Image encryption using DNA complementary rule and chaotic maps

Article *in* Applied Soft Computing · May 2012

DOI: 10.1016/j.asoc.2012.01.016

3 authors, including:

Xingyuan Wang
Dalian University of Technology
300 PUBLICATIONS **4,919** CITATIONS
SEE PROFILE

Abdurahman Kadir
20 PUBLICATIONS **371** CITATIONS
SEE PROFILE

Applied Soft Computing 12 (2012) 1457–1466

Contents lists available at SciVerse ScienceDirect

Applied Soft Computing

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

Image encryption using DNA complementary rule and chaotic maps

Hongjun Liu[a,b], Xingyuan Wang[a,*], Abdurahman kadir[c]

[a] School of Electronic and Information Engineering, Dalian University of Technology, Dalian 116024, China
[b] School of Information Engineering, Weifang Vocational College, Weifang 261041, China
[c] School of Computer Science and Engineering, Xinjiang University of Finance and Economics, Urumqi 830012, China

ARTICLE INFO

Article history:
Received 13 January 2011
Received in revised form 18 January 2012
Accepted 24 January 2012
Available online 31 January 2012

Keywords:
Image encryption
DNA coding
Complementary rule
Message Digest 5
PWLCM
Chebyshev chaotic maps

ABSTRACT

This paper proposes a novel confusion and diffusion method for image encryption. One innovation is to confuse the pixels by transforming the nucleotide into its base pair for random times, the other is to generate the new keys according to the plain image and the common keys, which can make the initial conditions of the chaotic maps change automatically in every encryption process. For any size of the original grayscale image, after being permuted the rows and columns respectively by the arrays generated by piecewise linear chaotic map (PWLCM), each pixel of the original image is encoded into four nucleotides by the deoxyribonucleic acid (DNA) coding, then each nucleotide is transformed into its base pair for random time(s) using the complementary rule, the times is generated by Chebyshev maps. Experiment results and security analysis show that the scheme can not only achieve good encryption result, but also the key space is large enough to resist against common attacks.

1. Introduction

In recent years, plenty of image encryption approaches have been proposed. The diffusion and confusion processes in cryptography proposed by Shannon [1] are successfully applied in image encryption. In order to disturb the high correlation among pixels, the Arnold cat map is often used to diffuse the pixel positions in many literatures [2–8], but this map has two shortages, one is that the iteration times are very limited, which is usually less than 1000 times; the other is that the width and height of the original image are required to be equal, or the image can not be completely permuted.

The chaotic map is often applied to generate the pseudo-random sequence to confuse the pixels [9]. For the chaotic map has sensitive dependence on initial conditions [10], experiment results show that applying more than one chaotic map can achieve larger key space [11]. Liu et al. proposed a cryptosystem based on multi-chaotic maps [12]. Patidar et al. proposed a substitution diffusion method using chaotic standard and logistic maps [13]. Mazloom and Eftekhari-Moghadam proposed a color image encryption algorithm based on coupled nonlinear chaotic map [14].

In the cryptographic system, it is very important to choose a good chaotic generator with desirable dynamical statistical properties. It is well known that some smooth chaotic systems, such as the Logistic map, there is a dense set of periodic windows for any range of parameter values [15], thus imposing restrictions for the practical application of such systems in chaotic cryptography [16], although there have been many image encryption schemes based on it [17]. Li et al. proved that Logistic map does not satisfy the requirements as a good random source [18]. Awad et al. compared the 1-D chaotic generators for digital data encryption, and the results showed that the PWLCM map is better than the Logistic map [19]. Akhshani et al. proposed the image encryption scheme based on 2D PWLCM maps [20].

Recently, the characteristics of DNA computing, massive parallelism, huge storage and ultra-low power consumption have been found [21,22]. Some researchers turned to use the complementary rule of DNA to encrypt image. Gehani et al. [23] presented an image encryption algorithm of one-time pad cryptography with DNA strands. Zhang et al. [24,25] proposed two Image encryption algorithms using the exclusive or (XOR) operation, bit shift and DNA addition and subtraction operation, but the 1-D or 2-D Logistic map is chosen to generate the chaotic sequence.

In this paper, we proposed a novel confusion and diffusion method for image encryption. For any size of the grayscale image, we permute the rows and columns respectively by the arrays generated by PWLCM instead of the Arnold cat map or the Logistic map. After encoding each pixel of the original image to four nucleotides by DNA coding, then use the complementary rule to transform each nucleotide into their base pair for different times, which are generated by Chebyshev chaotic maps. We use the MD5 hash of the plain image to generate the initial values and parameters of the

* Corresponding author.
E-mail addresses: smithliu@126.com (H. Liu), wangxy@dlut.edu.cn (X. Wang).

1568-4946/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.asoc.2012.01.016

chaotic maps, to make the keys change for each encryption without changing the common keys. Experiment results and security analysis show that the scheme not only can achieve good encryption result and large key space, but also can resist against common attacks.

2. DNA coding, complementary rule and chaotic maps

2.1. DNA coding and complementary rule

Each DNA sequence contains four nucleic acid bases, which are A (*adenine*), C (*cytosine*), G (*guanine*) and T (*thymine*), where A and T, C and G are complementary pairs [23]. In the total 4! = 24 kinds of coding, there are only 8 of them can meet the complementary rule, for example, the decimal digits "0123" (the corresponding binary number is "00011011") can be encoded into one of them, such as "CTAG", "CATG", "GTAC", "GATC", "TCGA", "TGCA", "ACGT" or "AGCT".

If we use the four nucleic acid bases C, T, A and G, to denote the binary value of 00, 01, 10 and 11 respectively, each 8-bit pixel value of the grayscale image can be encoded into a nucleotide string [26], for example, if the grayscale value of the pixel is 177, its binary value is "10110001", which can be expressed as the four 2-bit nucleotides "AGCT". Inversely, to decode the nucleotide string, we can get the pixel value. Suppose the size of original grayscale image I is $M \times N$, after converting it to a binary matrix I'', we can encode it by DNA coding and transform it into one-dimension sequence X, which can be expressed as follows.

$$X = \{x_1, x_2, \ldots, x_{4MN}\}, \quad x_i \in \{A, C, T, G\}. \tag{1}$$

The complementary rule must satisfies that, for each nucleotide x_i in the nucleotide string,

$$\begin{cases} x_i \neq B(x_i) \neq B(B(x_i)) \neq B(B(B(x_i))) \\ x_i = B(B(B(B(x_i)))) \end{cases}, \tag{2}$$

where $B(x_i)$ is the base pair of x_i, which can guarantee the complementary rule of injective mapping.

Abide by the rules of Eq. (2), the complementary pairs can be defined. That is, a unique counterpart is assigned to each base pair. The number of legal complementary rules should be considered, and there are total 6 group legal complementary rules, which are shown as follows:

$(AT)(TC)(CG)(GA)$, $(AT)(TG)(GC)(CA)$, $(AC)(CT)(TG)(GA)$,
$(AC)(CG)(GT)(TA)$, $(AG)(GT)(TC)(CA)$, $(AG)(GC)(CT)(TA)$.

For instance, we can choose one of the complementary rule, such as $(AT)(TG)(GC)(CA)$, to apply it in the proposed image encyption.

2.2. Generate the initial conditions of PWLCM system and Chebyshev maps by MD5 hash

In cryptography, MD5 is a widely used cryptographic hash function with 128-bit hash value. A MD5 hash is typically expressed as a 32 digit hexadecimal number. Even if there is only one bit difference between two images, their MD5 results will be completely different [27].

Before encrypting the original grayscale image, we firstly compute its MD5 hash M and divide it into four groups, and each group has eight hexadecimal numbers, i.e. $h_{j1}h_{j2}h_{j3}h_{j4}$, $j = 1, 2, \ldots, 8$. For each group, we convert it into a floating decimal number $d_j \in (0,0.1)$ by Eq. (3):

$$d_j = \text{hex } 2\,\text{dec}(h_{j1}h_{j2}h_{j3}h_{j4}) \times 10^{-6}. \tag{3}$$

Suppose the common initial values of the PWLCM system are x_0 and y_0, the parameters are p_x and p_y, for each specific grayscale image, the new initial values x'_0 and y'_0, the parameters p'_x and p'_y can be generated by Eq. (4):

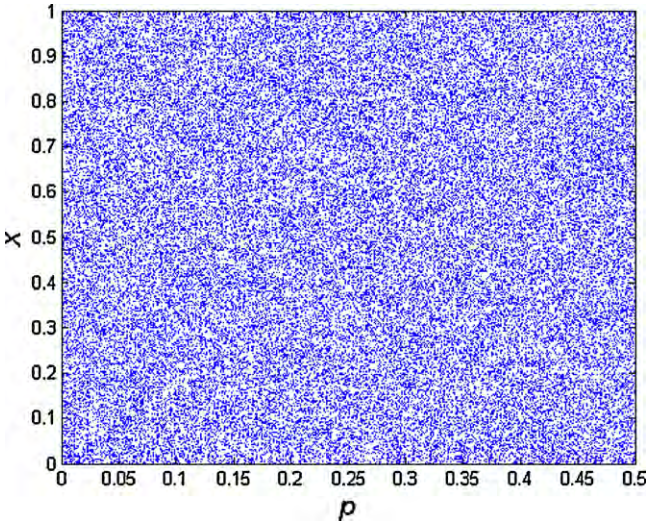

Fig. 1. The distribution of x with different p in 5000 iterations.

$$\begin{cases} x'_0 = x_0 + d_1 \\ y'_0 = y_0 + d_2 \\ p'_x = p_x + d_3 \\ p'_y = p_y + d_4 \end{cases} \tag{4}$$

Similarly, suppose the common initial values of the Chebyshev maps are z_0 and q_0, the parameters are w_z and w_q, for each grayscale image, the new initial values z'_0 and q'_0, the parameters w'_z and w'_q can be generated by Eq. (5):

$$\begin{cases} z'_0 = z_0 + d_5 \\ q'_0 = q_0 + d_6 \\ w'_z = w_z + d_7 \\ w'_q = w_q + d_8 \end{cases}. \tag{5}$$

By these means, we can ensure the generation of the keys dependent to the plain image, and that can make the keys change for every encryption procedure without changing the common keys [28].

2.3. Using PWLCM system to generate permutation arrays

The PWLCM system has gained increasing attention in chaos research recently due to its simplicity in representation, efficiency in implementation, as well as good dynamical behavior. The PWLCM can be described in Eq. (6):

$$x_{i+1} = F_p(x_i) = \begin{cases} x_i/p, & 0 \le x_i < p \\ (x_i - p)/(0.5 - p), & p \le x_i < 0.5, \\ F_p(1 - x_i), & x_i \ge 0.5 \end{cases} \tag{6}$$

where $x_i \in [0,1)$. When the control parameter $p \in (0,0.5)$, Eq. (6) evolves into chaotic state [10], p can be served as the secret key. The PWLCM system has uniform invariant distribution and very good ergodicity, confusion and determinacy [29], so it can provide excellent random sequence, which is suitable for cryptosystem. The distribution of x with different p of the PWLCM system is depicted in Fig. 1, where the values of x are uniformly distributed.

We use Eq. (6) to generate two sequences $X_M = \{x_1, x_2, \ldots, x_M\}$ and $Y_N = \{y_1, y_2, \ldots, y_N\}$ with the initial values x'_0 and y'_0, the parameters p'_x and p'_y generated by Eq. (4).

In order to diffuse the pixels by permuting the rows and columns respectively, we need to generate the rows permutation and columns permutation arrays. Firstly, we generate two arrays of

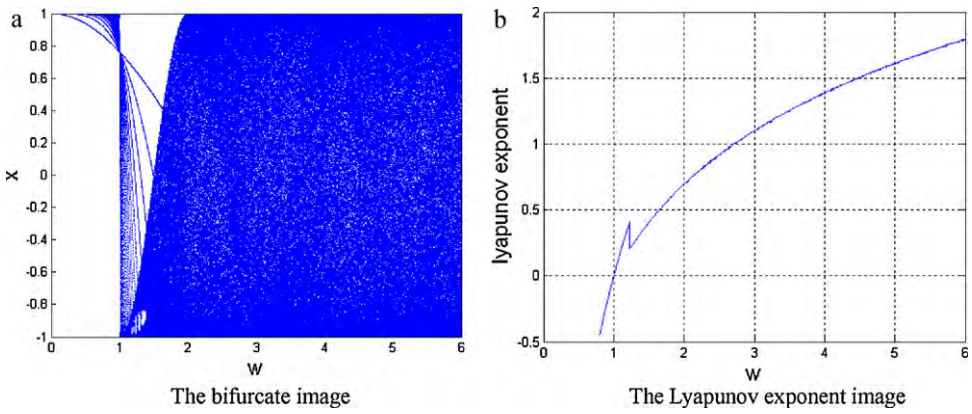

Fig. 2. The bifurcate image and Lyapunov exponent image of Chebyshev maps.

H and V to donate the numbers of rows and columns in ascending order.

$$H = \{1, 2, \ldots, M\}, \tag{7}$$

$$V = \{1, 2, \ldots, N\}. \tag{8}$$

Then we permute array H by Eq. (9) to get array H'.

$$H'(i) = H((x_i \times M) \bmod i), \quad x_i \in X_M, \quad i = M, M-1, \ldots, 2, 1. \tag{9}$$

Similarly, we can get array V' by Eq. (10).

$$V'(j) = V(((y_j \times N) \bmod j), \quad y_j \in Y_N, \quad j = N, N-1, \ldots, 2, 1. \tag{10}$$

2.4. Using Chebyshev maps to generate the iteration times sequence

The expression of Chebyshev maps is as follows:

$$z_{i+1} = \cos(w \ \cos^{-1} z_i), \quad -1 \le z_i \le 1, \tag{11}$$

where w is the degree of Chebyshev maps, its corresponding invariant density is as follows:

$$\rho(z) = \frac{1}{(\pi\sqrt{1-z^2})}. \tag{12}$$

Chebyshev maps have important properties of excellent cryptosystem [27]. If $w \in [2,6]$, the Lyapunov exponent of Chebyshev maps is positive, this predicates that the Chebyshev maps are chaotic. The bifurcate image and Lyapunov exponent image are shown in Fig. 2.

There are total $M \times N$ pixels in the original grayscale image, each 8-bit pixel can be expressed as four 2-bit nucleotides, so the size of sequence C is $4MN$. We use Eq. (11) to generate two sequences $Z = \{z_1, z_2, \ldots, z_{4MN}\}$ and $Q = \{q_1, q_2, \ldots, q_{4MN}\}$, with the new initial values z'_0 and q'_0, the parameters w'_z and w'_q generated by Eq. (5).

The sequence $P = \{p_1, p_2, \ldots, p_{4MN}\}$ generated by the Eq. (13) is to serve as the location, which will be used to get one digit from z_i.

$$p_i = (q_i \times 10) \bmod 15 + 1. \tag{13}$$

Simulation results show that the effective precision can be set to 10^{-15}, in order to enlarge the key space, we randomly selected one digit from 15 decimal digits, according to the location sequence P.

Finally we can get the sequence $C = \{c_1, c_2, \ldots, c_{4MN}\}$, $c_i \in \{0, 1, 2, 3\}$ by Eq. (14), to serve as the iteration times, which is one-to-one correspondent with the nucleotide sequence X generated by Eq. (1).

$$c_i = \text{int}(\text{extract}(z_i, p_i)) \bmod 4, \tag{14}$$

where the function extract(z_i,p_i) is to extract the p_i-th decimal digit from z_i.

3. Image encryption and decryption algorithm

3.1. Image encryption algorithm

Suppose the size of the original grayscale image I is $M \times N$, the encryption steps are as follows.

Input: Image I, the common initial values x_0, y_0, z_0 and q_0, the parameters p_x, p_y, w_z and w_q.
Output: The encrypted image.

Step 1. Compute the MD5 hash of the plain image, and then generate the new initial conditions by Eqs. (4) and (5).
Step 2. Permute the rows and columns of image I respectively, according to the arrays of H' and V' generated by Eqs. (9) and (10), to get the permuted image I'.
Step 3. Convert image I' into a binary matrix I'', and then encode it by DNA coding and transform it into one-dimension nucleotides sequence X.
Step 4. Generate the location sequence P, the iteration times sequence C by Eqs. (13) and (14). Compute the base pair of each nucleotide $x_i \in X$ for c_i time(s), as show in follows.
For each $x_i \in X$, do the following operation:
if $c_i = 0$, do not change d_i;
else if $c_i = 1$, $x_i = B(x_i)$;
else if $c_i = 2$, $x_i = B(B(x_i))$;
else if $c_i = 3$, $x_i = B(B(B(x_i)))$.
Step 5 Convert the sequence X into a two-dimension matrix, and then convert it into the encrypted image.

3.2. Image decryption algorithm

The decryption algorithm is the reverse process of encryption algorithm, and the steps are as follows.

Input: The encrypted image, the common initial values and parameters are the same as the encryption algorithm.
Output: The decrypted image.

Step 1. Convert the encrypted image into a binary matrix, and then encode the matrix into one-dimension nucleotides sequence X by DNA coding.
Step 2. According to the MD5 hash of the plain image, generate the new initial conditions by Eqs. (4) and (5).
Step 3. Generate the sequences P and C by Eqs. (13) and (14). Compute the complementary pair of each nucleotide $x_i \in X$ for $(4 - c_i) \bmod 4$ time(s) to get X'.

Step 4. Transform the sequence X' into two-dimension matrix, and then convert it into image I'.
Step 5. Recover the rows and columns of I' respectively, according to the arrays H' and V' generated by Eqs. (9) and (10), to get the decrypted image I.

4. Experimental results

Here we set the initial values and parameters of PWLCM system: $x_0 = 0.3675123321233133$, $y_0 = 0.5675123321233122$, $p_x = 0.3675123321233133$, $p_y = 0.1675123321233122$. For the Chebyshev maps, we set $z_0 = 0.6382911122234563$, $q_0 = 0.2282911122234561$, $w_z = 5.2992332345678933$ and $w_q = 4.2892332345678912$. The size of the original grayscale image is 256×256.

For the original images of Lena and Pepper, we permute their rows and columns respectively to diffuse the pixels, the permutation results are shown in Fig. 3.

We create confusion by encoding the permuted images into nucleotides and transform each nucleotide $d_i \in D$ into its base pair for $c_i \in C$ time(s). The results are shown in Fig. 4 (a) and (d).

The decryption algorithm reversely permutes the rows and columns, and then computes the base pair of each nucleotide, The results are shown in Fig. 4.

5. Performance and security analysis

5.1. Key space and sensitivity analysis

The high sensitivity to initial conditions is inherent to any chaotic system. To provide an encryption algorithm with high security, the key space should be large enough to make any brute force attack ineffective. The total key space is from the confusion and diffusion processes. Our encryption algorithm actually does have some of the following secret keys: (1) for the PWLCM system, the initial values x_0 and y_0, the parameters p_x and p_y; (2) for the Chebyshev maps, the initial values z_0 and q_0, the parameters w_z and w_q; (3) DNA coding and complementary rule.

For the PWLCM system, the sensitivity to the initial value and parameter are both considered as 10^{-16} [30]. If we set the precision decimal value of keys from 10^{-1} to 10^{-16}, the ratio of the different elements between two arrays is larger than 0.76, and it equals zero when the key difference is 10^{-17}, as the simulation results for x_0 and p_x are shown in Fig. 5, the same to y_0 and p_y, so the key space $S_{x_0} = S_{y_0} = 10^{16}$. For the variation of the parameters $p_x, p_y \in (0, 0.5)$, then $S_{p_x} = S_{p_y} = 0.5 \times 10^{16}$.

For the Chebyshev maps, the sensitivity of our algorithm to z_0 is illustrated in Fig. 6. When the tiny change in the initial value $\Delta z_0 = 10^{-15}$, the decrypted image is still indistinguishable. But when $\Delta z_0 = 10^{-16}$, the decipher result is uncertain, for example, when we encrypt the Lena image with $z_0 = 0.6382911122234563$, it can be successfully decrypted by $z_0 = 0.6382911122234564$, but when $z_0 = 0.6382911122234565$, the decrypted image is still indistinguishable.

We encrypt the Lena image with two close initial values of $\Delta z_0 = 10^{-15}$, the results are shown in Fig. 7, from the difference of Fig. 7(c) we can find that the encryption results are completely different. A large number of experimental results indicate that the key spaces for initial values are $S_{z_0} = S_{q_0} = 10^{15}$. Similarly, the variation of the parameters w_z and w_q in the chaotic region is between 2 and 6 with a step of 10^{-15}, when the tiny changes in the parameter values $\Delta w_z = 10^{-15}$ or $\Delta w_q = 10^{-15}$, the decrypted image is still indistinguishable, so $S_{w_z} = S_{w_q} \approx 4 \times 10^{15}$.

There are only 8 kinds of the DNA coding to meet the complementary rule, and there are altogether 6 kinds of legal complementary rules. So the total key space $S = 8 \times 6 \times S_{x_0} S_{y_0} S_{p_x} S_{p_y} S_{z_0} S_{q_0} S_{w_z} S_{w_q} \approx 1.92 \times 10^{126}$, which is much larger than 2^{100} [31], so the encryption algorithm has a large enough key space to resist all kinds of brute-force attacks. The comparison of the key space with the existing algorithms is shown in Table 1.

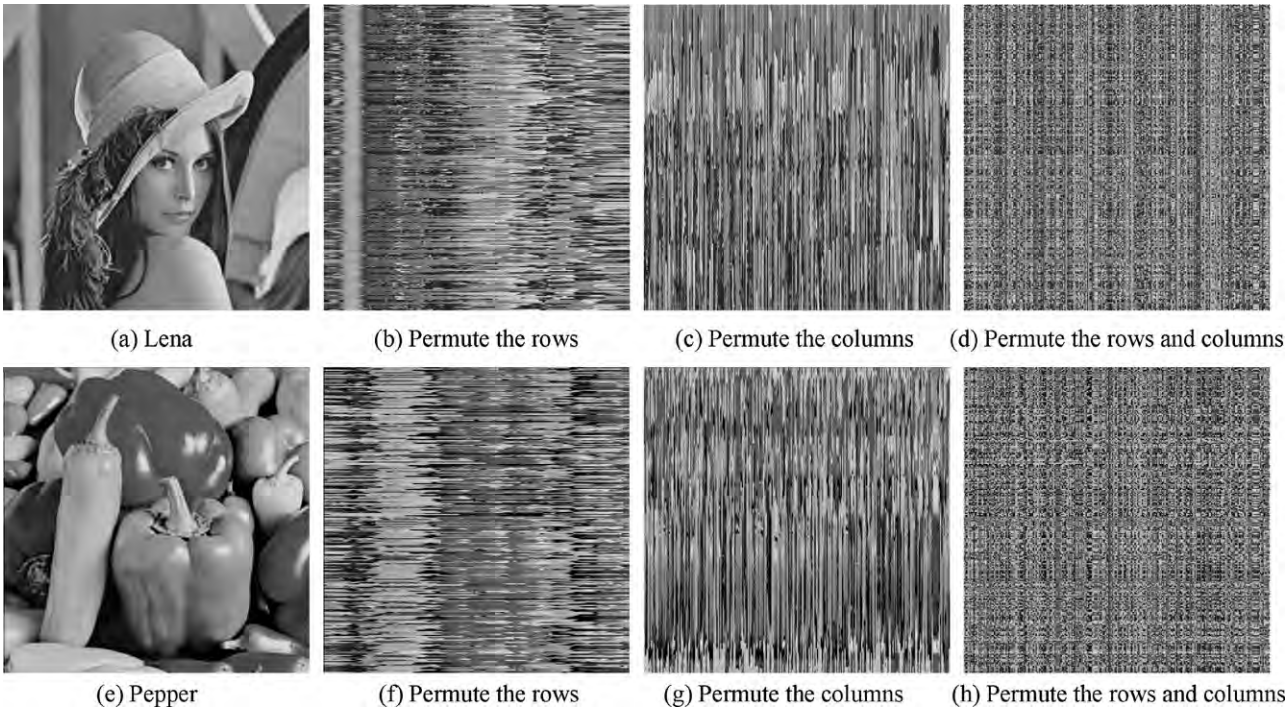

Fig. 3. The permutation results of Lena and Pepper.

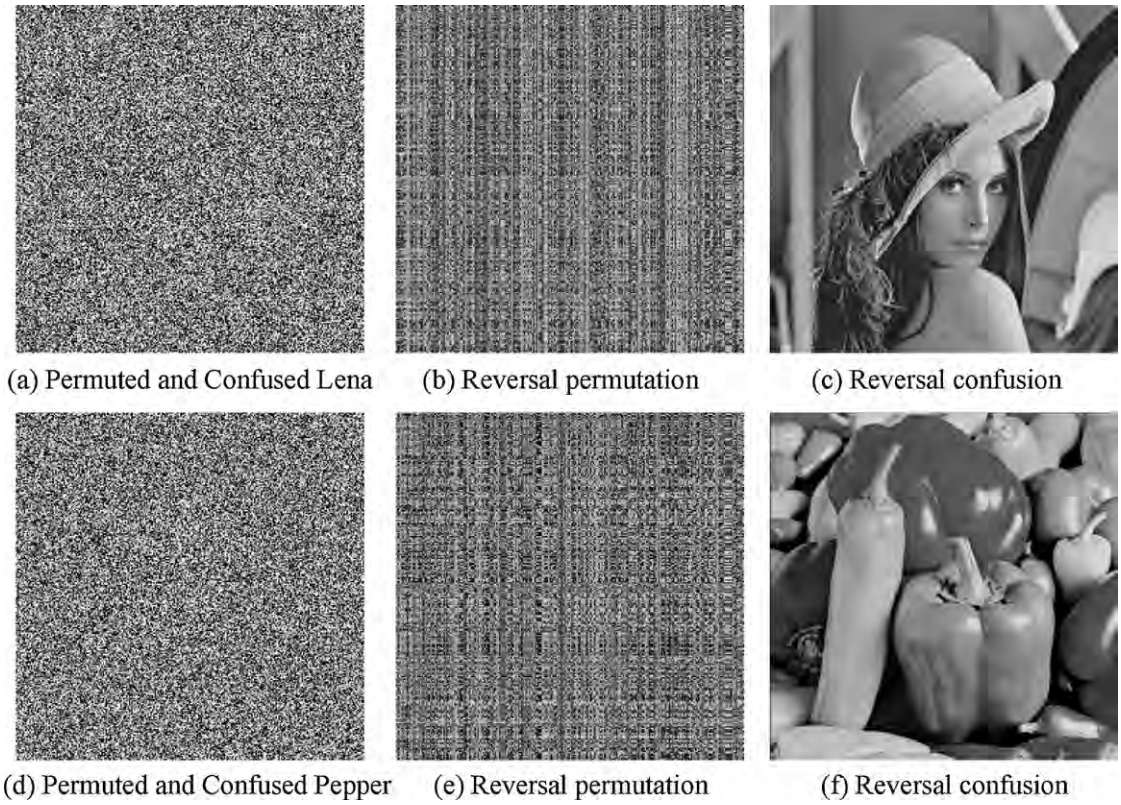

Fig. 4. Decryption: the reversal permutation and confusion results.

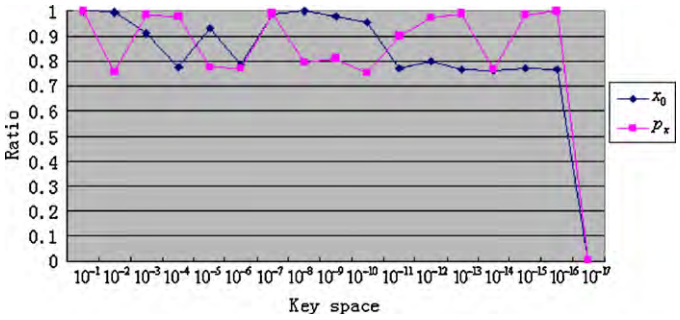

Fig. 5. Key space analysis of the PWLCM system.

5.2. Resistance to statistical attack

5.2.1. The gray histogram analysis

Considering the statistical analysis of the original image and the encrypted image, Fig. 8 shows the grayscale histograms of Lena and Pepper and their encrypted images. Comparing their histograms we can find that the pixel grayscale values of the original image are concentrated on some values, but the histograms of the encrypted images are relatively uniform, which makes the statistical attacks difficult.

Table 1
Compare the key space of the proposed algorithm with the existing algorithms.

Algorithms	Key space
Ref. [24]	10^{72}
Ref. [25]	10^{56}
Proposed algorithm	1.92×10^{126}

5.2.2. Correlation coefficient analysis

We randomly select 2500 pairs of adjacent pixels (in vertical, horizontal and diagonal directions) from the original image and encrypted image, and calculate their correlation coefficients of two adjacent pixels according to the following formula [32]:

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

where

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

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

Fig. 9 shows the correlation of two adjacent pixels in the original Lena image and its encrypted image of Fig. 4 (a), the results demonstrate that the correlations of adjacent pixels in the encrypted image are greatly reduced.

Table 2 shows the results of correlation coefficients of two adjacent pixels in Fig. 9, which is compared with the results in Refs. [24,25]. The results indicate that the correlation of two adjacent pixels of the plain image is significant, while that of the proposed

Table 2
The comparison of the correlation coefficients of Lena.

Correlation	Vertical	Horizontal	Diagonal
Plain Lena image	0.9132	0.9768	0.9428
Ref. [24]	0.0036	0.0023	0.0039
Ref. [25]	0.0057	0.0024	0.0027
Fig. 4(a)	0.0021	0.0004	−0.0038

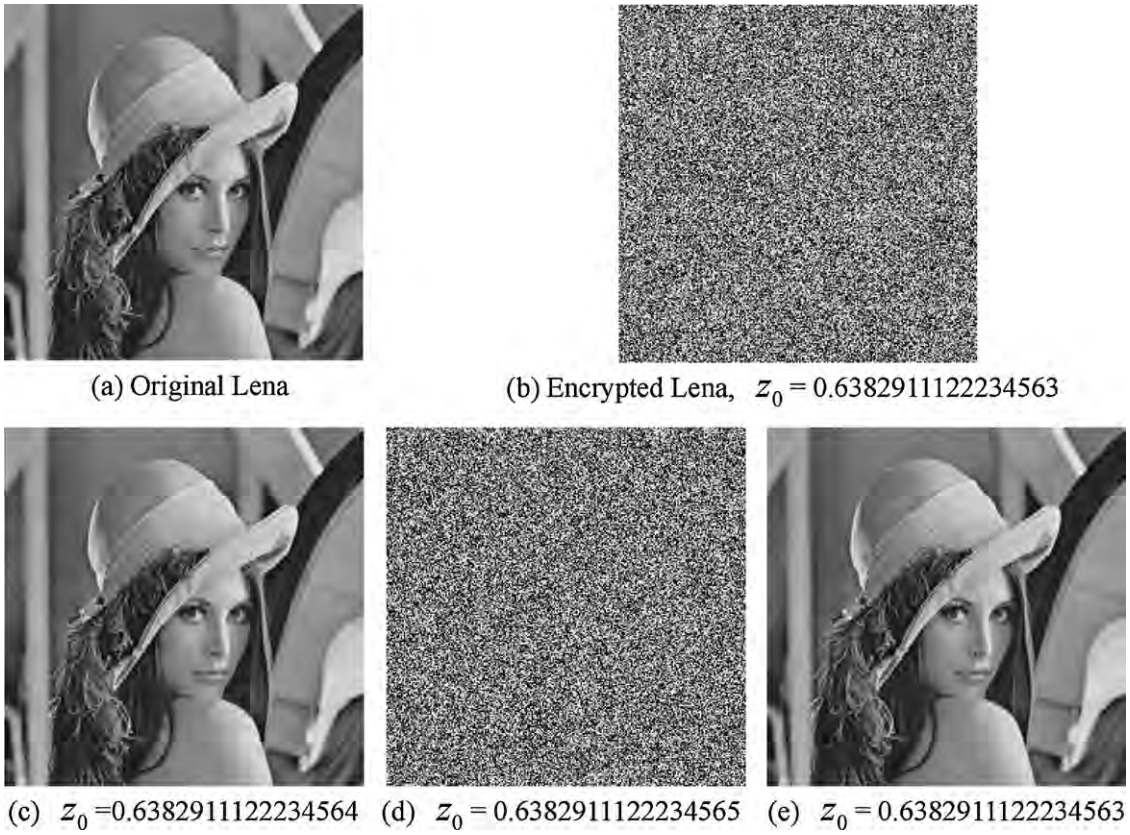

Fig. 6. Key sensitivity tests of the Chebyshev maps, where (c), (d) and (e) are the decrypted Lena with different initial values.

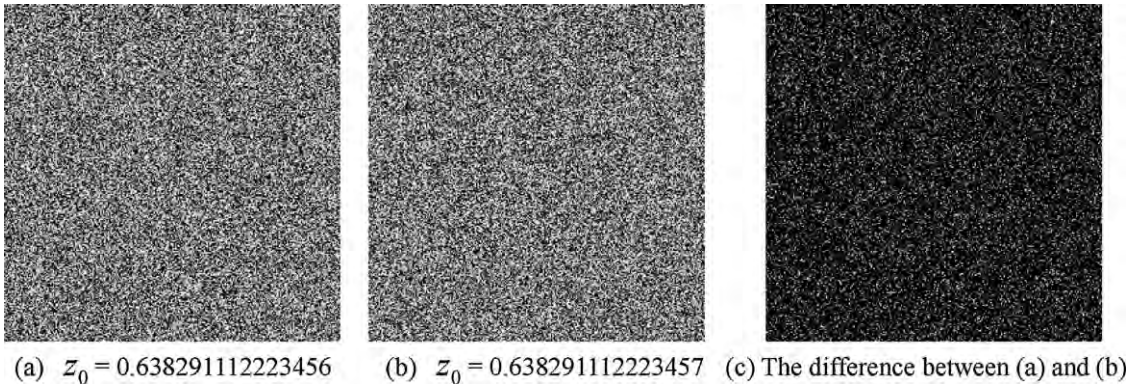

Fig. 7. The encrypted results of Lena with close initial values and their difference.

algorithm are lower than the existing ones, so the encryption effect is rather good.

5.3. Information entropy analysis

Information entropy is the most important feature of randomness. Let m be the information source, and the formula for calculating information entropy is [33]:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)}. \quad (16)$$

where $p(m_i)$ represents the probability of symbol m. Assume that there are 2^8 states of the information source and they appear with the same probability, according to Eq. (16), we can get the ideal $H(m) = 8$, which indicates that the information is random. Hence the information entropy of the encrypted image should be close to 8, the closer it gets to 8, the harder the cryptosystem leaves some information available. We use Eq. (16) to calculate the information entropy of the encrypted image of Lena, Pepper, Airplane and Barbara, Table 3 shows the entropy of the grayscale values: which are all close to the ideal value 8, so the probability of accidental information leakage is very little.

Table 3
The results of information entropy.

	Lena	Pepper	Airplane	Barbara
Plain image	7.4340	7.5764	6.7333	7.5800
Encrypted image	7.9874	7.9860	7.9780	7.9867

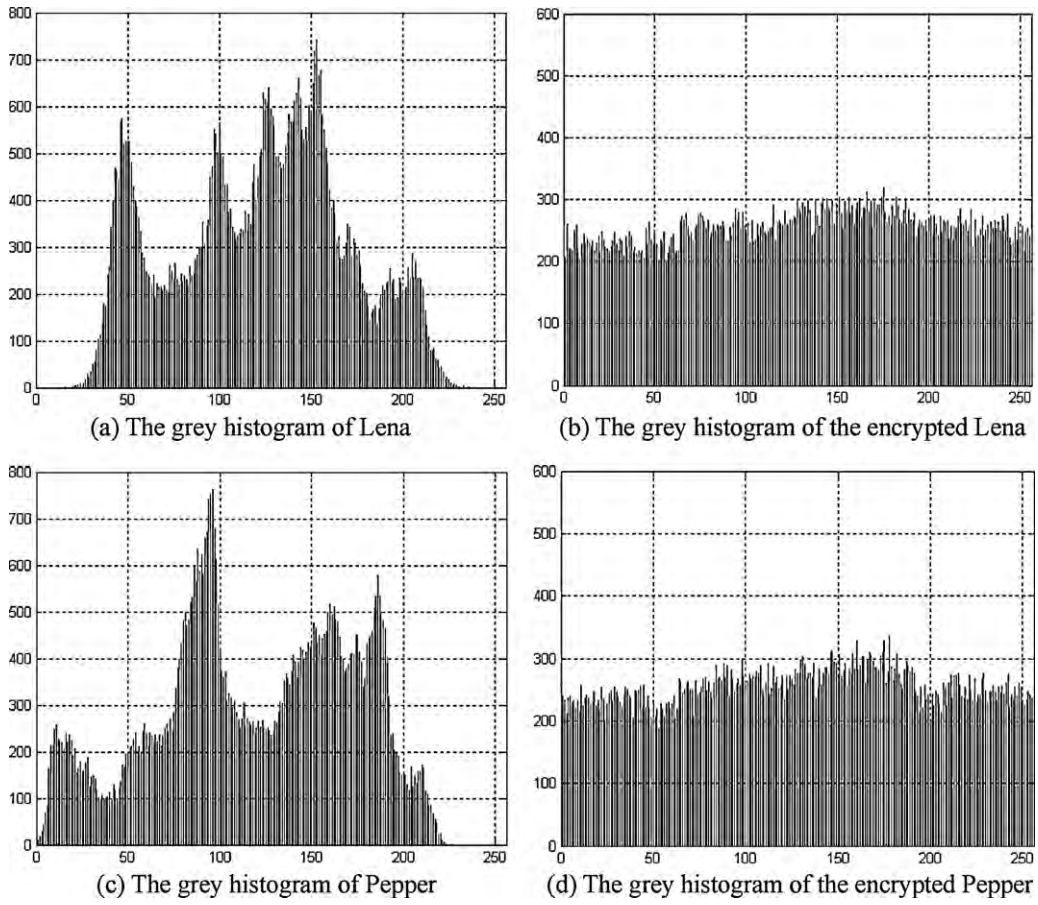

Fig. 8. The histograms of Lena and Pepper.

5.4. Differential attack

As a general requirement for all the image encryption schemes, the encrypted image should be greatly different from its original form. Such difference can be measured by means of two criteria namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI) [33]. The proposed cryptosystem can ensure two ciphered images completely different, even if there is only one bit difference between them.

Here are the formulas to calculate NPCR and UACI:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \tag{17}$$

$$\mathrm{UACI} = \frac{1}{L}\left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255}\right] \times 100\%, \tag{18}$$

where W and H represent the width and height of the image respectively. C and C' denote the encrypted images before and after one pixel of the plain image is changed. For the pixel at position (i,j), if $C(i,j) \neq C'(i,j)$, let $D(i,j) = 1$; else let $D(i,j) = 0$.

5.4.1. Correlation, NPCR and UACI of the encrypted images

We test the correlation coefficient, the NPCR and UACI of the original and encrypted images of Lena and Pepper respectively, their results are shown in Table 4. From the results we can find that our algorithm is robust against differential attack.

5.4.2. Sensitivity test of the plain images with one bit difference

We test two plain images by the same common initial values and parameters, as shown in Fig. 10(a) and (b). Fig. 10(a) is an "all-zero" plain image, and Fig. 10(b) has only one bit difference from Fig. 10(a), their encryption results and the difference are shown in Fig. 10(c)–(e).

Table 4
Correlation, NPCR and UACI of the encrypted Lena and Pepper.

Image	Correlation	NPCR (%)	UACI (%)
Ref. [24]	0.0033	99.61	38
Figs. 3(a) and 4(a)	−0.0169	99.6017	28.1370
Figs. 3(e) and 4(d)	−0.0125	99.6185	29.1988

We calculate the correlation coefficients of the encrypted images of Fig. 10(c) and (d), in Table 5, we summarize the correlation, NPCR, and UACI obtained between them. It is shown that the correlation between the two encrypted images is low. From the NPCR and UACI results we can find that our algorithm is very sensitive to tiny changes in the plain image, even if there is only one bit difference between two plain images, the decrypted images will be completely different.

5.5. Robustness against noise

One of the most important problems in a real-world communication technology is the robustness of a cryptosystem against noise. Very often signal-independent noise occurs while an image is being

Table 5
Correlation, NPCR and UACI of the encrypted images.

Image	Correlation	NPCR	UACI
Fig. 10(c) and (d)	0.0026	99.5376	32.5738

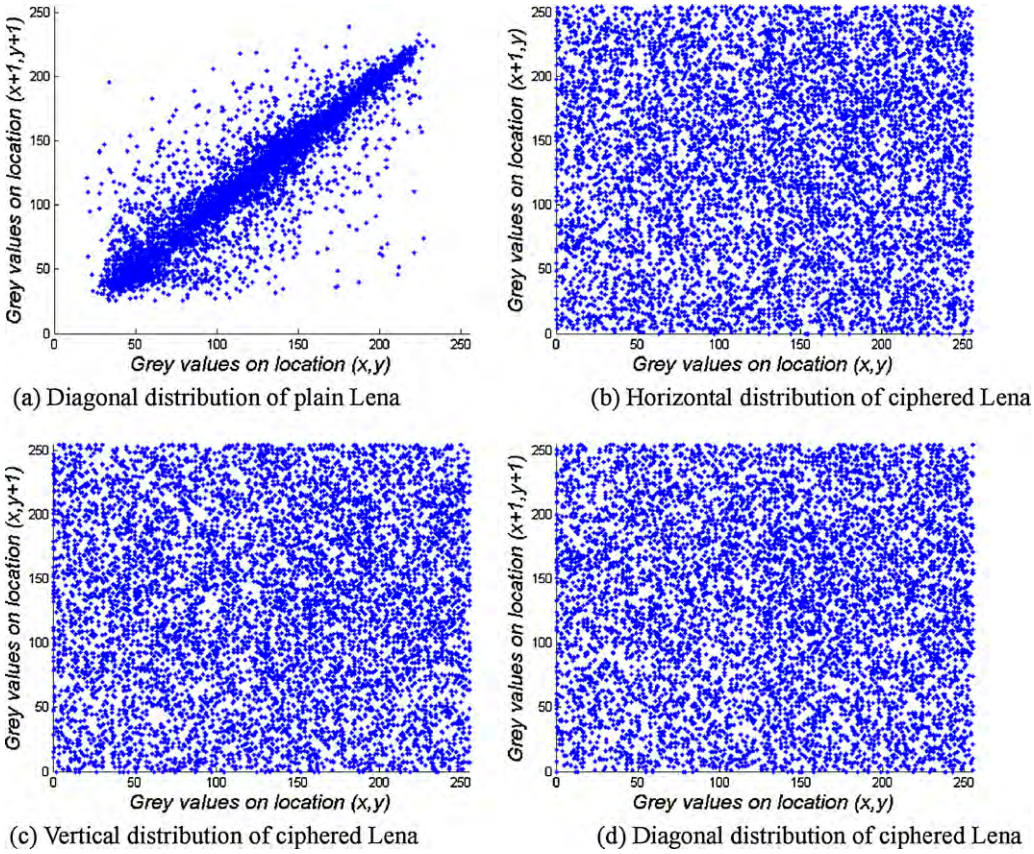

Fig. 9. Correlation of two adjacent pixels in the plain Lena and in the ciphered Lena.

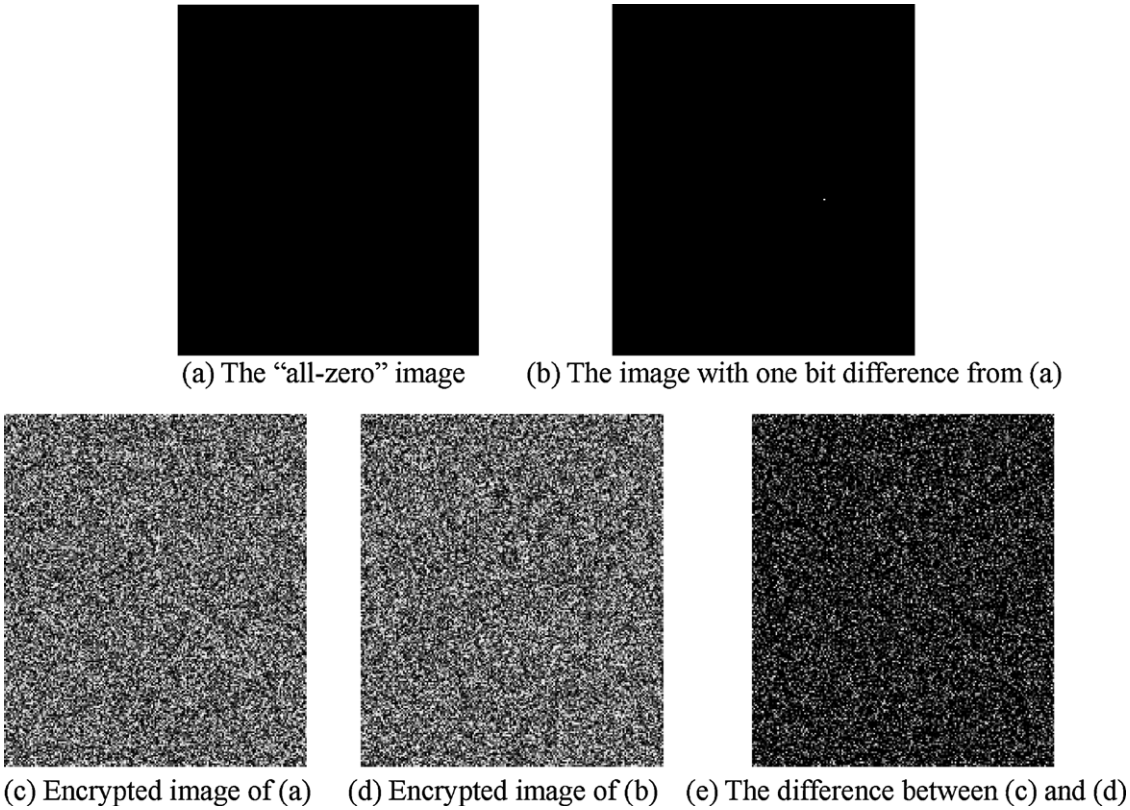

Fig. 10. The encryption results and difference of two images with one bit difference.

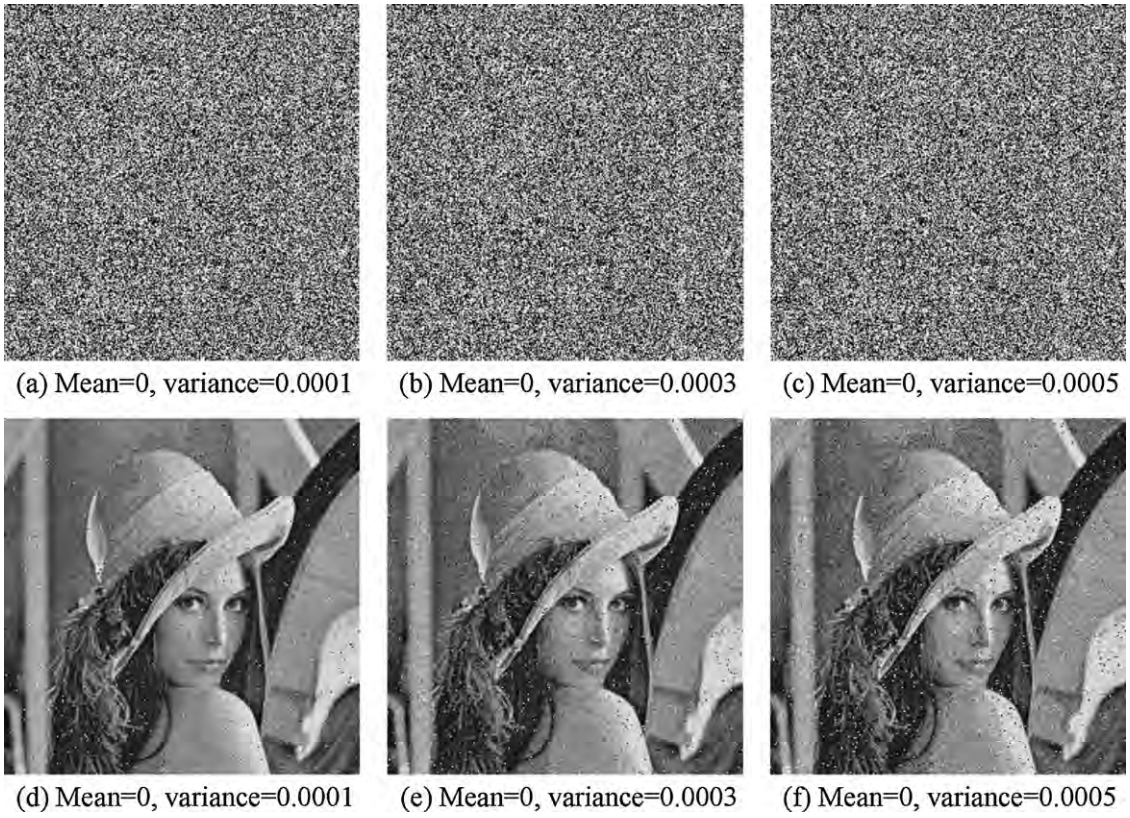

Fig. 11. The encrypted images with noise and the decrypted images.

transmitted electronically from the transmitter to the receiver. The error propagation phenomenon implies that errors in the encrypted image will lead to the errors in the decrypted image.

Some of the commonly used cryptosystems are very sensitive to noise. A small change in the encrypted image may induce a strong distortion in the decrypted image, which does not allow one to recuperate the original image. For example, the cryptosystem described in Ref. [34] also suffers from this drawback; an error in one pixel and one looses the original image completely. A good algorithm can de designed to avoid the propagation error in the decrypted image. For example, Awad et al. perturb the chaotic value using a maximal length linear feedback shift register (LFSR), then the permuted blocks are independent [33].

Our cryptosystem is robust against noise, as we firstly diffuse the pixels by permuting the rows and columns respectively, and then confuse each pixel by the DNA complementary rule. In the decryption process, the pixels changed by the noise will not propagate in the decrypted image, i.e. the domino effect does not exist.

We prefer to use the white Gaussian noise because it provides a reasonable assumption for the unavoidable randomness of the real physical channel, and the random numbers of white Gaussian noise are uniformly distributed.

Fig. 11 shows the encrypted Lena image that is affected by white Gaussian noise with different variances, and their decrypted ones. Table 6 shows the mean value of the correlation coefficients, NPCR and UACI of the noisy decrypted and the original Lena image, although the NPCR > 99% and the UACI > 28%, the noisy decrypted images can still maintain the overall information contained in the original image by visual inspection, and their correlation is still high.

Table 6
Correlation, NPCR and UACI between original and decrypted Lena under noise.

Image	Correlation	NPCR (%)	UACI (%)
Figs. 11(d) and 3(a)	0.9584	99.2094	28.4417
Figs. 11(e) and 3(a)	0.9198	99.6125	28.6448
Figs. 11(f) and 3(a)	0.9079	99.6155	28.8007

6. Conclusion

In this paper, we proposed a novel confusion and diffusion method for image encryption algorithm. We use the MD5 hash to ensure the initial conditions of the chaotic maps change with the plain image. After the rows and columns of the original image being diffused by arrays generated by PWLCM system, each pixel is encoded into four nucleotides by DNA coding. Then we use the complementary rule of DNA to transform each nucleotide into its base pair for random time(s), which is the pseudo-random sequence generated by Chebyshev chaotic maps. Experiment results and security analysis show that the scheme can not only achieve good encryption result, but also the key space is large enough to resist against common attacks.

Acknowledgements

The research is supported by the National Natural Science Foundation of China (Nos. 61173183, 60973152, and 60573172), the Superior University doctor subject special scientific research foundation of China (No. 20070141014), the National Natural Science Foundation of Liaoning province (No. 20082165), the Minority Nationality Technology Talent Cultivation Plan of Xinjiang (No. 201123116).

References

[1] C.E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28–4 (1949) 656–715.

[2] Q. Guo, Z.J. Liu, S.T. Liu, Color image encryption by using Arnold and discrete fractional random transforms in IHS space, Optics and Lasers in Engineering 48 (12) (2010) 1174–1181.
[3] W. Chen, C. Quan, C.J. Tay, Optical color image encryption based on Arnold transform and interference method, Optics Communications 282 (18) (2009) 3680–3685.
[4] G.D. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognition Letters 31 (5) (2010) 347–354.
[5] D. Xiao, X.F. Liao, P.C. Wei, Analysis and improvement of a chaos-based image encryption algorithm, Chaos, Solitons & Fractals 40 (5) (2009) 2191–2199.
[6] E. Lega, M. Guzzo, C. Froeschlé, Detection of Arnold diffusion in Hamiltonian systems, Physica D 182 (3–4) (2003) 179–187.
[7] G.R. Chen, Y.B. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.
[8] B. Alatas, E. Akin, A.B. Ozer, Chaos embedded particle swarm optimization algorithms, Chaos, Solitons & Fractals 40 (4) (2009) 1715–1734.
[9] T. Xiang, X.F. Liao, K.W. Wong, An improved particle swarm optimization algorithm combined with piecewise linear chaotic map, Applied Mathematics and Computation 190 (2) (2007) 1637–1645.
[10] F. Zheng, X.J. Tian, J.Y. Song, X.Y. Li, Pseudo-random sequence generator based on the generalized Henon map, The Journal of China Universities of Posts and Telecommunications 15 (3) (2008) 64–68.
[11] S. Mazloom, A.M. Eftekhari-Moghadam., Color image encryption based on coupled nonlinear chaotic map, Chaos, Solitons & Fractals 42 (3) (2009) 1745–1754.
[12] J.M. Liu, S.S. Qiu, F. Xiang, H.J. Xiao, A cryptosystem based on multi-chaotic maps, in: International Symposiums on Information Processing, 2008, pp. 740–743.
[13] V. Patidar, N.K. Pareek, K.K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation 14 (7) (2009) 3056–3075.
[14] S. Mazloom, A.M. Eftekhari-Moghadam, Color image encryption based on coupled nonlinear chaotic map, Chaos, Solitons & Fractals 42 (3) (2009) 1745–1754.
[15] D. Dutta, J.K. Bhattacharjee, Period adding bifurcation in a logistic map with memory, Physica D: Nonlinear Phenomena 237 (23) (2008) 3153–3158.
[16] A.N. Pisarchik, M. Zanin, Image encryption with chaotically coupled chaotic maps, Physica D: Nonlinear Phenomena 237 (20) (2008) 2638–2648.
[17] D. Dutta, J.K. Bhattacharjee, Period adding bifurcation in a logistic map with memory, Physica D 237 (23) (2008) 3153–3158.
[18] C.Q. Li, S.J. Li, G. Alvarez, G.R. Chen, K.T. Lo, Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations, Physics Letters A 369 (1–2) (2007) 23–30.
[19] A. Awad, S.E. Assad, Q.X. Wang, C. Vlădeanu, B. Bakhache, Comparative study of 1-D chaotic generators for digital data encryption, IAENG International Journal of Computer Science 35 (4) (2008) 483–488.
[20] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, Z. Hassan, A novel scheme for image encryption based on 2D piecewise chaotic maps, Optics Communications 283 (17) (2010) 3259–3266.
[21] T. Head, G. Rozenberg, R.S. Bladergroen, C.K.D. Breek, P.H.M. Lommerse, H.P. Spaink, Computing with DNA by operating on plasmids, Biosystems 57 (2) (2000) 87–93.
[22] X.D. Zheng, J. Xu, W. Li Parallel, DNA arithmetic operation based on n-moduli set, Applied Mathematics and Computation 212 (1) (2009) 177–184.
[23] A. Gehani, T.H. LaBean, J.H. Reif, DNA-based cryptography. DIMACS series in discrete mathematics, Theoretical Computer Science 54 (2000) 233–249.
[24] Q. Zhang, L. Guo, X.P. Wei, Image encryption using DNA addition combining with chaotic maps, Mathematical and Computer Modeling 52 (11–12) (2010) 2028–2035.
[25] Q. Zhang, Q. Wang, X.P. Wei, A novel image encryption scheme based on DNA coding and multi-chaotic maps, Advanced Science Letters 3 (4) (2010) 447–451 (Cuba, Logistic).
[26] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, C.H. Huang, Data hiding methods based upon DNA sequences, Information Sciences 180 (11) (2010) 2196–2208.
[27] H.J. Liu, X.Y. Wang, Color image encryption based on one-time keys and robust chaotic maps, Computers and Mathematics with Applications 59 (10) (2010) 3320–3327.
[28] R. Rhouma, S. Belghith, Cryptanalysis of a new image encryption algorithm based on hyper-chaos, Physics Letters A 372 (38) (2008) 5973–5978.
[29] A. Baranovsky, D. Daems, Design of one-dimensional chaotic maps with prescribed statistical properties, International Journal of Bifurcation and Chaos 5 (6) (1995) 1585–1598.
[30] D. Xiao, X.F. Liao, S.J. Deng, Parallel keyed hash function construction based on chaotic maps, Physics Letters A 372 (26) (2008) 4682–4688.
[31] G. Alvarez, S.J. Li, Some basic cryptographic requirements for chaos-based cryptosystem, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.
[32] R. Rhouma, S. Meherzi, S. Belghith, OCML-based colour image encryption, Chaos, Solitons & Fractals 40 (1) (2009) 309–318.
[33] A. Awad, D. Awad, Efficient image chaotic encryption algorithm with no propagation error, ETRI Journal 32 (5) (2010) 774–783.
[34] A.N. Pisarchik, N.J. Flores-Carmona, M. Carpio-Valadez, Encryption and decryption of images with chaotic map lattices, Chaos 16 (3) (2006), 033118-1/6.