International Journal of Bifurcation and Chaos, Vol. 28, No. 4 (2018) 1850047 (13 pages)

DOI: 10.1142/S0218127418500475

A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion

Qi Yin* and Chunhua Wang†
College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, P. R. China
**yinqi_hnu@163.com*
†*wch1227164@hnu.edu.cn*

Received July 21, 2017; Revised January 26, 2018

Based on the permutation-diffusion architecture, this paper introduces a more sensitive chaotic image encryption scheme using breadth-first search and dynamic diffusion to enhance the security and sensitivity. In the permutation stage, the plain image is traversed by breadth-first search, and then the whole permutation is performed to obtain a shuffled sequence. Similarly, the diffusion key stream is rearranged by breadth-first search. Moreover, a dynamic diffusion method is proposed to encrypt the shuffled sequence in the diffusion stage, which can ensure that encrypting each pixel is related to all other pixels and can enhance the sensitivity of the cryptosystem. In each phase, the hyper-chaotic system in this scheme generates pseudorandom sequences. The simulation results and performance analysis show that the proposed scheme has excellent performances and high security in resisting brute-force attack, statistical attack and differential attack.

Keywords: Image encryption; breadth-first search; dynamic diffusion; chaos.

1. Introduction

With the rapid development of network technology, the security of image transmission is becoming more and more important. However, due to some inherent features of images, such as huge data capacities, high correlation between image pixels and low entropy, the traditional algorithms, such as the data encryption standard (DES), international data encryption algorithm (IDEA) and advanced encryption standard (AES), are not suitable [Li *et al.*, 2007]. In recent years, many image encryption schemes based on chaotic system have been proposed to solve this problem.

Chaotic systems have some significant features, such as deterministic, pseudo-randomness, ergodicity, and they are sensitive to initial points and parameters. These features can enhance the security of the image encryption schemes. An image encryption method that was based on one-time keys and robust chaotic maps was proposed [Liu & Wang, 2010]. By means of rows and columns switch, Wang *et al.* [2015a] provided a fast image encryption algorithm which can achieve high speed. However, these schemes have small key space and weak security for their key stream was generated by logistic map. A variety of image encryption algorithms based on hyper-chaotic system have been proposed owing to which the hyper-chaotic systems have complex dynamic characteristics, a large enough key space and good sensitivity [Li *et al.*, 2017a; Liu *et al.*, 2016a; Norouzi & Mirzakuchaki, 2014; Mirzaei *et al.*, 2012; Zhu, 2012; Norouzi *et al.*, 2014]. In [Liu *et al.*, 2016a],

†Author for correspondence

the row and column shift permutation scheme was proposed to efficiently change the image pixel positions, and the row and column substitutions were applied to scramble the pixel values simultaneously. An image encryption method based on improved hyper-chaotic sequences with two rounds of diffusion operation was proposed [Zhu, 2012], while it can be broken with only two known plain images proved by [Li *et al.*, 2013]. Norouzi *et al.* [2014] proposed a chaotic image encryption scheme with only one round diffusion process which has large enough key space, while it could not resist the differential attacks proved by [Zhang *et al.*, 2014a]. Arroyo *et al.* [2013] proposed that it is not possible to avoid the security problems of that encryption architecture just by including a chaotic system as the core of the derived encryption system. Xie *et al.* [2017] scrutinized some properties of Fridrich's scheme with matrix theory and reported some minor defects of Solak's chosen-ciphertext attack method. Li *et al.* [2017a] proposed that the correlation in multimedia data can be used to support specific attacks and enhance breaking performance. Zhu and Sun [2012] have shown that the shuffling process can be separated from the confusion process, and the formulas of encryption were simple, which made the ciphertext unable to resist attacks from chosen-plaintext and -ciphertext. Recently, many DNA-based schemes have been proposed because of their effectiveness [Hu *et al.*, 2016; Zhang & Gao, 2015; Kumar *et al.*, 2016; Liu *et al.*, 2016b; Enayatifar *et al.*, 2014; Wang *et al.*, 2015b; Xue *et al.*, 2010]. An image encryption scheme combining chaos with cycle operation for DNA sequences was proposed [Hu *et al.*, 2016]. Wang *et al.* [2015b] combined the merits of the DNA method and the CML systems to propose an image encryption scheme. Xue *et al.* [2010] proposed the novel image encryption algorithm based on the DNA sequence and multi-chaotic maps, despite the weakness as determined by the five keys kept unchanged for different image encryption processes [Zhang *et al.*, 2014b]. SHA-3 is the newest cryptographic hash function and Ye *et al.* [2016] proposed a novel image encryption algorithm, in which a new wave-line-based permutation was designed with SHA-3 function. Furthermore, a number of bit-level image encryption algorithms have been proposed [Xu *et al.*, 2016; Zhou *et al.*, 2014; Fu *et al.*, 2011; Teng & Wang, 2012; Zhang *et al.*, 2012]. A bit-level image encryption scheme based on piecewise linear chaotic maps (PWLCM) was proposed, which can permute the bits in one bitplane into any other bitplane [Xu *et al.*, 2016]. Teng and Wang [2012] proposed a bit-level image encryption based on spatiotemporal chaotic system which is self-adaptive.

The main purpose of the permutation process is to break the correlation between adjacent pixels of an image. In the above permutation schemes such as the row and column shift permutation scheme and the wave-line permutation scheme, all rows of the image are circularly shifted in the horizontal direction. And then, all columns of the image are circularly shifted in the vertical direction to get the scrambled image. Because two changes of image pixels' position are carried out in two orthogonal directions, it leads to the correlation that cannot completely break between adjacent pixels of an image in the horizontal and vertical directions. On the other hand, in the above schemes based on the permutation-diffusion architecture, the scrambled key stream and the diffusion key stream are independent of each other, which causes the scrambled key sequence and the diffusion key sequence to be broken separately. Besides, each encrypted pixel is not related to all other pixels, thus resulting in low security and sensitivity.

In order to overcome the above drawbacks, a new chaotic image encryption scheme using breadth-first search and dynamic diffusion is proposed. The breadth-first search is firstly used to transform an image into a sequence, and then the sequence is divided into 4×4 matrices to be traversed using breadth-first search. Thus the correlation between adjacent pixels of an image in all directions can be broken. Meanwhile, the diffusion key stream is rearranged using breadth-first search in the control of the scrambled key stream, which can enhance security. Furthermore, we also propose a dynamic diffusion method in diffusion stage to enhance sensitivity. The key depends not only on key stream but also on all other pixels when each pixel is encrypted, and the hyper-chaotic system in this scheme generates pseudorandom sequences in each phase. The simulation results and performance analysis show that the proposed scheme has high security and excellent performance.

The rest of this paper is organized as follows. In Sec. 2, the basic theories of breadth-first search and the hyper-chaotic system are described. In Sec. 3, the processes of image encryption and decryption are described in detail. The simulation results and

performance analysis are shown in Sec. 4. Finally, this paper is concluded in the last section.

2. Basic Theories

2.1. *Breadth-first search*

The breadth-first search is a way of traversing the graph. The traversal process can be described as that which starts from a vertex to the vertex adjacency, and then accesses the adjacency of these adjacencies until all points in the graph are traversed. There are two reasons for breadth-first search being suitable to encrypt image. The first is that any point in the matrix has horizontal adjacency and vertical adjacency. The second is that any matrix has four vertices. So for any matrix as input of the traversal process, four different sequences as output can be generated. This can enhance the security of the cryptosystem.

For example, the 4×4 matrix A is described as

$$A = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ s_5 & s_6 & s_7 & s_8 \\ s_9 & s_{10} & s_{11} & s_{12} \\ s_{13} & s_{14} & s_{15} & s_{16} \end{bmatrix}. \tag{1}$$

Starting from s_1, s_4, s_{13} and s_{16} respectively, Eq. (2) is obtained by traversing every element in matrix A using breadth-first search.

$$\begin{aligned} B_1(A) &= \{s_1, s_2, s_5, s_3, s_6, s_9, s_4, s_7, s_{10}, \\ &\quad s_{13}, s_8, s_{11}, s_{14}, s_{12}, s_{15}, s_{16}\}, \\ B_2(A) &= \{s_4, s_3, s_8, s_2, s_7, s_{12}, s_1, s_6, s_{11}, \\ &\quad s_{16}, s_5, s_{10}, s_{15}, s_9, s_{14}, s_{13}\}, \\ B_3(A) &= \{s_{13}, s_{14}, s_9, s_{15}, s_{10}, s_5, s_{16}, s_{11}, \\ &\quad s_6, s_1, s_{12}, s_7, s_2, s_8, s_3, s_4\}, \\ B_4(A) &= \{s_{16}, s_{15}, s_{12}, s_{14}, s_{11}, s_8, s_{13}, s_{10}, \\ &\quad s_7, s_4, s_9, s_6, s_3, s_5, s_2, s_1\}. \end{aligned} \tag{2}$$

2.2. *The hyper-chaotic system*

In our proposed encryption scheme, a pseudorandom sequence is generated by solving a hyper-chaotic system

$$\begin{cases} \dot{x} = a(y - x) + yz, \\ \dot{y} = bx - y - xz + w, \\ \dot{z} = xy - cz, \\ \dot{w} = dw - xz, \end{cases} \tag{3}$$

where a, b, c and d are system parameters [Niu *et al.*, 2010]. When $a = 3$, $b = 8/3$, $c = 55$ and $d = 1.3$, we obtain Lyapunov exponents: $\lambda_1 = 1.4164$, $\lambda_2 = 0.5318$, $\lambda_3 = 0$, $\lambda_4 = -39.1015$. It is obvious that the system exhibits a hyper-chaotic behavior. Here, we take the fourth-order Runge–Kutta method to solve (3) and obtain the four hyper-chaotic sequences.

3. The Proposed Image Encryption System

The block diagram of the proposed image encryption algorithm is given in Fig. 1.

Supposing that the plain image is denoted as P, whose size is $M \times N$, and we can conclude encryption steps as below.

3.1. *Encryption process*

Step 1. Use the initial values x_0, y_0, z_0, w_0 to produce four pseudorandom sequences x, y, z and w by iterating (3) for $N_0 + L/16$ times, where $L = M \times N$. To get rid of transient effect, we discard the first N_0 numbers of each sequence. Then we can obtain the two sequences $k_1 = \{k_1(i)\}_{i=1}^{L/16}$ and $k_2 = \{k_2(i)\}_{i=1}^{L/16}$ by

$$\begin{aligned} k_1(i) &= \mathrm{mod}(\mathrm{floor}((x(i) + y(i)) \\ &\quad - \mathrm{fix}(x(i) + y(i))) \times 10^{16}, 4), \end{aligned} \tag{4}$$

$$\begin{aligned} k_2(i) &= \mathrm{mod}(\mathrm{floor}((z(i) + w(i)) \\ &\quad - \mathrm{fix}(z(i) + w(i))) \times 10^{16}, 4), \end{aligned} \tag{5}$$

where $i = 1, 2, 3, \ldots, L/16$, $\mathrm{mod}(a, b)$ returns the remainder of a divided by b, $\mathrm{floor}(a)$ rounds the element of a to the nearest integer toward minus infinity, $\mathrm{fix}(a)$ takes the integer part of a.

Step 2. Use the first breadth-first search to traverse the original image P, resulting in a sequence S of size L.

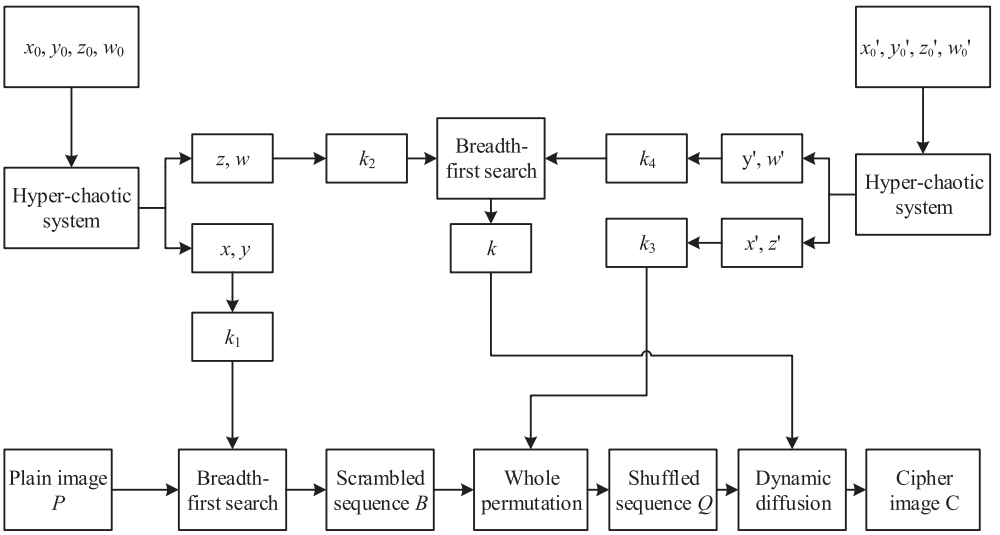


Fig. 1. Block diagram of the proposed image cryptosystem.

Step 3. Divide the sequence S into $L/16$ matrices of size 4×4, which are denoted by A_i ($i = 1, 2, 3, \ldots, L/16$).

Step 4. According to the value of $k_1(i)$, different traversal methods are selected in the matrix A_i to produce the ith sequence, that is:

If $k_1(i) = 0$, then the $B_1(A_i)$ is obtained;
If $k_1(i) = 1$, then the $B_2(A_i)$ is obtained;
If $k_1(i) = 2$, then the $B_3(A_i)$ is obtained;
If $k_1(i) = 3$, then the $B_4(A_i)$ is obtained.

Step 5. Repeat Step 4 until $L/16$ matrices have been traversed and $L/16$ sequences are obtained. Then we can obtain the scrambled sequence $B = \{b(i)\}_{i=1}^{L}$ by combining $L/16$ sequences.

Step 6. Using the initial values x_0', y_0', z_0', w_0' repeat (3) for $N_0 + L$ times to produce four pseudorandom sequences x', y', z' and w'. To get rid of transient effect, we discard the first N_0 numbers of each sequence. Then we can obtain the two sequences $k_3 = \{k_3(i)\}_{i=1}^{L}$ and $k_4 = \{k_4(i)\}_{i=1}^{L}$ by

$$k_3(i) = x'(i) + z'(i), \tag{6}$$

$$k_4(i) = \mathrm{mod}(\mathrm{floor}((y'(i) + w'(i)) \times 10^{15}), 256), \tag{7}$$

where $i = 1, 2, 3, \ldots, L$.

Step 7. Sort the sequence k_3 in ascending order, then the index sequence $T = \{t(i)\}_{i=1}^{L}$ can be obtained.

Step 8. Permutate the scrambled sequence B to get the shuffled sequence $Q = \{q(i)\}_{i=1}^{L}$ by

$$q(i) = b(t_i), \tag{8}$$

where $i = 1, 2, 3, \ldots, L$.

Step 9. Similarly, divide the sequence k_4 into $L/16$ matrices of size 4×4, then use the sequence k_2 to control traversing method of these matrices and obtain $L/16$ sequence, thus getting the key stream $k = \{k(i)\}_{i=1}^{L}$ by combining $L/16$ sequences.

Step 10. Set $i = 1$, define

$$\mathrm{sum}\,1 = \sum_{i=1}^{L} q(i) - q(1), \tag{9}$$

$$\mathrm{sum}\,2 = 0. \tag{10}$$

Encrypt the first pixel of the cipher image in the following way

$$C(1) = q(1) \oplus k(1) \oplus \mathrm{mod}(\mathrm{sum}\,1 + k(1), 256), \tag{11}$$

where $\oplus$ is the bit-level XOR operator.

Step 11. Update the values of sum 1 and sum 2 by

$$\mathrm{sum}\,1 = \mathrm{sum}\,1 - q(i), \tag{12}$$

$$\mathrm{sum}\,2 = \mathrm{sum}\,2 + C(i-1). \tag{13}$$

Step 12. Set $i = i + 1$, and encrypt the ith pixel of the cipher image by

$$C(i) = q(i) \oplus \mathrm{mod}(C(i-1) + k(j), 256) \oplus \mathrm{mod}(\mathrm{sum}\,1 + k(i), 256), \tag{14}$$

where $j = \mathrm{mod}(\mathrm{sum}\, 2 \times 10^{10}, L) + 1$. Obviously, encrypting each pixel is related to all other pixels. This means that for different plain image, the diffusion method will be different.

Step 13. Set $i = i + 1$, and return to Step 11 until i reaches L. Then we obtain the cipher image by transforming the sequence C into an $M \times N$ image.

3.2. *Decryption process*

The decryption algorithm is the reverse process of encryption algorithm.

4. Performance and Security Analysis

In this section, to prove the security of our scheme, the 256×256 traditional 8-bit grayscale images are used as the original images. The secret keys are set as ($x_0 = 1$, $y_0 = 0.949$, $z_0 = 1$, $w_0 = 1$, $x'_0 = 1.01$, $y'_0 = 0.95$, $z'_0 = 1.01$, $w'_0 = 1.01$) and then our proposed scheme is employed to encrypt original images with only one round. The relevant experimental results are shown in Fig. 2. Figures 2(a), 2(d) and 2(g) denote original images during the experiments. Figures 2(b), 2(e) and 2(h) are encrypted images which are completely invisible. Figures 2(c), 2(f) and 2(i) are decrypted images which are identical to original images.

4.1. *Key space analysis*

An idea image encryption algorithm should have a key space larger than 2^{100} to make brute-force attacks infeasible [Gonzalo & Li, 2006]. In the proposed algorithm, the initial secret keys are set as $(x_0, y_0, z_0, w_0, x'_0, y'_0, z'_0, w'_0)$, where $x_0, y_0, z_0, w_0, x'_0, y'_0, z'_0, w'_0$ are double-precision numbers, the key space of the image encryption scheme is $(10^{16})^8 = 10^{128} \approx 2^{384}$. Thus, the key space is large enough to resist all types of brute-force attacks.

4.2. *Statistical analysis*

4.2.1. *Histogram analysis*

As we all know, the image histogram represents the distribution of the pixel intensity values in an image. A good secure encryption system should make the histogram flat as much as possible. The histogram of Lena image and corresponding cipher images are shown in Fig. 3. The histogram of black image and corresponding cipher images are shown in Fig. 4. It shows that the numbers of each grayscale values of the cipher image are almost equal, which indicates that the encryption system can resist statistical attacks.

4.2.2. *Correlation analysis*

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

$$\gamma_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{15}$$

where $\mathrm{cov}(x, y) = E(x - E(x))(y - E(y))$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$ and $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$. Here, x and y are the gray values of two adjacent pixels, N is the total number of pixels selected from image.

To analyze and compare the correlation of adjacent pixels between original and encrypted images, we randomly select 4000 pairs of adjacent pixels at the horizontal, vertical, and diagonal directions of the Lena image and encrypted image. The correlation distribution is shown in Fig. 5. Obviously, the adjacent pixels of the original image have a strong correlation while the adjacent pixels of the encrypted image have a low correlation. Then we calculate the adjacent pixels' correlation coefficient of Lena, Peppers and Camera in horizontal, vertical, and diagonal directions. The results are shown in Table 1, from which we can clearly see that the correlation coefficients of the original images are close to 1 while those of the encrypted images are around 0 in all directions. This further proves that the scheme can effectively resist statistical attacks.

4.2.3. *Information entropy*

The information entropy is estimated as

$$H(m) = -\sum_{i=0}^{2^N - 1} p(m_i) \log_2 p(m_i), \tag{16}$$

where N is the number of bits corresponding to the symbol m_i, and $p(m_i)$ is the probability of symbol m. The ideal entropy value for a ciphered image should be 8, which means that the more the

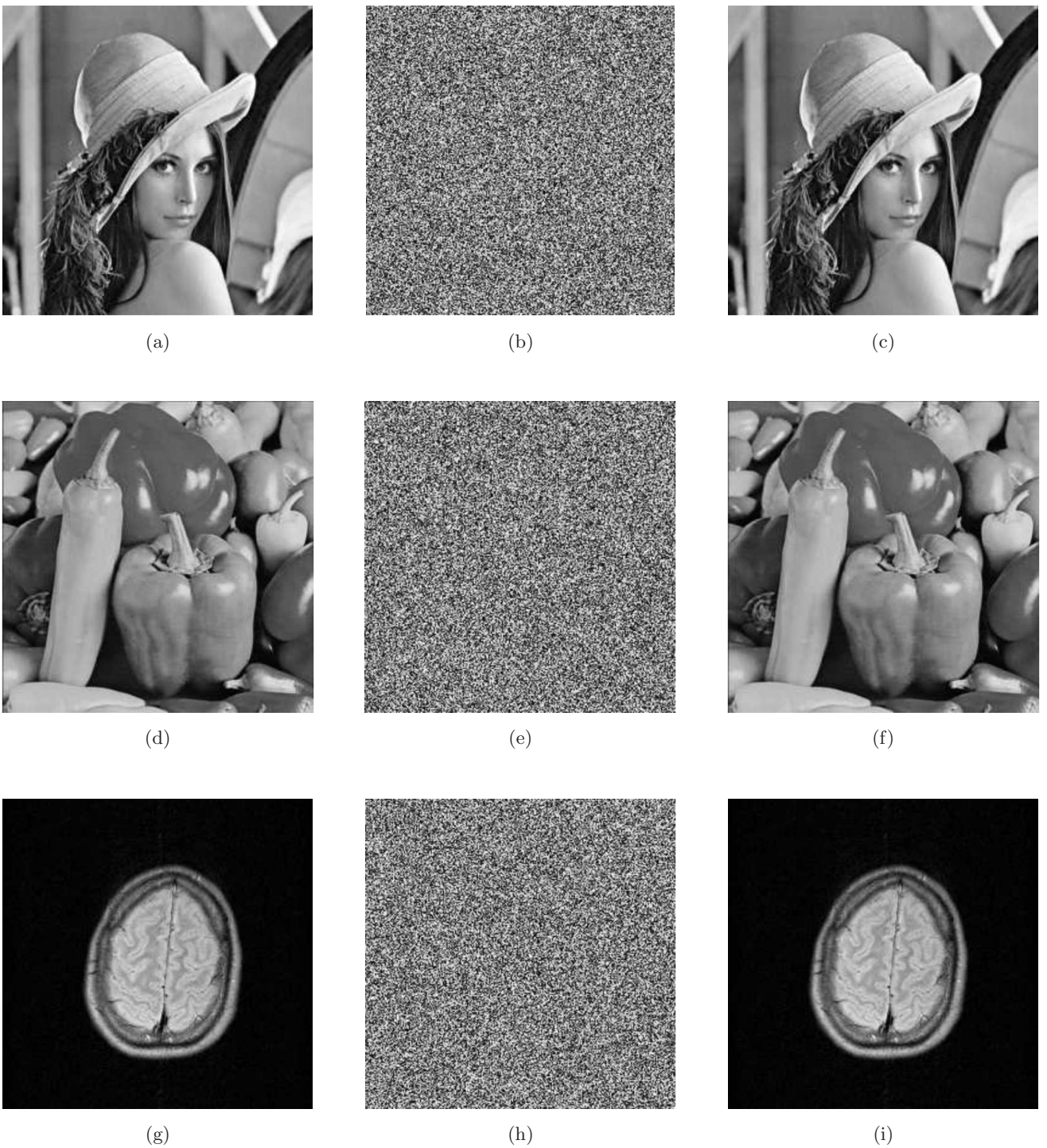


Fig. 2. Experimental results: (a) original image of Lena, (b) encrypted image of Lena, (c) decrypted image of Lena, (d) original image of Peppers, (e) encrypted image of Peppers, (f) decrypted image of Peppers, (g) original image of Brain, (h) encrypted image of Brain and (i) decrypted image of Brain.

distribution of a gray value is uniform, the greater the information entropy. We calculate the information entropy of some gray images and the corresponding cipher images, and then compare the calculated results with the ones in [Wang *et al.*, 2015a; Zhu, 2012; Teng & Wang, 2012]. The results are shown in Table 2. From the table, we can clearly see that the entropies of the encrypted images using our scheme are all close to 8. This proves the scheme is secure to resist the entropy attack.

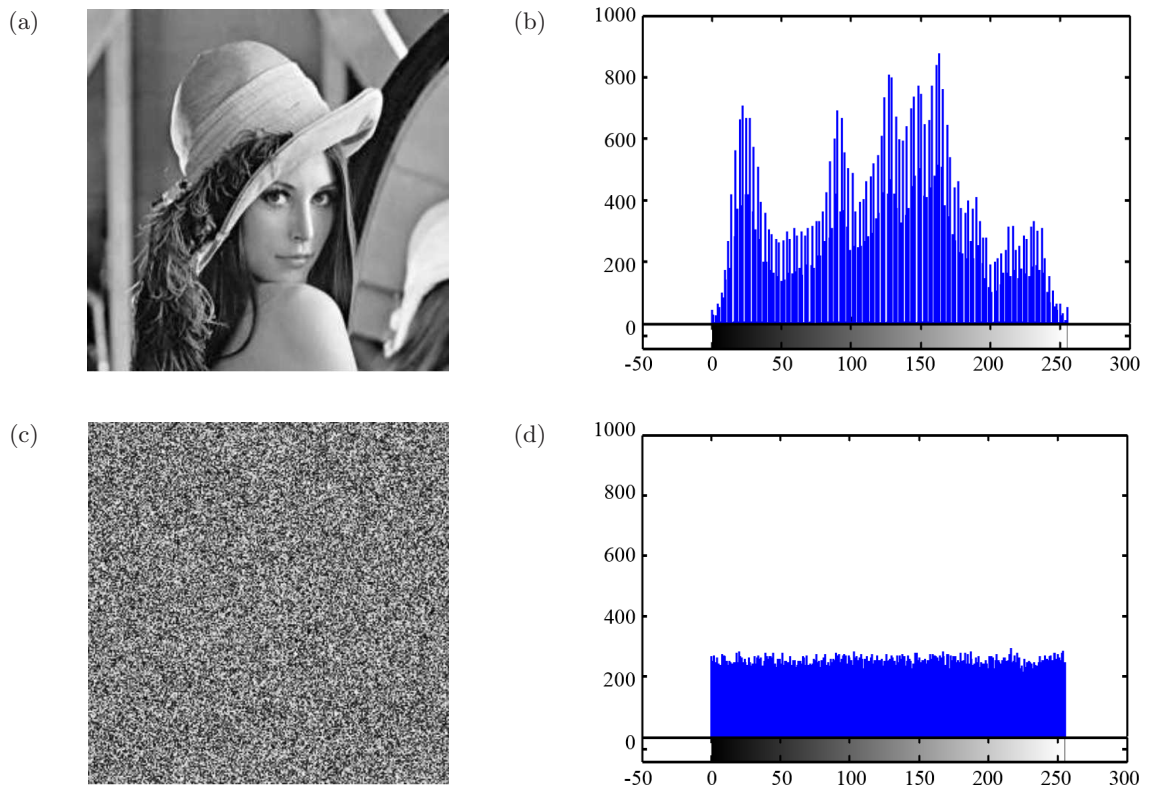


Fig. 3. Histogram analysis: (a) original image of Lena, (b) histogram of original image, (c) encrypted image of Lena and (d) histogram of encrypted image.

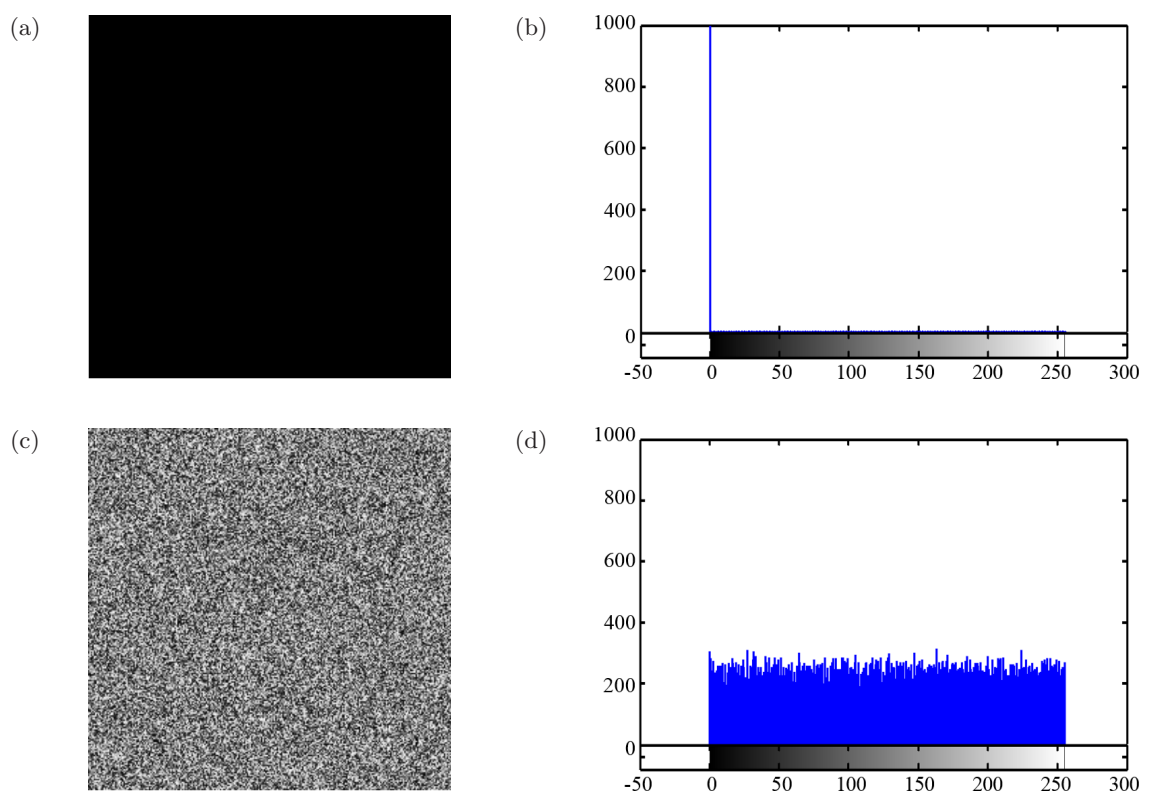


Fig. 4. Histogram analysis: (a) original image of black image, (b) histogram of original image, (c) encrypted image of black image and (d) histogram of encrypted image.

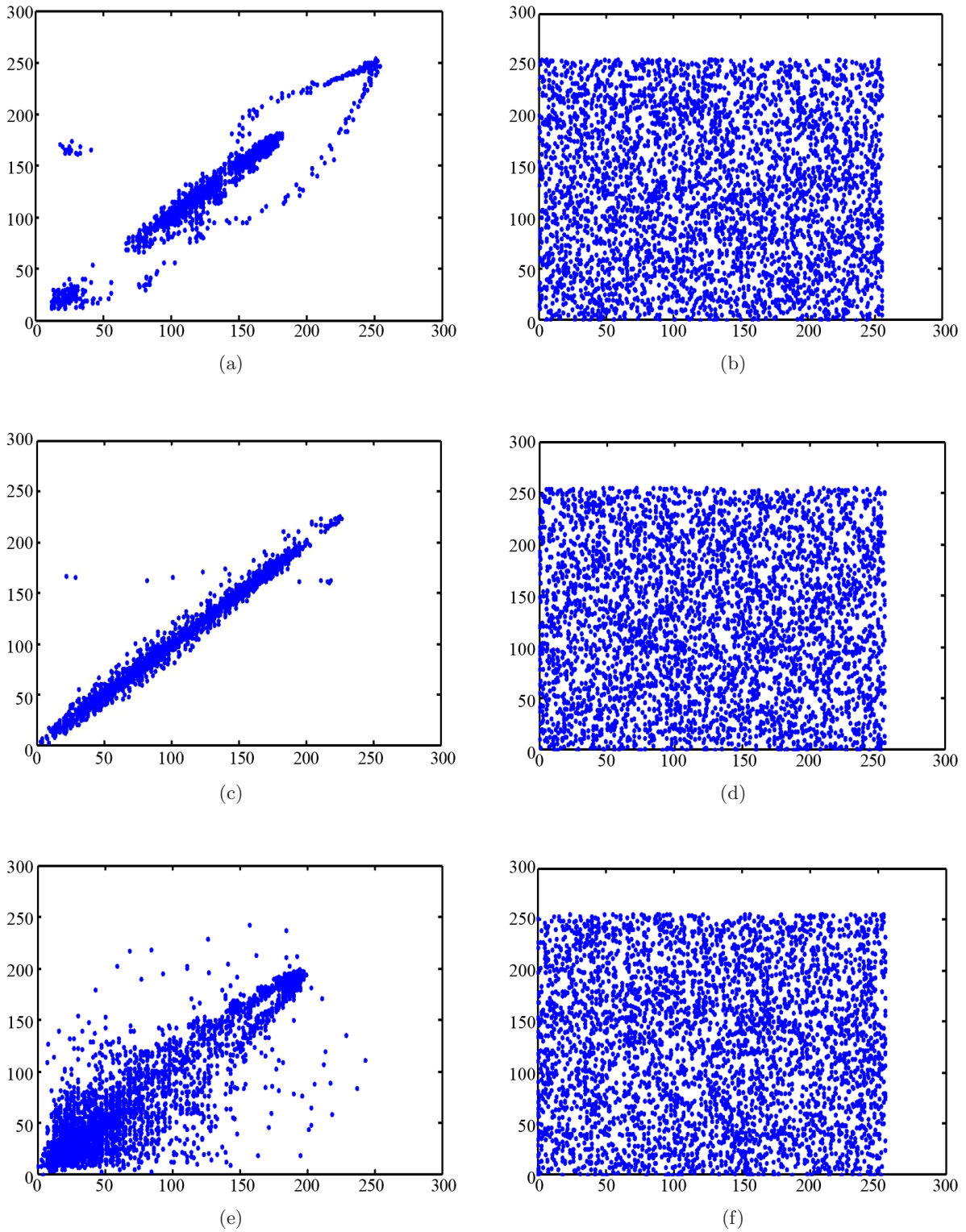


Fig. 5. The correlation plots of Lena image and corresponding ciphered image of Lena: (a) horizontal correlation of Lena image, (b) horizontal correlation of ciphered image, (c) vertical correlation of Lena image, (d) vertical correlation of ciphered image, (e) diagonal correlation of Lena image and (f) diagonal correlation of ciphered image.

Table 1. Correlation coefficients of the original and encrypted images.

Direction	Horizontal	Vertical	Diagonal
Plain image of Lena	0.9503	0.9926	0.9075
Cipher image of Lena	−0.0156	−0.0022	−0.0028
Plain image of Peppers	0.9421	0.9707	0.9264
Cipher image of Peppers	0.0067	−0.0098	0.0007
Plain image of Camera	0.9683	0.8733	0.8977
Cipher image of Camera	0.0025	−0.0041	0.0004

4.3. *Resisting differential attack analysis*

To resist the differential attack, a secure encryption system should ensure that any minor changes in the plain image would cause significant effects on the difference between the cipher images. NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are usually used for differential attack analysis and defined by

$$\mathrm{NPCR} = \frac{\sum_{i,j}}{M \times N} \times 100\%, \tag{17}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j}\frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100\%, \tag{18}$$

where c_1 and c_2 denote two images that have same size $M \times N$, and $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0, & c_1(i,j) = c_2(i,j), \\ 1, & c_1(i,j) \neq c_2(i,j). \end{cases} \tag{19}$$

In this test, Lena, Peppers and Brain are used as original images for testing. We calculate the values of NPCR and UACI to test the effects of a 1-bit change in the plain image on the corresponding cipher images. The results are shown in Tables 3 and 4. From the tables, we can see that the scheme show better performances against differential attacks than the ones in [Wang *et al.*, 2015a; Zhu, 2012; Teng & Wang, 2012].

Table 2. Information entropy.

Image		Lena	Peppers	Brain
Original image		7.2072	7.5256	5.0421
Encrypted image	Ours	7.9979	7.9979	7.9975
	Wang's	7.9972	7.9973	7.9972
	Zhu's	7.9977	7.9973	7.9972
	Teng's	7.8974	7.8692	7.9868

Table 3. NPCR performance.

Image	Lena (%)	Peppers (%)	Brain (%)
Ours	99.61	99.62	99.61
Wang's	99.27	99.03	99.41
Zhu's	99.41	99.42	99.41
Teng's	93.21	92.57	65.75

4.4. *Key sensitivity test*

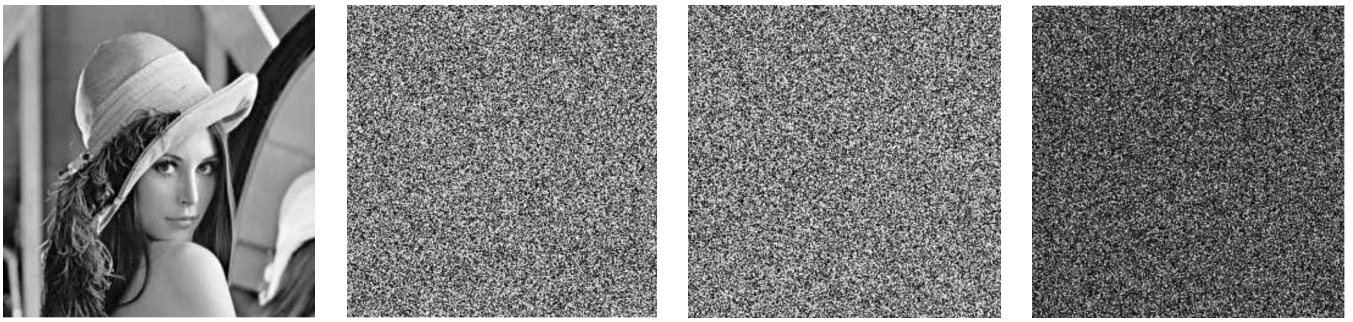
A high security cryptosystem must be sensitive to the key. In this test, we check the sensitivity of the key from the encryption phase and decryption phase.

In the encryption phase, the original keys and the slightly modified keys are used to encrypt the Lena image respectively. The original keys are set as ($x_0 = 1$, $y_0 = 0.949$, $z_0 = 1$, $w_0 = 1$, $x'_0 = 1.01$, $y'_0 = 0.95$, $z'_0 = 1.01$, $w'_0 = 1.01$) and the slightly modified keys are set as ($x_0 = 1+10^{-15}$, $y_0 = 0.949$, $z_0 = 1$, $w_0 = 1$, $x'_0 = 1.01$, $y'_0 = 0.95$, $z'_0 = 1.01$, $w'_0 = 1.01$). The original Lena image is shown in Fig. 6(a), and the two cipher images are shown in Figs. 6(b) and 6(c) which correspond to original keys and slightly modified keys respectively. The difference between the two cipher images is shown in Fig. 6(d). It is clear that slightly different keys will produce two completely different cipher images.

In the decryption phase, the correct decryption keys and the incorrect decryption keys are used to decrypt the same cipher image respectively. The correct decryption keys and the incorrect decryption keys are the same as the original encryption keys and the slightly modified encryption keys, respectively. The original Lena image and the corresponding cipher image of the original keys are shown in Figs. 7(a) and 7(b). The decrypted images using the incorrect decryption keys and the correct decryption keys are shown in Figs. 7(c) and 7(d).

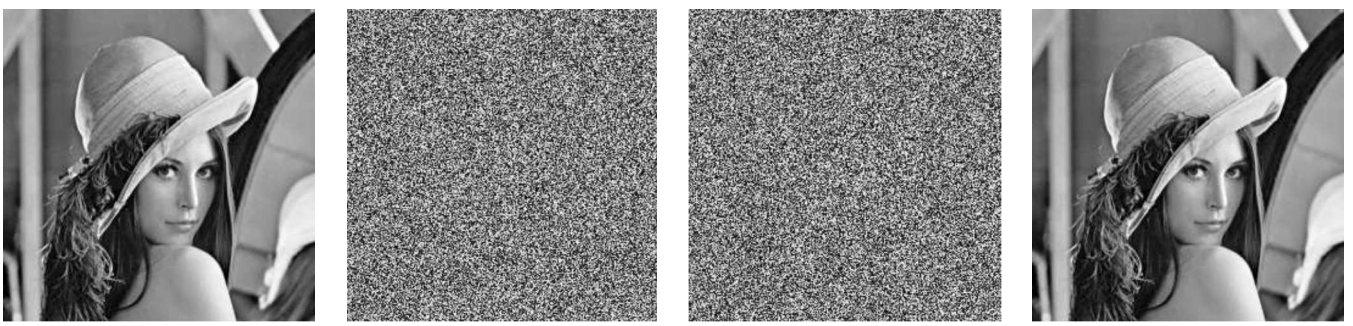
Table 4. UACI performance.

Image	Lena (%)	Peppers (%)	Brain (%)
Ours	33.46	33.41	33.42
Wang's	33.28	33.27	33.49
Zhu's	33.26	33.27	33.27
Teng's	32.48	30.24	18.73



(a) (b) (c) (d)

Fig. 6. Key sensitivity test for image encryption: (a) Lena image, (b) encrypted image using the original key, (c) encrypted image using the modified key and (d) the difference between (b) and (c).



(a) (b) (c) (d)

Fig. 7. Key sensitivity test for image decryption: (a) Lena image, (b) encrypted image using the original key, (c) decrypted image using the incorrect decryption key and (d) decrypted image using the correct decryption key.

It is clear that the slightly different decryption keys cannot decrypt the cipher image.

4.5. *Peak signal-to-noise ratio analysis*

The PSNR (peak signal-to-noise ratio) is used as a measure of encryption quality and can be calculated by

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [P(i,j) - C(i,j)]^2, \quad (20)$$

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{I_{\max}^2}{\mathrm{MSE}}\right), \quad (21)$$

where $M \times N$ is the size of image, $P(i,j)$ is the pixel value of original image, $C(i,j)$ is the pixel value of encrypted image, $I_{\max}$ is the maximum pixel value of the image. Obviously, the value of PSNR should be as small as possible to ensure the efficiency of the algorithm.

To prove the quality of encryption, the value of PSNR is computed for the encryption of Lena, Peppers and Brain by different algorithms. The results are shown in Table 5. It is clear that encrypting Lena, Peppers and Brain, the proposed algorithm indicates a smaller PSNR value than the ones in [Zhang & Gao, 2015; Xu *et al.*, 2016; Zhou *et al.*, 2014] and the PSNR values for different encrypted images are very low. Therefore, the encryption quality of the proposed algorithm is superior.

4.6. *Computational complexity and speed performance analysis*

The speed performance for the whole encryption process is one of the important parameters to evaluate the efficiency of any designed algorithm. In this part, we provide the computational complexity of

Table 5. PSNR for the encryption.

Image	Ours	Zhang's	Xu's	Zhou's
Lena	8.4100	9.3228	9.1772	9.2337
Peppers	8.9448	8.9327	9.0442	8.8772
Brain	5.7375	9.0443	8.9604	9.1145

Table 6. Number of operations.

Operation	Number of Operation	Summation
Sum	$\left(15+\frac{13}{16}\right)n^2+14N_0-5$	$\left(34+\frac{15}{16}\right)n^2+22N_0-6$
Multiplication	$\left(10+\frac{5}{8}\right)n^2+8N_0-1$	
XOR	$2n^2$	
Mod	$\left(4+\frac{1}{8}\right)n^2-2$	
Fix	$\frac{1}{8}n^2$	
Floor	$\left(1+\frac{1}{8}\right)n^2$	
Reshape	1	
Permutation	n^2	
Breadth-first search	$\frac{1}{8}n^2+1$	

our algorithm for the gray image of size $n \times n$. The number of mathematical and breadth-first search is shown in Table 6. From the table, we can see that the total number of operations is $(34+15/16)n^2+22N_0-6$. Thus, the computational complexity of the algorithm could be denoted as $O(n^2)$. In addition, the "sum", "multiplication", "floor" and "fix" operations waste computations on most computed bits [Li *et al.*, 2017c]. In our scheme, the "add", "multiplication", "floor", "fix" operations are mainly used to generate pseudorandom sequences. Therefore, the encryption process does not take too much time even when relatively large images are encrypted.

In order to analyze the speed performance better, we use Matlab (R2014a) to test the speed of the encryption algorithm on a personal computer with Windows 7 64-bit operating system, Intel Core i3-2370M CPU @ 2.40 MHz and 4 GB memory. The 256×256 Lena, Peppers and Brain are tested. When different images are encrypted with one round, the time cost of different algorithms are listed in Table 7. It is clear that the proposed algorithm is faster than the ones in [Zhang & Gao, 2015; Xu *et al.*, 2016; Zhou *et al.*, 2014; Teng & Wang, 2012].

Table 7. Speed analysis.

	Ciphered Time (s)				
Image	Ours	Zhang's	Xu's	Zhou's	Teng's
Lena	0.417	0.624	1.512	1.224	1.835
Peppers	0.448	0.673	1.547	1.263	1.862
Brain	0.429	0.651	1.525	1.285	1.823

5. Conclusion

In this paper, a chaotic image scheme using breadth-first search and dynamic diffusion is proposed. The permutation-diffusion architecture is employed in this scheme. Firstly, the plain image is traversed using breadth-first search for getting the scrambled sequence B. Secondly, the scrambled sequence B is permuted to obtain the shuffled sequence. Finally, we disturb the diffusion key stream using breadth-first search and propose a dynamic diffusion method to encrypt the shuffled sequence. The proposed dynamic diffusion method can assure that encrypting each pixel is related to all other pixels and enhances the sensitivity of the cryptosystem. The hyper-chaotic system in this scheme generates pseudorandom sequences in each phase. We carry out many experiments to prove the security of this scheme. Various types of common security and performance analysis have shown that the proposed scheme has high security and excellent performance.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61571185), the Natural Science Foundation of Hunan Province, China (No. 2016JJ2030) and the Open Fund Project

of Key Laboratory in Hunan Universities (No. 15K027).

References

Arroyo, D., Diaz, J. & Rodriguez, F. B. [2013] "Cryptanalysis of a one round chaos-based substitution permutation network," *Sign. Process.* **93**, 1358–1364.

Enayatifar, R., Abdullah, A. H. & Isnin, I. F. [2014] "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.* **56**, 83–93.

Fu, C., Lin, B. B., Miao, Y. S., Liu, X. & Chen, J. J. [2011] "A novel chaos-based bit-level permutation scheme for digital image encryption," *Opt. Commun.* **284**, 5415–5423.

Gonzalo, A. & Li, S. J. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation and Chaos* **16**, 2129–2151.

Hu, T., Liu, Y., Gong, L. H. & Ouyang, C. J. [2016] "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlin. Dyn.* **87**, 1–16.

Kumar, M., Iqbal, A. & Kumar, P. [2016] "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Sign. Process.* **125**, 187–202.

Li, S. J., Chen, G. R., Cheung, A., Bharat, B. & Lo, K. [2007] "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. Circuits Syst. Video Technol.* **17**, 214–223.

Li, C. Q., Liu, Y. S., Xie, T. & Chen, M. Z. Q. [2013] "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlin. Dyn.* **73**, 2083–2089.

Li, C. Q., Lin, D. D., Lü, J. H. & Hao, F. [2017a] "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia*.

Li, C. Q., Lin, D. D. & Lü, J. [2017b] "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE Multimedia* **24**, 64–71.

Li, Y. P., Wang, C. H. & Chen, H. [2017c] "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.* **90**, 238–246.

Liu, H. J. & Wang, X. [2010] "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.* **59**, 3320–3327.

Liu, W. H., Sun, K. H. & Zhu, C. X. [2016a] "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.* **84**, 26–36.

Liu, Y., Wang, J., Fan, J. & Gong, L. H. [2016b] "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences," *Multimed. Tools Appl.* **75**, 4363–4382.

Mirzaei, O., Yaghoobi, M. & Irani, H. [2012] "A new image encryption method: Parallel sub-image encryption with hyper chaos," *Nonlin. Dyn.* **67**, 557–566.

Niu, Y. J., Wang, X. Y., Wang, M. J. & Zhang, H. G. [2010] "A new hyperchaotic system and its circuit implementation," *Nonlin. Sci. Numer. Simul.* **15**, 3518–3524.

Norouzi, B. & Mirzakuchaki, S. [2014] "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlin. Dyn.* **78**, 995–1015.

Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S. & Mohammad, M. R. [2014] "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimed. Tools Appl.* **71**, 1469–1497.

Teng, L. & Wang, X. Y. [2012] "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Opt. Commun.* **285**, 4048–4054.

Wang, X. Y., Wang, Q. & Zhang, Y. Q. [2015a] "A fast image algorithm based on rows and columns switch," *Nonlin. Dyn.* **79**, 1141–1149.

Wang, X. Y., Zhang, Y. Q. & Bao, X. M. [2015b] "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.* **73**, 53–61.

Xie, E. Y., Li, C. Q., Yu, S. M. & Lü, J. H. [2017] "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Sign. Process.* **132**, 150–154.

Xu, L., Li, Z., Li, J. & Wei, H. [2016] "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.* **78**, 17–25.

Xue, X. L., Zhang, Q., Wei, X. P., Guo, L. & Wang, Q. [2010] "An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps," *J. Comput. Theor. Nanosci.* **7**, 397–403.

Ye, G. D., Zhao, H. Q. & Chai, H. J. [2016] "Chaotic image encryption algorithm using wave-line permutation and block diffusion," *Nonlin. Dyn.* **83**, 2067–2077.

Zhang, W., Wong, K. W., Yu, H. & Zhou, Z. L. [2012] "An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion," *Opt. Commun.* **285**, 2343–2354.

Zhang, Y. S., Wen, W. Y., Su, M. & Li, M. [2014a] "Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik* **125**, 1562–1564.

Zhang, Y. S., Xiao, D., Wen, W. Y. & Li, M. [2014b] "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlin. Dyn.* **76**, 1645–1650.

Zhang, S. & Gao, T. [2015] "An image encryption scheme based on DNA coding and permutation of hyper-image," *Multimed. Tools Appl.* **24**, 1–14.

Zhou, Y. C., Cao, W. J. & Chen, C. L. [2014] "Image encryption using binary bitplane," *Sign. Process.* **100**, 197–207.

Zhu, C. X. [2012] "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.* **285**, 29–37.

Zhu, C. X. & Sun, K. H. [2012] "Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms," *Acta Phys. Sin.* **61**, 120503.