized the two-dimensional chaotic cat map to 3D for designing a real-time secure symmetric encryption scheme. Haq et al. [40] constructed a 4D mixed chaotic map with hyperchaotic properties and high randomness behavior by using the 1D Sine map and the 2D Thinker bell map and then introduced a novel image encryption scheme based on the proposed chaotic system and symmetric group S8 permutation. According to the above research, it is found that these methods adopt chaotic systems of different orders, and the performance of these image encryption methods is closely related to the dynamic characteristics of chaotic systems [41, 42]. Some encryption methods have poor performance because of the small distribution range of attractors and the poor unpredictability of chaotic sequences generated by the chaotic map. In this paper, we aim to design a new hyperchaotic system with better ergodicity and unpredictability of sequence and apply it to a high-security image encryption method.

The images transmitted in the network are mainly color images. Most encryption algorithms for color images include two types. One is to encrypt the R, G, B color channels, respectively, which breaks the internal link between the three color channels of the image. Gao et al. [43] divided color image into R, G, B primary colors and then scrambled and diffused three

primary colors by the improved Hénon sequences. Noura et al. [44] used a hybrid 2D composite chaotic map combined with a sine–cosine cross-chaotic map to encrypt three color channels, respectively. The other is to transform the three-dimensional image matrix of a color image into a two-dimensional matrix before encryption, which increases the number of iterations of chaotic system and encryption and reduces the efficiency of encryption. Teng et al. [45] vertically combined the R, G, B matrixes of color images into a two-dimensional matrix and then perform cycle shift scrambling and selecting diffusion based on a cross 2D hyperchaotic map. The purpose of this paper is to design a more efficient and secure color image encryption method.

In this paper, we propose a cross-operation coupling model and construct a novel hyperchaotic system (2D-CSCM) through the Chebyshev map and Sine map. The better hyperchaotic properties of the system are proved by phase diagram, bifurcation diagram, Lyapunov exponent spectra, information entropy and 0–1 test. Considering the features of a color image matrix, a Rubik's Cube scrambling method is proposed in this paper. The three-dimensional bit-level matrix of a color image is randomly scrambled by row transform and column transform similar to the Rubik's Cube. Pixel values of the scrambled image matrix are diffused by three-dimensional row diffusion and column diffusion. Simulation experiments and analysis show that this algorithm improves the efficiency and security of color image encryption.

The remainder of this paper is organized as follows. Section 2 proposes the model of the novel two-dimensional hyperchaotic map 2D-CSCM; then the dynamic behaviors are analyzed. In Sect. 3, a novel color image encryption algorithm is proposed. Section 4 introduces the decryption algorithm. Section 5 analyzes the simulation results and security analysis of the proposed algorithm. In Sect. 6, the conclusion is given.

2 Chaotic system

2.1 Definition of 2D-CSCM

Some existing chaotic cryptosystems have many shortcomings because of the uncomplex dynamic

characteristics of the chaotic system. In view of this situation, the cross-operation coupling model is proposed in this chapter to construct a novel hyperchaotic map, which is shown in Fig. 1.

In the structure diagram, there are two input signals x_n, y_n and two output signals x_{n+1}, y_{n+1} . F and G are chaotic maps, f is a nonlinear function, and \oplus and \ominus represent the addition and subtraction of the input signals, respectively. The expression of the model is given as

$$\begin{cases} x_{n+1} = F(f(x_n - y_n)) \\ y_{n+1} = G(x_n + y_n) \end{cases} \quad (1)$$

In the model of cross-operation coupling, the nonlinear function f is chosen as $\cos(x)$, and the chaotic maps F and G are set as the Chebyshev map and Sine map. Chebyshev map and Sine map are two classical one-dimensional chaotic maps, whose expressions are, respectively, defined as Eqs. (2) and (3).

$$x_{n+1} = \cos(\alpha \cos^{-1}(x_n)) \quad (2)$$

$$y_{n+1} = \beta \sin(\pi y_n), \beta \in (0, 1] \quad (3)$$

Then a novel two-dimensional Chebyshev–Sine coupling map (2D-CSCM) is obtained as

$$\begin{cases} x_{n+1} = \cos(\alpha \cos^{-1}(\sin(x_n - y_n))) \\ y_{n+1} = \beta \sin(\pi(x_n + y_n)) \end{cases} \quad (4)$$

where α, β are control parameters, and $\alpha, \beta \in [2, +\infty)$.

2.2 Performance analysis of 2D-CSCM

2.2.1 Phase diagram

The dynamic behavior of chaotic system can be observed directly from phase diagram. The phase trajectory of chaotic motion is an unclosed curve that can be observed through the phase plane graph. Attractors of a chaotic system with good chaotic

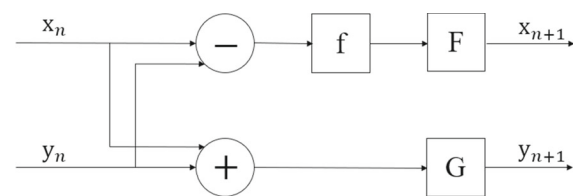


Fig. 1 Structural diagram of the cross-operation coupling mode

behaviors usually occupy a large area in the phase diagram. For the chaotic system proposed in this chapter, we set the initial values $(x_0, y_0) = (1, 1)$, set the control parameters $\alpha = 5, \beta = 5$, and iterate the system 50,000 times; the generated phase diagram of 2D-CSCM is shown in Fig. 2a. It can be seen that the system exhibits chaotic behavior under the parameters set above, and the trajectory of the system completely covers the whole phase plane, which indicates the output variables of this system have excellent ergodicity.

In addition, phase diagram analysis is also carried out for several 2D chaotic maps in use, and the optimal initial states and control parameters are selected for each chaotic map to obtain the best chaotic performance. The phase diagrams of 2D-SIMM [36], 2D-SLMM [7] and 2D-Logistic [41] are shown in Fig. 2b–d, respectively. It can be seen that the attractor range of 2D-CSCM is much larger than that of 2D-SIMM, 2D-SLMM and 2D-Logistic, indicating that 2D-CSCM has better ergodicity.

2.2.2 Bifurcation diagram

Bifurcation diagram is another important method to analyze the dynamic behavior of chaotic system. The motion state of the system will be different along with the change of control parameters, which can be demonstrated by bifurcation diagram. For the 2D-CSCM proposed in this chapter, setting the initial values $(x_0, y_0) = (1, 1)$, the bifurcation diagrams of 2D-CSCM are illustrated in Fig. 3. Setting the control parameter $\alpha = 4$, when β in the range of $(2, 6)$, the corresponding bifurcation diagram is illustrated in Fig. 3a. Similarly, setting the control parameter $\beta = 4$, when α in the range of $(2, 6)$, the result is illustrated in Fig. 3b. It can be seen that there is no periodic state in both bifurcation diagrams, indicating that the system exhibits the chaotic state in a wide range of parameters.

2.2.3 Lyapunov exponent spectrum

The Lyapunov exponent spectrum of the chaotic system can effectively represent the sensitivity of the system to the initial value when the system evolves over time. For a high-order chaotic system, the number of Lyapunov exponents is equal to the number of orders, so the 2D-CSCM proposed in this chapter has

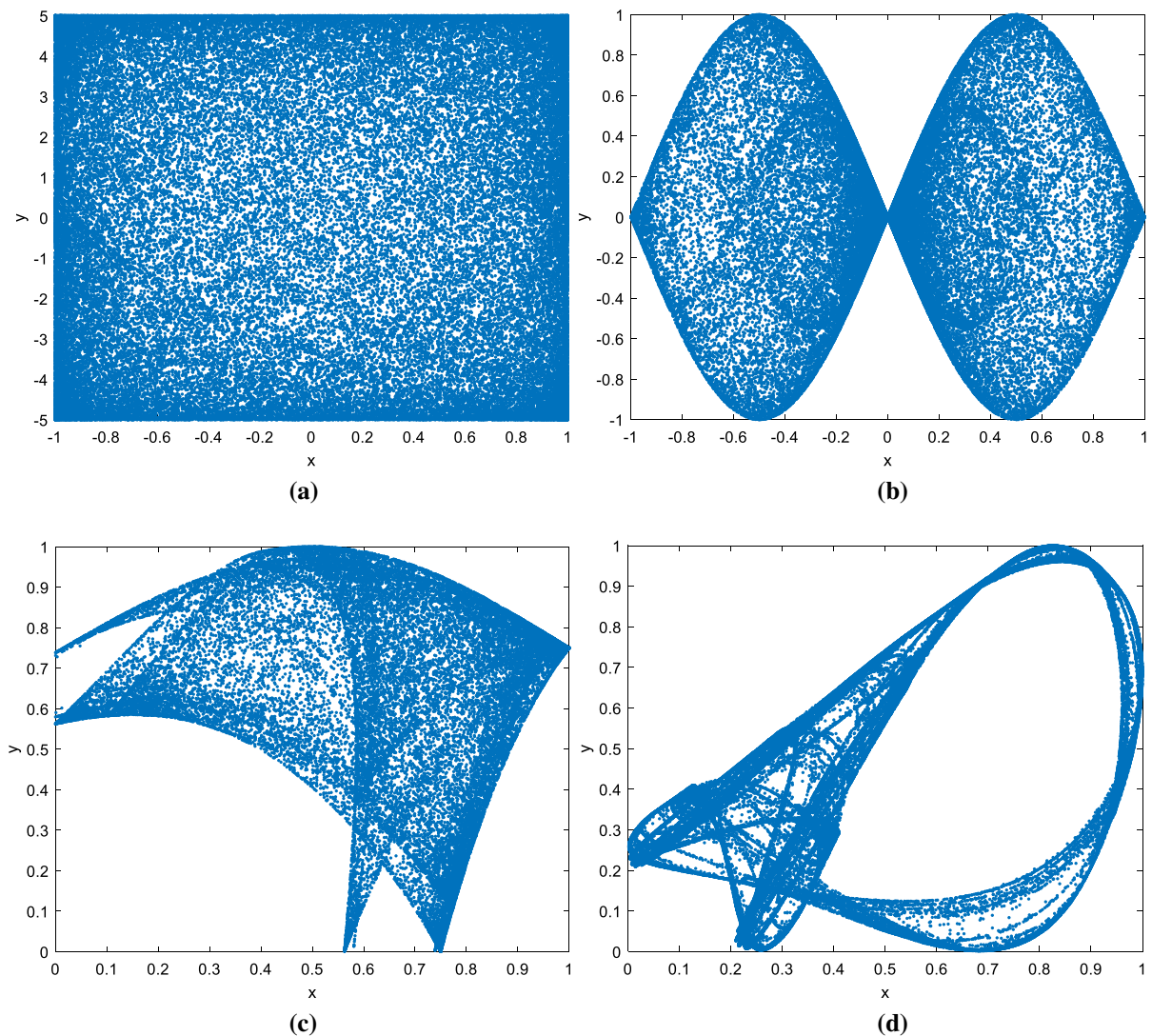


Fig. 2 Phase diagrams of chaotic maps. **a** 2D-CSCM with $\alpha = 5, \beta = 5$. **b** 2D-SIMM with $\alpha = 1, \beta = 5$. **c** 2D-SLMM with $\alpha = 1, \beta = 3$. **d** 2D-Logistic with $r = 1.19$

two Lyapunov exponents. When setting $\beta = 4$, the Lyapunov exponent spectrum of 2D-CSCM is illustrated in Fig. 4a. It can be observed that when $\alpha \in (2, 6)$, the chaotic system has two positive Lyapunov exponents, indicating that the system is in the hyperchaotic state. Similarly, setting control parameter $\alpha = 4$, when $\beta \in (2, 6)$, the system is in the hyperchaotic state, which is illustrated in Fig. 4b. It can be seen that the system always exhibits the hyperchaotic state within the parameters set above, which indicates that it has complex dynamic behavior and is suitable for a cryptosystem.

2.2.4 Complexity analysis

The complexity of the chaotic system is one of the important methods to describe the dynamic characteristics of the chaotic system. The complexity analysis of chaotic system is used to measure the degree to which chaotic sequences approximate to random sequences [46, 47]. The main idea of the image encryption method based on the chaotic system is to apply the pseudo-random sequence generated by a chaotic system to the process of image encryption, so the complexity of the chaotic sequence will greatly

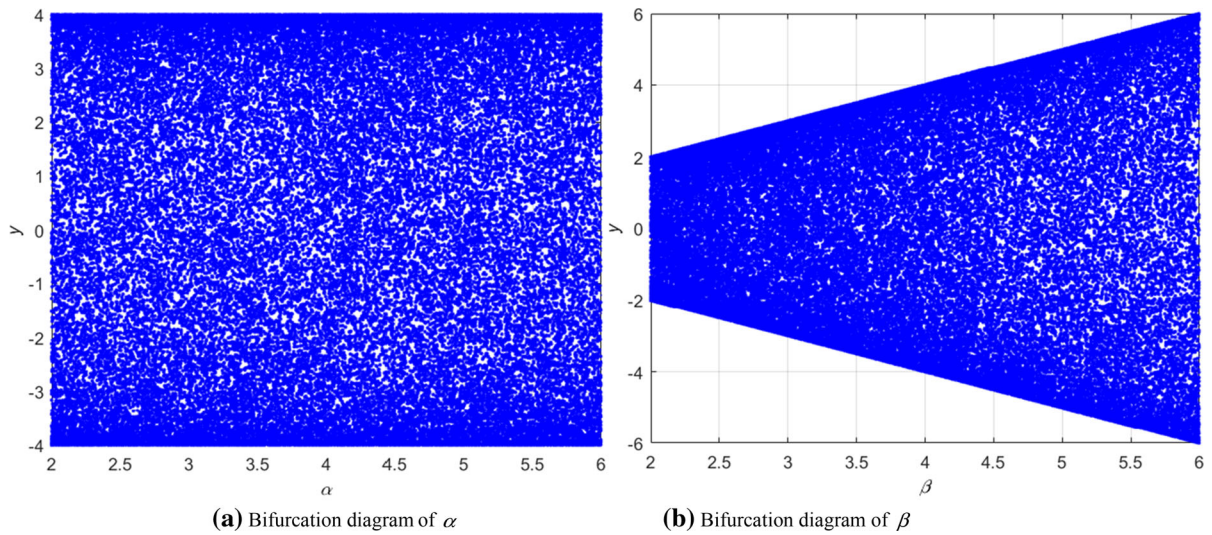


Fig. 3 Bifurcation diagram of 2D-CSCM

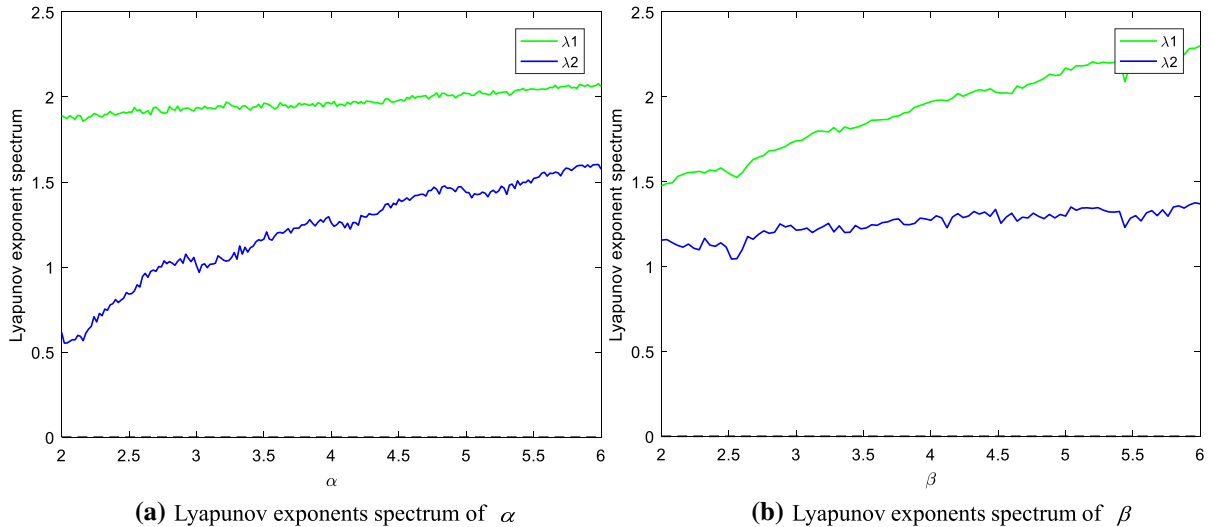


Fig. 4 Lyapunov exponents spectrum of 2D-CSCM

affect the security of encryption algorithm. Therefore, we analyze the complexity of our chaotic system in this section to demonstrate its superior performance. Notably, the larger the complexity value is, the more chaotic sequence is approximate to the random sequence, and the higher the security of the corresponding application system will be. At present, there are many algorithms to calculate the complexity of chaotic pseudo-random sequences. In this chapter, the permutation entropy (PE) algorithm is chosen to evaluate the complexity of 2D-CSCM. The PE complexity graph of control parameters α and β is

shown in Fig. 5. As can be seen from the graphs, permutation entropy proves that 2D-CSCM has large sequence complexity value which is close to ideal value 1. Figure 6 shows the comparison of permutation entropy between 2D-CSCM and different chaotic maps. It is obvious that the complexity of 2D-CSCM is greater than that of several classical 1D chaotic maps and other newly proposed 2D chaotic maps. As a result, the chaotic sequence generated by 2D-CSCM shows better complexity and unpredictability and can generate more secure key sequences.

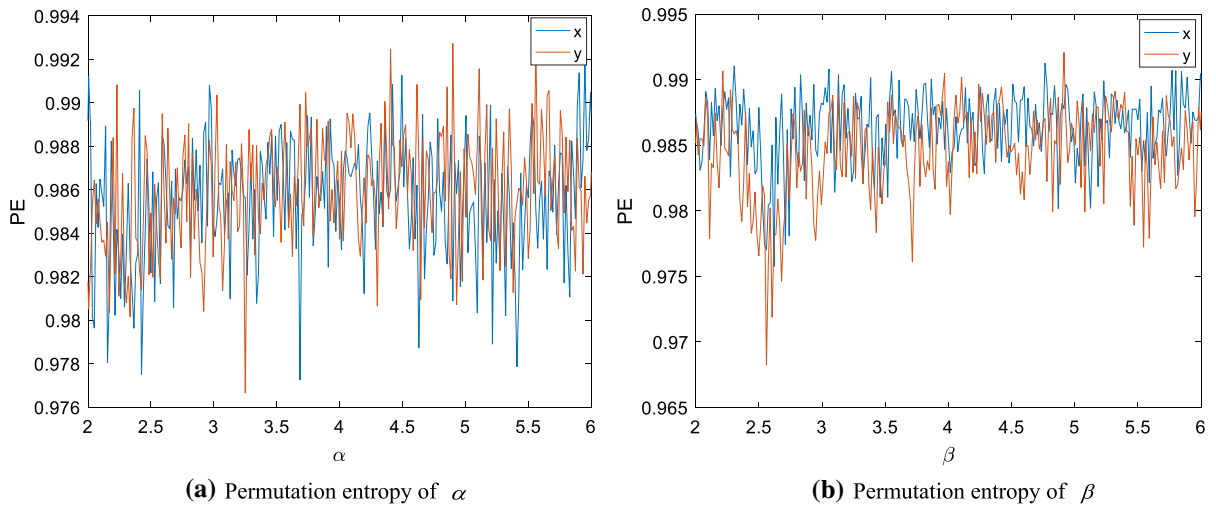


Fig. 5 Complexity graph of 2D-CSCM

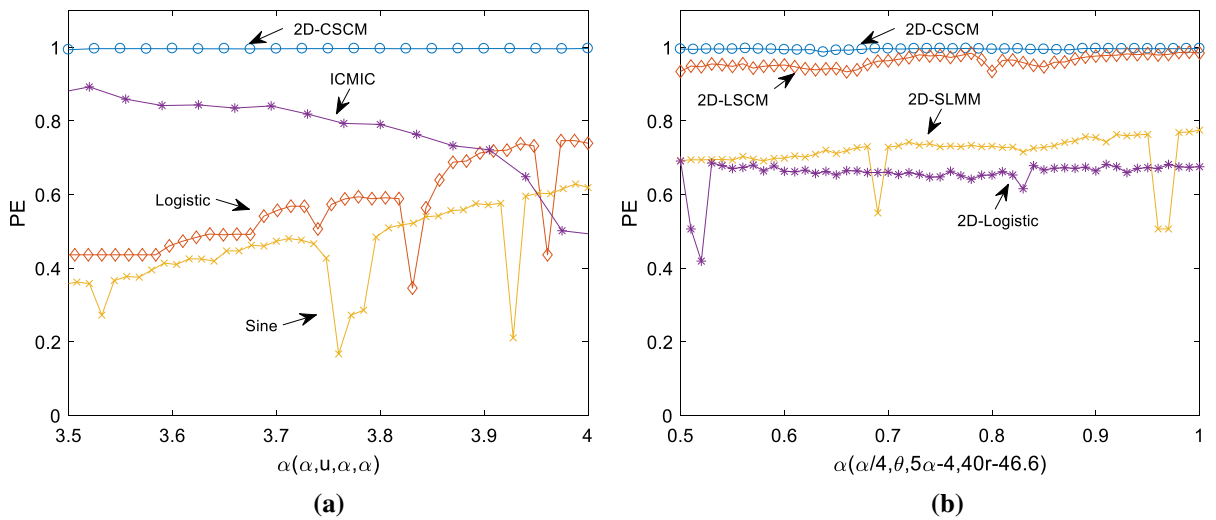


Fig. 6 Permutation entropy of different maps. **a** 2D-CSCM, ICMIC map, Logistic map and Sine map. **b** 2D-CSCM, 2D-LSCM, 2D-SLMM and 2D-Logistic

2.2.5 0–1 test

Gottwald GA and Melbourne I proposed a reliable binary test method for determining whether a given deterministic dynamical system is chaotic or non-chaotic [48, 49]. Different from the usual method of calculating the maximal Lyapunov exponent, this method is applied directly to the time series data without phase space reconstruction and is generally suitable for any deterministic dynamical system. To comprehensively reflect the dynamic characteristics of the proposed system, we conduct 0–1 test and show the

chaotic behaviors of our system through the test results in this section. It can be seen from the trajectory of the 0–1 test result that the trajectory of a regular system is bounded, while that of a chaotic system is unbounded which is similar to the Brownian motion. Setting the initial values $(x_0, y_0) = (1, 1)$ and control parameters $(\alpha, \beta) = (4, 4)$, the 0–1 test result of the sequence x and y is shown in Fig. 7a, b. The test results show that the trajectory of the sequence x and y is Brownian motion, indicating the proposed system is a chaotic system.

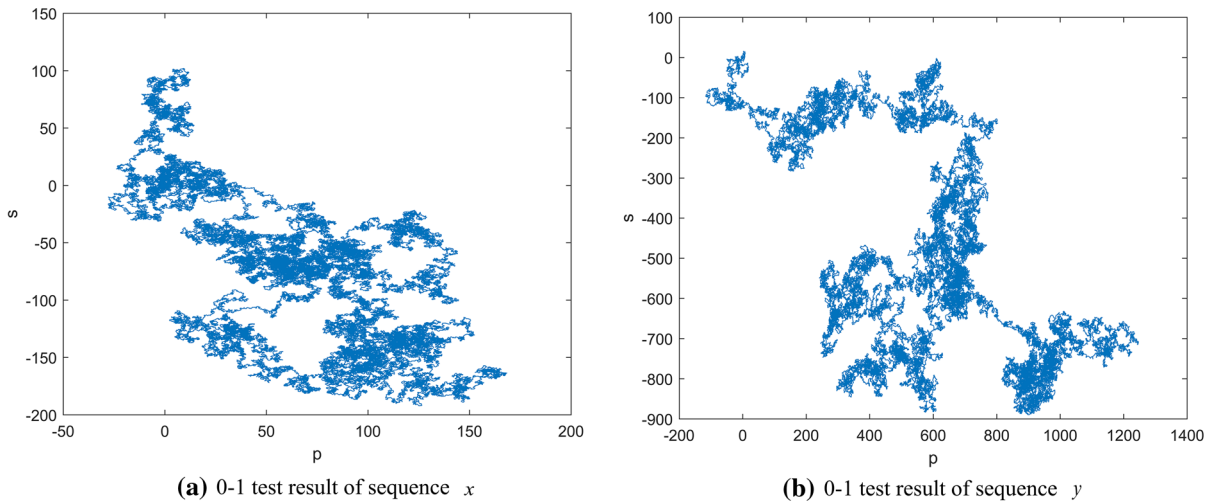


Fig. 7 0–1 test result of 2D-CSCM

3 Proposed encryption algorithm

Based on the chaotic sequences generated by the proposed two-dimensional hyperchaotic system, a novel color image encryption algorithm is proposed in this chapter. The proposed algorithm includes Rubik’s Cube scrambling and two rounds of three-dimensional matrix diffusion, the flowchart of which is shown in Fig. 8.

3.1 Generation of key and system parameters

Hash algorithm is extremely sensitive to change of input and can resist plaintext attack effectively, the output of the hash algorithm is irreversible. The secret

key of the encryption algorithm proposed in this paper is generated by the hash algorithm because of its security. Input the pixel value of the plaintext image into the SHA-512 function to produce a 128-bit string key K . The key is divided into eight 16-bit strings and then converted into eight decimal sub-keys $k_1, k_2 \dots k_8$ according to Eq. (5).

$$k_i = \text{hex2dec}(K(16 \times i - 15 : 16 \times i)), i = 1 \dots 8 \tag{5}$$

where $\text{hex2dec}(x)$ represents converting the hexadecimal character x to a decimal number, $K(x : y)$ represents taking the x – th to y – th value of K .

The control parameters α, β and initial values x_0, y_0 of 2D-CSCM are obtained by processing the sub-keys:

$$\begin{cases} \alpha = \text{mod}(\text{sqrt}(k_1 \times M \times N)/k_8 \times 10^{10}, 0.5) + 4 \\ \beta = \text{mod}(\text{sqrt}(k_2 \times M \times N)/k_7 \times 10^{10}, 0.5) + 4 \\ x_0 = \text{mod}(\text{sqrt}(k_3 \times M \times N)/k_6 \times 10^{10}, 0.5) + 1 \\ y_0 = \text{mod}(\text{sqrt}(k_4 \times M \times N)/k_5 \times 10^{10}, 0.5) + 1 \end{cases} \tag{6}$$

where $\text{mod}()$ represents the modulo operation, $\text{sqrt}(x)$ represents the square root of x , M is the number of rows, and N is the number of columns.

3.2 Rubik’s Cube scrambling

The purpose of scrambling is to average the image statistics and make the image information uniform by

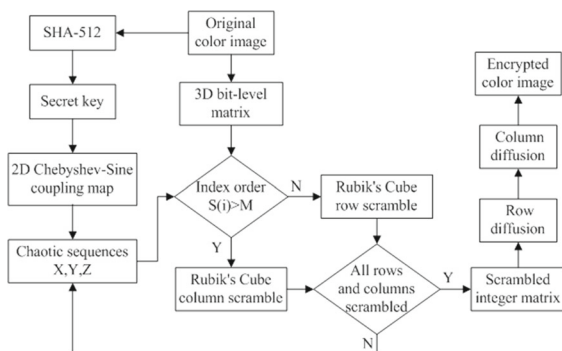


Fig. 8 Flowchart of the proposed encryption algorithm

changing the position of image pixels. We introduced the concept of Rubik’s Cube into the process of color image matrix scrambling and proposed a Rubik’s Cube scrambling method for color images, which shuffles the 3D bit-level matrix of the color image directly.

Step 1. The color plaintext image is input to get an image matrix P with the size of $M \times N \times 3$. Convert pixel values in matrix P into 8-bit binary values and obtain the binary matrix P' with the size of $M \times 8N \times 3$.

Step 2. The control parameters and initial values of 2D-CSCM are generated from Eq. (6). Iterate the 2D-CSCM $M \times N \times 3 + t$ times, and discard the first t values to prevent transient effect, where $t = 500$. Then we get two chaotic sequences x, y . The two chaotic sequences x, y are further processed to obtain two shuffling sequences X, Y and a selecting sequence Z according to Eq. (7).

$$\begin{cases} X = \text{mod}(\text{ceil}(x(1 : 3M) \times 10^{14}), 3M) \\ Y = \text{mod}(\text{ceil}(y(1 : 3 \times 8N) \times 10^{14}), 3 \times 8N) \\ Z = \text{mod}(\text{ceil}(x(3M + 1 : 3M + M + 8N) \times 10^{14}), M + 8N) \end{cases} \tag{7}$$

where $\text{ceil}(x)$ represents rounding element x to the nearest integer greater than or equal to x .

Then obtain the index order S of selecting sequence Z from $[Z1, S] = \text{sort}(Z)$, where $\text{sort}(Z)$ represents sorting the elements of Z in ascending order.

Step 3. The Rubik’s Cube scrambling method proposed in this section is mainly divided into row scrambling and column scrambling. The total number of rows and columns in the matrix P' is $M + 8N$. Traverse elements in index order sequence $S(i)$, $i = 1, 2, \dots, M + 8N$, pixel values of the $S(i) - M$ -th column in the matrix P' are scrambled when $S(i) > M$, otherwise, pixel values of the $S(i)$ -th row are scrambled.

Step 4. When pixel values of the $S(i) - M$ -th column are scrambled, the pixel values of the $S(i) - M$ -th column in the three dimensions of P' are scanned into an array P_1 with the length of $3 \times M$ as $[P'(:, S(i) - M, 1), P'(:, S(i) - M, 2), P'(:, S(i) - M, 3)]$. P_1 is scrambled by a chaos-based shuffle algorithm. The process is to swap the number at a random position with the last number in the unprocessed array each time until all positions have been processed. The random position is obtained by chaotic sequences X , which is described as Eq. (8).

$$\begin{cases} \text{Exchange}(P_1(i), P_1(RP_1(i))), i = 3 \times M, 3 \times M - 1, \dots, 2 \\ RP_1(i) = \text{mod}(X(i), i - 1) + 1, i = 3 \times M, 3 \times M - 1, \dots, 2 \end{cases} \tag{8}$$

Similarly, when pixel values of the $S(i)$ -th row are scrambled, the pixel values of the $S(i)$ -th row in the three dimensions are scanned into an array P_2 with the length of $3 \times 8N$ as $[P'(S(i), :, 1), P'(S(i), :, 2), P'(S(i), :, 3)]$, then P_2 is scrambled by chaos-based shuffle algorithm, the process of row scrambling is described as Eq. (9).

$$\begin{cases} \text{Exchange}(P_2(i), P_2(RP_2(i))), i = 3 \times 8N, 3 \times 8N - 1, \dots, 2 \\ RP_2(i) = \text{mod}(Y(i), i - 1) + 1, i = 3 \times 8N, 3 \times 8N - 1, \dots, 2 \end{cases} \tag{9}$$

Assume a color image matrix with the size of $4 \times 4 \times 3$ and two chaotic sequences X, Y , the scrambling process of the first row and then the fourth column is shown in Fig. 9. It can be seen that the pixels in the first row and the fourth column have changed a lot.

Step 5. Convert pixel values in the scrambled matrix P' into decimal values and obtain the scrambled integer matrix P'' with the size of $M \times N \times 3$. The position and value of the pixels in the image matrix are changed to a great extent by the bit-level scrambling process.

3.3 Diffusion process

We proposed a color image diffusion method in which pixel values are diffused through three-dimensional row diffusion and three-dimensional column diffusion.

Step 1. The two chaotic sequences x, y are further processed to obtain two diffusion matrixes X', Y' with the size of $M \times N \times 3$ according to Eqs. (10) and (11).

$$\begin{cases} X' = \text{mod}(\text{ceil}(x(1 : 3 \times M \times N) \times 10^{13}), 256) \\ Y' = \text{mod}(\text{ceil}(y(1 : 3 \times M \times N) \times 10^{13}), 256) \end{cases} \tag{10}$$

$$\begin{cases} X' = \text{reshape}(X', M, N, 3) \\ Y' = \text{reshape}(Y', M, N, 3) \end{cases} \tag{11}$$

where $\text{reshape}(A, s1, s2, \dots, sk)$ represents reshaping the array A into a $s1 \times s2 \times \dots \times sk$ model array.

Step 2. In the process of row diffusion, the pixel values of each row in the three dimensions of the matrix P'' are diffused with the pixel values in the

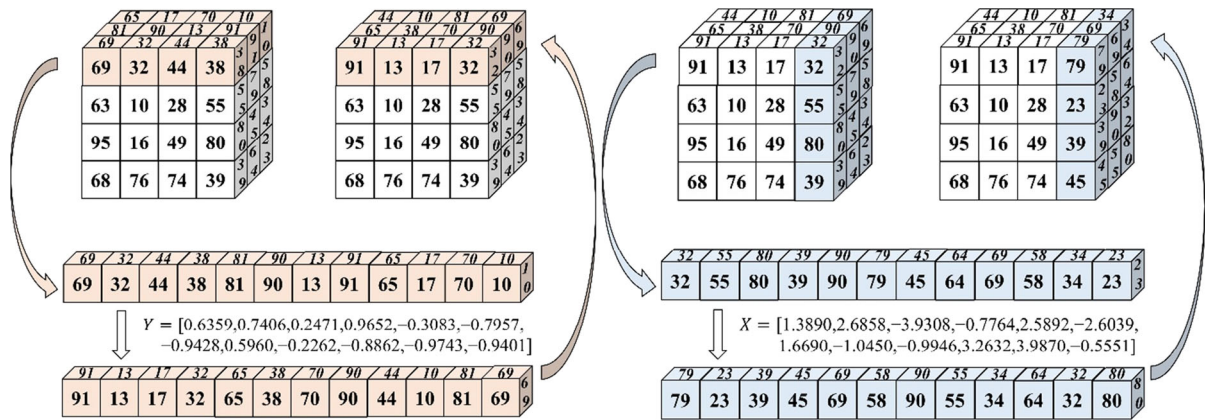


Fig. 9 Rubik's Cube scrambling

previous dimension and the values of the corresponding row in the diffusion matrix X' . Row diffusion is described as Eq. (12).

$$\begin{cases} D(1, :, 1) = (P'(1, :, 1) \ll 3) \oplus X'(1, :, 1) \\ D(i, :, k) = ((P'(i, :, k) \oplus D(i, :, k-1)) \ll 3) \oplus X'(i, :, k), k \neq 1 \\ D(i, :, k) = ((P'(i, :, k) \oplus D(i-1, :, 3)) \ll 3) \oplus X'(i, :, k), k = 1, i \neq 1 \end{cases} \quad (12)$$

where $D()$ is the result of row diffusion, $A \ll m$ represents that the binary of A is cyclically shifted to the left by m -bit, \oplus represents XOR operation, $i = 1, 2 \dots M, k = 1, 2, 3$.

Step 3. In the process of column diffusion, the pixel values of each column in the three dimensions of the matrix D are diffused with the pixel values in the previous dimension and the values of the corresponding column in the diffusion matrix Y' . Column diffusion is described as Eq. (13).

$$\begin{cases} C(:, 1) = (D(:, 1) \ll 3) \oplus Y'(:, 1) \\ C(:, j, k) = ((D(:, j, k) \oplus C(:, j, k-1)) \ll 3) \oplus Y'(:, j, k), k \neq 1 \\ C(:, j, k) = ((D(:, j, k) \oplus C(:, j-1, 3)) \ll 3) \oplus Y'(:, j, k), k = 1, j \neq 1 \end{cases} \quad (13)$$

where $C()$ is the result of column diffusion, $j = 1, 2 \dots N, k = 1, 2, 3$.

Step 4. After the above steps, the final ciphertext image C is obtained.

4 Decryption algorithm

Step 1. The reverse of three-dimensional column diffusion is described as Eq. (14).

$$\begin{cases} C'(:, 1) = (C(:, 1) \oplus Y'(:, 1)) \\ C'(:, j, k) = ((C(:, j, k) \oplus Y'(:, j, k)) \gg 3) \oplus C'(:, j, k-1), k \neq 1 \\ C'(:, j, k) = ((C(:, j, k) \oplus Y'(:, j, k)) \gg 3) \oplus C'(:, j-1, 3), k = 1, j \neq 1 \end{cases} \quad (14)$$

where $A \gg m$ represents the binary of A is cyclically shifted to the right by m -bit.

Step 2. The reverse of three-dimensional row diffusion is described as Eq. (15).

$$\begin{cases} C''(1, :, 1) = (C'(1, :, 1) \oplus X'(1, :, 1)) \\ C''(i, :, k) = ((C'(i, :, k) \oplus X'(i, :, k)) \gg 3) \oplus C''(i, :, k-1), k \neq 1 \\ C''(i, :, k) = ((C'(i, :, k) \oplus X'(i, :, k)) \gg 3) \oplus C''(i-1, :, 3), k = 1, j \neq 1 \end{cases} \quad (15)$$

Step 3. The pixel values in the matrix C'' are converted into 8-bit binary values to obtain the binary matrix D' with the size of $M \times 8N \times 3$. Traverse elements in index order sequence $S(i)$, $i = M + 8N, M + 8N - 1, \dots, 1$, pixel values of the $S(i) - M$ -th column are scanned into an array P'_1 and then reverse shuffled based on chaotic sequences X when $S(i) > M$, otherwise, pixel values of the $S(i)$ -th row are scanned into an array P'_2 and then reverse shuffled based on sequences Y . The reverse column scrambling and reverse row scrambling are described as Eqs. (16) and (17).

$$\begin{cases} \text{Exchange}(P'_1(i), P'_1(RP'_1(i))), i = 2, 3, \dots, 3 \times M \\ RP'_1(i) = \text{mod}(X(i), i - 1) + 1, i = 2, 3, \dots, 3 \times M \end{cases} \quad (16)$$

$$\begin{cases} \text{Exchange}(P'_2(i), P'_2(RP'_2(i))), i = 2, 3, \dots, 3 \times 8N \\ RP'_2(i) = \text{mod}(Y(i), i - 1) + 1, i = 2, 3, \dots, 3 \times 8N \end{cases} \quad (17)$$

Step 4. The matrix D' is converted into a decimal matrix and then the decryption image D is obtained.

5 Experimental results and security analysis

In this chapter, the performance of the proposed encryption algorithm is analyzed from many aspects by testing several color images of different sizes. The color images tested in the experiment include 256×256 Lena, 512×512 Baboon, 512×768 Motorcycle, 768×512 Sailboat and 1024×1024 Pepper. The plain images, encrypted images and decrypted images are shown in Fig. 10. It can be seen from the test results that the encrypted images hide the plaintext information well, indicating that the proposed algorithm has a good encryption effect on color images of any sizes.

5.1 Key space

A large key space ensures that the encryption algorithm can effectively resist violent attacks. From the perspective of cryptography, the key space should be greater than 2^{100} to provide high-security performance. The encryption algorithm proposed in this paper contains a 512-bit secret key, so the key space of the algorithm is 2^{512} , which is obviously greater than 2^{100} . Therefore, the encryption algorithm proposed in this paper has a better ability to resist violent attacks.

5.2 Histogram

For a digital image, the histogram is the statistics of gray level distribution in the image, which can intuitively reflect the number of different gray levels, so the histogram of the plaintext image has statistical significance. After encryption, the resulting ciphertext image should break the statistical distribution of the plaintext image. In the histogram of the encrypted

image, the frequency of each gray level should be as equal as possible, so that the histogram is uniform. Evenly distributed histograms indicate that image information is well hidden. Figure 11 shows the histograms of the plaintext images and ciphertext images tested in this chapter. The histograms of the encrypted image are all well-distributed enough to resist statistical attacks.

5.3 Differential attack analysis

Differential attack is a kind of selective plaintext attack, in which the attacker obtains two ciphertext images by making a slight change to the plaintext image and using the encryption algorithm to process two different plaintext images, respectively. By comparing and analyzing the differences between the two ciphertext images, the attacker can find the connection between the plaintext image and the ciphertext image. For a secure encryption algorithm, when the plaintext image changes slightly, the corresponding ciphertext should change significantly, which means that it has good resistance to differential attacks. The ability to resist the differential attack is measured by the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). The formula of NPCR and UACI is defined by Eqs. (18)–(20).

$$\text{NPCR} = \frac{\sum_{ij} D(i, j)}{M \times N} \times 100\% \quad (18)$$

$$D(i, j) = \begin{cases} 1, C_1(i, j) \neq C_2(i, j) \\ 0, C_1(i, j) = C_2(i, j) \end{cases} \quad (19)$$

$$\text{UACI} = \frac{1}{M \times N} \left[\sum_{ij} \frac{|C_1(i, j) - C_2(i, j)|}{255} \right] \times 100\% \quad (20)$$

where C_1 and C_2 , respectively, represent the ciphertext images generated by the encryption algorithm for the plaintext images with only one pixel difference. M and N indicate the number of rows and columns of the ciphertext image, respectively. For a digital image with a gray level of 256, the ideal NPCR value and UACI value are 99.6094% and 33.4635%, respectively.

The NPCR and UACI results of different tested images in this chapter are listed in Table 1. Table 2 shows the NPCR and UACI performance comparison



(a) Original Lena image (b) Encrypted Lena image (c) Decrypted Lena image



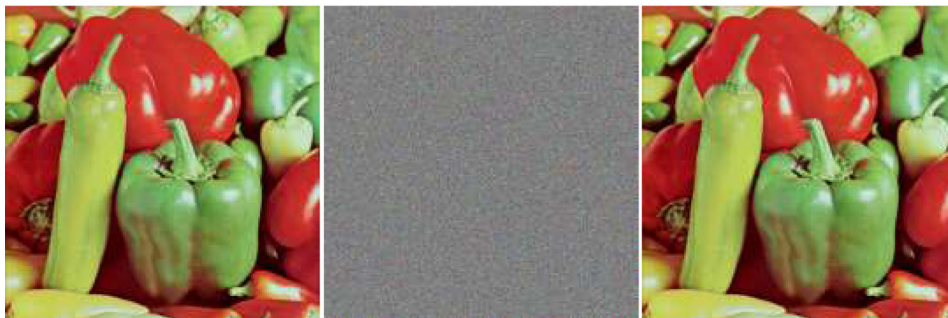
(d) Original Baboon image (e) Encrypted Baboon image (f) Decrypted Baboon image



(g) Original Sailboat image (h) Encrypted Sailboat image (i) Decrypted Sailboat image



(j) Original Motorcycle image (k) Encrypted Motorcycle image (l) Decrypted Motorcycle image



(m) Original Pepper image (n) Encrypted Pepper image (o) Decrypted Pepper image

Fig. 10 Encryption and decryption results of color images

Fig. 11 Histogram of original image and encrypted image

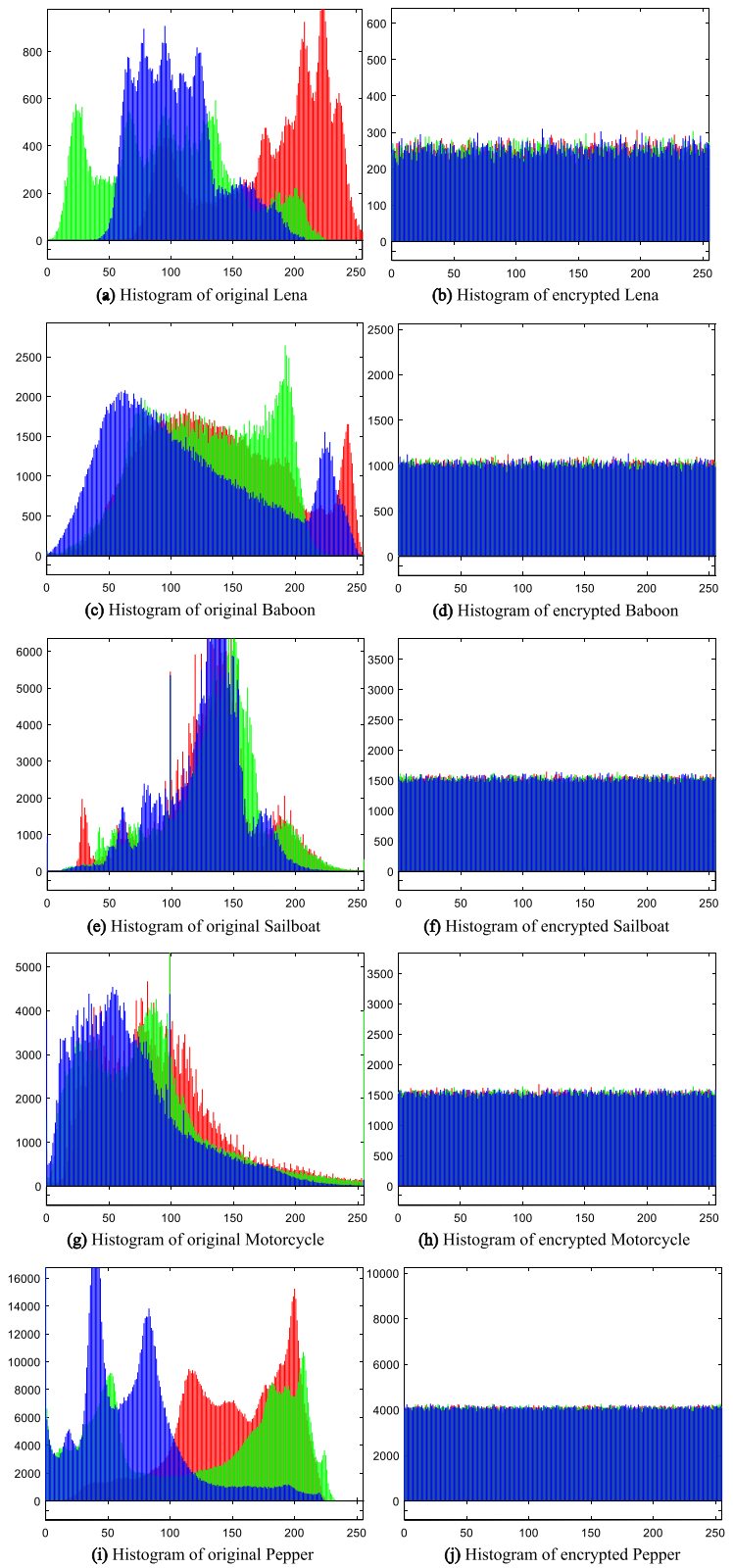


Table 1 Results of NPCR and UACI performance

Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Lena	99.6124	99.6063	99.6063	33.5176	33.4437	33.3704
Baboon	99.6010	99.6334	99.6246	33.4455	33.4965	33.4772
Sailboat	99.5850	99.5936	99.6101	33.4646	33.4560	33.4757
Motorcycle	99.6035	99.5931	99.6137	33.4493	33.4712	33.4968
Pepper	99.6107	99.6120	99.6066	33.4779	33.4486	33.4785
Mean	99.6025	99.6077	99.6123	33.4710	33.4632	33.4597

Table 2 Comparison of NPCR and UACI performance with other methods

Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Proposed	99.6025	99.6077	99.6123	33.4710	33.4632	33.4597
Ref. [3]	99.6561			33.4973		
Ref. [4]	99.5834			33.5314		
Ref. [5]	99.757			33.120		
Ref. [8]	99.5461	99.7066	99.6272	35.9229	36.6366	36.1533
Ref. [36]	99.61	99.61	99.61	33.34	33.34	33.34
Ref. [38]	99.6197	99.6117	99.6113	33.4423	33.4539	33.4647
Ref. [45]	99.6182	99.611	99.6114	33.4775	33.46	33.4564

of our algorithm with other methods. The comprehensive performance of NPCR and UACI of our algorithm is closer to the ideal theoretical value. Therefore, our algorithm has a better ability to resist differential attacks.

5.4 The correlation between adjacent pixels

To prevent attackers from obtaining effective information of the image by analyzing the correlation between adjacent pixels, the adjacent pixels in the ciphertext image must be as irrelevant as possible, that is, the correlation coefficient between adjacent pixels should be close to 0. The formula of the correlation coefficient r_{xy} is defined as Eq. (21).

where x and y are the gray values of two adjacent pixels in the image, $E(x)$ and $D(x)$ are the mathematical expectation and variance of x , respectively, $cov(x, y)$ is the covariance of x and y , and r_{xy} is the correlation coefficient.

$$\left\{ \begin{aligned} r_{xy} &= \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \\ E(x) &= \frac{1}{N} \sum_{i=1}^N x_i \\ D(x) &= \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \\ cov(x, y) &= \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)] \end{aligned} \right. \quad (21)$$

Randomly select adjacent pixels from plaintext Lena image and ciphertext image in the horizontal, vertical and diagonal directions, the corresponding correlation distributions of R, G, B channels are shown in Fig. 12. Table 3 lists the correlation coefficients of adjacent pixels in plaintext images and ciphertext images. It can be found that the proposed algorithm greatly reduces the correlation between adjacent pixels in ciphertext images. The comparison of the correlation coefficients between the proposed algorithm and other methods in horizontal, vertical and diagonal directions is indicated in Table 4. It can be seen that although some methods have better correlation coefficients in a certain direction, the

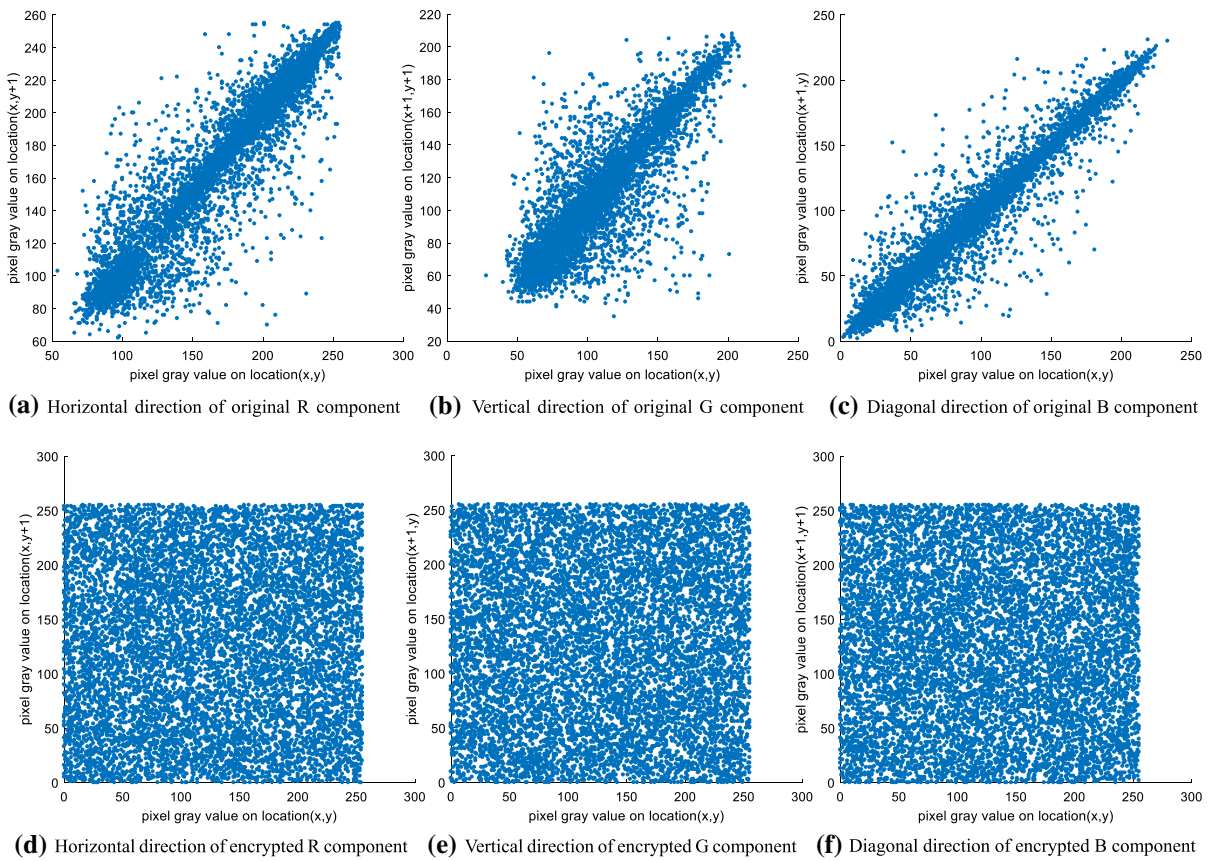


Fig. 12 Correlation distribution of plaintext image and encrypted image

Table 3 Correlation coefficients of ciphertext image and plaintext image

Image	Plaintext image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.969619	0.981948	0.952485	0.003496	- 0.000815	- 0.001055
Baboon	0.897008	0.833566	0.803960	0.002686	0.000187	0.000134
Sailboat	0.949887	0.958191	0.918254	0.001202	0.000587	0.001274
Motorcycle	0.898330	0.887201	0.851065	- 0.000231	0.001754	0.000531
Pepper	0.993474	0.994143	0.988268	- 0.002907	0.001687	- 0.002265
Mean	0.941664	0.931010	0.902807	0.000849	0.000680	- 0.000276

comprehensive performance of our algorithm in three directions is better than that of most other methods.

5.5 Information entropy

Information entropy is used to measure the uncertainty of digital images, and is an important indicator of randomness. The larger the information entropy of the image, the higher the uncertainty of the information it

contains. The mathematical expression of information entropy is defined as Eq. (22).

$$H(m) = - \sum_{i=1}^L p(m_i) \log_2 p(m_i) \tag{22}$$

where m_i represents the i -th pixel value, $p(m_i)$ is the probability of the symbol m_i , L is the gray level of image pixels. For a digital image with a gray level of

Table 4 Comparison of correlation coefficient with other methods

Image	Direction		
	Horizontal	Vertical	Diagonal
Proposed	0.000849	0.000680	− 0.000276
Ref. [1]	0.0003	− 0.0008	− 0.0003
Ref. [3]	− 0.0045	− 0.0023	0.0007
Ref. [4]	0.0083	− 0.0021	− 0.0025
Ref. [8]	0.0080	− 0.0032	− 0.0210
Ref. [19]	− 0.038118	− 0.029142	0.002736
Ref. [36]	0.00327	0.00663	0.00197
Ref. [38]	− 0.0049	0.0067	0.0006
Ref. [45]	0.001044	0.000746	0.000037

Table 5 Information entropy analysis

Image	R	G	B
Lena	7.9972	7.9974	7.9975
Baboon	7.9993	7.9994	7.9991
Sailboat	7.9995	7.9996	7.9995
Motorcycle	7.9996	7.9995	7.9995
Pepper	7.9998	7.9998	7.9998

256, the ideal value of information entropy is 8. When the information entropy value of the ciphertext image is close to 8, it indicates that the encryption algorithm has high security.

Table 5 calculates the information entropy of the encrypted images, and Table 6 shows the comparison of the information entropy between the proposed algorithm and other methods. The information entropy of R, G, B channels of our algorithm is quite close to the ideal value, which indicates that the proposed algorithm is highly secure.

5.6 Cropping and noise attacks

In the process of ciphertext image transmission, it is likely that partial data will be lost or disturbed by noise, which causes the receiver to fail to decrypt the correct plaintext image quickly.

A secure encryption algorithm must be able to resist data loss and cropping attacks. The test results of the

Table 6 Comparison of information entropy with other methods

Image	R	G	B
Proposed	7.9993	7.9994	7.9991
Ref. [1]	7.9023	7.9026	7.9021
Ref. [3]	7.9974	7.9974	7.9974
Ref. [36]	7.9975	7.9972	7.9973
Ref. [38]	7.9939	7.9939	7.9939
Ref. [40]	7.9974	7.9969	7.9973
Ref. [43]	7.9973	7.9972	7.9966
Ref. [45]	7.9912	7.9913	7.9914

image Lena subjected to data loss and noise attack are shown in Fig. 13. It can be seen that the image can still be decrypted and the main information of the image can be recognized regardless of the degree of data loss and noise attack. The test results prove that the proposed algorithm has high robustness.

5.7 Key sensitivity

Key sensitivity is one of the important indexes of secure cryptosystem. Due to the sensitivity of the chaotic system to initial values, a small change in the key will lead to significant changes in the encrypted image and failure of decryption. Figure 14 shows the decryption results when the initial values and parameters of the chaotic system are changed slightly, respectively. It can be found that slight changes in each parameter will lead to decryption failure. The test results show that the proposed algorithm is very sensitive to secret key.

5.8 Running performance

The proposed algorithm directly scrambles and transforms the three-dimensional matrix of the color image, avoiding the process of matrix transformation and reducing the number of iterations of the chaotic system. Therefore, the proposed algorithm exhibits rapid encryption and decryption efficiency. The running performance was tested on MATLAB 2020b, Intel Core i7-8750H CPU @2.20 GHz with 8 GB RAM and Windows 10 operating system. Table 7 lists the encryption and decryption times for tested images

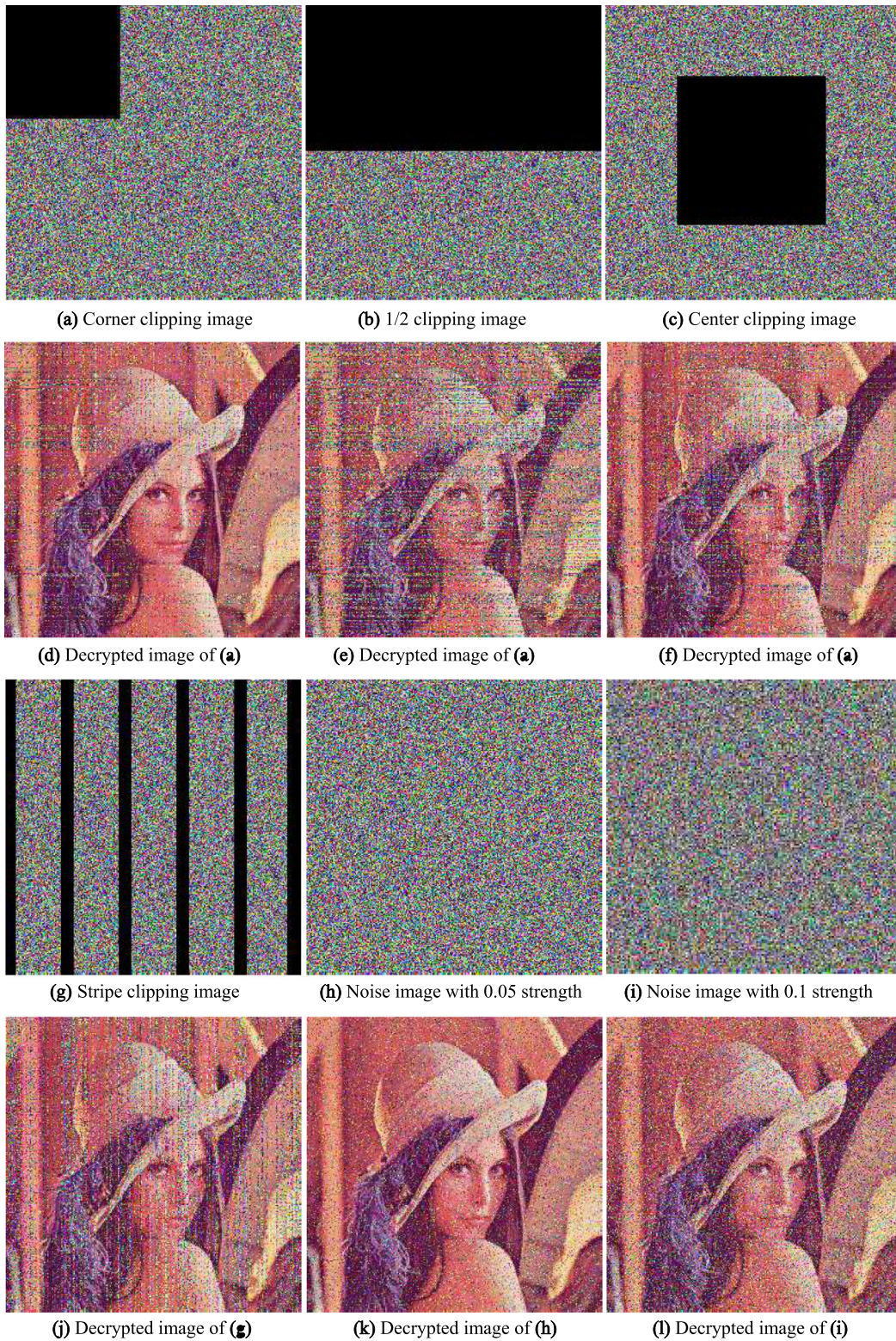


Fig. 13 Test results of cropping and noise attacks

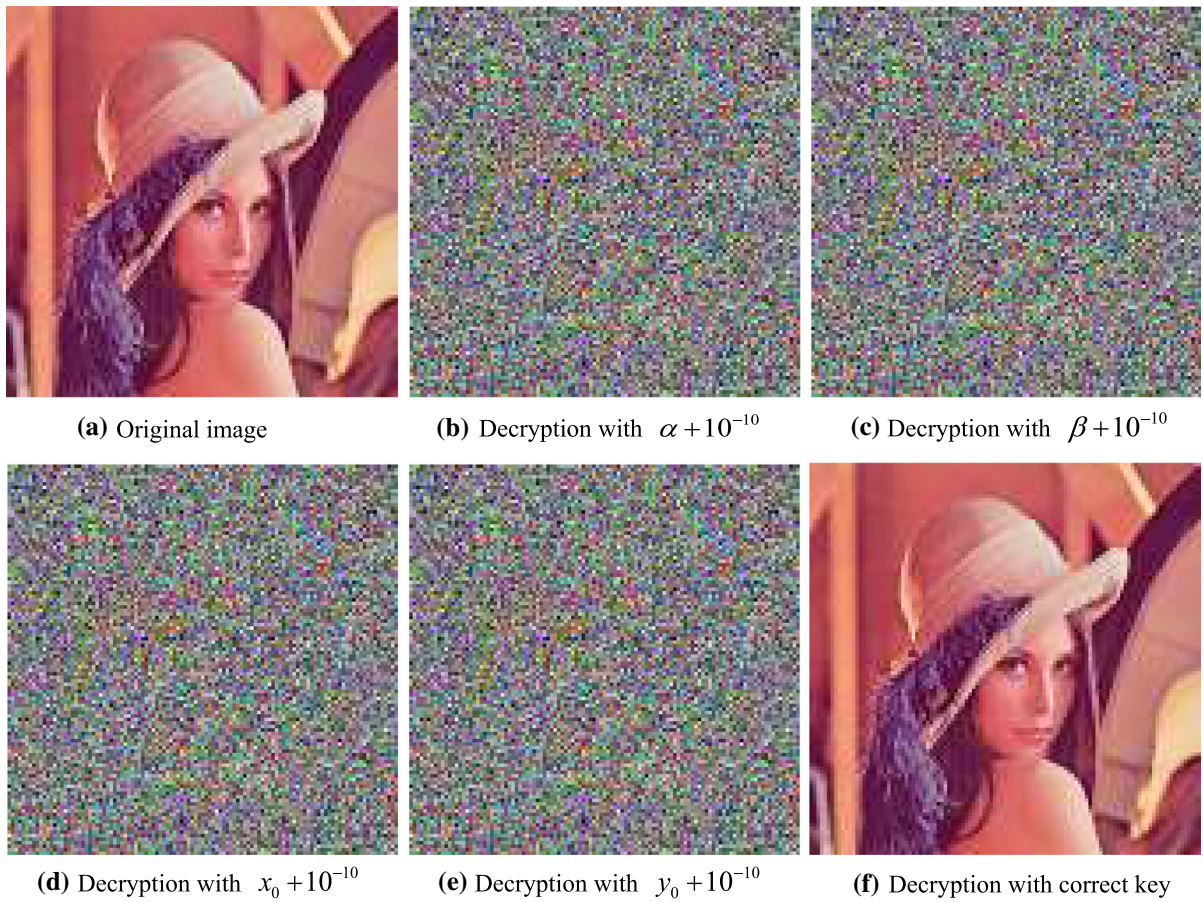


Fig. 14 Test results of key sensitivity

Table 7 Encryption and decryption time analysis

Image	Size	Encryption time (s)	Decryption time (s)
Lena	256 × 256	0.332128	0.259251
Baboon	512 × 512	1.305322	1.026494
Sailboat	768 × 512	1.920701	1.583331
Motorcycle	512 × 768	1.934233	1.556199
Pepper	1024 × 1024	5.183828	4.116702

of different sizes. It can be seen that the proposed algorithm completes image encryption and decryption in a few seconds. Table 8 shows the running time of our algorithm compared with other methods when encrypting and decrypting images of size 512 × 512. Obviously, our color image encryption algorithm has a better comprehensive running performance.

6 Conclusion

In this paper, the cross-operation coupling model is proposed to design a new hyperchaotic system. Derived from the Chebyshev map, Sine map and a nonlinear function $\cos(x)$, this paper constructs a novel two-dimensional Chebyshev-Sine coupling map (2D-CSCM). Phase diagram, bifurcation diagram, Lyapunov exponent spectra, information entropy analysis and 0–1 test illustrate that the proposed

Table 8 Comparison of encryption and decryption time with other methods

Methods	Encryption time (s)	Decryption time (s)
Proposed	1.305322	1.026494
Ref. [1]	2.3213	–
Ref. [4]	6.185524	6.093565
Ref. [8]	1.4933	7.8065
Ref. [38]	1.431	1.633
Ref. [45]	1.769709	0.837978

hyperchaotic system exhibits complex hyperchaotic behavior. The key of the proposed encryption algorithm is generated by the hash function SHA-512 to improve the sensitivity to the plaintext image. In the process of encryption, the 3D bit-level matrix of color plaintext image is directly shuffled by Rubik's Cube scrambling method. Then the scrambled matrix is diffused by three-dimensional row diffusion and three-dimensional column diffusion based on chaotic sequences. Test results and security analysis of different sizes of color image encryption prove that the proposed algorithm has high security and efficiency and can resist various attacks.

Funding The work is funded by the National Natural Science Foundation of China (Grant Nos. 61927803, 61071025, 61502538 and 61501525) and the Natural Science Foundation of Hunan Province of China (Grant No. 2015JJ3157).

Data availability Data sharing is not applicable to this article.

Declarations

Conflict of interest The authors declared that they have no conflicts of interest to this work.

References

- Sun, J.: A chaotic image encryption algorithm combining 2D chaotic system and random XOR diffusion. *Phys. Scr.* **96**(10), 105208 (2021)
- Khan, M., Jamal, S.S., Hazzazi, M.M., Ali, K.M., Hussain, I., Asif, M.: An efficient image encryption scheme based on double affine substitution box and chaotic system. *Integration* **81**, 108–122 (2021)
- Zhongyun, H., Zhihua, Z., Yongyong, C., Yuanman, L.: Color image encryption using orthogonal Latin squares and a new 2D chaotic system. *Nonlinear Dyn.* **104**, 4505–4522 (2021)
- Wang, X., Chen, S., Zhang, Y.: A chaotic image encryption algorithm based on random dynamic mixing. *Opt. Laser Technol.* **138**, 106837 (2021)
- Pourasad, Y., Ranjbarzadeh, R., Mardani, A.: A new algorithm for digital image encryption based on chaos theory. *Entropy* **23**(3), 341 (2021)
- Linqing, H., Shuting, C., Xiaoming, X., Mingqing, X.: On symmetric color image encryption system with permutation-diffusion simultaneous operation. *Opt. Lasers Eng.* **115**, 7–20 (2019)
- Zhongyun, H., Yicong, Z., Chi-Man, P., Philip Chen, C.L.: 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **297**, 80–94 (2015)
- Ahmad, I., Shin, S.: A novel hybrid image encryption-compression scheme by combining chaos theory and number theory. *Signal Process Image Commun.* **98**, 116418 (2021)
- Zhou, W., Wang, X., Wang, M., Li, D.: A new combination chaotic system and its application in a new Bit-level image encryption scheme. *Opt. Lasers Eng.* **149**, 106782 (2022)
- Coppersmith, D.: The data encryption standard (DES) and its strength against attacks. *IBM J. Res. Dev.* **38**(3), 243–250 (1994)
- Toughi, S., Fathi, M.H., Sekhavat, Y.A.: An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal Process.* **141**, 217–227 (2017)
- Chatterjee, A., Dhanotia, J., Bhatia, V., et al.: Optical image encryption using fringe projection profilometry. Fourier Fringe analysis, and RSA algorithm. In: 2017 14th IEEE India Council International Conference (INDICON), 2017: pp. 1–5.
- Gupta, S., Jain, A.: Efficient image encryption algorithm using DNA approach. In: International conference on computing for sustainable global development. IEEE, pp. 726–731 (2015).
- Wu, X., Kurths, J., Kan, H.: A robust and lossless DNA encryption scheme for color images. *Multimed. Tools Appl.* **77**(10), 12349–12376 (2018)
- Wang, X.Y., Luan, D.P.: A novel image encryption algorithm using chaos and reversible cellular automata. *Commun Nonlinear Sci Numer Simul* **18**, 3075–3085 (2013)
- Yaghouti, N.A., Moattar, M.H., Torshiz, M.N.: Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **90**, 225–237 (2017)
- Zhang, D., Liao, X., Yang, B., et al.: A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform. *Multimed Tools Appl* **77**(9), 1–18 (2017)
- Kong, D., Shen, X.: Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Opt Laser Technol* **57**(4), 343–349 (2014)
- Zhou, M., Wang, C.: A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Process.* **171**, 107484 (2020)
- Sahari, M.L., Boukemara, I.: A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. *Nonlinear Dyn.* **94**(1), 723–744 (2018)

21. Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., Zhou, R., Cao, Y., Ding, X.: A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Process.* **161**, 227–247 (2019)
22. Dragoi, I.-C., Coltuc, D.: On local prediction based reversible watermarking. *IEEE Trans. Image Process.* **24**, 1244–1246 (2015)
23. Gong, L., Qiu, K., Deng, C., Zhou, N.: An optical image compression and encryption scheme based on compressive sensing and rsa algorithm. *Opt. Lasers Eng.* **121**, 169–180 (2019)
24. Lorenz, E.N.: *Deterministic Nonperiodic Flow*. American Meteorological Society, Boston (1963)
25. May, R.M.: Simple mathematical models with very complicated dynamics. *Nature* **261**, 459–467 (1976). <https://doi.org/10.1038/261459a0>
26. Feigenbaum, M.J.: The universal metric properties of nonlinear transformations. *J. Stat. Phys.* **21**(6), 669–706 (1979)
27. Peng, H.H., Xu, X.M., Yang, B.C., Yin, L.Z.: Implication of two-coupled differential Van der Pol duffing oscillator in weak signal detection. *J. Phys. Soc. Jpn.* **85**(4), 044005 (2016)
28. Luo, J.J., Xu, X.M., Ding, Y.P., Yang, B.C., Yuan, Y.B., Sun, K.H., Yin, L.Z.: Application of a memristor-based oscillator to weak signal detection. *Eur. Phys. J. Plus* **133**(6), 239–249 (2018)
29. Thajeel, S.A., Al-Tamimi, M.S.H.: An improve image encryption algorithm based on multi-level of chaotic maps and lagrange interpolation. *Iraqi J. Sci.* **59**(1A), 179–188 (2018)
30. Yang, F., et al.: Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Opt. Lasers Eng.* **129**, 106031 (2020)
31. Zhang, Y.Q., Wang, X.Y.: Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. *Nonlinear Dyn.* **77**(3), 687–698 (2014)
32. Liu, L., Jiang, D., Wang, X., Rong, X., Zhang, R.: 2D Logistic-adjusted-chebyshev map for visual color image encryption. *J. Inf. Secur. Appl.* **60**, 102854 (2021)
33. Qiaoyun, X., Kehui, S., Chun, C., Congxu, Z.: A fast image encryption algorithm based on compressive sensing and hyperchaotic map. *Opt. Lasers Eng.* **121**, 203–2014 (2019)
34. Hua, Z., Jin, F., Xu, B., et al.: 2D Logistic-Sine-coupling map for image encryption. *Signal Process* **149**, 148–161 (2018)
35. Tang, Z., Song, J., Zhang, X.: Multiple-image encryption with bit-plane decomposition and chaotic maps. *Opt. Lasers Eng.* **80**, 1–11 (2016)
36. Liu, W., Sun, K., Zhu, C.: A fast image encryption algorithm based on chaotic map. *Opt Lasers Eng.* **84**, 26–36 (2016)
37. Hu, Y., Li, Q., Ding, D., Jiang, L., Yang, Z., Zhang, H., Zhang, Z.: Multiple coexisting analysis of a fractional-order coupled memristive system and its application in image encryption. *Chaos Solitons Fractals Interdiscip J Nonlinear Sci Nonequilib Complex Phenomena* **152**, 111334 (2021)
38. Wang, X., Zhao, M.: An image encryption algorithm based on hyperchaotic system and DNA coding. *Opt. Laser Technol.* **143**, 107316 (2021)
39. Guanrong, C., Yaobin, M., Charles, K.C.: A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fract* **21**(3), 749–761 (2004)
40. ul Haq, T., Shah, T.: 4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion. *J Inf Secur Appl* **61**, 102931 (2021)
41. Yue, W., Yang, G., Jin, H., et al.: Image encryption using the two-dimensional logistic chaotic map. *J. Electron. Imag.* **21**(1), 3014 (2012)
42. Zhongyun, H., Fan, J., Binxuan, X., Hejiao, H.: 2D Logistic-Sine-coupling map for image encryption. *Signal Process* **149**, 148–161 (2018)
43. Gao, X.: A color image encryption algorithm based on an improved Hénon map. *Phys. Scr.* **96**(6), 065203 (2021)
44. Khalil, N., Sarhan, A., Alshewimy, M.A.M.: An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Opt. Laser Technol.* **143**, 107326 (2021)
45. Teng, L., Wang, X., Yang, F., Xian, Y.: Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. *Nonlinear Dyn* **105**, 1859–1876 (2021)
46. Bandt, C., Pompe, B.: Permutation entropy: a natural complexity measure for time series. *Phys. Rev. Lett.* **88**(17), 174102 (2002)
47. He, S., Sun, K., Wang, H.: Complexity analysis and DSP implementation of the fractional-order Lorenz hyperchaotic system. *Entropy* **17**(12), 8299–8311 (2015)
48. Gottwald, G.A., Melbourne, I.: A new test for chaos in deterministic systems. *Proc R Soc A Math Phys Eng Sci* **460**(2042), 603–611 (2004)
49. Gottwald, G.A., Melbourne, I.: Testing for chaos in deterministic systems with noise. *Phys. D* **212**(1–2), 100–110 (2005)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.