Color Image Encryption Based on Cross 2d Hyperchaotic Map Using Combined Cycle Shift Scrambling and Selecting Diffusion

Lin Teng (tenglin@mail.dlut.edu.cn)
Dalian Maritime University https://orcid.org/0000-0002-3758-4439
Xingyuan Wang
Dalian Maritime University
Feifei Yang
Dalian Maritime University
Yongjin Xian
Dalian Maritime University

Research Article

Keywords: Cross 2D hyperchaotic map, color image encryption, combined cycle shift scrambling, selecting diffusion

Posted Date: March 9th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-247406/v1

Version of Record: A version of this preprint was published at Nonlinear Dynamics on July 5th, 2021. See the published version at https://doi.org/10.1007/s11071-021-06663-1.

Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion

Lin Teng[1*], Xingyuan Wang[1, 2], Feifei Yang[1], Yongjin Xian[1]

(1 School of Information Science and Technology, Dalian Maritime University, Dalian, 116026, China)

(2 Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, Guilin 541004, China)

Corresponding author: Lin Teng (e-mail: tenglin@mail.dlut.edu.com).

Abstract: A novel color image encryption algorithm based on a cross 2D hyperchaotic map is proposed in this paper. The cross 2D hyperchaotic map is constructed using one nonlinear function and two chaotic maps with cross structure. Chaotic behaviors are illustrated using bifurcation diagrams, Lyapunov exponent spectra and phase portraits, etc. In the color image encryption algorithm, the keys are generated using hash function SHA-512 and the information of plain color image. First, the color plain image is converted to a combined bit-level matrix and permuted by the chaos based row and column combined cycle shift scrambling method. Then the scrambled integer matrix is diffused according to the selecting sequence which depends on the chaotic sequence. Last, the cipher color image is obtained by decomposed the diffused matrix. Simulation results show that the algorithm can encrypt the color image effectively and has good security.

keywords: Cross 2D hyperchaotic map; color image encryption; combined cycle shift scrambling; selecting diffusion

1. Introduction

With the rapid development of Internet, big data, artificial intelligence and 5G communications, a large amount of information has been digitized and transmitted over the network. As an important information carrier, the security of digital image attracts more and more attention. Because of color images contain richer information than grey-level images, the related research in color image encryption has become a research hotspot[1-10].

Image encryption is different from text encryption, because image has the characteristics of massive data capacity and high correlation between pixels. Therefore, traditional encryption technologies such as DES, IDES and RSA are no longer suitable for image encryption. Chaotic system has the characteristics of sensitivity to control parameters and initial conditions, ergodicity, random like behavior and unpredictable orbit. It corresponds to the concepts of key design, confusion, diffusion and round robin in cryptography, which makes chaos theory have great potential in the field of cryptography.

In recent years, many chaos-based image encryption algorithms have been developed[11-20]. Due to the limited precision of the computer, the dynamic behavior of most low dimensional

chaotic systems degenerates, which leads to the defects of small key space and weak security performance. The image encryption algorithms designed by using high-dimensional continuous chaotic system still have defect that the cipher image can be cracked by known plaintext attack or selected plaintext attack[21-24]. In addition, the computational complexity and time cost of the encryption algorithm are increased.

Hyperchaotic systems with multiple positive Lyapunov exponents usually have more complex and richer dynamic behaviors than chaotic systems which can enhance the randomness and higher unpredictability of the corresponding system[25]. Therefore, when applied to encryption, the hyperchaotic system can generate larger key space and more complex random sequences. Using hyperchaotic system to design color image encryption algorithm will greatly improve the security of the algorithm[26-32].

How to design encryption algorithm based on the characteristics of color image and chaotic system still has a large research value. In recent years, some new chaotic maps have been applied to image encryption algorithms[33-37]. Some of the new chaotic maps still have defects that trajectory is not distributed in the whole phase space or has no complex dynamic behavior.

In view of the above shortcomings, we design a nonlinear discrete cross 2D hyperchaotic map, and propose a color image encryption algorithm based on this map. The 2D hyperchaotic map is constructed using one nonlinear function and two chaotic maps with cross structure. Chaotic behaviors are illustrated using bifurcation diagrams, Lyapunov exponent spectra and phase portraits, etc. Simulation results show that the cross 2D hyperchaotic map has good chaotic performance. In the color image encryption algorithm, the keys are related to the plain color image, that is, different plain image will generate different keys which will enhance the security to resist the chosen plaintext/ciphertext attack. The color plain image is converted to a combined bit-level matrix and permuted by the chaos based row and column combined cycle shift scrambling method. Then the scrambled integer matrix is diffused according to the selecting sequence which depends on the chaotic sequence. The cipher color image is obtained by decomposed the diffused matrix. The proposed encryption algorithm makes the three color components of color image affect each other to eliminate the correlations between them. Simulation results show that the algorithm can encrypt the color image effectively and has good security.

The rest of this paper is organized as follows. Section 2 introduces the model of the nonlinear cross 2D hyperchaotic map. In section 3, the dynamic behaviors of proposed cross 2D hyperchaotic map is analyzed. Section 4 describes the encryption and decryption algorithm of color image. In section 5, the experiments results and the security of the algorithm are evaluated. Section 6 concludes the paper.

2. Cross 2D hyperchaotic map

In this paper, a cross 2D hyperchaotic map is proposed, and the structure is shown in Figure 1. This model has two inputs and two cross outputs, which is when input is x_n the output is y_{n+1}, and when input is y_n the output is x_{n+1}. Function f is a nonlinear function, functions F and G are two chaotic maps. The + sign represents the addition of two input terms. The mathematical expression of the model is shown in Formula (1).

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

where F and G can be chosen as any one-dimensional chaotic map.

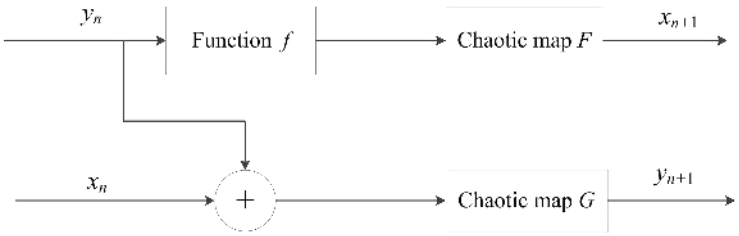


Figure 1 Diagram of Nonlinear cross 2D hyperchaotic map

The chaotic map F is chosen as the infinite collapse map[38] defined as

$$x_{i+1} = \sin\left(\frac{\alpha}{x_i}\right) \tag{2}$$

where its control parameter $\alpha \neq 0$. And the chaotic map G is chosen as the Sine map in this paper. The Sine map is given as

$$x_{i+1} = \beta \sin(\pi x_i) \tag{3}$$

where β is a control parameter and it has an interval of (0,1]. The nonlinear function f is set to sin function, that is $f(x) = \sin(x)$. So the mathematical expression of the modified 2D coupled chaotic map model is set to

$$\begin{cases} x_{i+1} = \sin\left(\dfrac{\alpha}{\sin(y_i)}\right) \\ y_{i+1} = \beta \sin(\pi(x_i + y_i)) \end{cases} \tag{4}$$

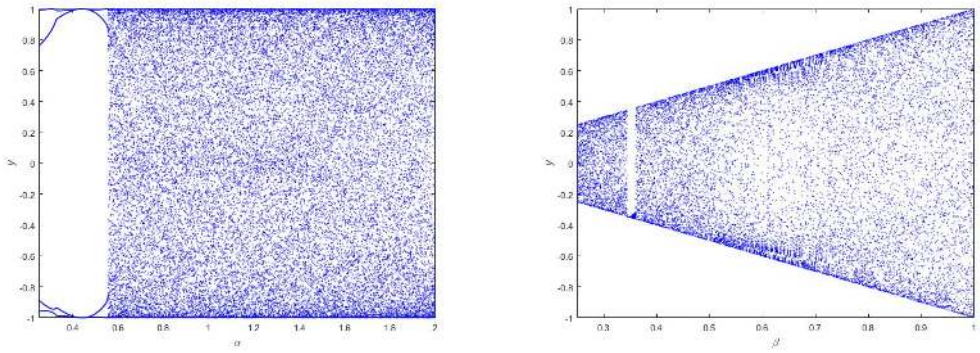
where its control parameter $\alpha \neq 0$, $\beta \in (0,1]$, the initial value $y_0 \neq 0$.

3 Dynamics analysis of the cross 2D hyperchaotic map

3.1 Bifurcation diagram

The dynamical behaviors of a chaotic system can be evaluated by its bifurcation diagram. A bifurcation diagram shows the changes of the system motion state along with the control parameters. The evolution process of the system can be directly observed by the bifurcation diagram. Set the initial conditions $x_0 = 0.3$ and $y_0 = 0.6$. Fixing $\beta = 1$, the bifurcation diagram for control parameter α over the range [0.25, 2] is generated in Figure 2(a). From Figure 2(a),

we can see that the system goes through periodic state to chaotic orbit. When $0.55 < \alpha \le 2$, the system exhibits the chaotic behavior. Fixing $\alpha = 1$, the bifurcation diagram for control parameter β over the range [0.1, 1] is generated in Figure 2(b). It can be acquired that the system exhibits the periodic behavior between (0.34, 0.353), and the system can generate chaotic attractors all through the remaining range.



(a) Bifurcation diagram for y against α (b) Bifurcation diagram for y against β

Figure 2 Bifurcation diagrams of the proposed system

3.2 Lyapunov exponent spectrum

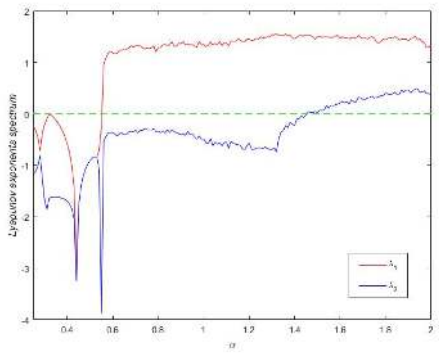
The Lyapunov exponent represents the numerical characteristics of the average exponential divergence rate of adjacent trajectories in phase space. It is one of the characteristics used to identify the chaotic characteristics of dynamic systems. For a high-order dynamic system, due to the different directions of the initial separation vector, the exponential divergence rate will be different, so there are multiple Lyapunov exponents, and the number of Lyapunov exponents is equal to the order of the system. Therefore the two dimensional system has two Lyapunov exponents. The Lyapunov exponents of the system are two negatives indicates the system is in fixed points. When the system is in periodic orbits, the Lyapunov exponents of the system are one zero and one negatives. When the system is in chaotic orbits, the Lyapunov exponents of the system are one positive, one negative. When the system is in hyperchaotic state, the Lyapunov exponents of the system are two positives. Hyperchaotic systems usually have more complex and richer dynamic behaviors than chaotic systems, which enhance the randomness and unpredictability.

Fixing $\beta = 1$ and varying α, the Lyapunov exponents spectrum is shown in Figure 3(a). It can be seen that when $\alpha \in (1.55,\ 1.47)$, the largest Lyapunov exponent is positive, so the system is in chaotic state. When $\alpha \in [1.47,\ 2]$, the two Lyapunov exponents are both positive, so the system can generate hyperchaotic attractors.

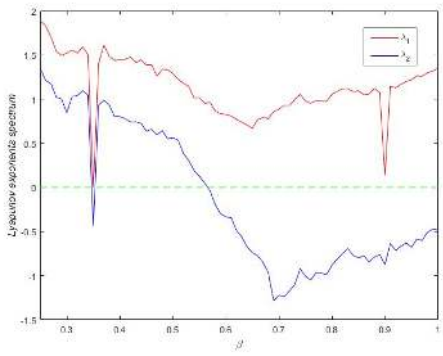
Figure 3(b) shows the Lyapunov exponents spectrum varying β when $\alpha = 1$. We can see that the system exhibits the periodic behavior when $\beta \in (0.34,\ 0.353)$. There are two positive

Lyapunov exponents when $\beta \in [0.25,\ 0.34] \cup [0.354,\ 0.56]$, and the system is in hyperchaotic state. The system can exhibits chaotic attractor in the range of $\beta \in (0.56,\ 1]$.

It can be seen that the spectrum of Lyapunov exponents spectrums and the bifurcation diagrams are one to one correspondence.



(a) Lyapunov exponents spectrum varying α

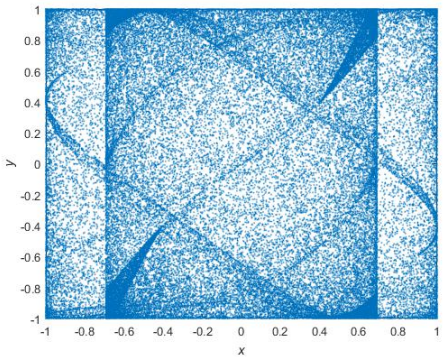


(b) Lyapunov exponents spectrum varying β

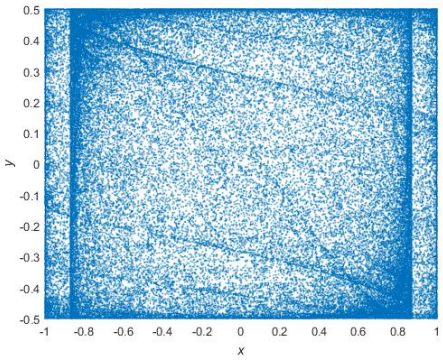
Figure 3 Lyapunov exponents spectrum

3.3 Attractor phase diagram

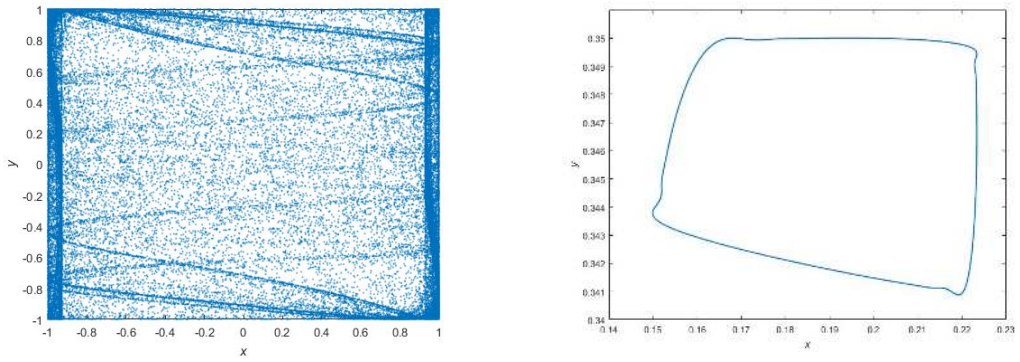
A chaotic system with good chaotic performance usually has complex attractors which occupy a large area in the phase diagram. Set the initial conditions $x_0 = 0.3$ and $y_0 = 0.6$, the attractor phase diagrams are generated in Figure 4. The system generate the hyperchaotic attractors as shown in phase diagrams Figure 4(a) and Figure 4(b) when parameters $\alpha = 2$, $\beta = 1$ and $\alpha = 1$, $\beta = 0.5$. When parameters $\alpha = 1$ and $\beta = 1$, the attractor phase diagram is shown in Figure 4(c), the system generate the chaotic attractor. When parameters $\alpha = 1$ and $\beta = 0.35$, the system exhibits the periodic behavior as shown in Figure 4(d).



(a) α =2 β =1



(b) α =1 β =0.5

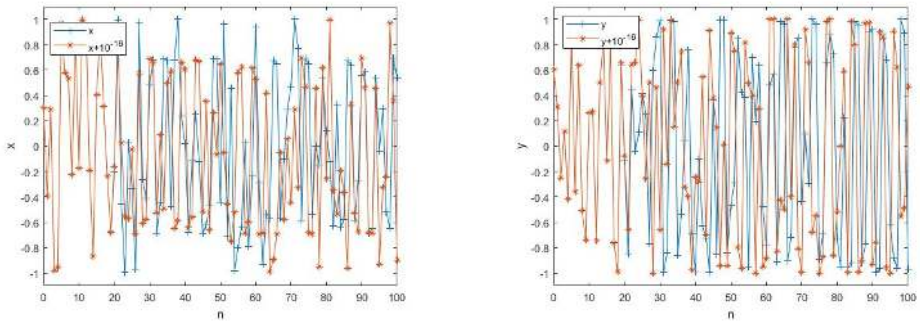


(c) α =1 β =1 (d) α =1 β =0.35

Figure 4 Attractor phase diagrams

3.4 Sensitivity analysis of initial value

A good performance chaotic system is very sensitive to initial value. Slightly different initial value will produce totally different chaotic trajectory. To analysis the initial sensitivity of the proposed hyperchaotic system, the initial values are changed 10^{-16}, and the experiment results are shown in Figure 5. It can be seen that the proposed hyperchaotic system is very sensitive to initial values.



(a) x_0 changed 10^{-16} (b) y_0 changed 10^{-16}

Figure 5 Initial value sensitivity

4. Cross 2D hyperchaotic map based color image encryption and decryption algorithm

As the proposed cross 2D hyperchaotic map has good chaotic performance, a color image encryption and decryption algorithm based on this chaotic map is proposed in this section. Figure 6 shows the flowchart of proposed encryption algorithm which includes permutation process and diffusion process.

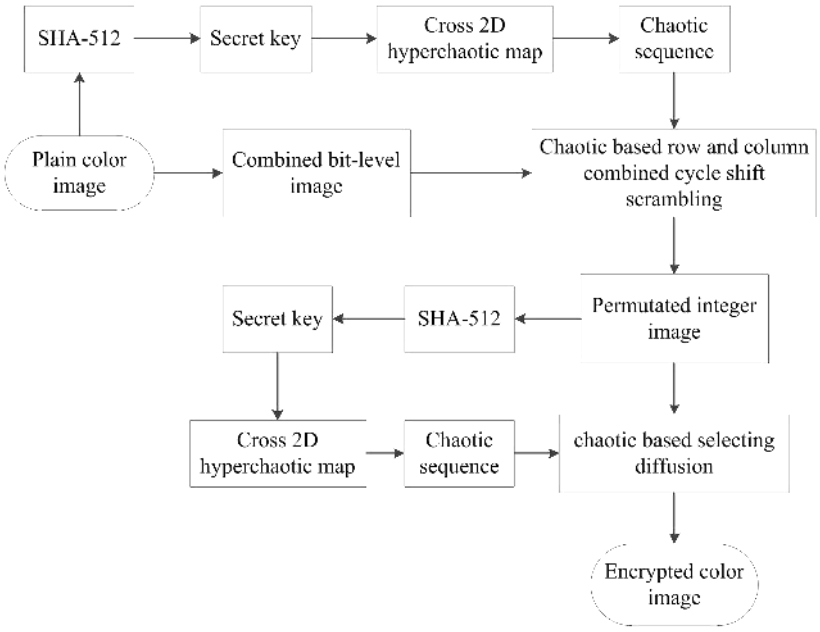


Figure 6 Flowchart of proposed encryption algorithm

4.1 Key generation

Because of the irreversibility and strong security of hash algorithm, we use it to generate the key of the color image encryption algorithm. A 512-bit secret key K is generated by SHA-512 hash function $K = SHA_{512}(\ )$, which the input value of this hash algorithm is related to the plain color image in order to increase the security and able to resist select plaintext/ ciphertext attack. Divide the 512-bit key K into 8-bit blocks, which can be expressed as $K=k_1,k_2,...,k_{64}$. K is processed and grouped in sub-keys as follows:

$$\begin{cases} K1 = \dfrac{k_1 \oplus k_2 \oplus ... \oplus k_{16}}{256} \\ K2 = \dfrac{k_{17} \oplus k_{18} \oplus ... \oplus k_{32}}{256} \\ K3 = \dfrac{k_{33} \oplus k_{34} \oplus ... \oplus k_{48}}{256} \\ K4 = \dfrac{k_{49} \oplus k_{50} \oplus ... \oplus k_{64}}{256} \end{cases} \tag{5}$$

4.2 Chaos based row and column combined cycle shift scrambling

In the scrambling processing, the image pixels positions are changed to average the statistical information of the image, so the energy of the image can be uniform. A chaos based row and column combined cycle shift scrambling method is proposed:

Step 1. Suppose the size of the image matrix is $M\times N$, that is M rows and N columns. Set the row vectors PR and column vectors PC. Process rows and columns together, there are $M+N$ vectors.

Step 2. Select a chaotic sequence X_1 with length $M+N$, chaotic sequence X_2 with length M

and chaotic sequence X_3 with length N. The chaotic sequences are further processed by

$$X_1'(i) = \mathrm{mod}(ceil(X_1(i) \times 10^{15}), M+N), \quad 1 \le i \le M+N \tag{6}$$

$$X_2'(j) = \mathrm{mod}(ceil(X_2(j) \times 10^{15}), N), \quad 1 \le j \le M \tag{7}$$

$$X_3'(k) = \mathrm{mod}(ceil(X_3(k) \times 10^{15}), M), \quad 1 \le k \le N \tag{8}$$

where *ceil*(*x*) returns the smallest integer greater than or equal to *x*, mod( ) represents the modular operation.

Step 3. Sort the sequence X_1', record the transform position *TP* of every element in the chaotic sequence, thus the length of vector *TP* is *M*+*N* and the elements of *TP* are all non-repeating integers between 1 and *M*+*N*.

Step 4. Exchange the locations of image elements using row and column combined cycle shift by

$$\begin{cases} PR(TP(i)) = circshift(PR(TP(i)), X_2'(j)), \ j = j+1 & TP(i) \le M \\ PC(TP(i)-M) = circshift(PC(TP(i)-M), X_3'(k)), k = k+1 & TP(i) > M \end{cases} \tag{9}$$

where $circshift(A, SHIFTSIZE)$ circularly shifts the values in the array *A* by *SHIFTSIZE* elements. When $TP(i) \le M$, circularly shift the $TP(i)$ th row by $X_2'(j)$ elements to the right. When $TP(i) > M$, circularly shift the $TP(i) - M$ th column by $X_3'(k)$ elements down.

Take an image matrix with the size of 4×4 as an example shown in Figure 7. Where *TP*= {8, 1, 4, 7, 3, 2, 5, 6}, X_2' = {3, 2, 3, 1}, X_3' = {2, 0, 1, 3}. It can be seen that each pixel changes its position after only one scrambling turn.

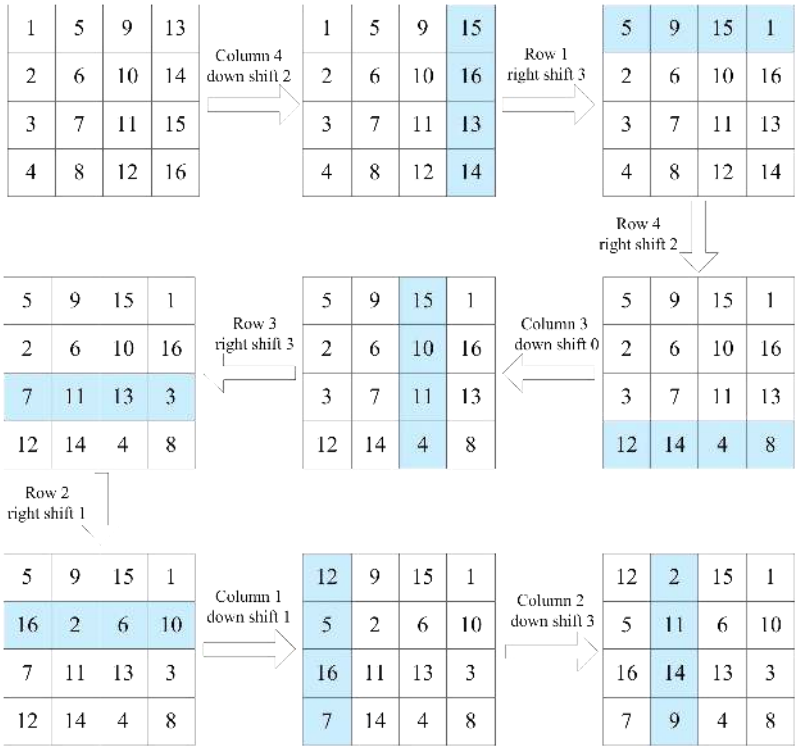


Figure 7 4×4 matrix scrambled by row and column combined cycle shift

4.3 Permutation process

Step 1. Without loss of generality, assume the size of the color plain-image P is $M\times N$. And the color image has three components: red (R), green (G) and blue (B). The value of each component pixel is range from 0 to 255. So each pixel can transform to 8-bit binary value. Therefore, an $M\times N$ size color image P can be extended to three binary image matrixes R_b, G_b and B_b with size $M\times 8N$. Combine the R_b, G_b and B_b matrixes vertically and get a combined image matrix P_b with $3\times M$ rows, $8\times N$ columns. Thus the three components of the color image can be affected by each other.

Step 2. Set the permute key $K_{permute} = SHA_{512}(R,G,B)$, which R, G and B are all the pixels in each color components of plain-image, so that different plain-image will get different key. Obtain the sub-keys $K1$, $K2$, $K3$, $K4$ according to equation (5), and set the parameters and initial conditions of chaotic system (4) using:

$$\begin{cases} \alpha = \mathrm{mod}(K1, 0.5) + 1 \\ \beta = \mathrm{mod}(K2, 0.5) + 0.6 \\ x_0 = \mathrm{mod}(K3, 1) \\ y_0 = \mathrm{mod}(K4, 1) \end{cases} \tag{10}$$

Step 3. Iterate the chaotic system (4) $3M+8N+k$ times, k is the length of the sequence discarded for better chaos. Where $k = \mathrm{mod}(sum(R+G+B), 100) + 500$, and $sum(R+G+B)$ means the sum of all the elements in three components. Get the chaotic sequences

$x(i) = \{x_1, x_2, ..., x_{3M+8N}\}$ and $y(i) = \{y_1, y_2, ..., y_{3M+8N}\}$.

Step 4. Use the chaos based row and column combined cycle shift scrambling method described in section 4.2 to permute the bit-level image matrix P_b with the size of $3M \times 8N$. Where the chaotic sequence $X_1 = x(i)$ (i=1, 2,…, $3M+8N$), $X_2 = y(i)$ (i=1, 2,…, $3M$), $X_3 = y(i)$ (i=$3M$+1,…, $3M$+$8N$). A permutated bit-level image matrix P_b' is generated.

Step 5. Transform P_b' to an integer image matrix denoted as P' with the size of $3M \times N$. The position of pixels are changed as well as the value of the pixels in the permutated image P'.

4.4 Diffusion process

In diffusion process, the pixel values of an image are modified so that a tiny change in one-pixel spreads out to as many pixels as possible. The proposed diffusion equation is chosen according to the selecting sequence which depends on the chaotic sequence.

Step 1. Set the diffuse key $K_{diffuse} = SHA_{512}(P'([i\ j\ k],:))$, where $P'([i\ j\ k],:)$ is the ith row, jth row and kth row of permutated image matrix P'. Obtain the sub-keys $K1'$, $K2'$, $K3'$, $K4'$ according to equation (5), and set the parameters and initial conditions of chaotic system (4) using equation (10).

Step 2. Iterate the chaotic system (4) $3M \times N + k_1$ times, where $k_1 = \mathrm{mod}(sum(sum(P'(:, i:j))), 100) + 500$, $P'(:, i:j)$ is the ith to jth columns of P'. Discard the former k values of the chaotic sequences. Get the chaotic sequences $x'(i) = \{x_1', x_2', ..., x_{3M \times N}'\}$ and $y'(i) = \{y_1', y_2', ..., y_{3M \times N}'\}$.

Step 3. The selecting sequence $S(i) = \{s_1, s_2, ..., s_{3M \times N}\}$ and the diffusion sequence $D(i) = \{d_1, d_2, ..., d_{3M \times N}\}$ can be calculated using equation (11) and equation (12)

$$S(i) = \mathrm{mod}(ceil(x'(i) \times 10^{15}), 3) \tag{11}$$

$$D(i) = \mathrm{mod}(ceil(y'(i) \times 10^{15}), 256) \tag{12}$$

Step 4. The encrypted combined image pixel matrix $C'(i) = \{c_1', c_2', ..., c_{3M \times N}'\}$ can be acquired from the diffusion matrix D and the permuted image P' according to the chaotic based selecting diffusion equations:

$$\begin{cases} C'(i) = \mathrm{mod}(P'(i) + D(i), 256) & S(i) = 0 \\ C'(i) = \mathrm{mod}(P'(i) - D(i), 256) & S(i) = 1 \\ C'(i) = P'(i) \oplus D(i) & S(i) = 2 \end{cases} \tag{13}$$

where $\oplus$ denotes bit-level *XOR* operator.

Step 5. Convert C' into the *R*, *G* and *B* color matrix vertically to get its cipher color image *C* with the size of $M \times N$.

4.5 Decryption algorithm

Decryption algorithm is the reverse of encryption using the permute key $K_{permute}$ and the diffuse key $K_{diffuse}$ provided in the encryption algorithm, that means $K_{permute}$ and $K_{diffuse}$ should be provided and known in the decryption process.

Step 1. Obtain the cipher image *C* and convert it into the *R*, *G* and *B* color matrix. Combine the color matrixes vertically and get a combined encrypted image matrix C' with 3×*M* rows, *N* columns.

Step 2. Use the same diffuse key $K_{diffuse}$ as the encryption algorithm to obtain the same selecting sequence $S(i)$ and the diffusion sequence $D(i)$.

Step 3. The matrix C_D can be acquired from the diffusion matrix *D* and the encrypted image matrix C' using inverse diffusion process equations:

$$\begin{cases} C_D(i) = \mathrm{mod}(C'(i) - D(i), 256) & S(i) = 0 \\ C_D(i) = \mathrm{mod}(C'(i) + D(i), 256) & S(i) = 1 \\ C_D(i) = C'(i) \oplus D(i) & S(i) = 2 \end{cases} \tag{14}$$

Step 4. Extended the matrix C_D to its binary image matrixes C_{Db}. Use the same permute key $K_{permute}$ as the encryption algorithm to obtain the same chaotic sequences X_1, X_2 and X_3 in the encryption permutation process.

Step 5. The matrix C_P can be acquired use the reverse row and column combined cycle shift scrambling equation (15) to reverse permute the bit-level image matrix C_{Db}.

$$\begin{cases} PR(TP(i)) = circshift(PR(TP(i)), -X_2'(j)), \ j = j + 1 & TP(i) \le M \\ PC(TP(i) - M) = circshift(PC(TP(i) - M), -X_3'(k)), k = k + 1 & TP(i) > M \end{cases} \tag{15}$$

Step 6. Transform C_P to an integer image matrix denoted as C_I with the size of 3*M*×*N*. Convert C_I into the *R*, *G* and *B* color matrix vertically to obtain the decrypted image.

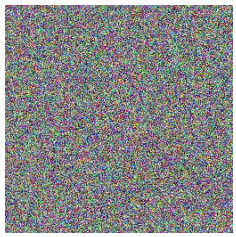
5. Experimental results and performance analysis

The experimental results and performance of the proposed algorithm is analyzed. In order to

verify the effectiveness of the proposed algorithm, numerical simulations are performed on several images.

The chosen sample images are the different sizes color images of 256×256 House, 500×480 Baboon, 512×512 Lena, 512×512 Peppers, 720×576 Barbara and 768×512 Parrots. Figure 7 shows the encryption and decryption results for House, Baboon, Lena, barabra and Parrots images and the encrypted image is similar to noise image without any visual information leakage.

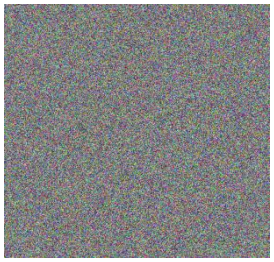
(a) House



(b) Encrypted image of (a)

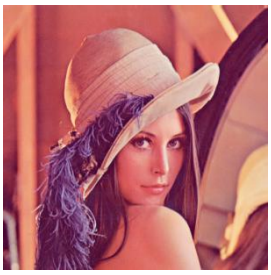
(c) Decrypted image of (b)

(d) Baboon

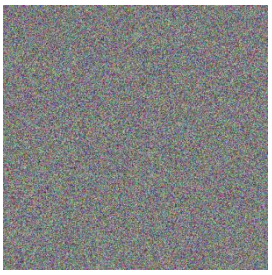


(e) Encrypted image of (d)

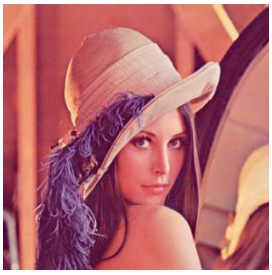
(f) Decrypted image of (e)



(g) Lena

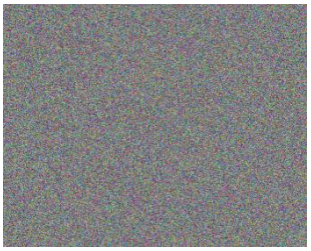


(h) Encrypted image of (g)



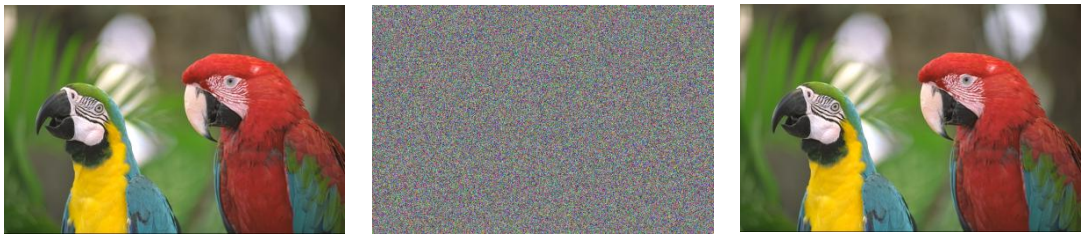
(i) Decrypted image of (h)

(j) Barbara



(k) Encrypted image of (j)

(l) Decrypted image of (k)



(m) Parrots (n) Encrypted image of (m) (o) Decrypted image of (n)

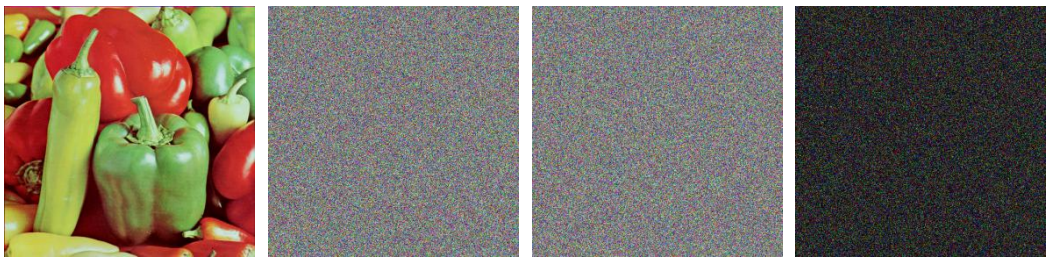
Figure 7 Encryption and decryption results

5.1 Key space analysis

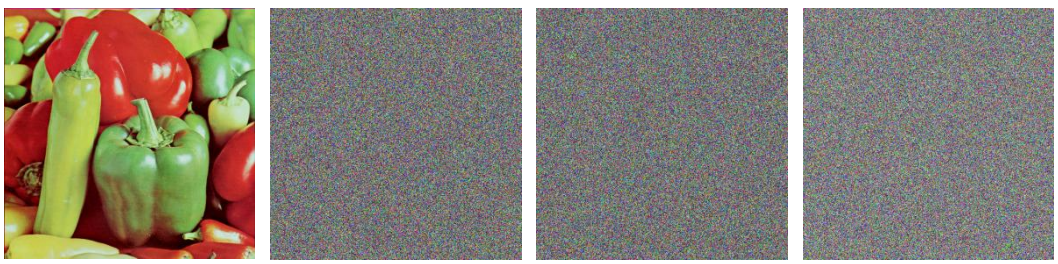
The encryption algorithm with larger key space can better resist brute-force attacks and has higher security. In the proposed algorithm, the key includes the initial conditions x_0, y_0, x_0', y_0', parameters α, β, α', β' and the discard length k, k_1 of the chaotic system in the permutation and diffusion processes. Because the computational precision is 10^{-16}, the size of the key space of for one round encryption is $10^{16\times 8} \approx 2^{425}$ which is much bigger than 2^{100}. So the key space is large enough to resist any brute-force attack.

5.2 Key sensitivity analysis

Key sensitivity is an important feature for high security image encryption algorithm. Slightly different key used in encryption will produce totally different cipher image. And minor changes in the key used for decryption will cause decryption failure. To analysis the key sensitivity of the proposed algorithm, the encryption and decryption keys are changed 10^{-16}. Figure 8 shows the experimental results of the key sensitivity. A slightly changes in any encrypt keys will lead to the completely different cipher images. And a tiny change of one key will generate completely different images and cannot obtain the correct decryption image.



(a) Peppers (b) Encrypted image (c) Encrypted image with $x_0' + 10^{-16}$ (d) The difference between (b) and (c).

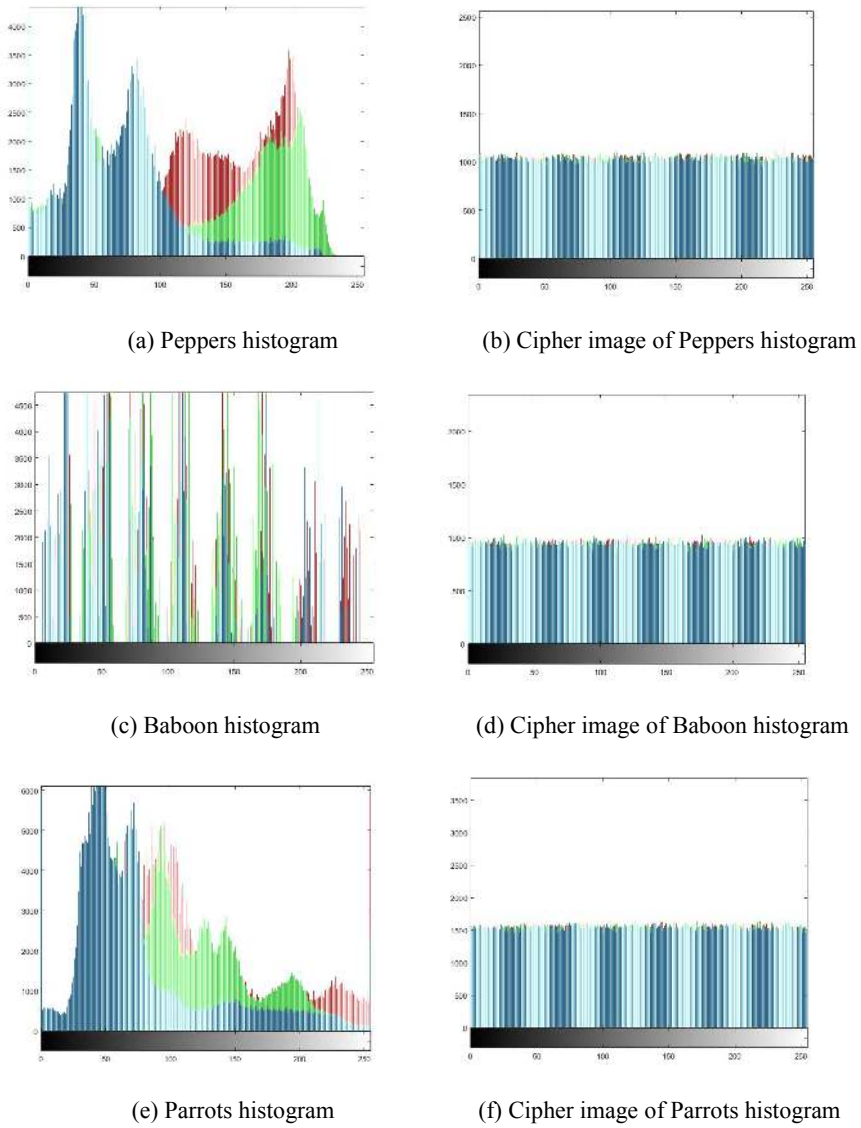


(e) Decrypted with correct key (f) Decrypted with $\beta+10^{-16}$ (g) Decrypted with x_0+10^{-16} (h) Decrypted with $y_0'+10^{-16}$

Figure 8 Key sensitivity

5.3 Histogram

The image histogram shows the distribution information of pixel values. In order to prevent the statistical analysis attack to recover any meaningful information from the histogram of the cipher image, it is import for the cipher image to have uniform distribution. Figure 9 shows the histograms of the plain images and corresponding cipher images. As shown in Figure 9, the histograms distribution of the cipher images are uniform, which makes it difficult for attackers to attack cipher image through statistical analysis.



(a) Peppers histogram (b) Cipher image of Peppers histogram

(c) Baboon histogram (d) Cipher image of Baboon histogram

(e) Parrots histogram (f) Cipher image of Parrots histogram

Figure 9 Histogram of different plain images and cipher images.

5.4 Correlation of adjacent pixels

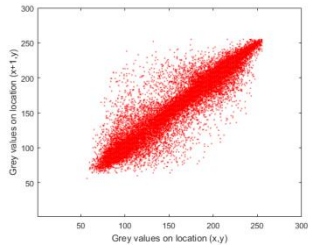
There is a high correlation between adjacent pixels in plain images, which can leak the statistic information for attackers. Therefore, the cipher image should reduce the correlation

between adjacent pixels as much as possible. Calculate the correction coefficient of each pair by using the following formulas:

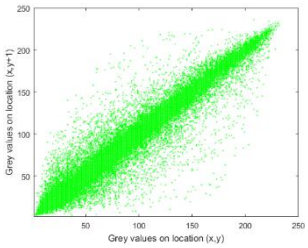
$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{16}$$

where $E(\mathrm{x}) = \frac{1}{N}\sum_{i=1}^{N} x_i$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$, $\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$, x and y are grey-scale values of two adjacent pixel in the image.

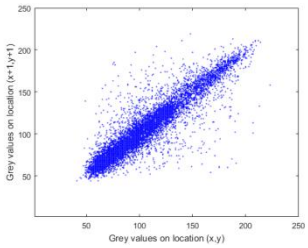
The correlation distribution of horizontally, vertically and diagonally adjacent pixels of the color components of original Lena image and encrypted image are shown in Figure 10. The results of correlation between adjacent pixels of the images tested in this paper have been provided in Table 1. It can be seen from the figure and table that the correlation of adjacent pixels of the encrypted image is significantly reduced to satisfies zero co-correlation, which shows that the encryption algorithm has good security.



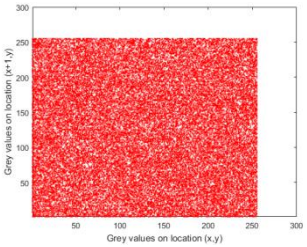
(a) Horizontally adjacent pixels in the red component of Lena image



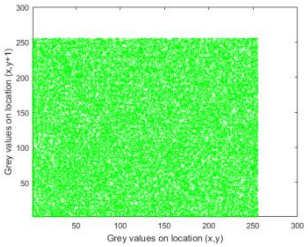
(b) Vertically adjacent pixels in the green component of Lena image



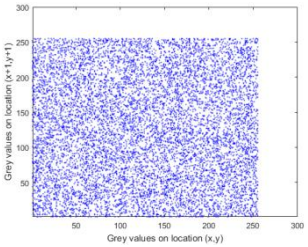
(c) Diagonally adjacent pixels in the blue component of Lena image



(d) Horizontally adjacent pixels in red component of encrypted image



(e) Vertically adjacent pixels in green component of encrypted image



(f) Diagonally adjacent pixels in blue component of encrypted image

Figure 10 Correlation of adjacent pixels of plain image and cipher image

Table 1 Correlation coefficients of plain image and ciphered image.

Image	Direction		
	Horizontal	Vertical	Diagonal
House	0.976027	0.957512	0.941427
Encrypted House	0.002455	0.002587	0.000420
Baboon	0.904796	0.868943	0.836901
Encrypted Baboon	0.000553	-0.000029	-0.000420

Lena	0.9774	0.962438	0.972488
Encrypted Lena	0.000617	-0.000535	-0.000411
Peppers	0.978912	0.968976	0.970080
Encrypted Peppers	0.002505	0.001836	-0.000575
Barbara	0.916137	0.889445	0.906666
Encrypted Barbara	0.001323	0.001164	0.000961
Parrots	0.988276	0.978517	0.977365
Encrypted Parrots	-0.001189	-0.000545	0.000062

5.5 Information entropy analysis

Information entropy is used to quantitatively measure and calculate the randomness of information sources. The entropy $H(m)$ of a message source *m* can be calculated as

$$H(m)=\sum_{i=0}^{2^N-1} p(m_i)\log\frac{1}{p(m_i)}. \tag{17}$$

where $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. For an ideally completely random image, the value of information entropy is 8.

The information entropy for plain images and their corresponding encrypted images are calculated in Table 2. The encrypted image information entropy is very close to the theoretical value 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against the entropy attack.

Table 2 The results of information entropy.

Image	*R*	*G*	*B*
House	6.4311	6.5389	6.2320
Encrypted House	7.9892	7.9896	7.9892
Baboon	6.4998	6.4445	6.2709
Encrypted Baboon	7.9913	7.9916	7.9917
Lena	7.2531	7.5940	6.9684
Encrypted Lena	7.9912	7.9913	7.9914
Peppers	7.3388	7.4764	7.0410
Encrypted Peppers	7.9915	7.9914	7.9912
Barbara	7.7068	7.5275	7.5872
Encrypted Barbara	7.9919	7.9916	7.9918
Parrots	7.4699	7.4814	7.1577
Encrypted Parrots	7.9916	7.9915	7.9916

5.6 Differential attack

A secure image encryption algorithm should be highly sensitive to any subtle changes in the plaintext image, which means that one pixel of the plaintext image change will produce a completely different cipher image.

The number of pixels change rate (NPCR) while one pixel of plain image changed and the

unified average changing intensity (UACI) between the plain image and ciphered image are used to test the differential attack. Here are the formulas to calculate NPCR and UACI:

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

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{19}$$

where M and N represent the rows and columns of the image respectively, C_1 and C_2 are respectively the ciphered images before and after one pixel of the plain image is changed.

The experiment results of NPCR and UACI are listed in Table 3. From Table 3 we can see that the NPCR and UACI values are very close to the theoretical value, and the proposed cryptosystem could resist plaintext attack and differential attack effectively.

Table 3 NPCR and UACI values (%)

Image	NPCR	UACI
House	99.66	33.52
Baboon	99.59	33.49
Lena	99.62	33.47
Peppers	99.61	33.48
Barbara	99.62	33.43
Parrots	99.61	33.48
Average	**99.6183**	**33.4783**

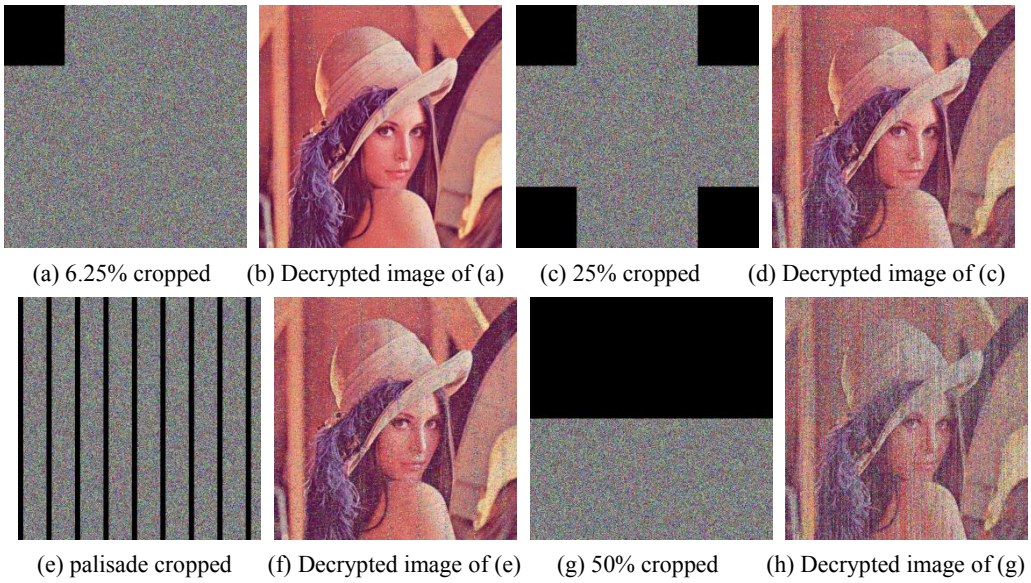
5.7 Noise and data loss attacks

Image data is easily experience the noise and data lost during transmission. A high security image encryption algorithm should be able to resist noise and data loss attacks. Salt and pepper noises with different density are added into the encrypted Lena image. It can be seen from Figure 11 that the decrypted image can still be recovered successfully, and the noises could not prevent us from visually recognizing the decrypted image contents.

(a) Noise strength 0.01 (b) Noise strength 0.05 (c) Noise strength 0.1 (d) Noise strength 0.25

Figure 11 The decryption results with different density noises

The lost data cipher images and corresponding decrypted images are shown in Figure 12. The experimental results show that the higher degree of image loss, the less clear the decrypted image is. But even if half of the image is lost, the image can still be decrypted and recognized. The proposed algorithm is robust to noise attacks and information loss attacks.



(a) 6.25% cropped (b) Decrypted image of (a) (c) 25% cropped (d) Decrypted image of (c)

(e) palisade cropped (f) Decrypted image of (e) (g) 50% cropped (h) Decrypted image of (g)

Figure 12 Data loss attack

5.8 Running Performance

In order to calculate the performance of this algorithm, the experiments are simulated by utilizing the MATLAB R2017a with Intel(R) Core (TM) i5-8300H CPU@2.30GHz and 4.0G RAM on Windows 10 OS. Table 4 shows the running time of encrypt images in this paper. When encryption different color images with different sizes, the encryption program can achieve good running performance within a few seconds.

Table 4 Execution time analysis (seconds)

Image	Size	Time
House	256×256	0.472762
Baboon	500×480	1.808773
Lena	512×512	1.841536
Peppers	512×512	1.884963
Barbara	720×576	2.952509
Parrots	768×512	2.829411

6. Conclusion

This paper designed a cross 2D hyperchaotic map, which is constructed using one nonlinear function and two chaotic maps with cross structure. Numerous experiments such as bifurcation diagrams, Lyapunov exponent spectra and phase portraits are carried out to illustrate the complex chaotic behavior of the proposed hyperchaotic map. Simulation results show that the nonlinear cross 2D hyperchaotic map has good chaotic performance. In the color image encryption algorithm, the keys are generated using hash function SHA-512 and the information of plain color image. First, the color plain image is converted to a combined bit-level matrix and permutated by the chaotic based row and column combined cycle shift scrambling method. Then the scrambled integer matrix is diffused according to the selecting sequence. The cipher color

image is obtained by decomposed the diffused matrix. The proposed encryption algorithm makes the three color components of color image affect each other to eliminate the correlations between them. Simulation results show that the algorithm can encrypt the color image effectively and has good security to resist various kinds of attacks.

Funding: This work is supported by the China Postdoctoral Science Foundation (No: 2020M680933), National Natural Science Foundation of China (Nos: 61701070, 61672124), the Doctoral Start-up Foundation of Liaoning Province (No: 2018540090), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103), Jinan City '20 universities' Funding Projects Introducing Innovation Team Program (No: 2019GXRC031), Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (No: MIMS20-M-02).

Conflict of Interest: The authors declare that they have no conflict of interest.

References

[1] Xiong ZG, Wu Y, Ye CH, Zhang XM, Xu F. Color image chaos encryption algorithm combining CRC and nine palace map. Multimedia Tools and Applications, 2019, 78(22): 31035-31055.

[2] Sneha PS, Sankar S, Kumar AS. A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(3):1289-1308.

[3] Wang XY, Li ZM. A color image encryption algorithm based on Hopfield chaotic neural network. Optics and Lasers in Engineering, 2019, 115: 107-118.

[4] Chai X, Bi J, Gan Z, et al. Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Signal Processing, 2020, 176:107684.

[5] Wang XY, Guan NN. A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation. Optics & Laser Technology, 2020, 131: 106366.

[6] Zhou J, Zhou N R, Gong L H. Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix. Optics & Laser Technology, 2020, 131:106437.

[7] Wang L, Ran Q, Ma J. Double quantum color images encryption scheme based on DQRCI. Multimedia Tools and Applications, 2020, 79(9-10): 6661-6687.

[8] Wu XJ, Kan HB. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Applied Soft Computing, 2015, 37: 24-39.

[9] Niyat AY, Moattar MH, Torshiz MN. Color image encryption based on hybrid hyper-chaotic system and cellular automata. Optics & Lasers in Engineering, 2017, 90:225-237.

[10] Parvaz R, Zarebnia M. A combination chaotic system and application in color image encryption. Optics & Laser Technology, 2018, 101:30-41.

[11] Wang SC, Wang CH, Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. Optics and Lasers in Engineering, 2020, 128: 105995.

[12] Wang XY, Zhang JJ, Cao GH. An image encryption algorithm based on ZigZag transform and LL compound chaotic system. Optics and Laser Technology, 2019, 119: 105581.

[13] Nestor T, Kengne J, Abd-El-Atty B, et al. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Information Sciences, 2020, 515: 191-217.

[14] Wang XY, Gao S. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Information Sciences, 2020, 507:16-36.

[15] Farah M A B, Guesmi R, Kachouri A, et al. A Novel Chaos Based Optical Image Encryption Using fractional Fourier transform and DNA Sequence Operation. Optics & Laser Technology, 2019, 121:105777.

[16] Xian YJ, Wang XY, Yan XP, Li Q, Wang XY. Image encryption based on chaotic sub-block scrambling and chaotic digits selection diffusion. Optics and Lasers in Engineering, 2020, 134: 106202.

[17] He Y, Zhang YQ, Wang XY. A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system. Neural Computing and Applications, 2020, 32:247-260.

[18] Liu H, Zhang Y, Kadir A, et al. Image encryption using complex hyper chaotic system by injecting impulse into parameters. Applied Mathematics and Computation, 2019, 360:¶ 83-93.

[19] Wang XY, Feng L, Li R, Zhang FC. A fast image encryption algorithm based on Non-Adjacent Dynamically Coupled Map Lattice Model. Nonlinear Dynamics, 2019, 95(4): 2797-2824.

[20] Wang XY, Sun HH. A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function. Optics and Laser Technology, 2020, 122: 105854.

[21] Zhu C, Sun K. Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps. IEEE Access, 2018, 6: 18759-18770.

[22] Farajallah M, Assad S E, Deforges O. Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. Multimedia Tools & Applications, 2018, 77(21): 28225-28248.

[23] Ge X, Lu B, Liu F, et al. Cryptanalyzing an image encryption algorithm with compound chaotic stream cipher based on perturbation. Nonlinear Dynamics, 2017, 90(2): 1141-1150.

[24] Wen H, Yu S, Lü JH. Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. Entropy, 2019, 21(3): 246.

[25] Rössler, O.E. An Equation for Hyperchaos. Physics Letters A, 1979, 71, 155-157.

[26] Zhu SQ, Zhu CX. Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding. ENTROPY, 2020, 22(7): 772.

[27] Xu C, Sun J, Wang C. An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems. International Journal of Bifurcation and Chaos, 2020, 30(4): 2129-2151.

[28] Bouslehi H, Seddik H. Innovative image encryption scheme based on a new rapid hyperchaotic system and random iterative permutation. Multimedia Tools & Applications, 2018, 77(23):1-23.

[29] Cheng G, Wang C, Chen H. A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture. International Journal of Bifurcation and Chaos, 2019, 29(09):1950115.

[30] Kaur M, Singh D, Sun K, et al. Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map. Future Generation Computer Systems, 2020, 107:333-350.

[31] Wang MX, Wang XY, Wang CP, et al. Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption. Chaos Solitons & Fractals, 2020, 139:110028.

[32] Ouyang X, Luo Y, Liu J, et al. A color image encryption method based on memristive hyperchaotic system and DNA encryption. International Journal of Modern Physics B, 2020, 34(4):2050014.

[33] Hou W, Li S, He J, et al. A Novel Image-Encryption Scheme Based on a Non-Linear Cross-Coupled Hyperchaotic System with the Dynamic Correlation of Plaintext Pixels. Entropy, 2020, 22(7):779.

[34] Liu W, Sun K, He Y, et al. Color Image Encryption Using Three-Dimensional Sine ICMIC Modulation Map and DNA Sequence Operations. International Journal of Bifurcation and Chaos, 2017, 27(11):1750171.

[35] Cao W, Mao Y, Zhou Y. Designing a 2D infinite collapse map for image encryption. Signal Processing, 2020,

171:107457.

[36] Wang MX, Wang XY, Zhao TT, Zhang C, Xia ZQ, Yao NM. Spatiotemporal chaos in improved Cross Coupled Map Lattice and its application in a bit-level image encryption scheme. Information Sciences, 2021, 544: 1-24

[37] Mansouri Ali, Wang Xingyuan. A novel one dimensional sine powered chaotic map and its application in a new image encryption scheme. Information Sciences, 2020, 520: 46-62

[38] He D, He C, Jiang L G, et al. Chaotic characteristics of a one-dimensional iterative map with infinite collapses. IEEE Transactions on Circuits & Systems I Fundamental Theory & Applications, 2001, 48(7):900-906.

Figures

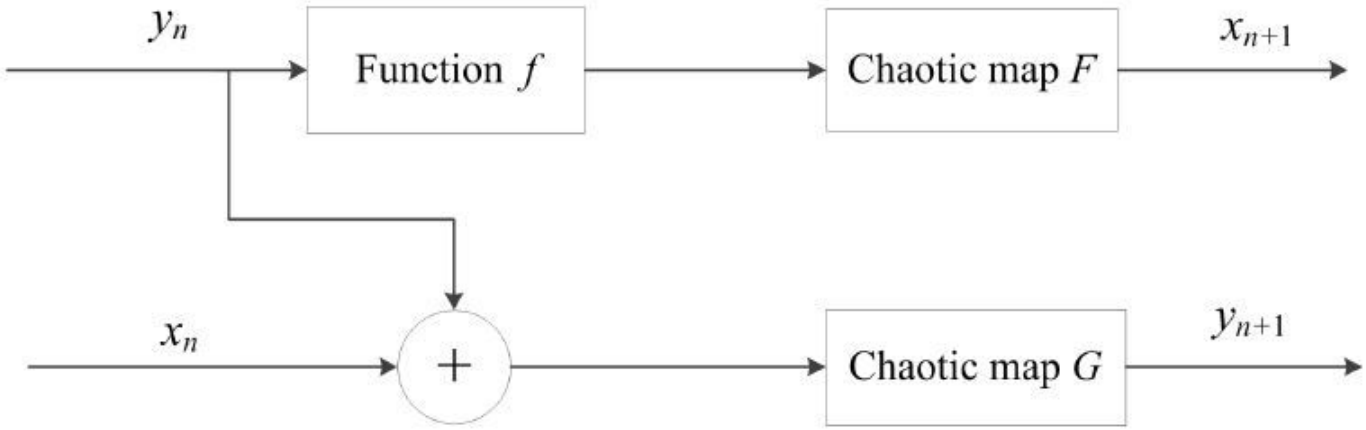


Figure 1

Diagram of Nonlinear cross 2D hyperchaotic map

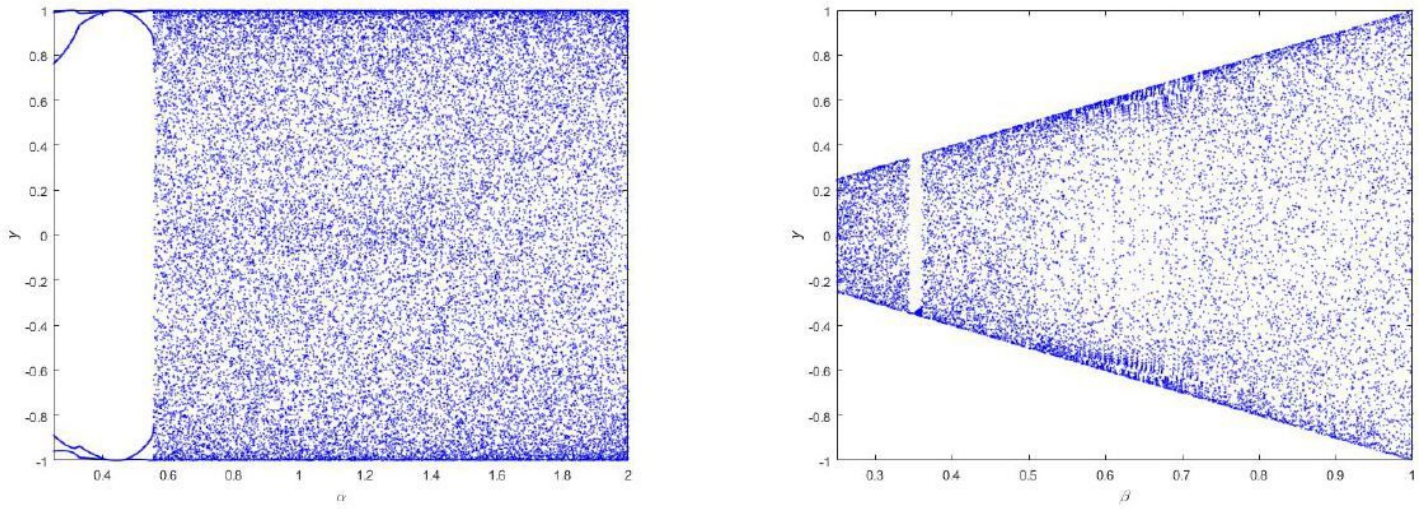
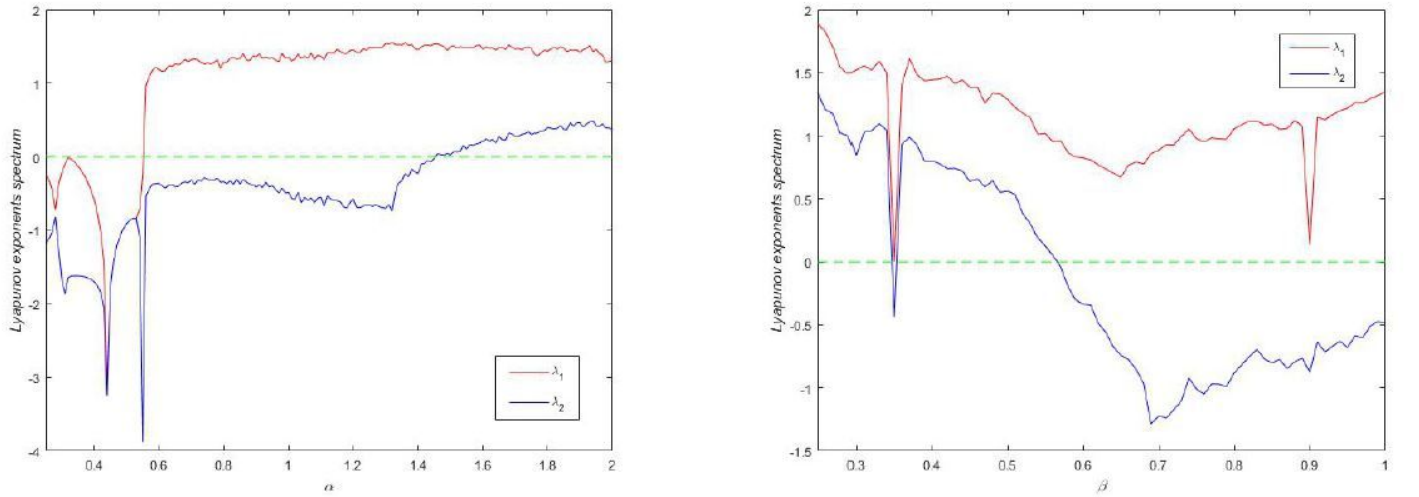


Figure 2

Bifurcation diagrams of the proposed system



(a) Lyapunov exponents spectrum varying α

(b) Lyapunov exponents spectrum varying β

Figure 3

Lyapunov exponents spectrum

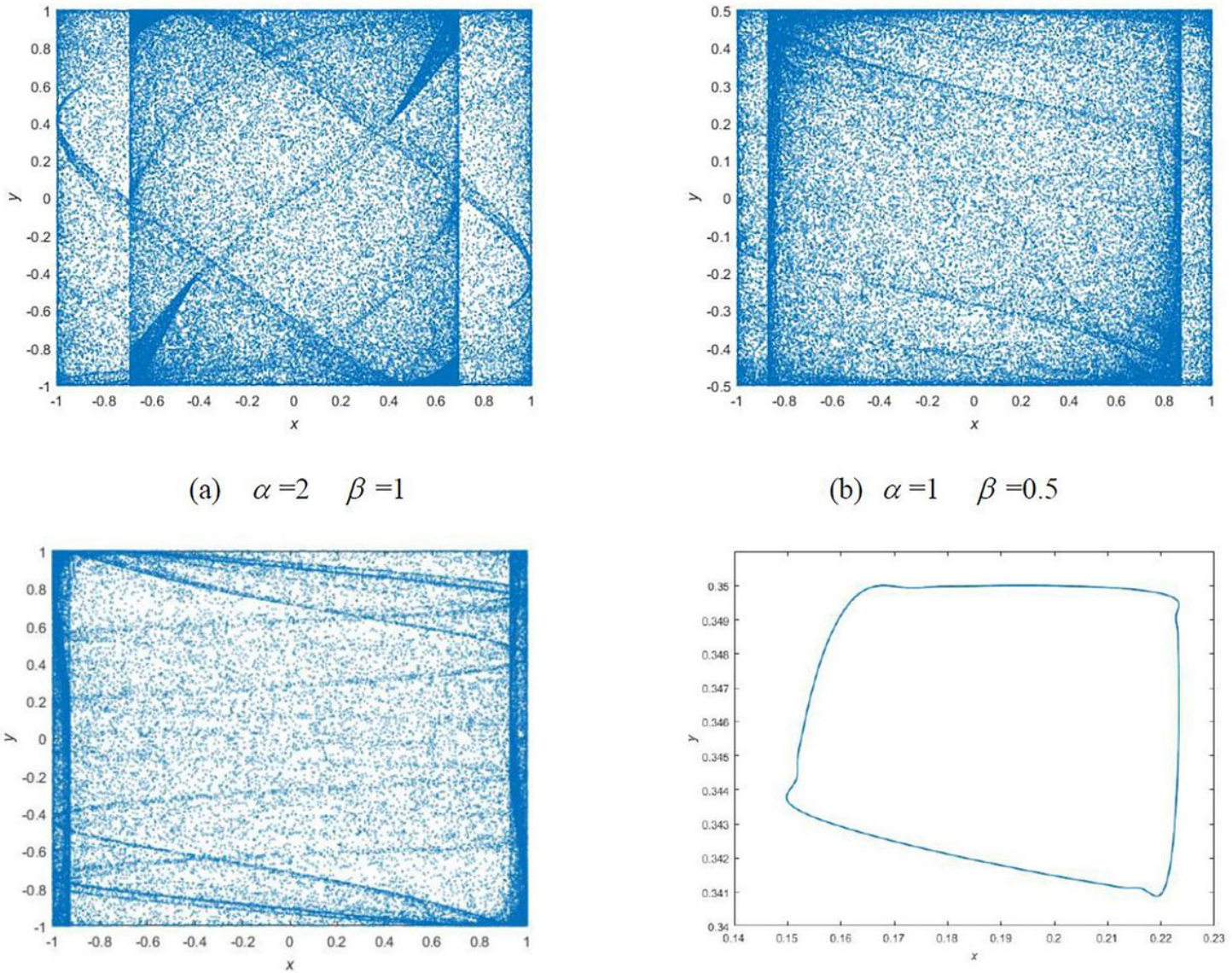
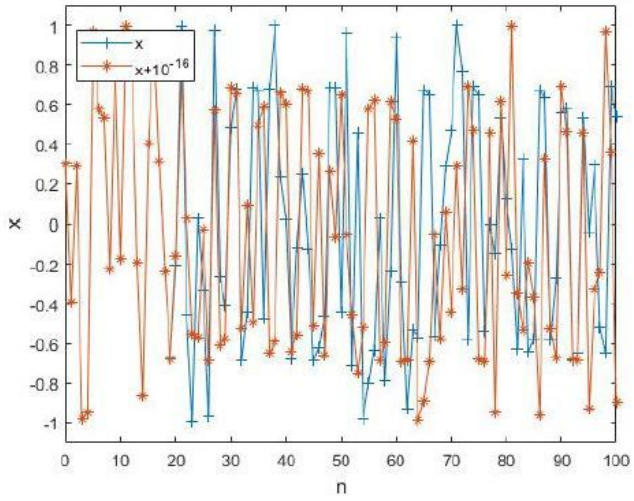
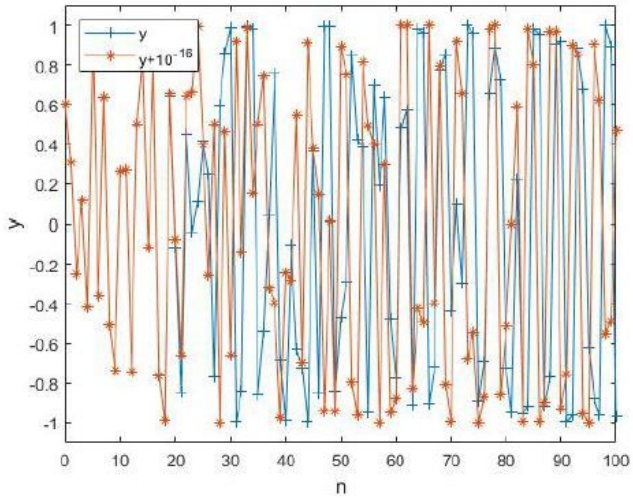


Figure 4

Attractor phase diagrams



(a) x_0 changed 10^{-16}



(b) y_0 changed 10^{-16}

Figure 5

Initial value sensitivity

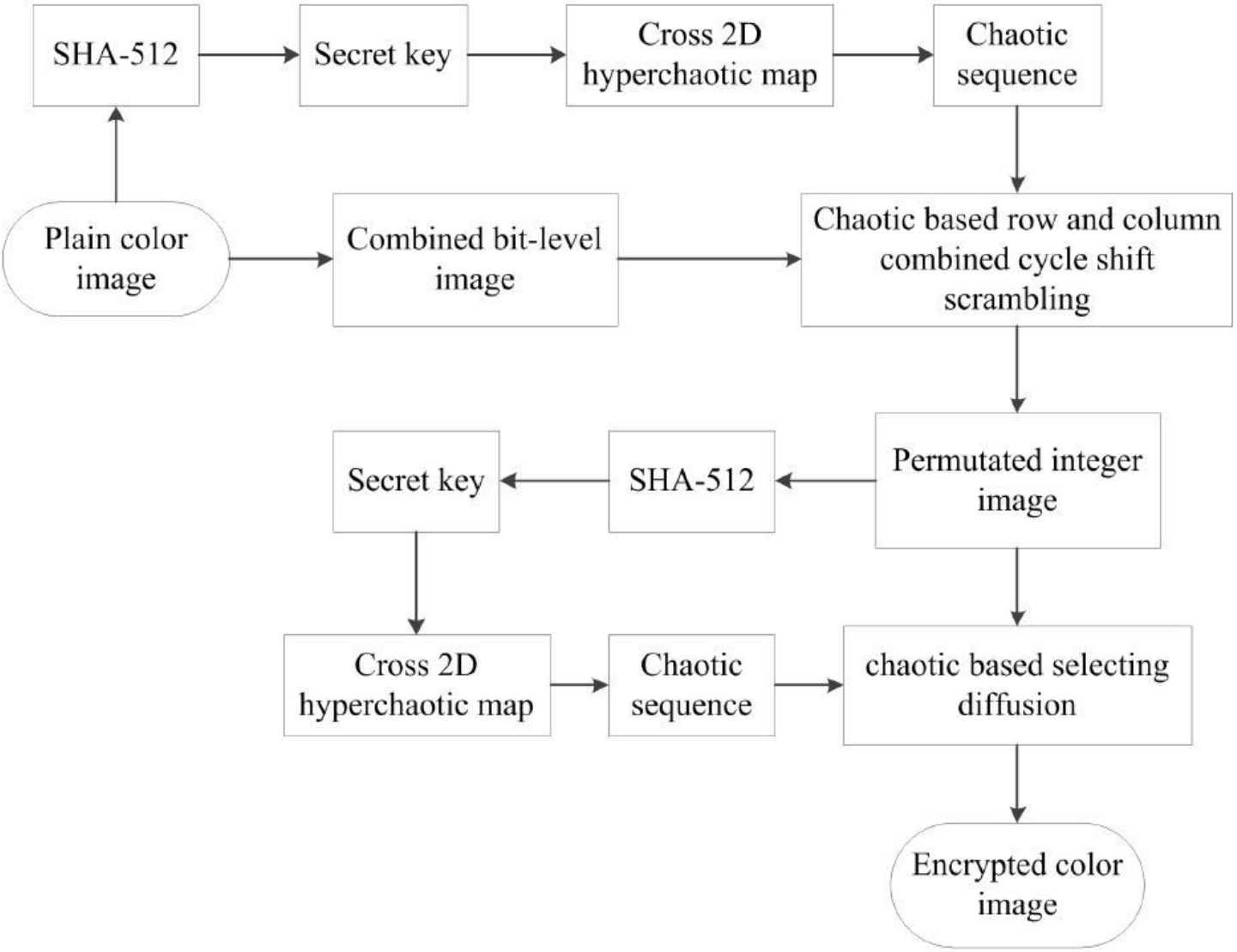


Figure 6

Flowchart of proposed encryption algorithm

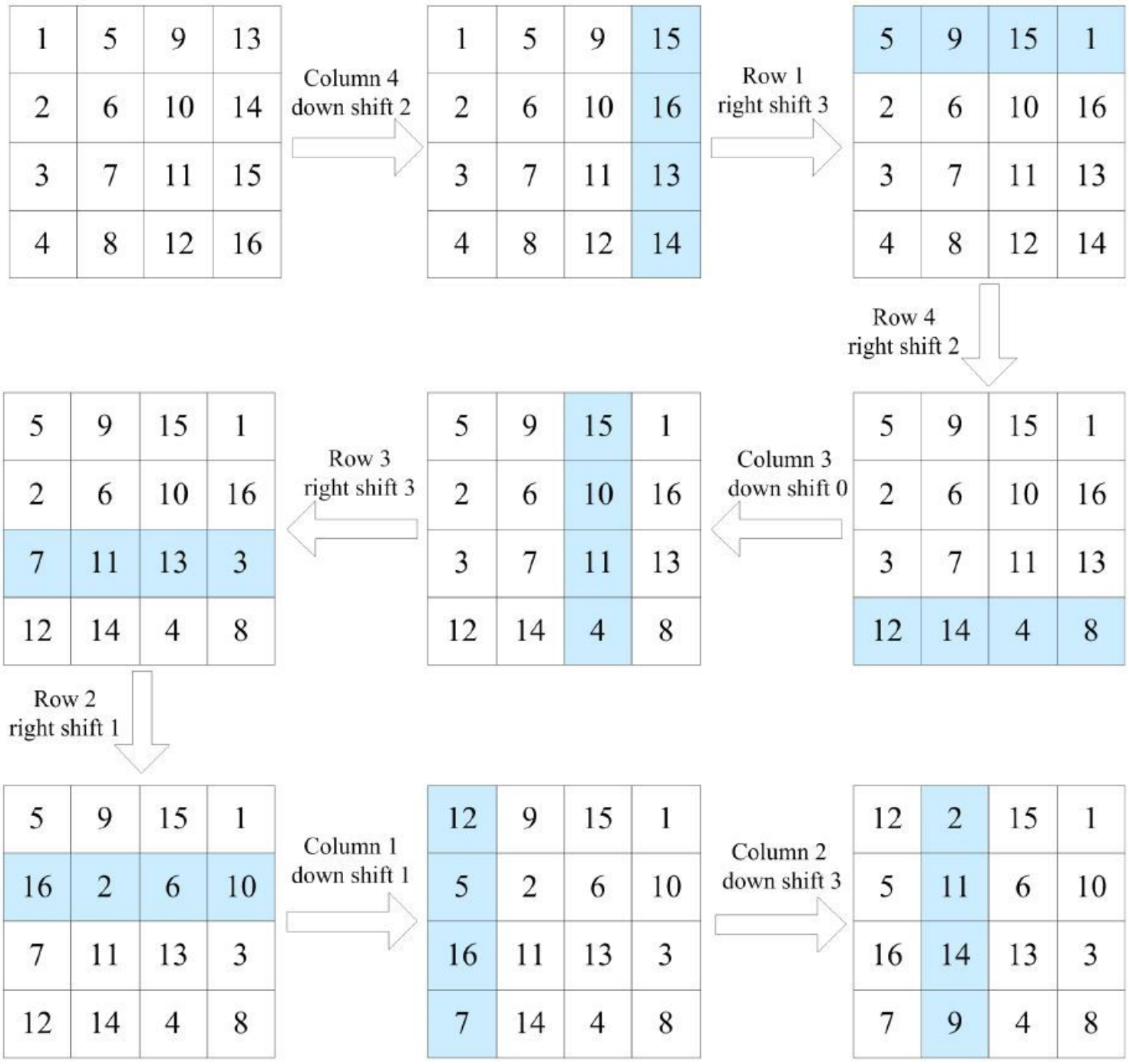


Figure 7

4×4 matrix scrambled by row and column combined cycle shift

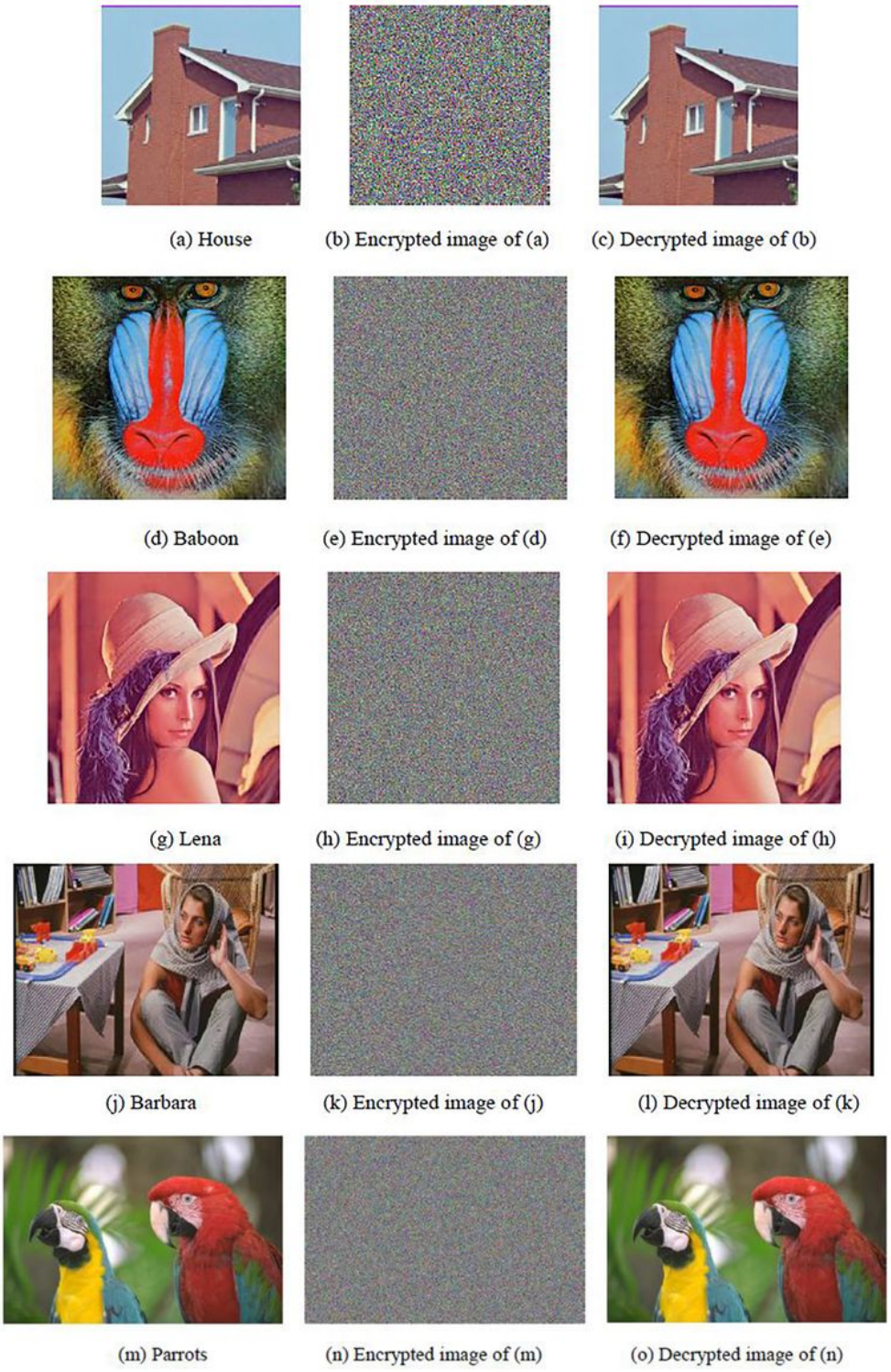


Figure 8

Encryption and decryption results

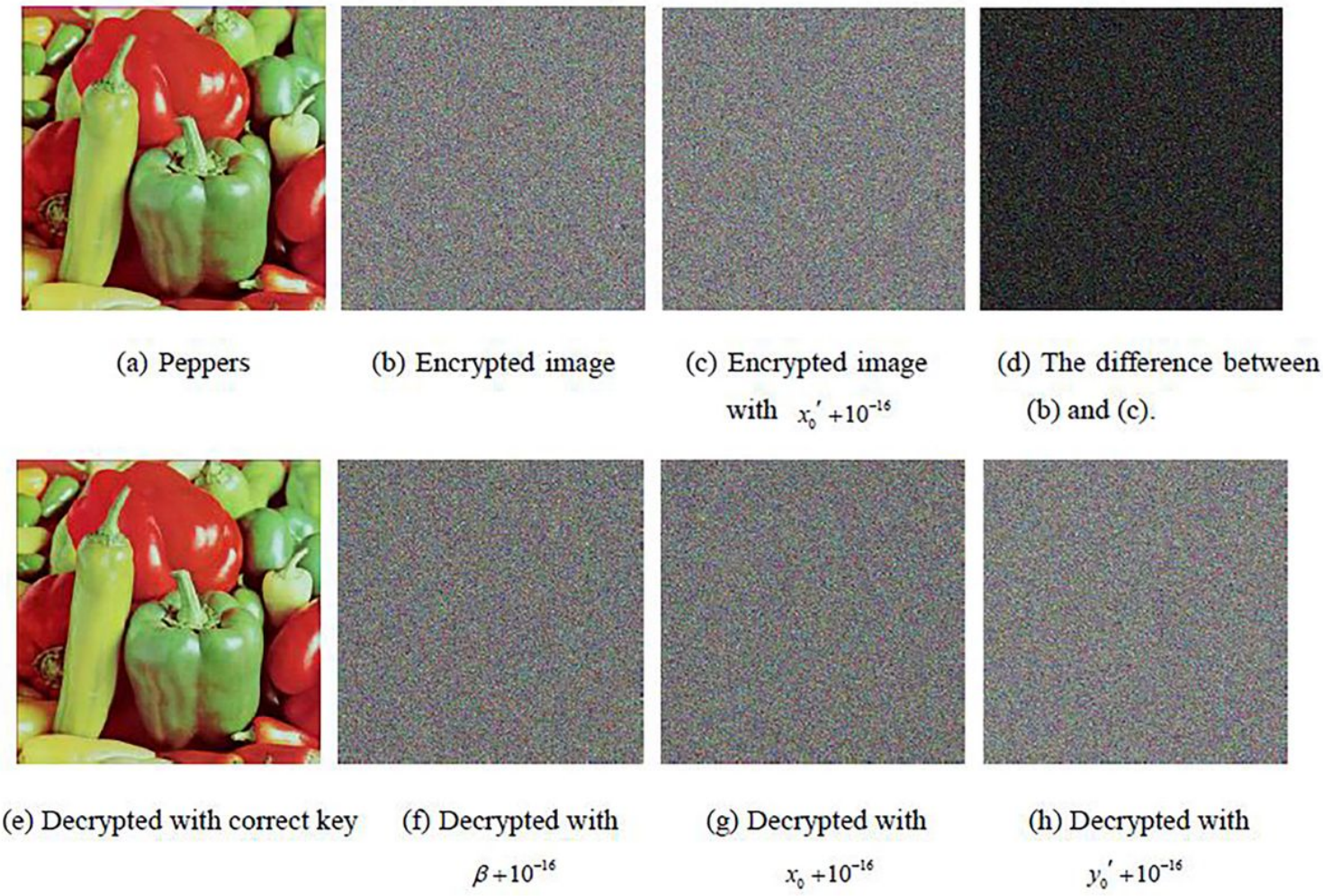


Figure 9

Key sensitivity

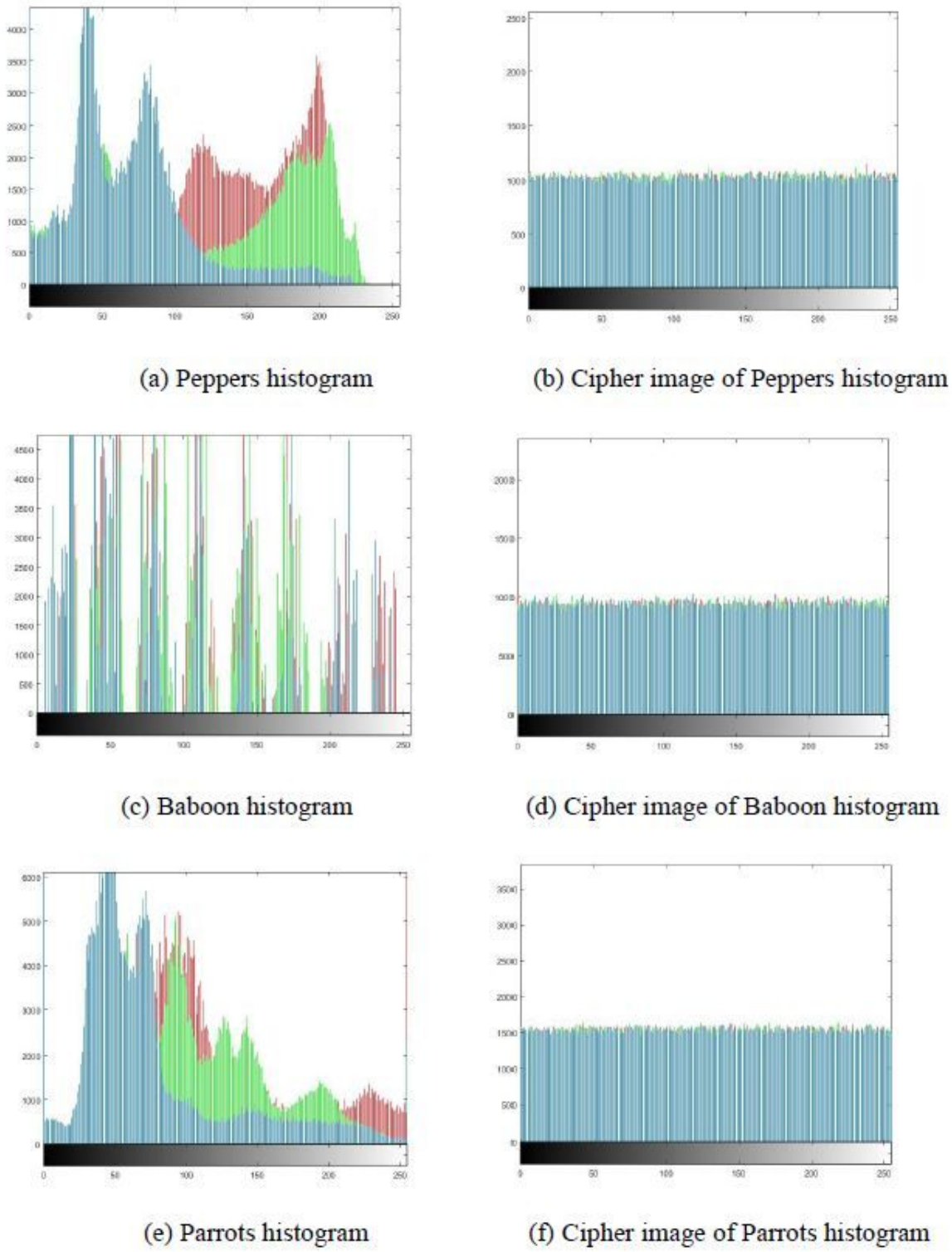
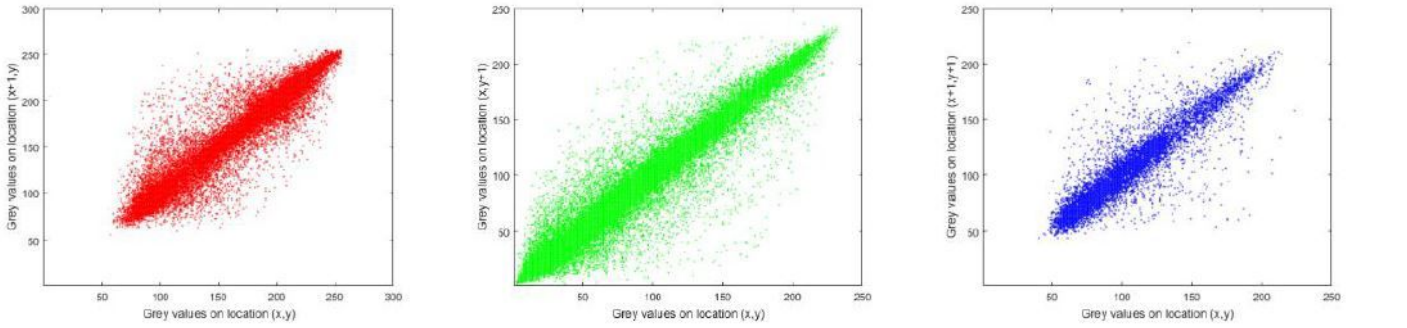


Figure 10

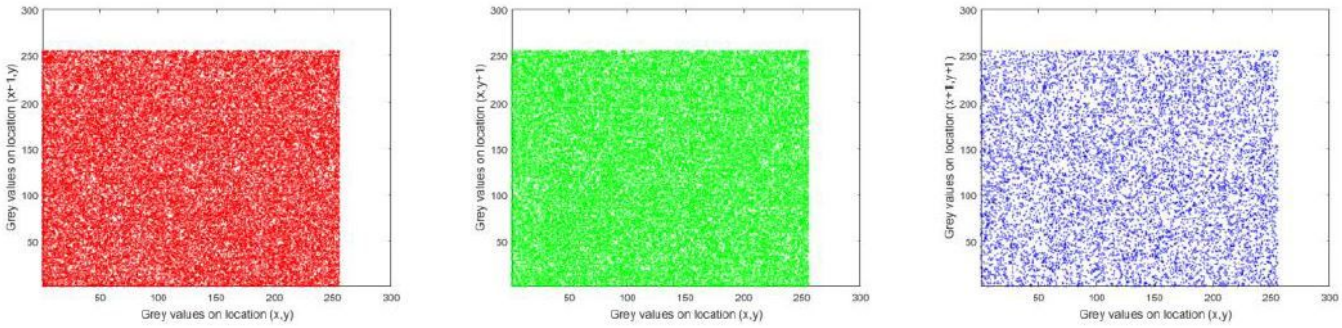
Histogram of different plain images and cipher images.



(a) Horizontally adjacent pixels in the red component of Lena image

(b) Vertically adjacent pixels in the green component of Lena image

(c) Diagonally adjacent pixels in the blue component of Lena image



(d) Horizontally adjacent pixels in red component of encrypted image

(e) Vertically adjacent pixels in green component of encrypted image

(f) Diagonally adjacent pixels in blue component of encrypted image

Figure 11

Correlation of adjacent pixels of plain image and cipher image

(a) Noise strength 0.01

(b) Noise strength 0.05

(c) Noise strength 0.1

(d) Noise strength 0.25

Figure 12

The decryption results with different density noises

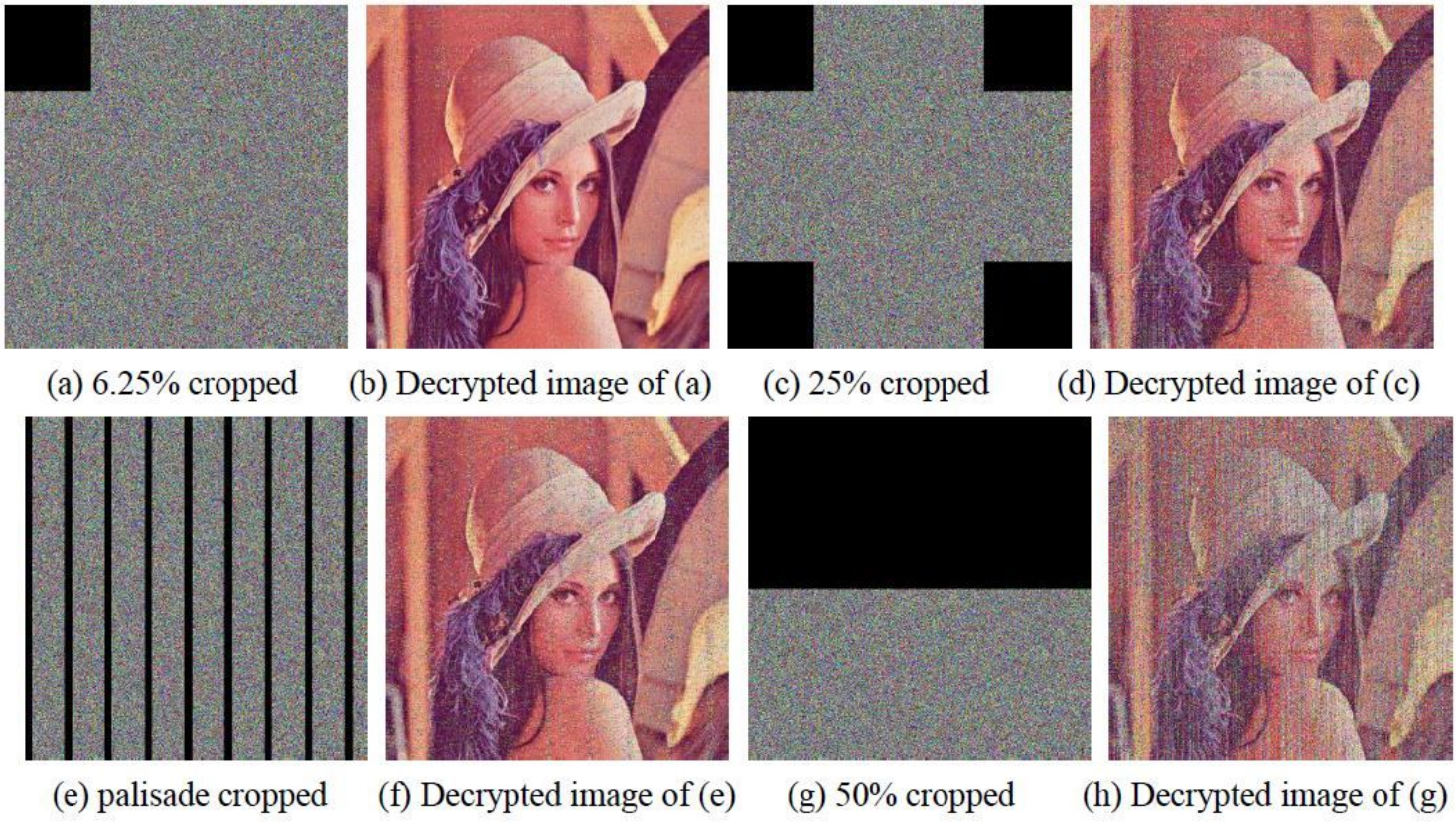


Figure 13

Data loss attack