Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-08273-x

A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems

Cong Xu [1] • Jingru Sun [1] • Chunhua Wang [1]

Received: 28 November 2018 / Revised: 5 September 2019 / Accepted: 22 September 2019
Published online: 06 December 2019

Abstract
In this paper, we propose a new image encryption algorithm based on bit-plane matrix rotation and two hyper chaotic systems. The algorithm first decomposes the plain-image into eight bit planes and constructs a three-dimensional (3D) matrix. Then the sub-matrix of the 3D bit-plane matrix is rotated in different directions controlled by PRNS generated by a hyper-chaotic system. Finally, the pixel values of the intermediate image are modified by using another key stream. Furthermore, the initial values of diffusion and parameters related with generating chaotic sequences are produced by the MD5 hash function of the plain-image, which enhances the correlation between the encryption process and the plain-image. Simulation experiments are presented to analyze the image encryption scheme in terms of key space, histogram, information entropy, key sensitivity and adjacent pixels correlation index. Theoretical analysis and experimental results demonstrate that the proposed algorithm has excellent performance and suffcient security level.

Keywords Image encryption · Chaos · Bit-plane · Rotation · Chaotic · Cryptography

1 Introduction

With the rapid development of multimedia technology and the popularity of the Internet, the security of image transmission has been received intensive attentions. However, because of the data size and high redundancy among the pixels of a digital image, traditional encryption algorithm, such as the data encryption standard (DES), international data encryption algorithm (IDES) and advanced encryption standard (AES) are not suitable for practical image encryption [16].

✉ Jingru Sun
jt_sunjr@hnu.edu.cn

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

Chaos is characterized in periodicity, ergodicity, pseudo-randomness and high sensitivity to initial conditions and parameters. Since the British mathematician Matthews proposed the first chaos-based encryption algorithm in 1989 [27], various chaotic systems have been widely applied in encryption [28, 29]. Currently, the chaotic map can be divided into two categories: one-dimensional (1D) [10] and higher-dimensional (HD) [31] chaotic maps. 1D chaotic system is widely used in image encryption for the properties of fewer parameters and variables, simple structure, and shorter time of generating chaotic sequence. For example, Li et al. proposed an image encryption scheme with chaotic tent map [19]. A stream-cipher algorithm based on one-time keys and robust chaotic maps was designed by Liu et al. [22]. Wang et al. proposed a fast image encryption algorithm based on logistic map [42]. However, a common problem of these schemes is small size of the key space. In contrast, high-dimensional chaotic maps [13], especially hyper chaotic maps [53–55], have more variables and parameters, more complex dynamic characteristics and larger key space. Thus HD chaotic map is the potential ideal model for image encryption.

The typical image encryption system based on chaotic system includes both confusion module and diffusion module. In [3, 6, 11, 12, 14, 21, 37, 39, 40, 48, 49], a number of image encryptions based on pixel-level confusion were proposed, the confusion stages of these algorithms just changes the positions of pixel without changing the pixel value, and the chaotic sequence generated by chaotic system is independent of the plain image. Therefore, it could not resist the chosen-plaintext attack and chosen-ciphertext attack [17, 18, 20, 51]. Permutation methods based on bit-level can change the position and value of the pixels simultaneously, so a variety of image encryption algorithms based on bit-level permutation were proposed [4, 7, 8, 23, 35, 47, 52]. Generally, bit-level permutation can overcome the disadvantages of typical pixel-level scramble, and it is more efficient for image encryption.

Recently, image encryption algorithms based on bit-plane permutation were proposed, where the original image is decomposed into eight binary images, and then combined into a large binary image [33, 34, 36]. The position of the large binary image is confused by the chaotic sequence, then the binary image is reassembled to obtain the cipher-image. In [15], an image encryption algorithm with random bit sequence generator was proposed, the image is partitioned into eight bit planes, and then the bits are permuted and substituted according to a chaotic sequence. Finally, the scrambled bit planes are combined into ciphertext images. In [24, 43, 46], to optimize the encryption system, the image is split into higher bit planes and lower bit planes, and then different bit planes are assigned with different encryption methods. The common feature of these algorithms is that each confusion operation can only scramble the bit positions between two bit planes at the same time. A few image encryption schemes confuse the positions of bits between multiple bit planes simultaneously.

Based on the above analysis, a three-dimension matrix is constructed by eight bit planes, and then a confusion method is used to scramble the position of bits between multiple planes, which can enhance the permutation effect and increasing the security of the encryption scheme. In this paper, a novel image encryption algorithm with bit-plane matrix rotation and hyper chaotic systems is proposed. First, the plain image is decomposed into eight binary bit-planes, which are further formed as a three-dimension (3D) bit-plane matrix of size $m \times n \times 8$. Then, bit-level scrambling is performed by rotating the sub-matrix of the bit-plane matrix in x-y or x-z or y-z direction, the positions of bits within multiple bit planes are confused simultaneously and effectively. Besides in the process of the rotation, the rotation direction, angle, size, and the position of sub-matrix are controlled by different chaotic sequences. Furthermore, diffusion is adopted to increase the security of the algorithm. To improve the algorithm's sensitivity with respect to the plain-image, MD5 hash value of the plain-image is used to generate the number of pre-iterations, which is related to generating chaotic sequences, and the initial value of diffusion process. The simulation results and performance analysis show that the proposed algorithm has excellent performance and strong rebustness against brute-force attack, statistical attack and differential attack.

The rest of the paper is organized as follows. In Sec. 2, the basic theories applied in the scheme are reviewed. In Sec. 3, the process of image encryption and decryption are described in detail. In Sec. 4, the simulation results and security analysis are presented. The last section conludes the paper.

2 Basic theories

2.1 Binary bit-plane decomposition

The binary bit-plane decomposition method (BBD) [50] is adopted in this paper. Pixel values in a grayscale image are integer numbers between 0 and 255, each pixel can be represented by an 8-bit binary sequence. Thus, the image can be decomposed into eight bit-planes, where the *i*th bit of the binary representation of each pixel is used to compose the *i*th bit-plane. Figure 1 shows a bit-plane decomposition of the Lena image.

2.2 Pseudo-random sequence generator

2.2.1 Hyper chaotic Lorenz system

The hyper chaotic Lorenz system can be described by

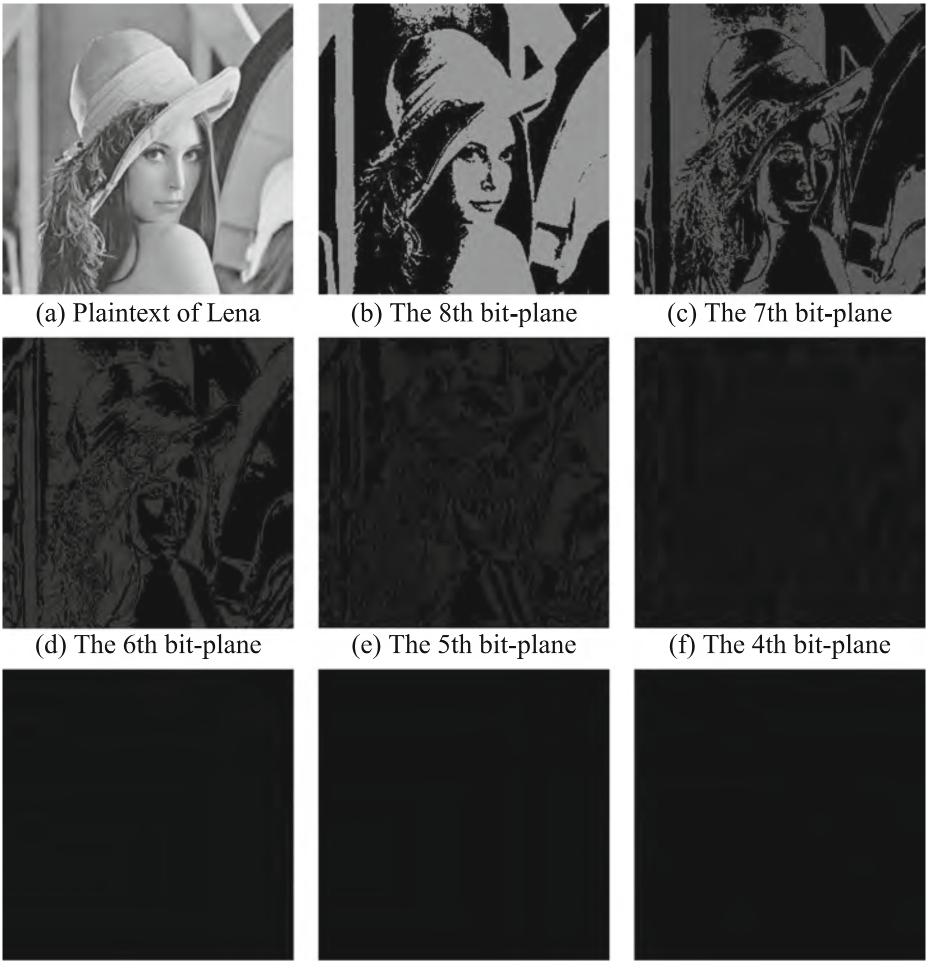
$$\begin{cases} \dot{x} = a(y-z) + w \\ \dot{y} = cx-y-xz \\ \dot{z} = xy-bz \\ \dot{w} = -yz + rw \end{cases} \tag{1}$$

where a, b, c and r are the control parameters [41]. According to the method presented by Ramasubramanian et al. [30]. When a = 10, b = 8/3, c = 28 and − 1.52 < r ≤ −0.06, the system is hyper chaotic, when r = −1, the Lyapunov exponents can be obtained as: $\lambda_1 = 0.3381$, $\lambda_2 = 0.1586$, $\lambda_3 = 0$, $\lambda_4 = -15.1752$. It is obvious that the system exhibits a hyper-chaotic behavior.

2.2.2 The 6D hyper chaotic system

In [9], Grassi et al. introduced a four-wing hyper chaotic attractor generated from two coupled identical Lorenz systems, which is described by

$$\begin{cases} \dot{x}_1 = a(x_2-x_1) \\ \dot{x}_2 = bx_1-x_2-x_1x_3 + \sigma_1(x_4-x_5) \\ \dot{x}_3 = x_1x_2-cx_3 \\ \dot{x}_4 = a(x_5-x_4) \\ \dot{x}_5 = bx_4-x_5-x_4x_6 + \sigma_2(x_1-x_2) \\ \dot{x}_6 = x_4x_5-cx_6 \end{cases} \tag{2}$$



(a) Plaintext of Lena (b) The 8th bit-plane (c) The 7th bit-plane

(d) The 6th bit-plane (e) The 5th bit-plane (f) The 4th bit-plane

(g) The 3rd bit-plane (h) The 2nd bit-plane (i) The 1st bit-plane

Fig. 1 Decomposition of Lena image based on bit-planes

where a, b and c are the positive system parameters, and $\sigma 1$ and $\sigma 2$ are the coupling parameters. When $a = 10$, $b = 28$, $c = 8/3$ and $\sigma 1 = \sigma 2 = 0.05$, the system is hyper chaotic.

2.3 MD5

MD5 is short for Message-digest Algorithm 5 which is developed by Rivest. MD5 takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

MD5 algorithm has the characteristics of anti-modification, if make any slight changes to the original data, even though just modify a byte, the resulting MD5 value will be completely different. Thus, in this paper MD5 algorithm is used to generate the control parameters of chaotic system. Even if there is only one bit different between two plain images, the control parameters of the corresponding chaotic system which is generated by the MD5 will be different completely.

3 The proposed image encryption system

The encryption process is illustrated in Fig. 2. First, the key streams generated by chaotic system are relevant to plain-image, and then the plain image is decomposed into eight bit planes. After that, bit-plane matrix rotation is utilized to strengthen the security of the cryptosystem. Finally, a cipher-image is produced by a diffusion operation.

3.1 Generation of key streams

The key streams are produced by the following steps.

Step 1: The pre-iterate number N_0 of the chaotic system and the initial value Q of diffusion are obtained by MD5 hash value of the plain image, which is denoted as

$$N_0 = \mathrm{mod}(H, 1500) \tag{3}$$

$$Q = \mathrm{mod}(H, 255) \tag{4}$$

where H is the decimal form of the MD5 hash value, mod (a, b) returns the remainder of a divided by b.

Step 2: With the initial values x_0, y_0, z_0 and w_0, four pseudo-random sequences x, y, z, and w are obtained by iterated Eq. (1) for $N_0 + L$ times, where $L = m \times n \times 8$. To avoid the

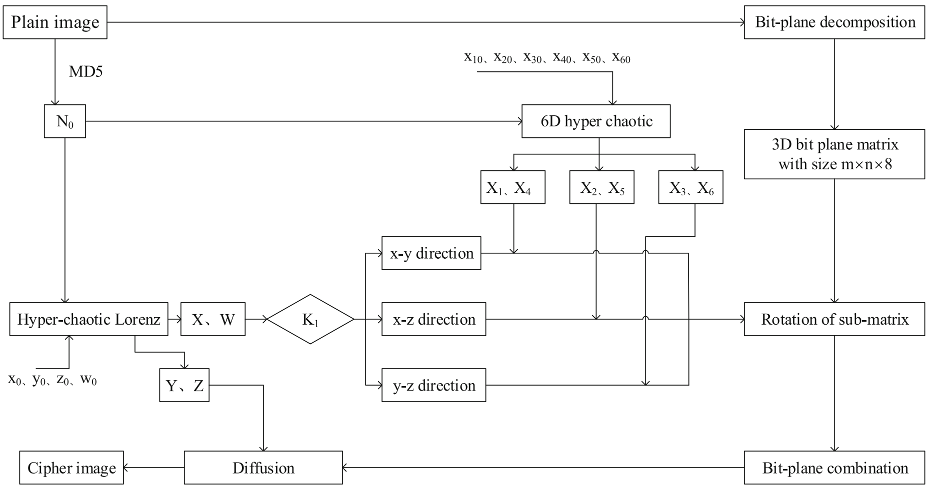


Fig. 2 The flow chart of the proposed encryption algorithm

transient effect, the first N_0 numbers of each sequence are discarded, and they are processed by

$$K_1(i) = \mathrm{mod}\left(\mathrm{floor}\left((x(i) + w(i)) \times 10^{13}\right), 3\right) \tag{5}$$

$$K_2(i) = \mathrm{mod}\left(\mathrm{floor}\left(y(i) \times 10^{13}\right), 256\right) \tag{6}$$

$$K_3(i) = \mathrm{mod}\left(\mathrm{floor}\left(z(i) \times 10^{13}\right), 256\right) \tag{7}$$

where floor(a) returns the value of a to the nearest integer less than or equal a. The length of K_1 is L, and that of K_2, K_3 are L/8.

Step 3: With the initial values x_{10}, x_{20}, x_{30}, x_{40}, x_{50} and x_{60}, six pseudo-random sequences x_1, x_2, x_3, x_4, x_5 and x_6 are obtained by iterated Eq. (2) for $N_0 + L$ times. To avoid the transient effect, the first N_0 numbers of each sequence are discarded. Then the six sequences are processed by the following equations:

$$K_5(i) = \mathrm{mod}\left(\mathrm{floor}\left(x_4(i) \times 10^{13}\right), 8\right) + 1 \tag{8}$$

$$K_6(i) = \mathrm{mod}\left(\mathrm{floor}\left(x_5(i) \times 10^{13}\right), \mathrm{n}\right) + 1 \tag{9}$$

$$K_7(i) = \mathrm{mod}\left(\mathrm{floor}\left(x_6(i) \times 10^{13}\right), m\right) + 1 \tag{10}$$

$$K_8(i) = \mathrm{mod}\left(\mathrm{floor}\left(x_1(i) \times 10^{13}\right), 4\right) \tag{11}$$

$$K_9(i) = \mathrm{mod}\left(\mathrm{floor}\left(x_2(i) \times 10^{13}\right), 4\right) \tag{12}$$

$$K_{10}(i) = \mathrm{mod}\left(\mathrm{floor}\left(x_3(i) \times 10^{13}\right), 4\right) \tag{13}$$

The lengths of K_τ ($\tau = 5, 6, 7, 8, 9, 10$) are all L.

3.2 Bit-plane matrix rotation phase

Here, rotation is employed to scramble bits in 3D bit-plane matrix. The sequence generated by Hyper-chaotic Lorenz system is utilized to select the direction of rotation. The plane, the position and size of related rotation sub-matrix are determined by sequence generated by 6D hyper chaotic. With these parameters, the corresponding sub-matrix is rotated. The process is described in details as follows.

Step 1: Decompose the plain-image P into eight bit planes using BBD as described in Sects. 2.1, and a 3D bit-plane matrix with size $m \times n \times 8$ is obtained, as shown in Fig. 3.

Step 2: According to the value of $Key_1(i) = K_1(i)$, the matrix is rotated in three directions, and the corresponding control sequence is different depended on different value of $Key_1(i)$.

i) If $Key_1(i) = 0$, the direction of rotation is x-y. That is, the bit-plane matrix is treated as a matrix of $m \times n \times 8$, and then we define $Key_2 = K_5$ and $Key_3 = K_8$.
ii) If $Key_1(i) = 1$, the direction of rotation is x-z. That is, the bit-plane matrix is treated as a matrix of $m \times 8 \times n$, and then we define $Key_2 = K_6$ and $Key_3 = K_9$.
iii) If $Key_1(i) = 2$, the direction of rotation is y-z. That is, the bit-plane matrix is treated as a matrix of $n \times 8 \times m$, and then we define $Key_2 = K_7$ and $Key_3 = K_{10}$.

Step 3: Because the 3D bit-plane matrix is composed of 2D planes, the size and number of 2D planes in different direction is determined as

i) If $Key_1(i) = 0$, the size of plane is $m \times n$, and the number of planes is 8;
ii) If $Key_1(i) = 1$, the size of plane is $m \times 8$, and the number of planes is n;
iii) If $Key_1(i) = 2$, the size of plane is $n \times 8$, and the number of planes is m;

The secret key $Key_2(i)$ is used to choose the i^{th} plane of the matrix for processing, e.g., if $Key_2(i) = 4$, the 4th plane of the matrix is chosen.

Step 4: Calculate the position and size of each sub-matrix in the 2D plane which is chosen in step 3. The sequence Key_3 is sorted in an ascending order. According to the position

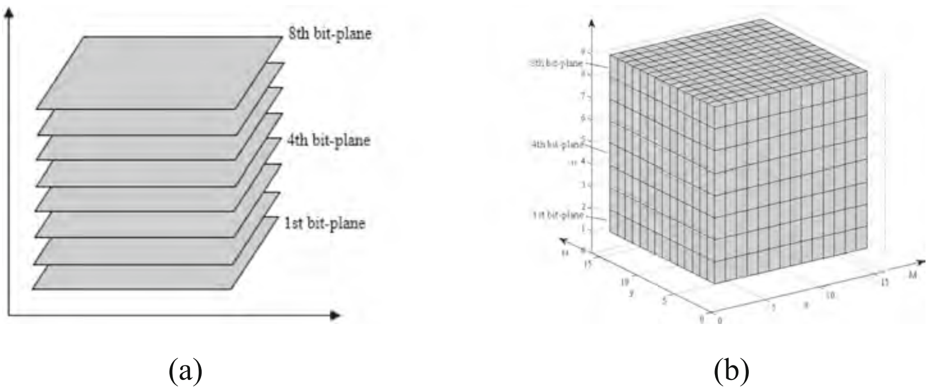


Fig. 3 **a** eight bit planes obtained by BBD; **b** 3D bit-plane matrix of size $m \times n \times 8$ is constructed by eight bit planes

in the initial sequence, a sequence$Key' = \{Key'_1, Key'_2, Key'_3, \ldots, Key'_{8\times m\times n}\}$ can be obtained. The row and column coordinate of the bit value in the upper-left corner of the corresponding sub-matrix is obtained by

$$temp(i) = \begin{cases} \mathrm{mod}\left(Key'(i), m \times \mathrm{n}\right), if\, \mathrm{mod}\left(Key'(i), m \times \mathrm{n}\right) \neq 0 \\ \mathrm{m} \times \mathrm{n}, \qquad \text{otherwise} \end{cases} \tag{14}$$

$$row(i) = \mathrm{ceil}(temp(i)/\mathrm{n}) \tag{15}$$

$$col(i) = \begin{cases} \mathrm{mod}(temp(i), n), if\ mod(temp(i), n) \neq 0 \\ n, \qquad \text{otherwise} \end{cases} \tag{16}$$

Then, the size of the sub-matrix is obtained by

$$r = \mathrm{m} - row + 1 \tag{17}$$

$$c = \mathrm{n} - col + 1 \tag{18}$$

$$size(i) = \min(r, c) \tag{19}$$

where the function ceil(a) returns the value of a to the nearest integer which is larger than or equal a.

Step 5: Calculate the counterclockwise rotation angle of the sub-matrix by

$$R(i) = \begin{cases} 0^\circ, & Key_3(i) = 0 \\ 90^\circ, & Key_3(i) = 1 \\ 180^\circ, & Key_3(i) = 2 \\ 270^\circ, & Key_3(i) = 3 \end{cases} \tag{20}$$

According to the rotation direction obtained in step 2, select different keys to obtain rotation angle. In Fig. 4, three examples of rotation in three directions and the sub-matrixes after rotation are obtained by the corresponding sequences and calculations.

Step 6: Repeat Step2~Step5 until i reaches L, and a matrix D with a size of m × n is obtained by bit-plane combination.

3.3 Diffusion phase

Diffusion can enhance the resistance to statistical attack and differential attack significantly, when the histogram of the cipher-image is fairly uniform [18]. To obtain a good diffusion

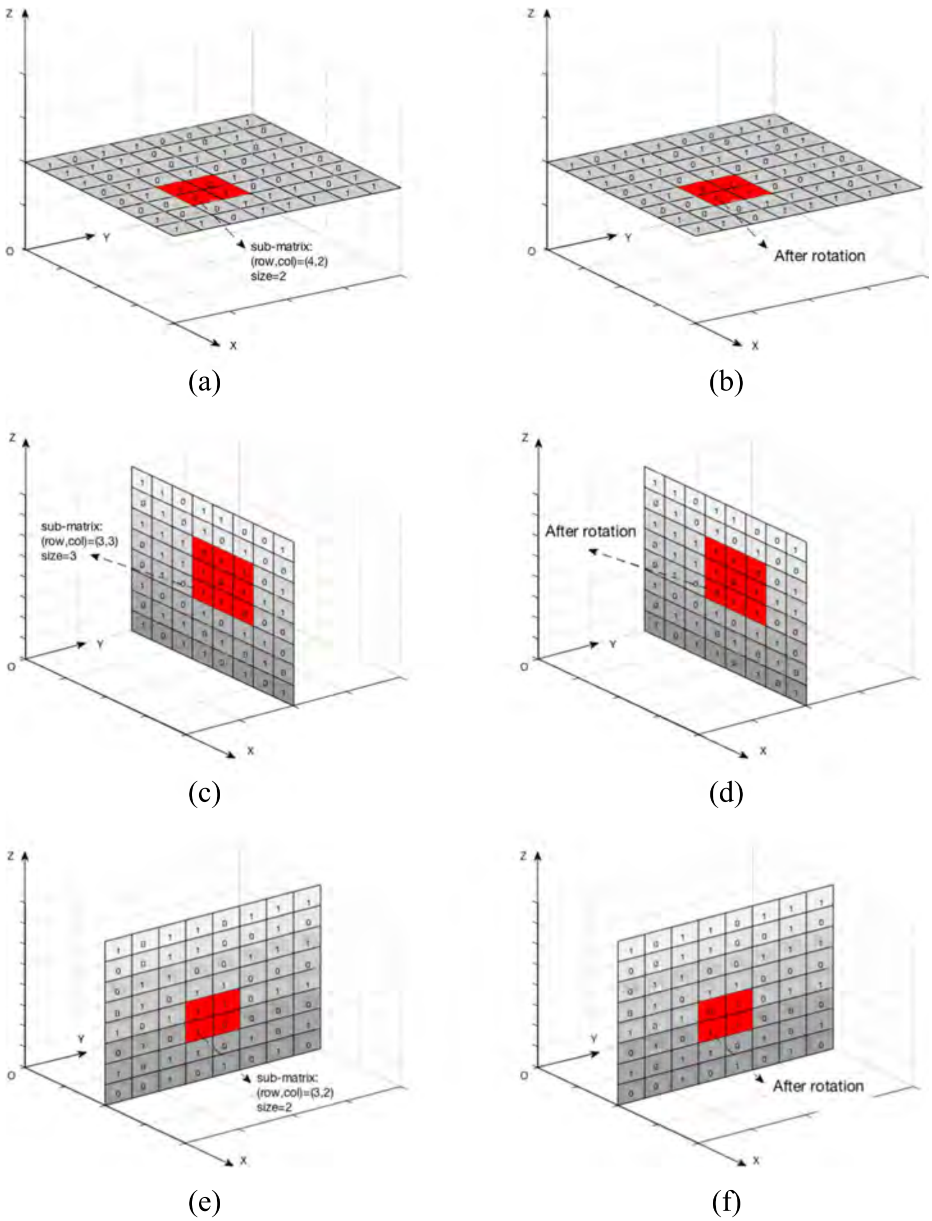


Fig. 4 Examples of rotation: **a** Original sub-matrix: according to Keys, the direction of rotation is x-y, the coordinate and size of the sub-matrix is as the picture shows; **b** the result of sub-matrix after 90° rotation. **c** Original sub-matrix: according to Keys, the direction of rotation is x-z, the coordinate and size of the sub-matrix are as the picture shows; **d** the result of sub-matrix after 270° rotation. **e** Original sub-matrix: according to Keys, the direction of rotation is y-z, the coordinate and size of the sub-matrix is as the picture shows; **f** the result of sub-matrix after 180° rotation

process, a key steam strongly related to the plain-image is utilized in diffusion. The process is outlined as follows.

Step 1: Convert a image matrix $D_{m \times n}$ to one dimensional vector, and encrypt the pixel of the cipher-image by

$$C(1) = \mathrm{mod}((K_2(1) + K_3(1)), 256) \oplus \mathrm{mod}((D(1) + Q), 256) \tag{21}$$

$$C(i) = \mathrm{mod}((K_2(i) + K_3(i)), 256) \oplus \mathrm{mod}((D(i) + C(i-1)), 256) \tag{22}$$

where Q is obtained by Eq. (4) and $i = 2, 3, \ldots, m \times n$.

Step 2: Repeat Step1 until i reaches $m \times n$, and a cipher-image can be obtained by transforming the sequence C into an $m \times n$ image.

3.4 Decryption phase

The decryption algorithm is the reverse process of encryption algorithm.

4 Experimental results and analysis

In the experiments, the images for testing have a size of 256×256 in 8-bit grayscale. The secret keys are set as ($x_0 = 3.3133$, $y_0 = 12.0546$, $z_0 = 40.8897$, $w_0 = -34.5677$) [41] and ($x_{10} = -2.23$, $x_{20} = 1.54$, $x_{30} = 0.09$, $x_{40} = 4.81$, $x_{50} = -3.60$, $x_{60} = 5.04$) [44]. The experiment results are shown in Fig. 5. Figure 5(a), (d), (g) denote original image. The encrypted images are shown in Fig. 5(b), (e), (h) and the decrypted images are shown in Fig. 5(c), (f), (i), which are identical to the original images.

4.1 Analysis of key space

A secure image encryption algorithm should possess a key space, which is larger than 2^{100}, to make brute-force attacks infeasible [1]. In the proposed encryption system, the keys are:

i) the given initial values of x_0, y_0, z_0, w_0, x_{10}, x_{20}, x_{30}, x_{40}, x_{50} and x_{60}.
ii) a 128-bit long hash value.

As for the given initial values of hyper-chaotic system, they are double-precision numbers, the key space size will be $(10^{16})^{10} = 10^{160}$. Furthermore, the security of MD5 with complexity of the best attack $S_{MD5} = 2^{64}$. So one can get the total key space $S = 2^{64} \times 10^{160} \approx 2^{544}$ which is large enough to resist the brute-force attack.

4.2 Anaylysis of histogram

An image histogram represents the distribution of the pixel intensity values within an image. For a good image encryption algorithm, the distribution of the cipher-image histogram should

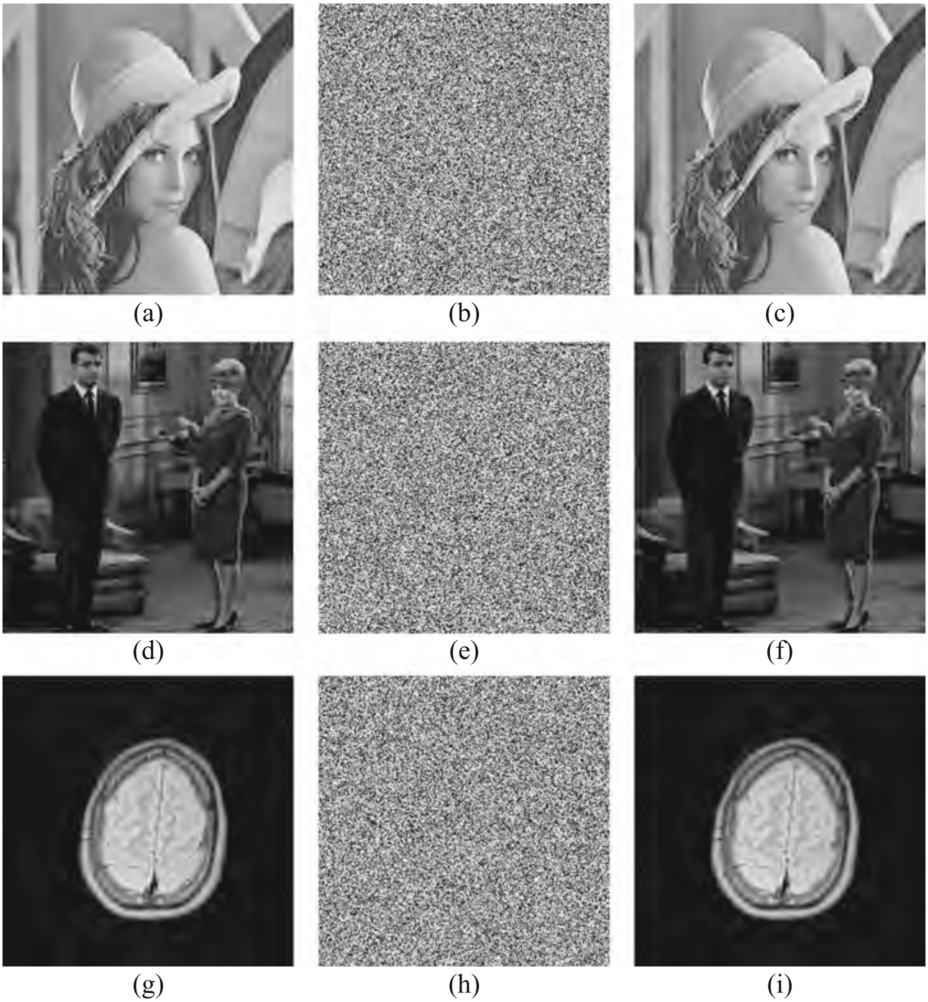


Fig. 5 Experimental results: **a** original image of Lena; **b** encrypted image of Lena; **c** decrypted image of Lena; **d** original image of Couple; **e** encrypted image of Couple; **f** decrypted image of Couple; **g** original image of Brain; **h** encrypted image of Brain; **i** decrypted image of Brain

be as uniform as possible. The histogram of the original images and corresponding cipher-images are shown in Fig. 6. It shows that the numbers of each grayscale value of the cipher image are almost equal, which indicates the excellent performance of the proposed scheme in resisting statistical attacks.

4.3 Correlation analysis

The adjacent pixels of the original image generally have a high correlation in the horizontal, vertical and diagonal directions. An ideal encryption algorithm can make the correlation coefficients of the pixels in the encrypted image have a sufficiently low correlation to resist statistical attacks. The correlation coefficient is calculated by

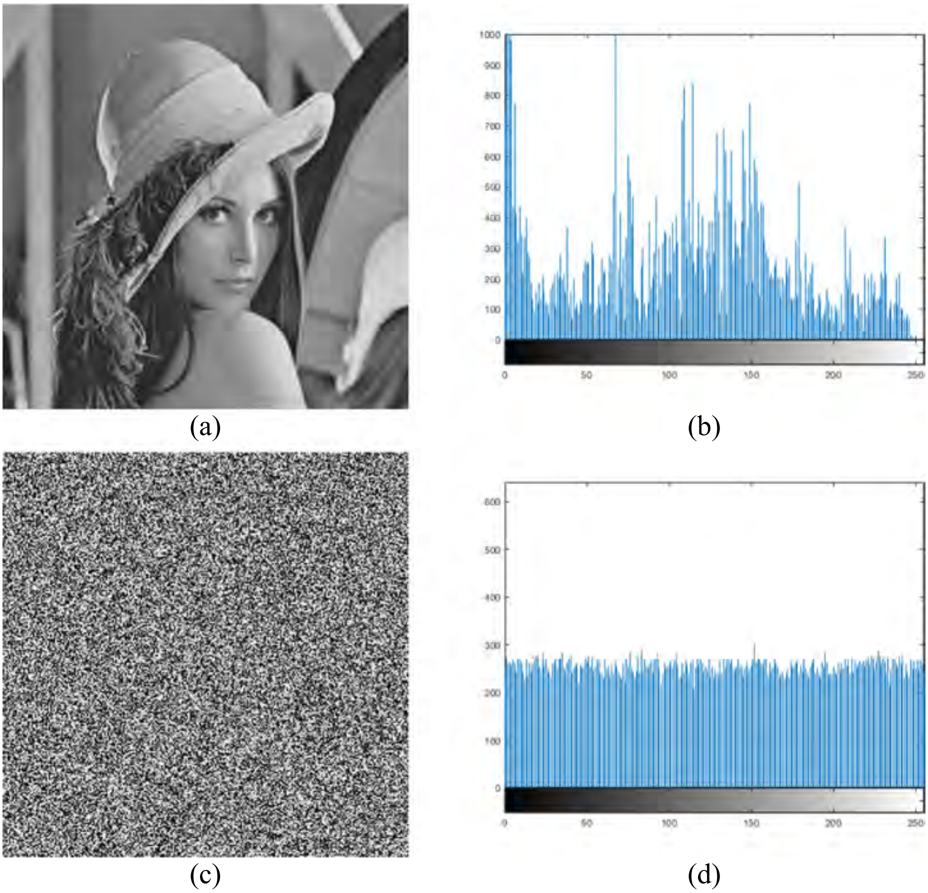


Fig. 6 Histogram analysis: **a** original image of Lena; **b** histogram of original image; **c** encrypted image of Lena; **d** histogram of encrypted image

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{23}$$

where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{24}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x_i)]^2 \tag{25}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x_i)][y_i - E(y_i)] \tag{26}$$

where x and y are the gray values of two adjacent pixels, N is the total number of pixels selected from image. The correlation coefficients among the 3000 pairs of adjacent pixels, which are randomly selected from the original and the encrypted images in the horizontal, vertical and diagonal directions are demonstrated in Table 1. It shows that the correction coefficients of the original image are very close to 1, while those of the encrypted image are around to 0 in all directions. The correlation distribution of the original and the encrypted images is shown in Fig. 7. As observed, the adjacent pixels of the original image have a strong correlation while the adjacent pixels of the encrypted image have a low correlation. Thus, the proposed encrypted algorithm can effectively resist statistical attacks.

4.4 Analysis of information entropy

The information entropy is the most important measure of randomness. For an 8-bit gray scale image, the ideal information entropy is H(s) = 8 bits, it is defined as

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i)\log_2 \frac{1}{P(s_i)} \tag{27}$$

where $P(s_i)$ represents the probability of the presence of a symbol s_i, and N represents the bit depth of the image [18]. When the entropy closely approach to eight, the possibility of attackers in decoding the cipher-images will be less. Table 2 shows the comparison of information entropy. From Table 2, it is obviously that entropies are close to 8, so the proposed algorithm has a good property of information entropy.

4.5 Analysis of key sensitivity

In the analysis, an original key is used to encrypt the Lena image and a modified key is used to decrypt the cipher-image. The original keys are set as ($x_0 = 3.3133$, $y_0 = 12.0546$, $z_0 = 40.8897$, $w_0 = -34.5677$, $x_{10} = -2.23$, $x_{20} = 1.54$, $x_{30} = 0.09$, $x_{40} = 4.81$, $x_{50} = -3.60$ and $x_{60} = 5.04$) and the slightly modified keys are set as ($x_0 = 3.3133 + 10^{-11}$, $y_0 = 12.0546$, $z_0 = 40.8897$, $w_0 = -34.5677$, $x_{10} = -2.23$, $x_{20} = 1.54$, $x_{30} = 0.09$, $x_{40} = 4.81$, $x_{50} = -3.60$ and $x_{60} = 5.04$). The original Lena image is shown in Fig. 8(a), and the corresponding cipher-image encrypted by the original key is shown in Fig. 8(b). The decrypted image for the incorrect decryption key is shown in Fig. 8(c), and the decrypted image for the correct decryption key is shown in Fig. 8(d). It is obvious that the slightly modified decryption key cannot decrypt the cipher-image. Therefore, the key sensitivity test shows that the proposed cryptosystem is pretty sensitive to the secret keys.

Table 1 Correlation coefficients of some plain-image and the corresponding cipher-images

Direction	Horizontal	Vertical	Diagonal
Plain-image of Lena	0.9429	0.9873	0.9169
Cipher-image of Lena	0.0015	−0.0137	−0.0006
Plain-image of Couple	0.9498	0.9580	0.9194
Cipher-image of Couple	0.0031	−0.0280	0.0006
Plain-image of Brain	0.9817	0.9861	0.9805
Cipher-image of Brain	0.0126	−0.0030	0.0010

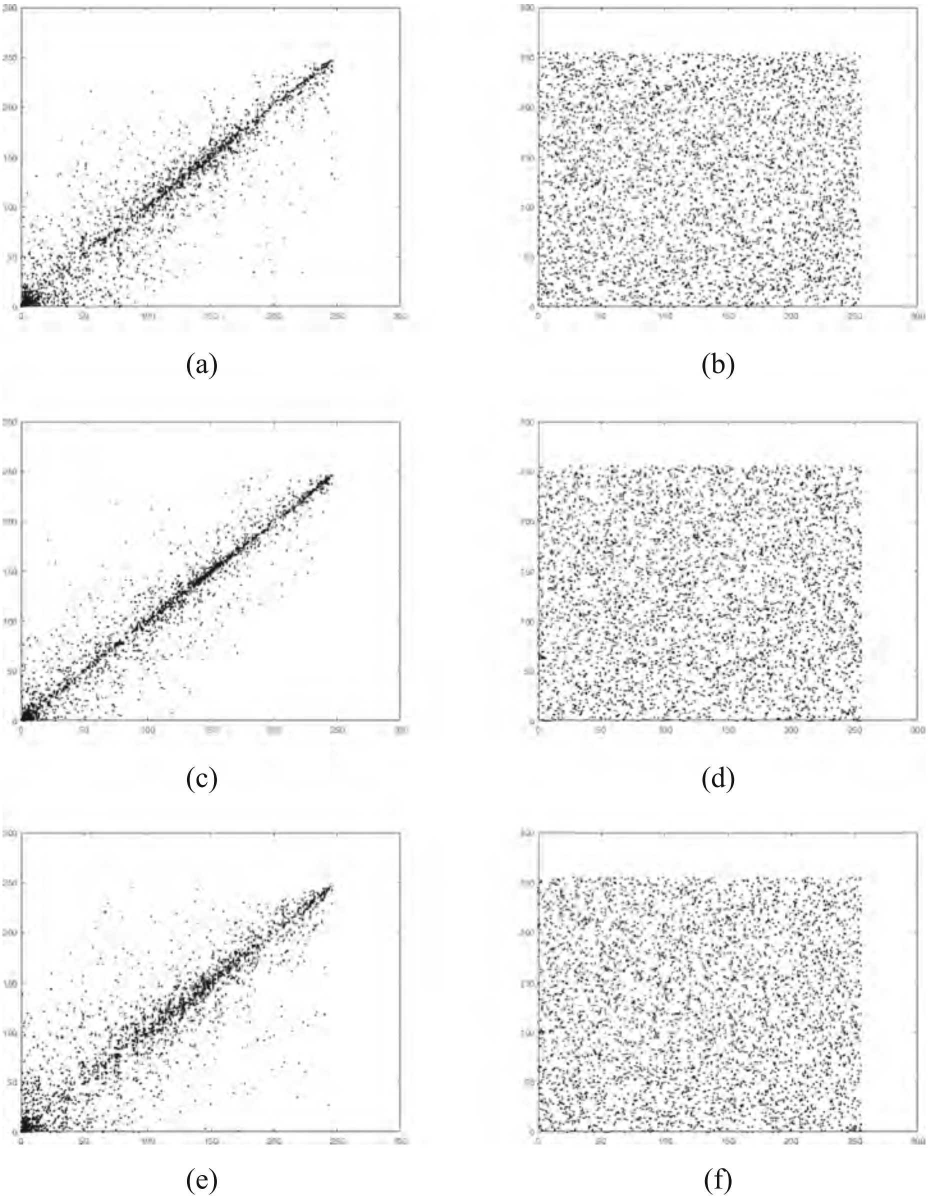


Fig. 7 The correlation plots of Lena and corresponding ciphered image of Lena: **a** horizontal correlation of Lena image; **b** horizontal correlation of ciphered image; **c** vertical correlation of Lena image; **d** vertical correlation of cipher image; **e** diagonal correlation of Lena image; **f** diagonal correlation of ciphered image

4.6 Analysis of differential attack

An opponent may makes a trivial change in the plain-image, encrypt two plain-images and then implements cryptanalysis by tracing the meaningful relationship between two cipher-images. NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) [26] are generally devoted to evaluating the impact caused by one-

Table 2 The results of information entropy

Algorithms	Images	H(s)
Proposed algorithm	Lena	7.9975
	Couple	7.9973
	Brain	7.9974
Ref. [47]	Lena	7.9974
Ref. []	Lena	7.9972

pixel change on the plain image. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively. They are defined by

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \tag{28}$$

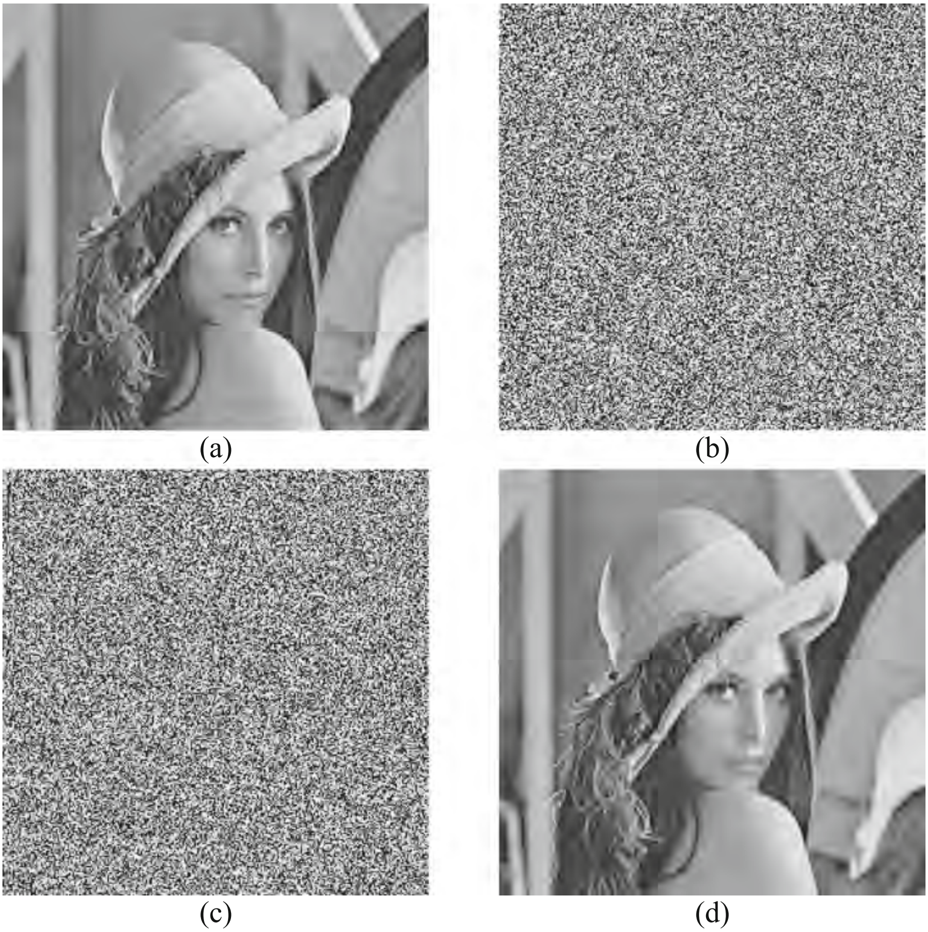


Fig. 8 Key sensitivity analysis: **a** original image; **b** encrypted image using the original key; **c** decrypted image using incorrect decryption key; **d** decrypted image using the correct decryption key

Table 3 NPCR and UACI performance

Algorithms	Images	NPCR	UACI
Proposed algorithm	Lena	0.9962	0.3354
	Couple	0.9962	0.3345
	Brain	0.9961	0.3355
Ref. [21]	Lena	0.9961	0.3333
Ref. [35]	Lena	0.9368	0.3334

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{29}$$

where C_1 and C_2 are two cipher-images whose plaintext has only a different pixel, and D(i, j) is defined by

$$D(i,j) = \begin{cases} 0, C_1(i,j) = C_2(i,j) \\ 1, \quad C_1(i,j) \neq C_2(i,j) \end{cases} \tag{30}$$

Here, the values of NPCR and UACI are calculated to test the effects of a 1-bit change in the plain image on the corresponding cipher image. The results are shown in Table 3. From the tables, it can be found that the proposed algorithm can achieve better performances against differential attacks compared with [21, 35].

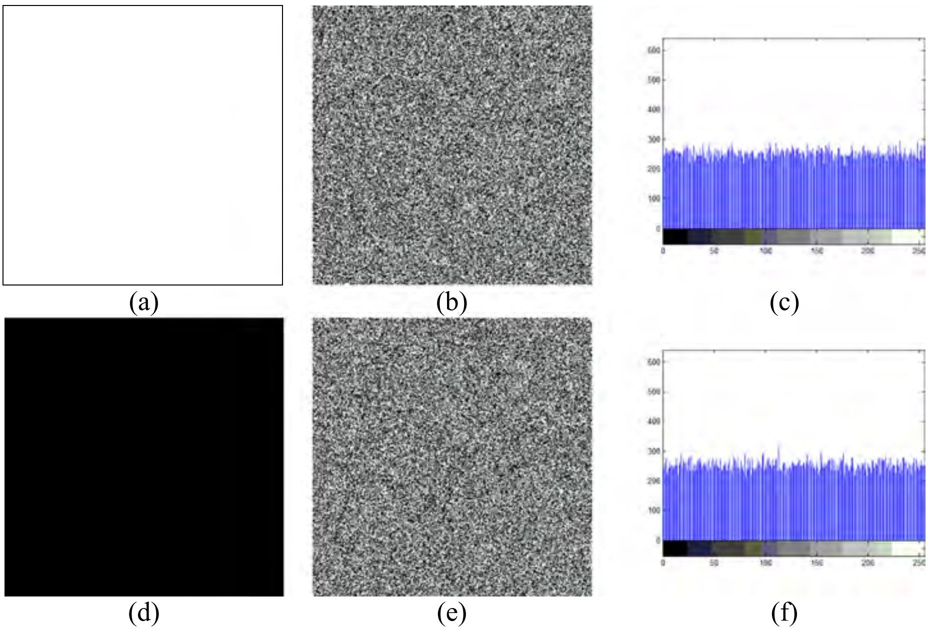


Fig. 9 Experiment results of special images. **a** all white image; **b** cipher image of (a); **c** histogram of (b); **d** all black image; **e** cipher image of (d); **f** histogram of (e)

Table 4 The encryption results of special images

	Entropy	Correlation coefficient		
		Horizontal	Vertical	Diagonal
Cipher image for all white image	7.9974	0.0303	−0.0451	0.0092
Cipher image for all black image	7.9972	−0.0096	−0.0089	−0.0140

4.7 Anaylysis of some typical attacks

In the cryptanalysis, there are four typical attacks: ciphertext-only attack, chosen-ciphertext attack, known-plaintext attack and chosen-plaintext attack. Among them, chosen-plaintext attack is the most powerful one. If an encryption algorithm can withstand chosen-plaintext attack, it has enough security level to resist other three attacks [5]. In our encryption scheme, MD5 hash value of the plain image is used to generate the number of pre-iterations, which is related chaotic sequence generation, and the initial value of diffusion process. That means the proposed algorithm uses different key stream when different images are encrypted. Hence, the key stream retrieved with one chosen plain-image cannot be used to decrypt other cipher-images, which implies the good performance in resisting chosen-plaintext attacks.

In a chosen-plaintext attack, some cryptanalysts try to find the secret key by choosing some special plain images, such as all black or white images [18]. To test the ability of defending this kind of attack, it is evaluated by using some special images as input images, the size of images for testing is 256 × 256. The experimental results are shown in Fig. 9, the information entropies and correlation coefficients of the cipher images are listed in Table 4. As shown in Fig. 9 and Table 4, the grayscale values of the cipher images are uniformly distributed, so the attacker cannot obtain useful information by encrypting some special images. From the above analysis, the proposed algorithm has a strong ability to withstand the chosen-plaintext attack and it can resist the above mentioned typical attacks.

4.8 Quality assessment of encrypted and decrypted image

The image quality assessment plays a variety of roles in image process applications. Here, PSNR (peak signal-to-noise ratio) and SSIM (structural similarity index metric) [38] are used for measuring image quality. The PSNR and SSIM between encrypted images and original image are listed in Table 5, the PSNR values are far lower than 20 dB and SSIM values are close to 0, which illustrate that the proposed method has a good encryption effect, and the original image have been significantly disturbed by the encryption process. While for the decrypted images, the PSNR and

Table 5 The PSNR and SSIM results between the original images and corresponding encrypted/decrypted images: 'O-E' represents the original and encrypted images, and 'O-D' denotes the original and decrypted images

	Lena	Peppers	Baboon	Brain
SSIM(O-E)	0.0088	0.0100	0.0103	0.0031
PSNR (O-E)	7.9709	8.8901	9.8217	5.7375
SSIM(O-D)	1	1	1	1
PSNR(O-D)	∞	∞	∞	∞

Table 6 Results of comparison

Comparing parameter	Proposed scheme	Ref. [32]	Ref. [25]	Ref. [45]	Ref. [2]
chosen-plaintext attack analysis	Yes	No	No	No	No
Key space	2^{544}	10^{45}	2^{140}	2^{203}	2.4×10^{112}
Information entropy	7.9975	7.9965	7.9973	7.9896	7.9973
NPCR	99.62%	98.97%	99.60%	99.60%	99.61%
UACI	33.54%	32.18%	33.49%	33.47%	28.61%
PSNR(O-E)	7.9709	9.2721	9.2089	8.1300	NA
SSIM(O-E)	0.0088	NA	0.0090	NA	NA

SSIM approach the desired values of ∞ and 1, respectively. It indicates that the decrypted images are completely the same as the original images.

5 Comparison with the state-of-the-art schemes

To demonstrate the good encryption performance of the proposed scheme, it is compared with some state-of-the-art schemes. "Lena" image of size 256×256 is used as a test image, the comparison results are listed in Table 6. It can be seen that our scheme is better than the methods in Refs. [2, 25, 32, 45] from the aspects of key space, information entropy, and PSNR. The NPCR, UACI values in this paper are close to the ideal values of 99.61% and 33.46%, and the SSIM value between the encrypted images and the original image is close to 0. Furthermore, the proposed scheme has a strong ability to withstand the chosen-plaintext attacks. Thus, the proposed scheme is feasible and effective.

6 Conclusion

In this paper, a novel image encryption algorithm using bit-plane matrix rotation and hyper chaotic systems is proposed. In the cryptosystem, we first convert the plain-image into eight bit-planes. Then, a bit-plane matrix rotation method is introduced. The method scrambles bits in bit-plane matrix effectively with PRNS generated by the hyper chaotic systems. Besides, the MD5 hash value of the plain-image is utilized to get some parameters used in the encryption process. Thus the algorithm has a high relationship with the plain-image. Simulation results and performance analyses both demonstrate that the proposed algorithm has high security against the converntial attacks.

Acknowledgments This work is supported by the National Natural Science Foundation of China (Grant No.61571185), The Science and Technology Progress and Innovation Project of Hunan Transportation Department, China (Grant No.2018037) The Science and Technology Planning Project of Hunan Province (Grant No.2017GK4009), and the Open Fund Project of Key Laboratory in Hunan Universities (Grant No.16 K018).

References

1. Álvarez G, Li S (2006) Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos 16(8):2129–2151

2. Aqeel-ur-Rehman LXF, Hahsmi MA, Haider R (2018) An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik. 153:117–134
3. Belazi A, Abd Ellatif AA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170
4. Chai XL (2017) An image encryption algorithm based on bit level Brownian motion and new chaotic systems. Multimed Tools Appl 76(1):1159–1175
5. Chai XL, Fu XL, Gan ZH, Lu Y, Chen YR (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process 155:44–62
6. Chen JX, Zhu ZL, Fu C et al (2015) An efficient image encryption scheme using lookup table-based confusion and diffusion. Nonlinear Dynamics 81(3):1151–1166
7. Cheng GF, Wang CH, Chen H (2019) A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. Int J Bifurc Chaos 29(9):1950115
8. Fu C, Lin B, Miao Y et al (2011) A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 284(23):5415–5423
9. Grassi G, Severance FL, Miller DA (2009) Multi-wing hyperchaotic attractors from coupled Lorenz systems. Chaos, Solitons Fractals 41(1):284–291
10. Hilborn RC (1994) Chaos and nonlinear dynamics: an introduction for scientists and engineers. Am J Phys 62(9):861–862
11. Hua ZY, Zhou YC, Pun CM et al (2015) 2D Sine Logistic modulation map for image encryption. Inf Sci 297:80–94
12. Huang X (2012) Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dynamics 67(4):2411–2417
13. Jin J, Li C (2019) Fully Integrated Memristor and Its Application on the Scroll-Controllable Hyperchaotic System. Complexity 2019:1–8
14. Khan M (2015) A novel image encryption scheme based on multiple chaotic S-boxes. Nonlinear Dynamics 82(1–2):527–533
15. Khanzadi H, Eshghi M, Borujeni SE (2014) Image Encryption Using Random Bit Sequence Based on Chaotic Maps. Arab J Sci Eng 39(2):1039–1047
16. Li S, Chen G, Cheung A et al (2005) On the Design of Perceptual MPEG-Video Encryption Algorithms. IEEE Transactions on Circuits & Systems for Video Technology 17(2):214–223
17. Li CQ, Lin DD, Feng BB, Lü JH, Hao F (2018) Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy. IEEE Access 6:75834–75842
18. Li CQ, Lin D, Lü JH, Hao F (2018) Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE MultiMedia 25(4):46–56
19. Li CH, Luo GC, Qin K et al (2017) An image encryption scheme based on chaotic tent map. Nonlinear Dynamics 87(1):127–133
20. Li CQ, Zhang Y, Xie Y (2019) When an attacker meets a cipher-image in 2018: A year in review. Journal of Information Security and Applications 48:102361
21. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36
22. Liu HJ, Wang XY (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59(10):3320–3327
23. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16):3895–3903
24. Liu J, Yang D, Zhou H et al (2018) A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimed Tools Appl 77(8):10217–10233
25. Liu DD, Zhang W, Yu H, Zhu ZL (2018) An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion. Signal Process 151:130–143
26. Mao Y, Chen GR, Lian SG (2004) A novel fast image encryption scheme based on 3D chaotic baker maps. International Journal of Bifurcation and Chaos 14(10):3613–3624
27. Matthews R (1989) On the derivation of a "chaotic" encryption algorithm. Cryptologia 13(1):29–42
28. Peng F, Zhang X, Lin ZX, Long M (2019) A Tunable Selective Encryption Scheme for H.265/HEVC Based on Chroma IPM and Coefficient Scrambling. IEEE Transactions on Circuits and Systems for Video Technology. https://doi.org/10.1109/TCSVT.2019.2924910
29. Peng F, Zhu XW, Long M (2013) An ROI privacy protection scheme for H.264 video based on FMO and chaos. IEEE Transactions on Information Forensics and Security 8(10):1688–1699
30. Ramasubramanian K, Sriram MS (2000) A comparative study of computation of Lyapunov spectra with different algorithms. Physica D Nonlinear Phenomena 139(1):72–86
31. Rössler OE (1979) An Equation for Hyperchaos. Phys Lett A 71:155–157

32. Sukalyan S, Abhijit M, Sarbani P, Chaudhuri BB (2019) A selective bitplane image encryption scheme using chaotic maps. Multimed Tools Appl 78(8):10373–10400
33. Sun SL (2018) A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling. IEEE Photonics Journal 10(2):1–14
34. Tang Z, Song J, Zhang X et al (2016) Multiple-image encryption with bit-plane decomposition and chaotic maps. Opt Lasers Eng 80:1–11
35. Teng L, Wang XY (2012) A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt Commun 285(20):4048–4054
36. Teng L, Wang X, Meng J (2018) A chaotic color image encryption using integrated bit-level permutation. Multimed Tools Appl 77(16):6883–6896
37. Tong XJ (2013) Design of an image encryption scheme based on a multiple chaotic map. Commun Nonlinear Sci Numer Simul 18(7):1725–1733
38. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
39. Wang XY, Guo K (2014) A new image alternate encryption algorithm based on chaotic map. Nonlinear Dynamics 76(4):1943–1950
40. Wang XY, Teng L, Qin X (2012) A novel color image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
41. Wang XY, Wang MJ (2008) A hyperchaos generated from Lorenz system. Physica A Statistical Mechanics & Its Applications 387(14):3751–3758
42. Wang XY, Wang Q, Zhang YQ (2015) A fast image algorithm based on rows and columns switch. Nonlinear Dynamics 79(2):1141–1149
43. Wang X, Zhang HL (2015) A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun 342:51–60
44. Wu XJ, Wang DW, Kurths J, Kan HB (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inf Sci 349:137–153
45. Wu XJ, Wang KS, Wang XY, Kan HB, Kurths J (2018) Color image DNA encryption using NCA map-based CML and one-time keys. Signal Process 148:272–287
46. Xiang LY, Shen XB, Qin JH, Hao W (2019) Discrete multi-graph hashing for large-scale visual search. Neural Process Lett 49(3):1055–1069
47. Xu L, Li Z, Li J et al (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25
48. Yin Q, Wang CH (2018) A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion. International Journal of Bifurcation and Chaos 28(4):1850047
49. Zhang X, Zhao Z (2013) Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dynamics 75(1–2):319–330
50. Zhou Y, Cao W, Chen CLP (2014) Image encryption using binary bitplane. Signal Process 100(7):197–207
51. Zhu C, Liao C, Deng X (2013) Breaking and improving an image encryption scheme based on total shuffling scheme. Nonlinear Dynamics 71(1–2):25–34
52. Zhu ZL, Zhang W, Kwok-wo W (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 181(6):1171–1186
53. Zhou L, Wang CH, Zhou LL (2018) A novel no-equilibrium hyperchaotic multi-wing system via introducing memristor. International Journal of Circuit Theory and Applications 46 (1):84-98
54. Zhang X, Wang CH (2019) Multiscroll Hyperchaotic System with Hidden Attractors and Its Circuit Implementation. International Journal of Bifurcation and Chaos 29(09):1950117
55. Zhang X, Wang CH (2019) A novel multi-attractor period multi-scroll chaotic integrated circuit based on CMOS wide adjustable CCCII. IEEE Access 7:16336-16350

Cong Xu received the Bachelor's degree in communications engineering from Hunan City University, Yiyang, China. Currently, she is pursuing the Master's degree in College of Computer Science and Electronic Engineering, Hunan University, China. Her research interests include digital image encryption using Chaos theory and neural networks based on memristor.

Jingru Sun was born in Liaoyuan, China, in 1977. She received the Ph.D. degree from Hunan University, Changsha, China, in 2014. She is currently a lecturer of College of Computer Science and Electronics Engineering, Hunan University, Changsha, China. Her research interests include radio frequency circuit and current-mode circuit design, synchronization of memristor-based neural networks.

Chunhua Wang received the M.S. degree from Zhengzhou University, Zhengzhou, China, in 1994, and the Ph.D. degree from Beijing University of Technology, Beijing, China, in 2003. He is currently the Professor of College of Information Science and Engineering, Hunan University, Changsha, China. He is the Doctor tutor, director of advanced communication technology key laboratory of hunan universities, the member of academic committee of hunan university, the director of chaos and nonlinear circuit professional committee of circuit and system branch of China electronic society. Now, his research interests include memristor circuit, complex networks, chaotic circuit, chaos secure communication, current-mode circuit and neural networks based on memristor. He has presided over 8 national and provincial projects, and published more than 120 papers, among which more than 100 were retrieved by SCI.