Journal of Computers Vol. 29 No. 3, 2018, pp. 43-55
doi:10.3966/199115992018062903005

Bit Image Encryption Algorithm Based on Hyper Chaos and DNA Sequence

Ye Liu*, Tao Lin, Jun Wang, Hong-Mei Yuan

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
liuye@ncu.edu.cn, {lintao3611, wjncdx}@163.com, evelyn.yuanhm@hotmail.com

Received 04 December 2016, Revised 19 May 2017, Accepted 29 June 2017

Abstract. An image encryption algorithm based on hyper-chaos system and DNA plane is proposed. According to the characteristic that DNA located in high positions carries more than 94% information of image while DNA located in low positions carries less than 6% information, DNA plane is proposed. The corresponding positions of the DNA plane matrixes are rearranged by the described arrangement method to improve the performance of resisting noise attack. Simulation results show that the ability of resisting noise attack in balance sufficient plaintext sensitivity is improved for the presented bit image encryption algorithm and the described bit image encryption algorithm can resist the existing attacks.

Keywords: chaotic system, DNA bit matrix, DNA sequence, image encryption

1 Introduction

The traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) cannot meet the demand of image encryption because of the high correlation between adjacent pixels, redundancy and special storage format in an image. Thanks to the good properties of chaotic system such as low computational complexity, ergodicity, determinacy and high sensitivity to initial conditions and system parameters, the chaos system are very suitable for digital image encryption.

The chaos systems are often applied in the generation of pseudo-random sequence to confuse and diffuse the pixels [1]. In 1989, Matthews [2] proposed the first chaos-based image encryption algorithm. Since then, many chaos-based image encryption algorithms were described [3-7]. The classical chaos-based image encryption algorithms are partitioned into two stages: permutation and diffusion. Actually, permutation and diffusion are often combined in consideration of better encryption effect and higher security. Hyper-chaos systems are expected to be more valuable in image encryption algorithms because the hyper-chaos system has more than one positive Lyapunov exponents, more parameters and more complex dynamics characteristics. Hence, numerous hyper-chaos based image encryption algorithms have been presented by some researchers [8-10].

With the development of DNA computing, DNA cryptography is fueled as a new cryptography field. Owing to the outstanding features of DNA computing such as massive parallelism, huge storage and ultra-low power consumption [11], DNA cryptography has been taken more attention by some scholars [12]. However, DNA computing possesses expensive laboratory equipment and complex biological operations, which limits the scope of use in practice. Therefore, some researchers suggested that the realization of information encryption should depend on the basic theory of DNA computing, which was completely divorced from biological experiments. Recently, some image encryption algorithms based on DNA sequences and chaotic systems have been proposed by the researchers. In 2010, an image encryption algorithm based on chaotic system and DNA ADD operation was proposed [13], in which DNA ADD operation was designed and the chaotic system was combined with the DNA sequence. In 2012, an image encryption algorithm based on DNA sequence and hyper-chaos was presented. It has an

* Corresponding Author

excellent performance in information entropy and correlation of adjacent pixels, while without the feature to resist differential attack. Liu et al. [14] put forwarded an image encryption algorithm based on DNA complementary rules and chaotic mapping. A new DNA complementary rule was proposed. Moreover, MD5 of the image was exploited to influence the initial value of the chaotic system in order to achieve the goal of resisting the differential attack. In 2014, Huang et al. [15] suggested an algorithm based on hyper-chaos and DNA sequence. A new permutation method was proposed. Compared with the traditional permutation method, it is time-efficient. Rasul E et al. [16] described an image encryption algorithm based on genetic algorithms and DNA sequence. The algorithm achieved the best mask that is compatible with plain images by generating the offspring, mutation and measuring the entropy of DNA masks circularly. The information entropy of the encrypted image is very close to the information entropy of the ideal random image.

A bit image encryption algorithm, which is based on hyper chaos and DNA sequence, is designed. It is known to us that the capability of resisting noise attack is inversely related to the plaintext sensitivity. Therefore, most image encryption algorithms are weak against the noise attack if they have high plaintext sensitivity. To overcome this weakness, DNA plane is put forward in this encryption scheme. The DNA matrixes are divided into four DNA planes and different DNA plane carry unequal information ratio. According to the property that DNA located in high location carries more than 94% information of the image while DNA located in low location carries less than 6% information of the image, the change of DNA located in low locations has little effect on the decrypted image. Hence, the ability to resist noise attack is enhanced by the rearrangement operations of the DNA plane matrixes. Moreover, the initial value of chaotic system is associated with plain image for the resistance to known-plaintext attack and chosen-plaintext attack. As a result, we can make a balance between the plaintext sensitivity and the capability of resisting noise attack. The rest of the paper is organized as follows: Section 2 introduces the corresponding chaotic systems and DNA plane matrixes; Section 3 describes the description of the proposed algorithm; Section 4 shows the experimental results and performance analysis; the conclusion is given in Section 5.

2 Preliminaries

2.1 Chaotic System

2.1.1 LTS

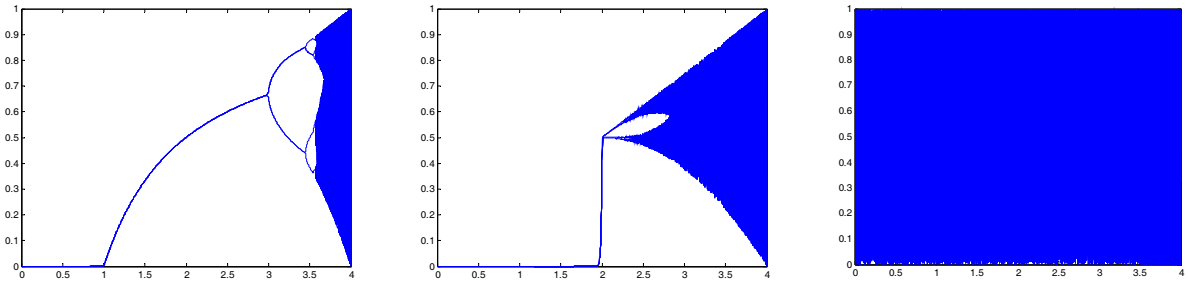
In 2014, Zhou proposed a simple and effective chaotic system combination of two existing 1D chaotic systems in [17]. The combined chaotic system is able to produce many new 1D chaotic systems with larger chaotic ranges and better chaotic behaviors compared with their seed maps. It is described as:

$$X_{n+1} = \left(F\left(a, X_n\right) + G\left(b, X_n\right)\right) \bmod 1 . \tag{1}$$

where $F\left(a, X_n\right)$ and $G\left(b, X_n\right)$ are two 1D chaotic systems, respectively. a and b are the systems parameters. The Logistic and Tent maps are utilized as seed maps to structure a new 1D chaotic system. The definition is described by the following equation.

$$X_{n+1} = \begin{cases} \left(rX_n\left(1 - X_n\right) + \left(4 - r\right)X_n / 2\right) \bmod 1 & X_i < 0.5 \\ \left(rX_n\left(1 - X_n\right) + \left(4 - r\right)\left(1 - X_n\right) / 2\right) \bmod 1 & X_i \geq 0.5 \end{cases} . \tag{2}$$

The system is called the Logistic-Tent system (LTS). The bifurcation diagrams of these maps are shown in Fig. 1. From Fig. 1, it is concluded that LTS has larger chaotic ranges and better chaotic behaviors than Logistic and Tent maps.



(a) is Logistic map (b) is Tent map (c) is LTS

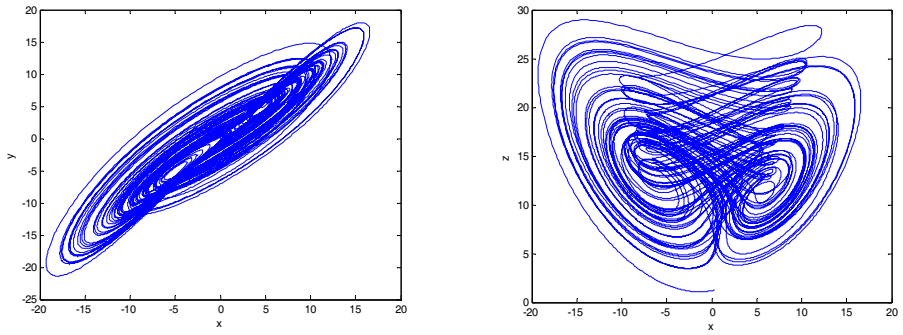
Fig. 1. The bifurcation diagrams of maps

2.1.2 Chen's Hyper Chaos

Chen's hyper-chaos system has more than one positive Lyapunov exponents. It has a more complex chaotic behavior, better randomness and higher uncertainty of chaotic systems than other chaos systems. It is described as:

$$\begin{cases} \dot{x} = -ax + ay \\ \dot{y} = -xz + dx + cy - q \\ \dot{z} = xy - bz \\ \dot{q} = x + k \end{cases} . \tag{3}$$

where a , b , c , d and k are system parameters. When $a = 36$, $b = 3$, $c = 28$, $d = -16$ and $-0.7 \le k \le 0.7$, the Chen's hyper-chaos system is in chaotic state [18]. Assuming that $k = 0.2$, Lyapunov exponents are calculated as: $\lambda_1 = 1.552$, $\lambda_2 = 0.023$, $\lambda_3 = 0$ and $\lambda_4 = -12.573$. The attractor of Chen's hyper-chaos system is shown in Fig. 2. The equations are taken by four-order Runge-Kutta method to obtain three sequences. The step of the Runge-Kutta is set to 0.001.



(a) x-y planes (b) x-z planes

Fig. 2. Attractors of Chen's hyper-chaotic system

2.2 DNA Plane

The grayscale of the original image $P_{M \times N}$ is 2^l . Each pixel value is expressed in binary form. The formula is as:

$$P(i,j) = A_l(i,j) \times 2^{l-1} + A_{l-1}(i,j) \times 2^{l-2} + \cdots A_x(i,j) \times 2^{x-1} + \cdots + A_1(i,j) \times 2^0 . \tag{4}$$

where $i \in (1,m)$, $j \in (1,n)$. $A_x(i,j)$ represents the binary value of pixel. A bit plane is constituted by the binary bits in the same position for all pixels. An image, whose grayscale is 2^l , has l bit planes and each

bit plane carries different information of the image. The formula calculating the information ratio of different bit plane carries within an image is given as follow:

$$p(i) = 2^{i-1} \Big/ \left(\sum_{i=1}^{8} 2^{i-1} \right), \quad i \in (1,8) \ . \tag{5}$$

The results are shown in Table 1. One pixel of an image, whose grayscale is 256, could be encoded in four DNA bases. DNA bases in the same position for all pixels form a DNA plane. And the information of the image DNA plane carries is equal to the information that two bit planes carries. The results are shown in Table 2.

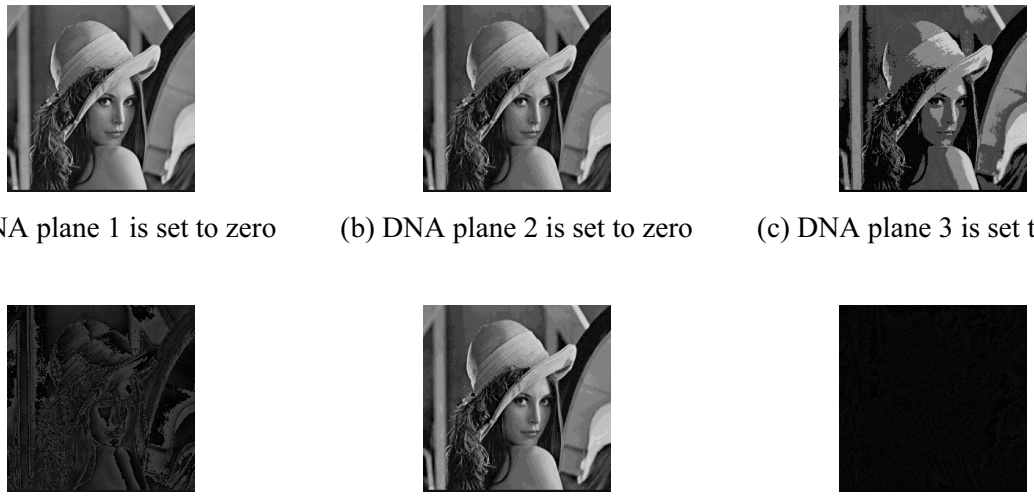
Table 1. The information ratio of different bit planes

Low four bit planes (%)				High four bit planes (%)			
1	2	3	4	5	6	7	8
0.39	0.78	1.57	3.14	6.27	12.55	25.10	50.20

Table 2. The information ratio of different DNA planes

1 (%)	2 (%)	3 (%)	4 (%)
1.17	4.71	18.82	75.30

From Table 2, it is observed that DNA planes located in high positions (DNA plane 3 and DNA plane 4) carry more than 94 percents of the information of the image while DNA planes located in low positions (DNA plane 1 and DNA plane 2) only carry less than 6 percents. The corresponding images, where different DNA plane is set to zero, are shown in Fig. 3. The image that DNA plane 1 is set to zero is shown as Fig. 3(a), DNA plane 2 as Fig. 3(b), DNA plane 3 as Fig. 3(c) and DNA plane 4 as Fig. 3(d), respectively. The image that both DNA plane 1 and 2 are set to zero is shown as Fig. 3(e), DNA plane 3 and 4 as Fig. 3(f). It is observed that DNA located in high positions has greater effect while DNA located in low positions has a very small effect.



(a) DNA plane 1 is set to zero (b) DNA plane 2 is set to zero (c) DNA plane 3 is set to zero

(d) DNA plane 4 is set to zero (e) DNA plane 1 and DNA plane 2 are set to zero (f) DNA plane 3 and DNA plane 4 are set to zero

Fig. 3. The images that different DNA planes are set to zero

2.3 DNA Sequence

DNA sequence contains four nucleic acid bases, which are A (adenine), G (guanine), C (cytosine) and T (thymine). A and T, G and C are complementary pairs. Similarly, 00 and 11, 01 and 10 are also complementary pairs. Thus, 00, 01, 10 and 11 can be encoded into four DNA bases A, G, C and T. There

are $4!=24$ kinds of encoding rules. But only 8 kinds meet the complementary rules. For example, a pixel value is 135, a DNA sequence [CAGT] can be obtained using DNA encoding rule 1. The pixel value could be obtained by the same DNA decoding rule. DNA encoding rule 1 is utilized in the proposed algorithm. The DNA encoding rules are shown in Table 3.

Table 3. DNA encoding rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

With the development of DNA computing, bio-computing and algebra operation based on DNA sequences were proposed, such as addition operation. There are 8 kinds of DNA ADD operations corresponding to the DNA encoding rules. One type of addition operation is shown in Table 4.

Table 4. One kind of DNA ADD operation

+	T	A	C	G
T	C	T	G	A
A	T	A	C	G
C	G	C	A	T
G	A	G	T	C

3 The Description of the Proposed Algorithm

3.1 Chaotic Sequences

The former 100 values of every chaotic sequence are discarded to avoid harmful effect of transitional procedure. Chaotic sequences generated by Chen's hyper-chaotic system are pretreated by Eq. (6).

$$S(i)=\text{floor}\left(\text{mod}\left(s(i)\times 10\,\text{^}\,14,256\right)\right). \tag{6}$$

The elements in $S(i)$ range from 0 to 255, where $\text{mod}(a,b)$ returns the remainder after division a/b. $\text{floor}(a)$ rounds the elements of a to the nearest integer towards minus infinity. $S(i)$ is decomposed into DNA Matrix to confuse and diffuse the plain image DNA matrix. Similarly, chaotic sequences generated by LTS are pretreated by Eq. (7).

$$X(i)=\text{floor}\left(\text{mod}\left(x(i)\times 10\,\text{^}\,14,24\right)\right)+1. \tag{7}$$

where $X(i)$ is range from 0 to 24, and $X(i)$ is used to choose the arrangement methods.

3.2 Method of Arrangement

There are four DNA plane matrixes used in the proposed algorithm. Assuming that the DNA plane matrixes are denoted by $B1$, $B2$, $B3$ and $B4$, respectively. There are $4!=24$ kinds of arrangement methods. Then the arrangement methods are chosen in accordance with the values of chaotic sequence generated by LTS. Owing to the one-to-one relationship between the values of chaotic sequence and arrangement methods, there are $24!=6.2045\times 10^{23}$ kinds of relationships. Hence, the presented bit image encryption algorithm has a considerable scope of options. While only one corresponding relation is applied in our bit image encryption algorithm. For example, assuming that C is a DNA matrix. When $X(n)=1,\ C(i,4\times j-3)=B2(i,j),\ C(i,4\times j-2)=B1(i,j),\ C(i,4\times j-1)=B4(i,j),\ C(i,4\times j)=B3(i,j).$

3.3 Confusion Algorithm

Confusion algorithm used in proposed algorithm was put forward in [15]. The detailed procedure is as follow: S_1 is used for row circular permutation while S_2 for column circular. For example, in the first row, the number of units circularly shifted to the right is equal to the value of $s_1(1)$; in the second row, the number of units circularly shifted to the right is equal to the value of $s_1(2)$; the remaining rows are permutated by the same approach. Similarly, for the column permutation, the *i*th column is circularly shifted to the bottom by $s_2(i)$ units. Hence, the proposed confusion algorithm does not have to index the chaotic sequences. The security of the provided bit image encryption algorithm is sufficient by circularly shifting the units in rows and columns. Thus, it could save much time.

3.4 Encryption Process

$P_{M\times N}$ is plain image. x_0 is the initial value of LTS. $s_1(1)$, $s_2(1)$, $s_3(1)$ and $s_4(1)$ are the initial values of Chen's hyper-chaotic system. The encryption steps are shown as follow:

Step 1. Input the plain image $P_{M\times N}$ and calculate the value of total pixels within the plain image sum. A value r is obtained by Eq. (8).

$$r = \mathrm{mod}(\mathrm{sum}, 256)/256 , \tag{8}$$

Step 2. Change the initial values of chaotic systems as follows:

$$x(1) = \mathrm{mod}(x_0 + r, 1) , \tag{9}$$

$$s_k(1) = \mathrm{mod}(s_k(1) + r, 1) , \quad k = 1,2,3,4 . \tag{10}$$

Step 3. Sequence X can be obtained by performing Eq. (2) with the initial value $x(1)$. Chaotic sequences S_1, S_2, S_3 and S_4 are achieved by iterating the Chen's hyper chaos system as described in Eq. (3) with the initial values s_1, s_2, s_3 and s_4. Confuse the plain image $P_{M\times N}$ with Sequences S_1 and S_2 to get Matrix $P'_{M\times N}$.

Step 4. Encode $P'_{M\times N}$ to obtain DNA Matrix $B_{m\times 4n}$ by DNA encoding rule 3.

Step 5. Separate $B_{m\times 4n}$ into DNA plane matrixes $B1_{m\times n}$, $B2_{m\times n}$, $B3_{m\times n}$ and $B4_{m\times n}$ in order.

Step 6. Encode Sequences S_1, S_2, S_3 and S_4 to obtain DNA Matrixes $C1_{m\times n}$, $C2_{m\times n}$, $C3_{m\times n}$ and $C4_{m\times n}$. Then they are taken DNA ADD operation with the DNA plane matrixes $B1_{m\times n}$, $B2_{m\times n}$, $B3_{m\times n}$ and $B4_{m\times n}$, respectively. Finally, DNA Matrixes $B1'_{m\times n}$, $B2'_{m\times n}$, $B3'_{m\times n}$ and $B4'_{m\times n}$ are generated.

Step 7. DNA Matrix $C_{m\times 4n}$ is obtained by performing the method of arrangement proposed in Section 3.2. And Sequence X is obtained in Step 3.

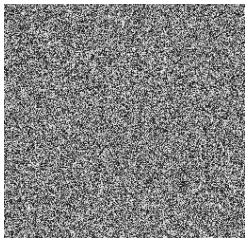
Step 8. Decode DNA Matrix $C_{m\times 4n}$ into cipher image $C_{m\times n}$ by DNA decoding rules.

Decryption steps are completely the reverse process of encryption steps.

4 Simulation Results and Analyses

The gray image 256×256 "Lena" is used to test the performance of the encryption scheme and MATLAB 2012a on a PC with an Intel Core i7, 2GHz CPU, 8 GB memory with a Windows 7 is utilized. The secrets are $x_0 = 0.4536$, $s_1(1) = 0.32$, $s_2(1) = -0.43$, $s_3(1) = 1.256$, $s_4(1) = 1$ and $\mathrm{sum} = 6407609$. Plain image and cipher image are shown as Fig. 4.

(a) Plain image



(b) Cipher image

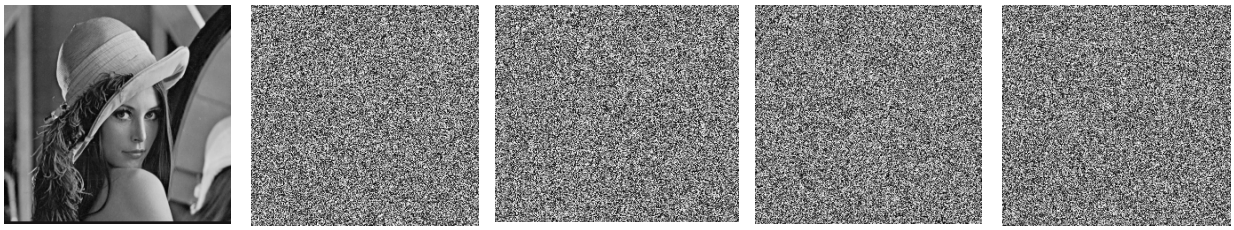
Fig. 4. Plain image and cipher image

4.1 Key Space

There are totally six secret keys. x_0 is a random number and sum is a fixed value for one image, the others are the initial values of chaos systems. Suppose that the precision of the initial values of Chen's hyper-chaotic system is 10^{-14}, the key space is greater than 2^{100} ($10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{56} > 2^{100}$). Therefore, the secret key space is large enough to resist exhaustive attack.

4.2 Key Sensitivity

A secure image encryption scheme should be sensitive to the keys, which means that a slight change in the secret keys would result in a completely different decrypted image. Some experiments are conducted to detect the key sensitivity. The encrypted image was decrypted by the secret keys among which only one is changed slightly while other keys unchanged. The image decrypted by the correct keys is shown in Fig. 5(a). The image decrypted by $s_1(1) = 0.32 + 10^{-14}$ is shown in Fig. 5(b). Similarly, the secret keys $s_2(1)$, $s_3(1)$ and $s_4(1)$ are respectively added 10^{-14} to decrypt the cipher image and the corresponding decrypted images are shown in Fig. 5(c), Fig. 5(d) and Fig. 5(e). Fig. 5(b), (c), (d) and (e) are found to be very different from the plain image, which indicates that the encrypted image could not be decrypted correctly even if any one of the keys changes slightly. Therefore, the algorithm owns certain sensitivity to the secret keys.

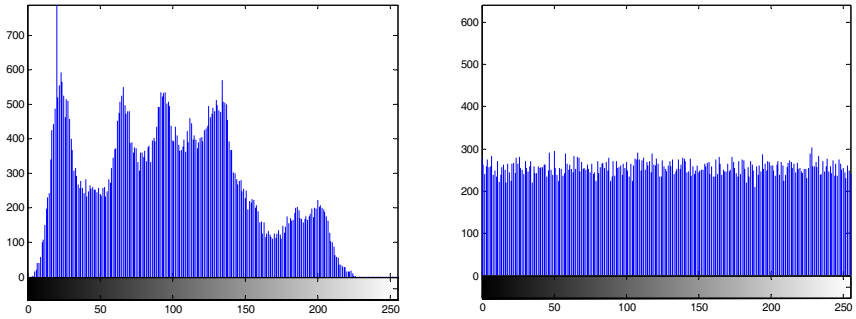


(a) correct keys (b) incorrect $s_1(1)$ (c) incorrect $s_2(1)$ (d) incorrect $s_3(1)$ (e) incorrect $s_4(1)$

Fig. 5. The image decrypted by the different keys

4.3 Histogram

The statistical characteristics of digital image could be expressed visually in histogram. Shannon proposed that the attackers could utilize statistical attack to break many cryptosystems. An effective image encryption system should significantly alter the inherently statistical properties of image. The histograms of the plain image and cipher image of Lena are shown in Fig. 6 (a) and Fig. (b). The figures are plotted by pixel values on the horizontal axis and the frequency of the corresponding pixel value on the vertical. Hence, the distribution of each gray value is shown in visual. By comparing their histograms, it could be found that the histogram of the encrypted image is relatively uniform. Thus, the proposed algorithm could effectively resist the statistical analysis.



(a) Plain image (b) Cipher image

Fig. 6. Histograms of the plain image and cipher image

4.4 Correlation Coefficients

There is a high correlation between two adjacent pixels within a plain image, which makes the algorithm easy to be attacked. It is necessary for a good image encryption algorithm to disrupt the correlation of adjacent pixels. And the strength of the linear relationship between adjacent pixels within an image could be quantitatively measured by its correlation coefficients. 8000 pairs of adjacent pixels (in vertical, horizontal and diagonal directions) are randomly selected from the plain and cipher images, respectively. The correlation coefficients of two adjacent pixels are calculated according to the following formula:

$$r_{xy} = \frac{\left|\operatorname{cov}(x,y)\right|}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{11}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \tag{12}$$

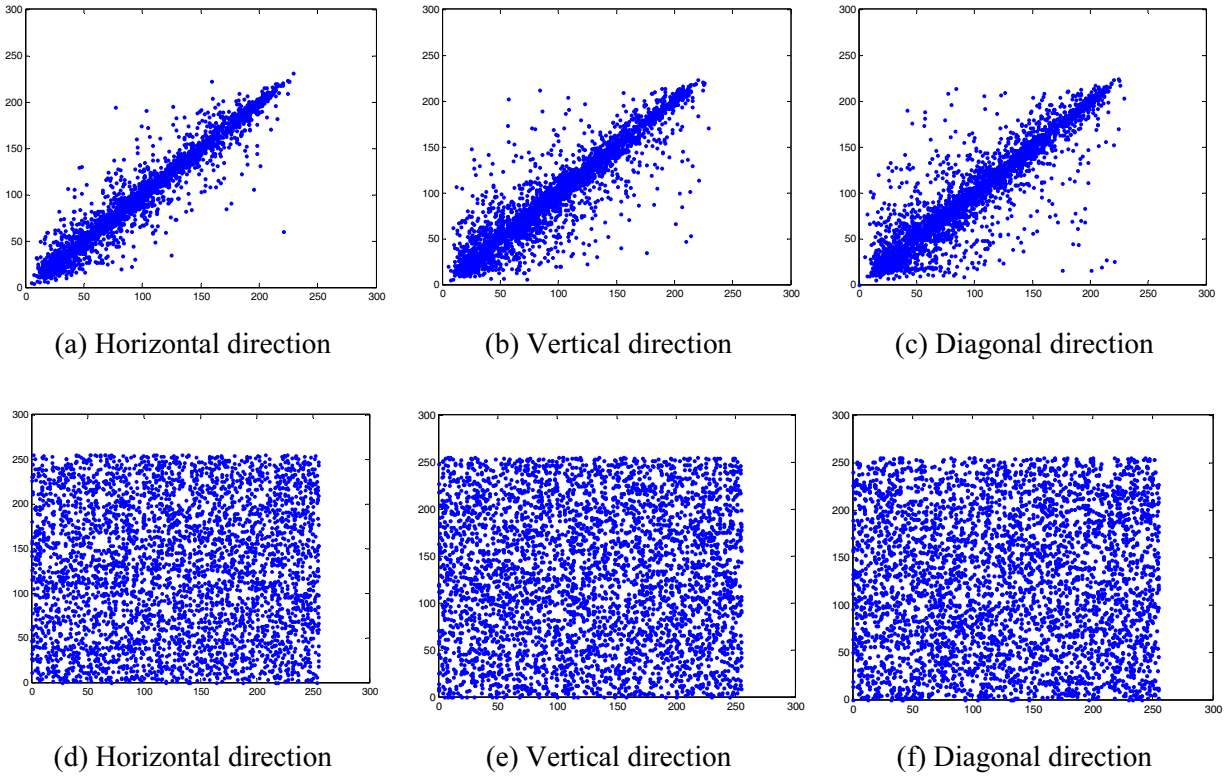
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{13}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2. \tag{14}$$

where x and y are the gray values of two adjacent pixels, $\operatorname{cov}(x,y)$ is covariance, $D(x)$ is variance and $E(x)$ is mean. The results are depicted in Table 5. It can be seen that the correlation coefficients of our encryption scheme is acceptable, though not necessarily the best. The correlation of the plain and cipher images are shown in Fig. 7. It is observed that the correlation of the image has been disrupted and the correlation coefficients of the encrypted image are very close to zero. It shows that the algorithm has weakened the strong correlation of the original image, which creates a difficult approach to useful information for attackers through the correlation of the cipher image.

Table 5. Correlation coefficients of the plain and cipher images

	Horizontal	Diagonal	Vertical
Plain image	0.9709	0.9392	0.9157
Cipher image	0.0090	0.0091	0.0098
Ref. [15]	0.0166	0.0032	0.0796
Ref. [20]	0.0008	0.0008	0.0001
Ref. [21]	-0.0044	-0.0126	0.0115
Ref. [22]	-0.0098	0.0034	0.0050
Ref. [23]	0.0021	0.0020	0.0147



(a) Horizontal direction (b) Vertical direction (c) Diagonal direction

(d) Horizontal direction (e) Vertical direction (f) Diagonal direction

Fig. 7. Correlation of adjacent pixels in the plain image and cipher image

4.5 Information Entropy

Entropy is one of the most important features in the randomness. The value of information entropy for an ideal random image is 8 bits according to Eq. (15).

$$H(m)=\sum_{i=0}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)}. \tag{15}$$

where $p(m_i)$ expresses the probability of symbol m. For a true random source emitting symbols with equal probability, the information entropy is 8 bits. For an ideally random 256 gray-scale image, its information entropy is 8 bits as. Actually, given that a practical information source seldom generates random messages, the information entropy of a meaningful image is usually less than 8 bits. Therefore, the security of the image cryptosystem is higher if the score of the information entropy is much closer to 8 bits. In order to quantificationally indicate the uncertainty degree of the encrypted image, the information entropy of the encrypted image is calculated over 100 times with different keys. The results are shown in Table 6. Similar experiments are performed to make a comparison with our scheme and Table 7 has depicted the corresponding results. It is observed that the information entropy values of the encrypted images are very close to 8bits. Hence, the encrypted images are close to ideal random images.

Table 6. Information entropy of the plain and cipher images

	Plain image	Cipher image		
		Max	Min	Average
Entropy(bit)	7.5031	7.9977	7.9966	7.9972

Table 7. Information entropy of the cipher images

Ours	Ref. [15]	Ref. [20]	Ref. [21]	Ref. [22]	Ref. [23]
7.9972	7.9895	7.9971	7.9969	7.9970	7.9970

4.6 Plaintext Sensitivity

The attackers can obtain some useful information of the plain images through analyzing the relations between two cipher images whose plain images are different merely in one pixel. In conclusion, a good image encryption algorithm should be sensitive to plain images i.e. two encrypted images are completely different even though only one pixel is different between the two plain images. Number of pixels change rate (NPCR) and unified average changing intensity (UACI) are exploited to measure this ability. The closer the values of NPCR are to 100% and the values of UACI to 33.3%, the better the encryption performance is [18-19]. The definitions are as follow:

$$D(i,j)=\begin{cases}0, & T_1(i,j)=T_2(i,j)\\ 1, & T_1(i,j)\neq T_2(i,j)\end{cases}, \tag{16}$$

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}D(i,j)}{W\times H}\times 100\%, \tag{17}$$

$$\mathrm{UACI}=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}\left|T_1(i,j)-T_2(i,j)\right|}{255W\times H}\times 100\%. \tag{18}$$

where M and N represent the width and the height of the image, respectively. T_1 and T_2 are two cipher images.

The results are tabulated in Table 8. It is found that the values of NPCR are greater than 99.60% and the values of UACI are very close to 33.3%. Thus, the provided bit image encryption algorithm is sensitive to the plaintext and it can resist differential attack. Moreover, the NPCR and UACI of some other image encryptions are tested in this section and the corresponding results are exhibited in Table 8. Compared with other image encryption schemes, the proposed image encryption scheme performs better in NPCR and UACI.

Table 8. NPCR and UACI of two cipher images

	Ours	Ref. [15]	Ref. [20]	Ref. [21]	Ref. [22]	Ref. [23]
NPCR(%)	99.6216	99.6521	99.6553	99.5559	99.5880	99.6063
UACI(%)	33.3477	33.3438	33.3377	33.2471	33.5183	33.4118

4.7 Noise Attack

Because one pixel of the image can be encoded into four DNA bases, it is possible to change four pixel values of the decrypted image for the general image encryption schemes when one pixel is altered within the cipher image. The DNA bit matrix is exploited in the presented bit image encryption algorithm for the reduction of the change. And each four DNA bases of ciphertext are composed of four DNA bases of plaintext on corresponding locations. According to the property that DNA located in high location carries more than 94% information of the image while DNA located in low location carries less than 6% information of the image, the change of DNA located in low locations has little effect on the decrypted image. If one pixel of the cipher image is changed, one pixel or none of the decrypted image had big change, which weakens the influence of the noise. In order to verify the ability of resisting noise attack, some experiments are conducted. Firstly, salt and pepper noises with different densities are added to the cipher images, respectively. Then, the decrypted images are reconstructed from the noisy cipher images. The decrypted images of the proposed algorithm are shown in Fig. 8 a1-e3; Fig. 8 b1, b2 and b3 are the decrypted images of [15]; Fig. 8 c1, c2 and c3 are the decrypted images of [20]; Fig. 8 d1, d2 and d3 are the decrypted images of [21]; Fig. 8 e1, e2 and e3 are the decrypted images of [22]; Fig. 8 e1, e2 and e3 are the decrypted images of [23], respectively. It is can be seen that the decrypted images of our encryption scheme minimally affected by the added noise. To quantificationally depict the degree of influence, PSNR are introduced in this section. The peak signal-to-noise ratio (PSNR) between plain

image and decrypted one is regarded as a standard to analyze the robustness and can be calculated by Eq. (19) and (20).

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (a(i,j) - b(i,j))^2 , \quad \textbf{(19)}$$

$$PSNR = 10 \log_{10} (\frac{I^2_{MAX}}{MSE}) . \quad \textbf{(20)}$$

where $M \times N$ is the size of the image, a and b are plain image and decrypted image. Respectively, the larger the value of PSNR, the stronger the ability to resist noise attacks. Table 9 compiles the PSNR comparisons between our cryptosystem and the algorithms of [15, 20-23]. It shows that the PSNR of the described encryption scheme achieves the best scores. Therefore, our image encryption scheme has the best robustness.

As shown in Table 8, the NPCR scores of [15, 20-23] are very close 99.60% i.e. the capability of these encryption systems is acceptable in resisting plaintext attack. As we all known, there is a negative correlation between the plaintext sensitivity and the resistance to noise attack for image encryption schemes generally. And it is proved by the simulation result shown in Figure 8 and Table 9, in which the robustness of these schemes performs not that well. It is not hard to found that both the robustness and plaintext sensitivity of our image encryption algorithm exhibit the best. Hence, by taking advantage of the DNA planes, our bit image encryption algorithm has improved the performance of resisting noise attack with considering the high plaintext sensitivity. From the comparison, it is concluded that the proposed algorithm possesses an excellent performance in anti-noise capacity.

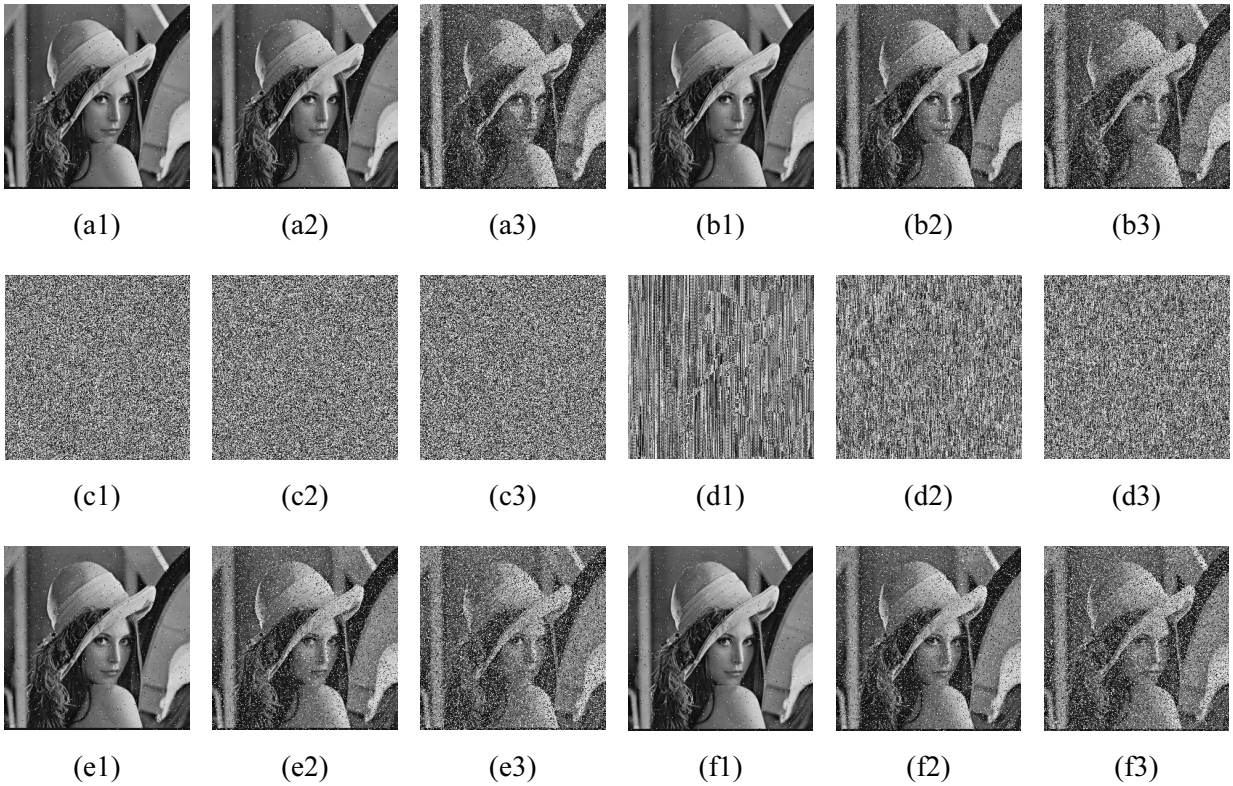


Fig. 8. The decrypted images from the cipher image of salt and pepper with different densities added: a1-f1 are the decrypted images from the cipher image of salt and pepper with a density of 0.01 added; a2-f2 are the decrypted images from the cipher image of salt and pepper with a density of 0.10 added; a3-f3 are the decrypted images from the cipher image of salt and pepper with a density of 0.25 added

Table 9. PSNR between the original image and decrypted images under salt and pepper noise

	Algorithm	Density of salt and pepper noise added		
		0.01	0.1	0.25
PSNR(dB)	ours	29.0728	18.5686	14.5387
	Ref. [15]	26.5537	16.7311	12.9623
	Ref. [20]	8.5714	8.5472	8.5259
	Ref. [21]	8.6918	8.5637	8.5201
	Ref. [22]	25.8947	16.1164	12.5716
	Ref. [23]	27.4387	17.8422	13.8145

5 Conclusion

In this paper, we proposed a bit image encryption algorithm based on Hyper Chaos and DNA sequence. The LTS and Chen's hyper chaos are applied to generate chaotic sequences for encrypting the image. Based on the theoretical knowledge of digital image, DNA plane matrix is proposed. The DNA matrix is divided into four DNA plane matrixes in accordance with the locations of DNA. And the four DNA plane matrixes are performed DNA ADD operation, respectively. The diffused DNA plane matrixes are rearranged for the purpose of making four DNA bases of ciphertext being composed of four corresponding locations DNA bases of plaintext. Experimental results have shown that our image cryptosystem has some remarkable performances:

High key sensitivity. Thanks to the initial values sensitivity of hyper chaos, the finally generated chaotic sequences will be totally different when a minor change is set into the initial value. Then a totally different cipher image is obtained after using the changed sequences.

High plaintext sensitivity. The cipher image is sensitive to the change of any pixel within the plain image. In result, the image encryption scheme is well in resisting plaintext attack.

Good noise robustness. When cryptosystems are sensitive to the change of the pixels, it is hard for them to decry the correct plain images of the noise-polluted cipher images. Therefore, when an encryption scheme shows high plaintext sensitivity, its noise robustness is usually poor. By exploiting the property that DNA located in different locations carries different percents of the information of an image, the resistance to noise attack of our image encryption scheme is improved. It has made a balance between the plaintext sensitivity and noise robustness.

The experiment results show that the proposed algorithm has good encryption effect, large secret key space and sufficient resistance to differential attack as well as noise attack. As the size of DNA matrix is 4 times than plain matrix, more chaotic sequences are needed to finish confusion and diffusion operation. Therefore, the corresponding encryption algorithm has slower speed. Hence, researches on creating more effective coding rules to reduce time loss is the development trend of future.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (grant nos. 61462061 and 61262084); the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (grant no. 20122BCB23002); the Natural Science Foundation of Jiangxi Province, China (grant no. 20151BAB207002).

References

[1] Y. Jiang, T.S. Hu, C.C. Huang, An improved particle swarm optimization algorithm, Applied Mathematics and Computation 193(1)(2007) 231-239.

[2] R. Matthews, On the derivation of a "chaotic" encryption algorithm, Cryptologia 13(1)(1989) 29-42.

[3] O. Mirzaei, M. Yaghoobi, H. Irani, A new image encryption method: parallel sub-image encryption with hyper chaos, Nonlinear Dynamic 67(1)(2012) 557-566.

[4] G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Communications 284(12)(2011)

2775-2780.

[5] B. Norouzi, S. Mirzakuchaki, S.M. Seyedzadeh, A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Multimedia Tools and Applications 71(3)(2014) 1469-1497.

[6] X.Y. Wang, Y.Q. Zhang, X.M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Optics and Lasers in Engineering 73(2015) 53-61.

[7] A.H. Abdullah, R. Enayatifar, M. Lee, A hybrid genetic algorithm and chaotic function model for image encryption, AEU-International Journal of Electronics and Communications 66(10)(2012) 806-816.

[8] H.G. Zhu, C. Zhao, X.D. Zhang, A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem, Signal Processing: Image Communication 28(6)(2013) 670-680.

[9] G.D. Ye, K.W. Wong, An image encryption scheme based on time-delay and hyperchaotic system, Nonlinear Dynamic 71(1-2)(2013) 259-267.

[10] X. Wu, D. Wang, J. Kurths, A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system, Information Sciences 349(2016) 137-153.

[11] 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.

[12] Q. Zhang, L.L. Liu, X.P. Wei, Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps, AEU-International Journal of Electronics and Communications 68(3)(2014) 186-192.

[13] Q. Zhang, L. Guo, X.P. Wei, Image encryption using DNA addition combining with chaotic maps, Mathematical and Computer Modeling 52(11)(2010) 2028-2035.

[14] H.J. Liu, X.Y. Wang, A. Kadir, Image encryption using DNA complementary rule and chaotic maps, Applied Soft Computing 12(5)(2012) 1457-1466.

[15] X.L. Huang, G. D. Ye, An image encryption algorithm based on hyper-chaos and DNA sequence, Multimedia Tools and Applications 72(1)(2014) 57-70.

[16] R. Enayatifar, A.H. Abdullah, I.F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Optics and Laser in Engineering 56(2014) 83-93.

[17] Y.C. Zhou, L. Bao, CLP. Chen, A new 1D chaotic system for image encryption, Signal Processing 97(2014) 172-182.

[18] T.G. Gao, Z.Q. Chen, A new image encryption algorithm based on hyper-chaos, Physics Letters A 372(4)(2008) 394-400.

[19] J.X. Chen, Z.L. Zhu, H. Yu, A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme, Optik-International Journal for Light and Electron Optics 125(11)(2014) 472-2478.

[20] Z. Eslami, A. Bakhshandeh, An improvement over an image encryption method based on total shuffling, Optics Communications 286(2013) 51-55.

[21] L. Xu, Z. Li, J. Li, A novel bit-level image encryption algorithm based on chaotic maps, Optics and Lasers in Engineering 78(2016) 17-25.

[22] X.Y. Wang, Y.Q. Zhang, X.M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Optics and Lasers in Engineering 73(2015) 53-61.

[23] R. Guesmi, MAB. Farah, A. Kachouri, A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2, Nonlinear Dynamics 83(3)(2016) 1123-1136.