Optics and Lasers in Engineering 90 (2017) 238–246

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation

Yueping Li, Chunhua Wang, Hua Chen*

School of Information Science and Engineering, Hunan University, Changsha 410082, China

ARTICLE INFO

Keywords:
Image encryption
Multi-wing
Hyper-chaos
Bit-level permutation

ABSTRACT

Recently, a number of chaos-based image encryption algorithms that use low-dimensional chaotic map and permutation-diffusion architecture have been proposed. However, low-dimensional chaotic map is less safe than high-dimensional chaotic system. And permutation process is independent of plaintext and diffusion process. Therefore, they cannot resist efficiently the chosen-plaintext attack and chosen-ciphertext attack. In this paper, we propose a hyper-chaos-based image encryption algorithm. The algorithm adopts a 5-D multi-wing hyper-chaotic system, and the key stream generated by hyper-chaotic system is related to the original image. Then, pixel-level permutation and bit-level permutation are employed to strengthen security of the cryptosystem. Finally, a diffusion operation is employed to change pixels. Theoretical analysis and numerical simulations demonstrate that the proposed algorithm is secure and reliable for image encryption.

1. Introduction

Multimedia communication has become more and more important with the rapid development in internet technology and multimedia technology. Therefore, the security of image information has become an increasingly serious issue. However, due to bulky data capacity, high redundancy and strong correlations among adjacent pixels, traditional encryption algorithms, such as DES and AES, are poorly suited to image encryption [1].

Chaotic system has many excellent intrinsic properties, such as ergodicity, aperiodicity, high sensitivity to initial conditions and control parameters and random-like behaviors. Therefore, researchers have proposed many image encryption algorithms based on chaotic systems [2–21]. The typical ciphers based on chaotic map can be partitioned into two stages: permutation and diffusion. In [2–12], a number of image encryption algorithms using pixel-level permutation have been proposed. The permutation operation of these algorithms just changes the position of the pixel. And the chaotic sequence generated by chaotic system is independent of the plaintext and diffusion process. Therefore, the ciphertext can be easily deciphered by chosen-plaintext attack and chosen-ciphertext attack [13–15]. In [16], an image encryption based on one-time keys is proposed. In [17], a novel chaotic block image encryption algorithm based on dynamic random growth technique is proposed. Although the schemes adopt some measures in the encryption process to improve security, but they cannot resist chosen-plaintext attack and chosen-ciphertext attack totally. To avoid attackers crack cryptosystems by using the order from top to bottom and from left to right, Wang et al. proposed dynamical pixel order for diffusion and sub-images division method [18]. Belazi et al. [19] proposed a new chaos-based partial image encryption scheme which encrypts only the requisite parts of the sensitive information in frequency domain of Lifting-Wavelet Transform (LWT) based on hybrid of chaotic maps and a new S-box. Liu et al. [20] proposed a fast image encryption algorithm. In this algorithm, the confusion and diffusion processes are combined for one stage. Wang et al. [21] proposed a novel hybrid color image encryption algorithm using two complex chaotic systems to enhance the security and enlarge key space of color image encryption. In [22–27], a variety of image encryption algorithms using bit-level permutation have been proposed due to the advantages of bit-level permutations, which can change the position and value of a pixel simultaneously. In [29], Wang et al. introduced the perceptron conception of a neural network to a chaotic encryption system, and proposed a new bit-level encryption algorithm based on mathematical model to improve security. In [30], a new bit-level encryption algorithm based on the spatiotemporal non-adjacent coupled map lattices which makes it possible for any bit in pixels to break the limit of its bitplane without extra space in permutation process. In [31], a novel bit-level image encryption algorithm based on chaotic maps is proposed to modify the statistical information that is in each bitplane. Recently, the characteristics of DNA computing, massive parallelism, huge storage and ultra-low power consumption have been found. A number of image encryption algorithms use DNA rule are proposed [28,32,33,37]. However, they have the same weakness as pixel-level image encryption algorithms.

* Corresponding author.

http://dx.doi.org/10.1016/j.optlaseng.2016.10.020
Received 8 August 2016; Received in revised form 22 October 2016; Accepted 24 October 2016
Available online 04 November 2016

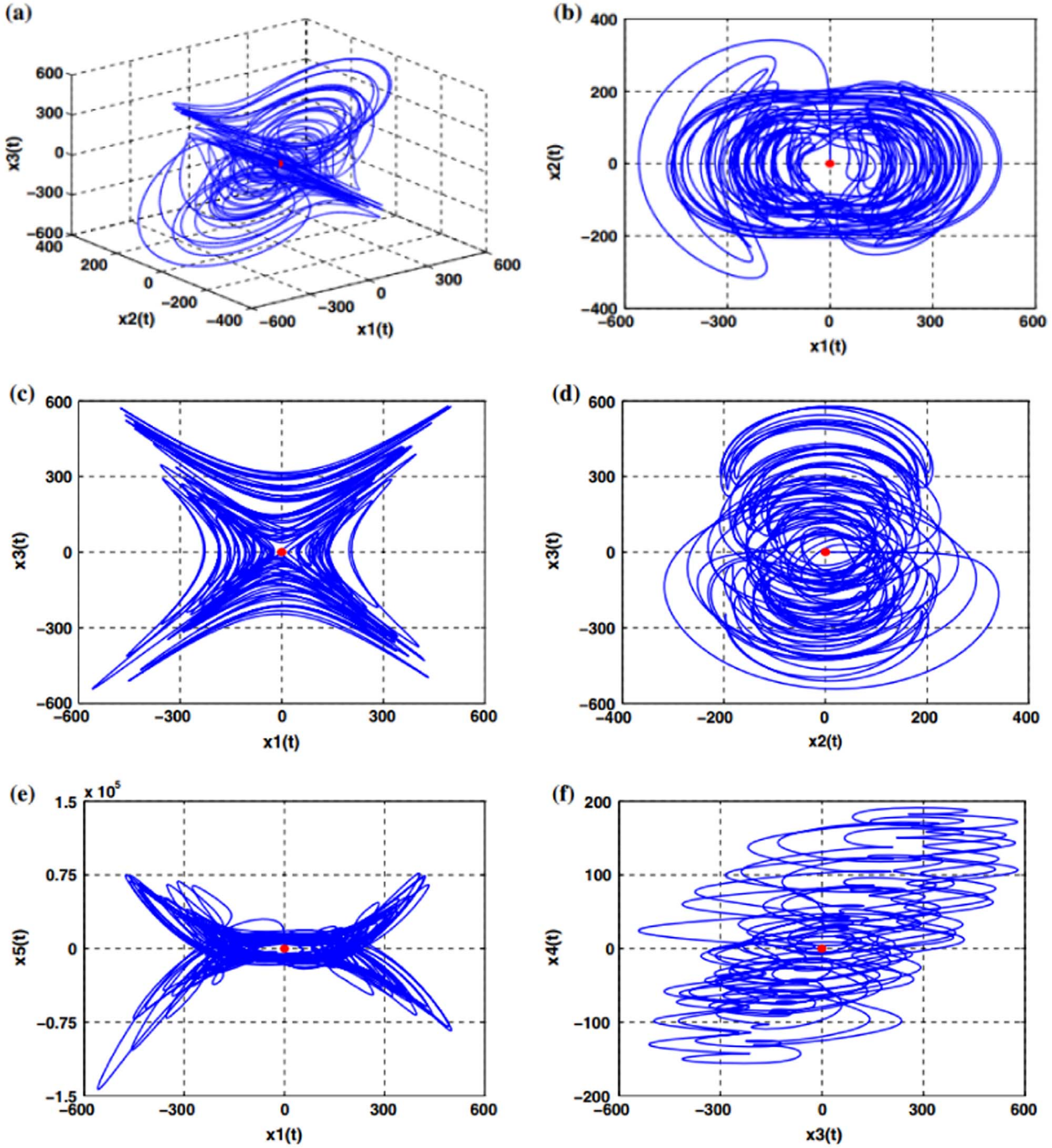


Fig. 1. Phase portraits of system (1) with parameters a=10, b=60, c=20, d=15, e=40, f =1, g =50, h =10, (a) 3D view in the x_1–x_2–x_3 space; (b) projection on x_1–x_2 plane; (c) projection on x_1–x_3 plane; (d) projection on x_2–x_3 plane; (e) projection on x_1–x_5 plane; (f) projection on x_3–x_4 plane.

In addition, compared with high-dimensional chaotic systems, image encryption algorithms employing the low-dimensional chaotic maps are not safe. Because high-dimensional chaotic systems, especially hyper-chaotic systems, have a larger key space, better sensitivity, more complex dynamic characteristics and randomness. The general methods that can decipher low-dimensional chaotic maps, such as phase space reconstruction and nonlinear prediction, are difficult to decipher high-dimensional chaotic systems. Therefore, a number of image encryption algorithms based on hyper-chaotic systems have been proposed [28,34–38]. In [34], Gao and Chen proposed a hyper-chaos-based image encryption algorithm using pixel-level permutation. Although this algorithm has the advantage of large key space, Ruouma and Belghith [35] proved that it could not resist the chosen-plaintext attack and the chosen-ciphertext attack; moreover, Jeng et al. [36] found that there is a weakness for Gao and Chen's algorithm and Ruouma and Belghith's improved algorithm, i.e., low sensitivity to change of plain-images. Meanwhile, hyper-chaos-based image encryption algorithms with DNA encoding were presented [28,37]. However, to date, there are not image encryption algorithms using pixel-level permutation and bit-level permutation.

To overcome the weaknesses above, this paper proposes a hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. First, the algorithm employs a hyper-chaotic system to resist the general methods which can decipher low-dimensional chaotic map. Meanwhile, the chaotic sequence generated by chaotic system is relevant to characteristics of plain-image. Therefore, different plain-images could get completely different chaotic sequences. The chosen-plaintext attack and chosen-ciphertext attack are void. Then, a pixel-level permutation is employed. Next, we use a bit-level permutation to scramble the image. Combining with pixel-level permutation and bit-level permutation can strengthen security of the cryptosystem. Finally, in diffusion operation, we add the pixels after pixel-level permutation. Compared with the existing hyper-chaos-based image encryption algorithms, the algorithm we propose is safer because we use pixel-level permutation, bit-level permutation and more complex chaotic system. Experiment results and simulation have shown that this algorithm not only performs well, but also can resist different attacks.

The paper is organized as follows. In Section 2, the hyper-chaotic system is introduced. In Section 3, we describe the proposed image encryption algorithm in detail. In Section 4, the simulation results and security analysis are presented, while the conclusions are reported in Section 5.

2. Chaotic system

The paper adopts a 5-D multi-wing hyper-chaotic system as follow [39]:

$$\begin{cases} \dot{x}_1 = -ax_1 + x_2x_3 \\ \dot{x}_2 = -bx_2 + fx_5 \\ \dot{x}_3 = -cx_3 + gx_4 + x_1x_2 \\ \dot{x}_4 = dx_4 - hx_1 \\ \dot{x}_5 = ex_5 - x_2x_1^2 \end{cases} \tag{1}$$

where x_1, x_2, x_3, x_4, x_5 are state variables and a, b, c, d, e, f, g, h are real constant parameters of system (1). Nonlinear terms in this dynamical system are $x_2 \times_3$, $x_1 \times_2$ and $x_2 \times_1{}^2$. We measure the phase portraits, dynamical behavior and bifurcation of the employed system as below [39–41].

2.1. Phase portraits of the hyper-chaotic system

We choose a=10, b=60, c=20, d=15, e=40, f=1, g=50, h=10 and initial conditions are (1, 1, 1, 1, 1). Also, the time step size to solve system is 0.001. Lyapunov exponents are L_1=9.979, L_2=1.96, L_3=0.005362, L_4=−19.13, L_5=−27.82; therefore, system (1) is hyper-chaotic. We can see chaotic behavior by phase portraits of the system (1) in Fig. 1.

2.2. Dynamical analysis of the hyper-chaotic system

The evolution of chaotic attractors in the system (1) will be presented through bifurcation diagrams. The system will be focused on parameter d for describing the dynamical behavior of the new system, and we set time step size 0.001, keep the absolute and relative error 0.000001 and choose the initial conditions $x1(0)$=1, $x2(0)$=1, $x3(0)$=1, $x4(0)$=1, $x5(0)$=1. The results will be obtained via varying parameter d by fixing the other parameters. When a=10, b=60, c=20, e=40, f=1, g=50, h=10, and d is variable in region [−5,20], the proposed system has different dynamical behaviors such as periodic orbit, chaotic and hyper-chaotic. The spectrum of Lyapunov exponents of the system (1) with respect to parameter d is shown in Fig. 2(a). When d∈[−5, 0], the maximum Lyapunov exponent is zero and system (1) has a periodic orbit. For d ∈ [0, 8.8], one positive Lyapunov exponent appears, and system (1) is chaotic. When d∈[8.8, 20] two positive Lyapunov exponents appear, therefore, system (1) is hyper-chaotic.

The bifurcation diagram versus d is illustrated in Fig. 2(b). By increasing d, Fig. 2(b) clearly shows the generation of the chaotic attractor.

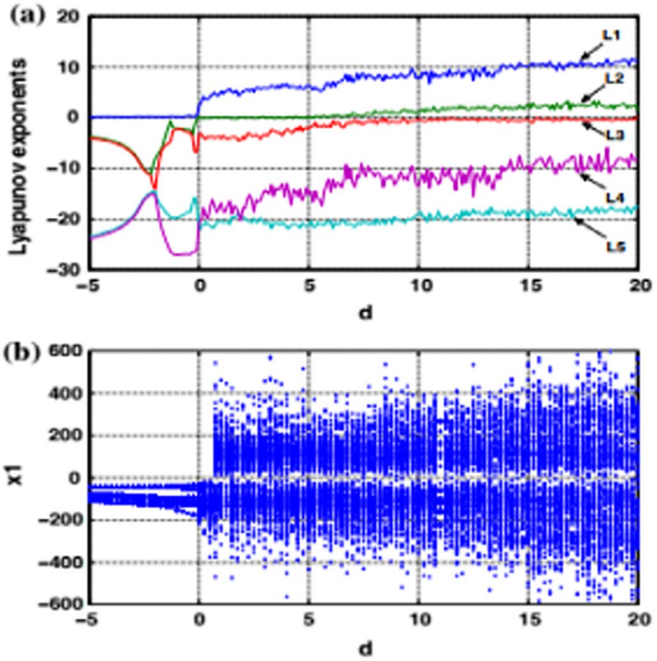


Fig. 2. Spectrum of Lyapunov exponents and bifurcation diagram of system (1) versus the parameter d∈[−5, 20].

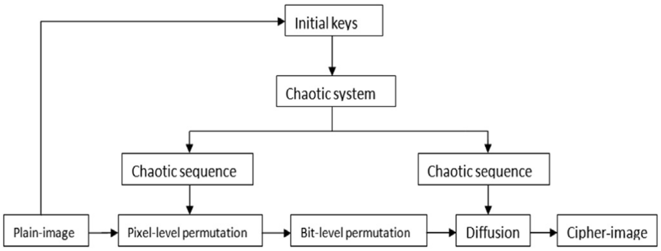


Fig. 3. The encryption process.

3. The proposed image encryption algorithm

The encryption process in the paper is shown in Fig. 3. First, the chaotic sequence generated by chaotic system is relevant to characteristics of plain-image. Then, a pixel-level permutation is employed to shuffle the plain-image. Next, a bit- level permutation is utilized to strengthen security of the cryptosystem. Finally, we can get cipher-image by a diffusion operation.

3.1. Pixel-level permutation process

We utilize a pixel-level permutation process to confuse plain-image totally. It can disrupt the correlation of adjacent pixels. The pixel-level permutation process is stated as follows.

Step1 Convert digital image matrix $A_{m\times n}$ to one-dimensional vector P={p_1 , p_2 , p_3 , ⋯ , $p_{m\times n}$}.
Step2 Calculate the sum of all pixels in the plain-image, and calculate the initial keys x_1, x_2, x_3, x_4, x_5 of chaotic system (1) according to formula (2).

$$\begin{cases} x_1 = \frac{sum + S}{2^{23} + S} \\ x_i = \bmod(x_{i-1} \times 10^6,\ 1) \quad i = 2,\ 3,\ 4,\ 5 \end{cases} \tag{2}$$

where S is size of the plain-image.

Step3 Make the chaotic system (1) for N_0+MN times iterations and discard the former N_0 values to avoid harmful effects. The chaotic sequence has MN elements, L={L_1 , L_2 , L_3 , ⋯ , $L_{m\times n}$}.

Step4 The chaotic sequence is sorted in ascending order. According to the pixel position in the initial sequence, we can obtain sequence L'={ L'_1 , L'_2 , L'_3 , ⋯ , $L'_{m\times n}$ }. Then, the sequence L' is applied to permute the image pixel positions P and get a shuffled sequence Q={Q_1 , Q_2 , Q_3 , ⋯ , $Q_{m\times n}$}.

3.2. Bit-level permutation process

In the process, we employ a bit-level permutation, to change bits of the pixel. Bit-level permutation process will recreate four new bytes to change bits of each byte by combining four bytes. Actually, it is mean that a column multiply a constant matrix. The bit-level permutation process is described as follows.

Step1 Divide the shuffled sequence Q into MN/16 matrices which are 4×4.

Step2 Get a new 4×4 matrix by to multiply a constant matrix and a 4×4 matrix, the constant matrix and the inversion matrix shown in Fig. 4.

Step3 Repeat Step2 until MN/16 matrices have executed a round of bit-level permutation operation. Then, we can obtain a matrix $D_{m\times n}$ by combining MN/16 matrices.

3.3. Diffusion process

Diffusion process can enhance the resistance to statistical attack and differential attack greatly, in which the histogram of the cipher-image is fairly uniform and is significantly different from that of the plain-image. To a good diffusion process, a key stream strongly related to plain-image should be used. When encrypting different plain-images, we can get completely different chaotic sequences in the encryption algorithm. The diffusion process is outlined as follows.

Step1 Utilize chaotic sequence L to obtain key stream according to formula (3).

$$K_i = \mathrm{mod}((abs(L_i) - floor(abs(L_i))) \times 10^{14}, 256) \tag{3}$$

Step2 Encrypt pixel values of the image matrix $D_{m\times n}$ by formula (4) and formula (5).

$$C_1 = \mathrm{mod}(D_1 + C_0, 256) \oplus \mathrm{mod}(Q_1 + K_1, 256) \tag{4}$$

$$C_i = \mathrm{mod}(D_i + C_{i-1}, 256) \oplus \mathrm{mod}(Q_i + K_i, 256) \quad i = 2, 3, \ldots, m \times n \tag{5}$$

where C_O is a constant, it can also be used as the encryption key.

Step3 Repeat Step2 until i=m×n, and we can get cipher-image C.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Fig. 4. The constant matrix and the inversion matrix.

3.4. The decryption

The decryption procedure is the reverse process of encryption. First, we should obtain the chaotic sequence generated by chaotic system. Then, inverse operation of diffusion is implemented by formula (6) to get the scrambled image *Di'*. Next, divide the scrambled image D' into MN/16 matrices and utilize the inversion matrix in section 2.3 to carry out inverse operation of bit-level permutation. Finally, we can obtain the plain-image P' by the inversion operation of pixel-level permutation.

$$D'_i = \mathrm{mod}((C_i \oplus \mathrm{mod}(Q_i + K'_i, 256) + 256) - C_{i-1}, 256) \quad i = 2, 3, \ldots, m \times n \tag{6}$$

4. Experimental results and performance analysis

In this section, we analyze the performance of the proposed scheme, including histograms, correlation coefficients, key space analysis, key sensitivity analysis and differential analysis. In the experiments, the images for testing are the 256×256 'Lena' image.

4.1. Key space

The key space is the total number of different keys that can be used in the encryption procedure. In the proposed algorithm, the secret keys include the initial values of the chaotic system, iteration times N0 and the constant C0. The computational precision of double-precision number is taken as 10^{16}. The precision of initial values are H_{x1}=*Hx2*=*Hx3*=*Hx4*=*Hx5*=10^{16} and the constant are *C0*=2^8.Therefore, the total key space is *H*=*N0C0Hx1Hx2Hx3Hx4Hx5*=*N0*×2^8×10^{80}≈N_O×2^{273}.

Especially when N0 is known, the key space is approximately 2^{273}. For an effective cryptosystem, the size of the key space should not be smaller than 2^{100} to make brute-force attacks infeasible [42]. It is clear that the encryption algorithm has a sufficiently large key space to resist all types of brute-force attacks.

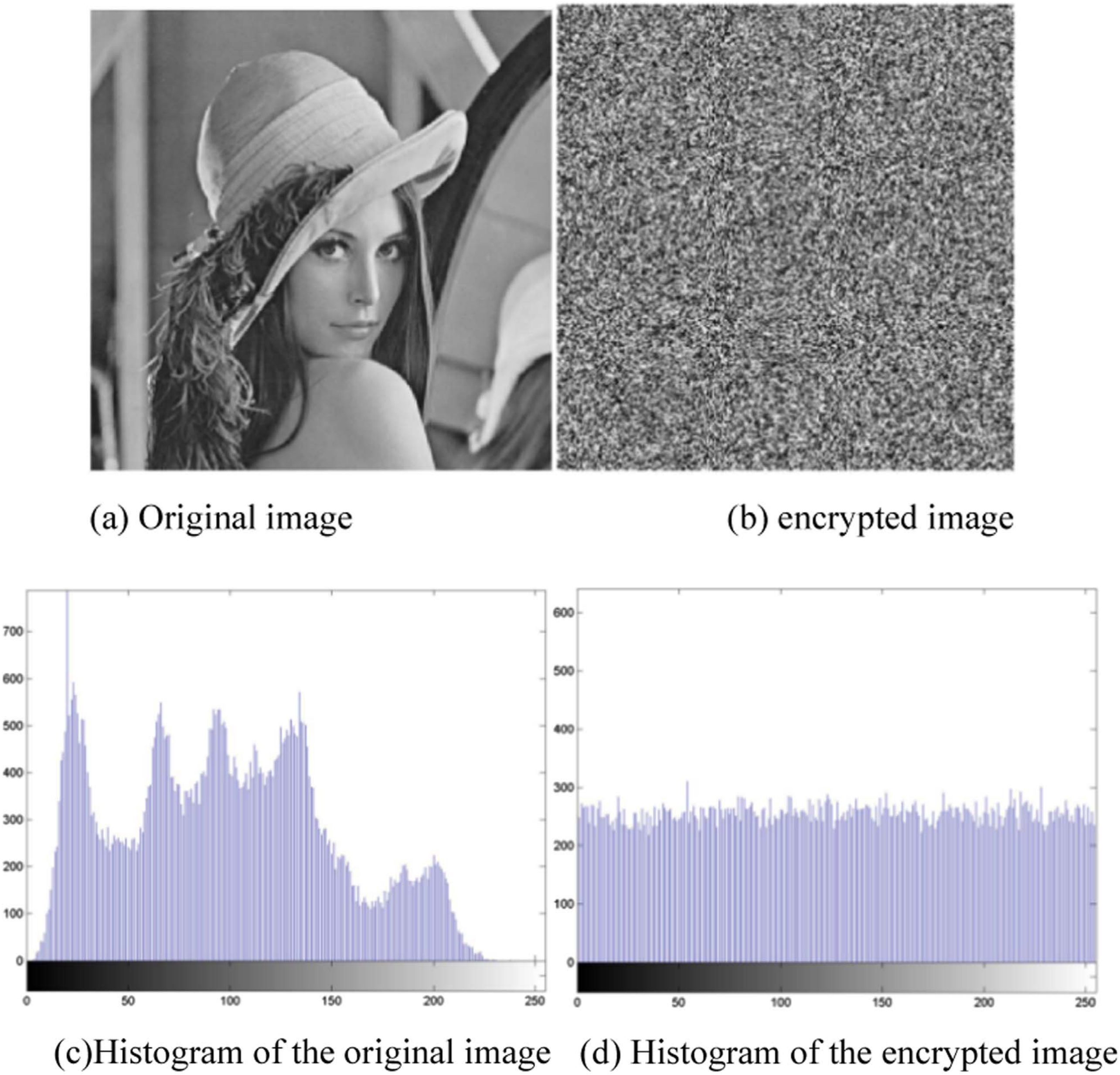
4.2. Histogram analysis

An image histogram represents the distribution of the pixel intensity values within an image. A secure encryption system can make the encrypted image have a uniform histogram to resist any statistical attacks. The histograms of the Lena image and the corresponding cipher images are shown in Fig. 5. In Fig. 5(d), all of the grayscale values of the cipher image are distributed uniformly over the interval [0255], which is significantly different from the distribution of the Lena image shown in Fig. 5(b).

For quantity analyses of each key, we calculate variances of histograms to evaluate the uniformity of the distribution of the ciphered image [43]. The lower value of variances indicates the higher uniformity of ciphered images. We also calculate the two variances of ciphered images which are encrypted by different secret keys on the same plaintext image. The closer of the two values of variances indicates the higher uniformity of ciphered images when the secret keys are varying. The variance of histograms is presented as follows:

$$\mathrm{var}(z) = \frac{1}{n^2}\sum_{i=2}^{n}\sum_{j=2}^{n}\frac{1}{2}(z_i - z_j)^2 \tag{7}$$

where Z is the vector of the histogram values which are Z ={z_1, z_2, ..., z_{256}}, z_i and z_j are the numbers of pixels whose gray values are equal to i and j respectively. In simulation experiments, we calculate two variances of histograms of two ciphered images by Eq. (7) from the same plaintext image with different secret keys. Only one parameter of secret keys is changed in such different secret keys. Table 1 lists the


(a) Original image

(b) encrypted image

(c)Histogram of the original image

(d) Histogram of the encrypted image

Fig. 5. Histogram analysis. (a) Original image (b) encrypted image (c) Histogram of the original image (d) Histogram of the encrypted image.

Table 1
Variances of histograms to all secret keys in the proposed algorithm.

Secret keys	x_1	x_2	x_3	x_4	x_5	N_O	C_O
Variances of ciper image	259.938	279.227	271	246.102	238	266.031	245.836

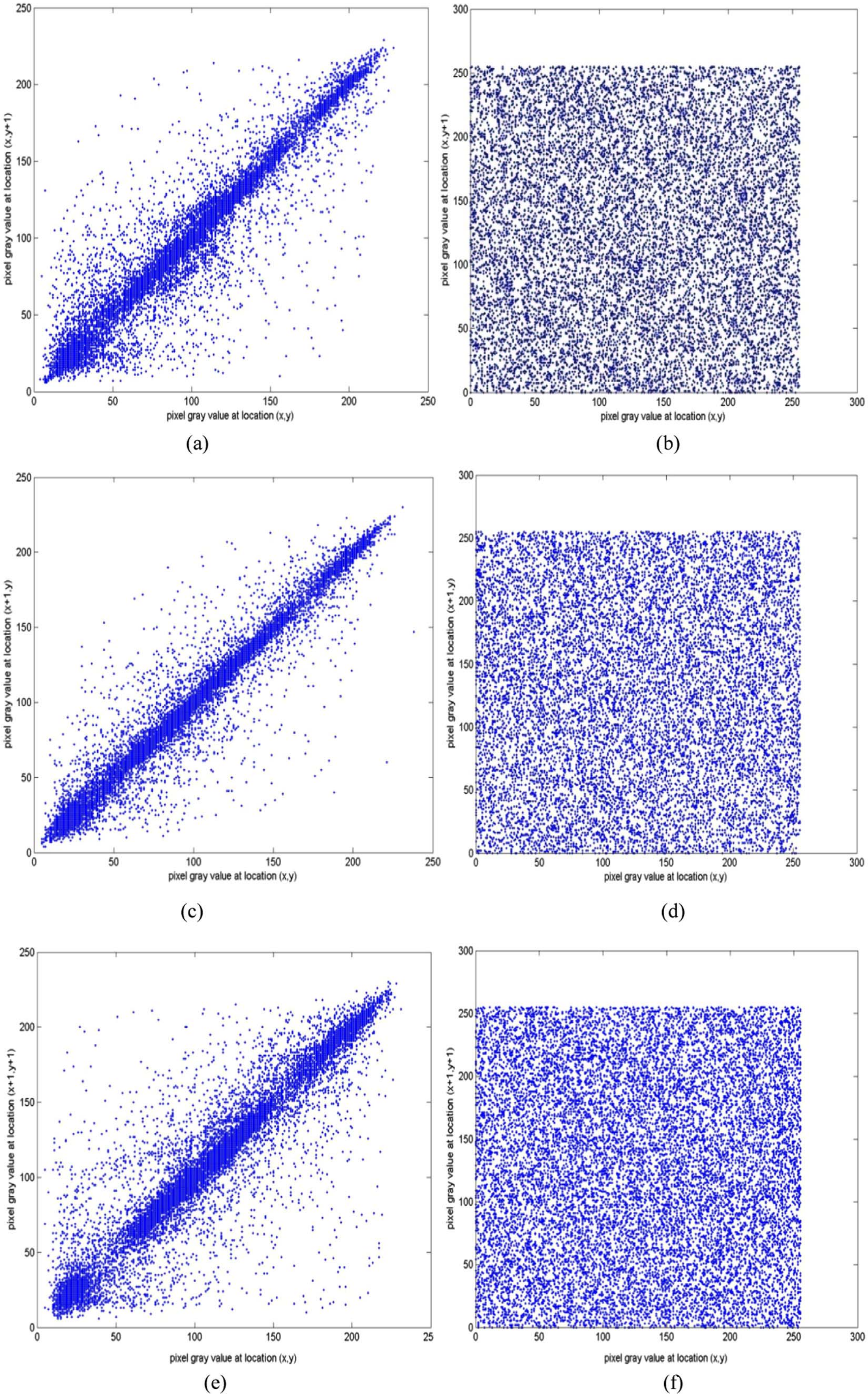
variances of histograms of ciphered Lena. In Table 1, the variances are obtained by the initial key x_1, x_2, x_3, x_4, x_5, and parameters N_O, C_O. The variance values are about 250, which indicate that the average fluctuation of number of pixels in each gray value is about 13 pixels. However, the variance value is 33860.0547 for histogram of the plaintext image Lena. Therefore, the proposed algorithm can resist any statistical attacks.

4.3. Correlation analysis

The adjacent pixels of the original image 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. To analyze and compare the correlations of the adjacent pixels in the plain and cipher image, 10,000 pairs of adjacent pixels in each direction are randomly chosen from the plain image and its encrypted image. The correlation distribution of two adjacent pixels in three directions is shown in Fig. 6. As observed, the distributions of adjacent pixels in the original image are highly concentrated, which means that the original image has a strong correlation. However, the distributions of the adjacent pixels in the original image's ciphered image are random, which means that the ciphered image has a low correlation.

Moreover, for calculating the correlation coefficient r_{xy} of each pair, we have used the following formulas:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$



(a) (b)

(c) (d)

(e) (f)

Fig. 6. Correlation of adjacent pixels in the plain-image and in the cipher-image: (a), (c) and (e) for the plain-image; (b), (d) and (f) for the cipher-image.

Table 2
Correlation coefficients of adjacent pixel.

Direction	Horizontal	Vertical	Diagonal
Plain image	0.9422	0.9682	0.9320
Cipher image	−0.0015	−0.0032	0.0008
Ref. [11]	0.0021	0.0046	0.0033
Ref. [12]	−0.0180	0.0035	0.0020
Ref. [23]	0.0242	0.0194	0.0024
Ref. [26]	−0.0230	0.0019	−0.0034
Ref. [28]	0.0056	0.0065	0.0073
Ref. [34]	0.0142	0.0074	0.0183

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{9}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{10}$$

$$\rho_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)\cdot D(y)}} \tag{11}$$

where x and y are the grayscale values of two adjacent pixels in the image, and N is the total number of pixels selected from the image. The results are shown in Table 2, which show that the correlation coefficients of the original image are close to 1, while those of the encrypted image are approximately 0 along all three directions. Table 2 shows that the adjacent pixels of the encrypted image have extremely low correlation and the proposed image encryption scheme has good confusion and diffusion properties.

4.4. Key sensitivity analysis

To guarantee the security of the cryptosystem, a good cryptosystem should be sensitive to the key. The key sensitivity must be analyzed. The incorrect plain image will be produced when we use different keys to decrypt the cipher-image. We use the original key to encrypt the Lena image and the modified key to decrypt the cipher-image. Their difference lies in the last digit after the decimal point of the first parameter. The original key is (0.765677163767260, 0.163767260150053, 0.260150052607060, 0.052607059478760 ,0.059478759765625), and the modified key is (0.765677163767261, 0.163767260150053, 0.260150052607060, 0.052607059478760, 0.059478759765625). The original Lena image is shown in Fig. 7(a), and the corresponding cipher-image of the original key is shown in Fig. 7(b). The decrypted image for the incorrect decryption key is shown in Fig. 7(c), and the decrypted image for the correct decryption key is shown in Fig. 7(d). It is clear that the slightly different decryption key cannot decrypt the cipher-image. Therefore, the key sensitivity test shows that the proposed cryptosystem has perfect sensitivity to the key.

4.5. Differential analysis

To resist a differential attack, a good cryptosystem should ensure that any tiny modification in the plain-image should cause a significant difference in the cipher-image. The NPCR (number of pixels change rate) and UACI (unified average changing intensity) [44] are usually

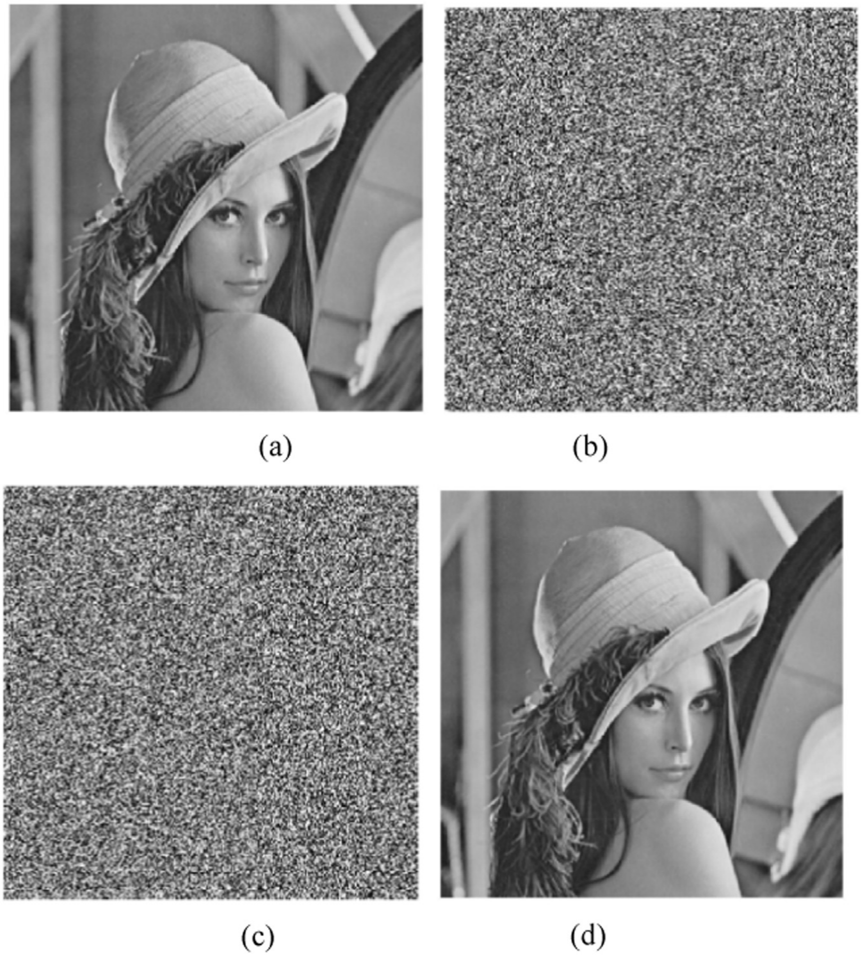
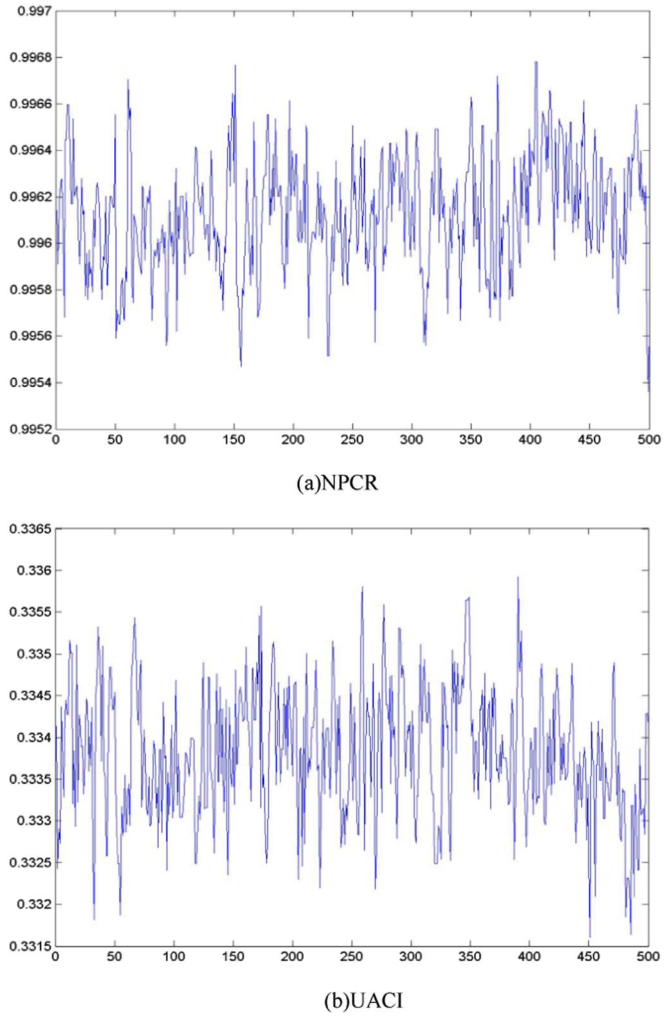


Fig. 7. Key sensitivity analysis. (a) The Lena image; (b) the encrypted image using the original key; (c) the decrypted image with an incorrect security key; and (d) the decrypted image with the correct security key.



(a)NPCR

(b)UACI

Fig. 8. The NPCR and UACI of 500 images that only change one pixel. (a) NPCR (b) UACI.

used for differential attack analysis. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively. These concepts are defined by Eqs. (12) and (13) below:

$$R_{NPCR} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i, j) \times 100\% \tag{12}$$

$$I_{UACI} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \tag{13}$$

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

$$D(i, j) = \begin{cases} 0 & C_1(i, j) = C_2(i, j) \\ 1 & C_1(i, j) \neq C_2(i, j) \end{cases} \tag{14}$$

To compare the performance, we choose 500 cipher-images whose plaintext has only a different pixel. As observed, the NPCR and UACI are obtained as shown in Fig. 8 by the proposed algorithm. This finding shows that the proposed scheme can resist differential attack effectively.

4.6. Information entropy analysis

The information entropy is the most important measure of randomness. The source of information is defined as m, and we can obtain the following formula for calculating information entropy:

Table 3
The results of information entropy.

Image	Our proposed scheme	Ref. [22]	Ref. [26]	Ref. [27]
Lena	7.9972	7.9972	7.9968	7.9893

$$H(m) = \sum_{i=0}^{M-1} p(m_i)\log\frac{1}{p(m_i)} \tag{15}$$

where M is the total number of symbols $m_i \in m$; $p(m_i)$ denotes the probability of symbols. It is assumed that an information source sends out 256 symbols, and we may get theoretical value $H(m)$=8 by Eq. (15). The more it gets close to 8, the less possible for attackers to decode cipher images. Table 3 shows the comparison of information entropy. From Table 3, it is known that entropies are close to 8, so the proposed algorithm has a good property of information entropy.

5. Conclusions

In this paper, we propose a hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. It can overcome the common weaknesses of the algorithm based on low-dimensional chaotic map for it is based on a hyper-chaotic system. Then, pixel-level permutation and bit-level permutation are employed to strengthen security of the cryptosystem. We carry out many experiments, including histogram analysis, key sensitivity analysis, key space analysis, correlation analysis and differential analysis to show that the proposed algorithm is secure and reliable for image encryption.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61571185, No. 61672216, No. 61674054), The Natural Science Foundation of Hunan Province, China (No. 2016JJ2030) and the Open Fund Project of Key Laboratory in Hunan Universities (No.15K027).

References

[1] Li SJ, Chen GR, Cheung A, Bhargava B, Lo K-T. On the design of perceptual MPEG Video encryption algorithms. IEEE Trans Circuits Syst Video Technol 2007;17:214–23.
[2] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos Appl Sci Eng 1998;8:1259–84.
[3] Huang XL. Image encryption algorithm using chaotic chebyshev generator. Nonlinear Dyn 2012;67:2411–7.
[4] Wang XY, Guo K. A new image alternate encryption algorithm based on chaotic map. Nonlinear Dyn 2014;76:1943–50.
[5] Zhang XP, Zhao ZM. Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dyn 2014;75:319–30.
[6] Zhang GJ, Liu Q. A novel image encryption method based on total shuffling scheme. Opt Commun 2011;284:2775–80.
[7] Wang XY, Teng L, Qin X. A novel color image encryption algorithm based on chaos. Signal Process 2012;92:1101–8.
[8] Tong XJ. Design of an image encryption scheme based on a multiple chaotic map. Commun Nonlinear Sci Numer Simul 2013;18:1725–33.
[9] Akhshani A, Akhavan A, Lim S-C, Hassana Z. An image encryption scheme based on quantum logistic map. Commun Nonlinear Sci Numer Simul 2012;17, [4653–4561].
[10] Hua ZY, Zhou YC, Pun CM, Chen CLP. 2D sine logistic modulation map for image encryption. Inf Sci 2015:29780–94.
[11] Chen JX, Zhu ZL, Fu C. An efficient image encryption scheme using lookup table-based confusion and diffusion. Nonlinear Dyn 2015;81:1151–66.
[12] Liu LF, Miao SX. A new image encryption algorithm based on logistic chaotic map with varying parameter. Springerplus 2016:5.
[13] Xiao D, Liao XF, Wei PC. Analysis and improvement of a chaos-based image encryption algorithm. Chaos Solitons and Fractals 2009;40:2191–9.
[14] Zhu CX, Liao CL, Deng XH. Breaking and improving an image encryption scheme based on total shuffling scheme. Nonlinear Dyn 2013;71:25–34.
[15] Wang XY, He GX. Cryptanalysis on a novel image encryption method based on total

shuffling scheme. Opt Commun 2011;284:5804–7.

[16] Liu HJ, Wang XY. Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 2010;59:3320–7.

[17] Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015;66:10–8.

[18] Wang XY, Zhang YQ, Liu LT. An enhanced sub-image encryption method. Opt Lasers Eng 2016;86:248–54.

[19] Belazi A, El-Latif A, Diaconu A, Rhouma R, Belghith S. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 2017;88:37–50.

[20] Liu WH, Sun KH, Zhu CX. A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 2016;84:26–36.

[21] Wang LY, Song HJ, Liu P. A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt Lasers Eng 2016;77:118–25.

[22] Zhu ZL, Zhang W, Kwok-wo W. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 2011;181:1171–86.

[23] Teng L, Wang XY. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt Commun 2012;285:4048–54.

[24] Fu C, Lin BB, Miao YS, Liu X, Chen JX. A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 2011;284:5415–23.

[25] Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284:3895–903.

[26] Wang XY, Zhang HL. A color image encryption with heterogeneous bit permutation and correlated chaos. Opt Commun 2015;342:51–60.

[27] Xu L, Li Z, Li J. A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 2016;78:17–25.

[28] Wang XY, Zhang HL. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems. Nonlinear Dyn 2016;83:333–46.

[29] Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 2010;62:615–21.

[30] Zhang YQ, Wang XY. A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 2015;26:10–20.

[31] Xu L, Li Z, Li J, Hua W. A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 2016;78:17–25.

[32] Liu HJ, Wang XY, Kadir A. Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 2012;12:1457–66.

[33] Chai XL, Chen YR, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng 2017;88:197–213.

[34] Gao TG, Chen ZQ. A new image encryption algorithm based on hyper-chaos. Phys Lett A 2008;372:394–400.

[35] Rhouma R, Belghith S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Phys Lett A 2008;372:5973–8.

[36] Jeng FG, Huang WL, Chen TH. Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes. Signal Process: Image Commun 2015;34:45–51.

[37] Zhang Q, Guo L, Wei X. A novel image fusion encryption algorithm based on DNA sequence operation and hyperchaotic system. Optik 2013;124:3596–600.

[38] Tong XJ, Liu Y, Zhang M, Xu H, Wang Z. An image encryption scheme based on hyperchaotic rabinovich and exponential chaos maps. Entropy 2015;17:181–96.

[39] Amin Z. Complex dynamics in a 5-D hyper-chaotic attractor with four-wing, one equilibrium and multiple chaotic attractors. Nonlinear Dyn 2015;81:585–605.

[40] Wang XY, Wang MJ. A hyperchaos generated from Lorenz system. Physica A 2008;387:3751–8.

[41] Zhang YQ, Wang XY. Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice. Physica A 2014;402:104–18.

[42] Alvarez G, Li SJ. Some basic cryptographic requirements for chaos-based crypto-systems. Int J Bifurc Chaos 2006;16:2129–51.

[43] Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 2014;273:329–51.

[44] Mao YB, Chen GR, Lian SG. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurc Chaos 2004;14:3613–24.