Contents lists available at ScienceDirect

Mathematical and Computer Modelling

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

Image encryption using DNA addition combining with chaotic maps

Qiang Zhang *, Ling Guo, Xiaopeng Wei

Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian, 116622, China

ARTICLE INFO

Article history:
Received 23 September 2009
Received in revised form 25 December 2009
Accepted 31 January 2010

Keywords:
Image encryption
DNA sequence
Addition
Security

ABSTRACT

A new image encryption scheme based on DNA sequence addition operation and chaos is presented. First, a DNA sequence matrix is obtained by encoding the original image, then, divide the DNA sequence matrix into some equal blocks and use the DNA sequence addition operation to add these blocks. Next, perform the DNA sequence complement operation to the result of the added matrix by using two Logistic maps. Finally, decode the DNA sequence matrix from the third step, and we can get the encrypted image. The simulation experimental results and security analysis show that our scheme not only can achieve good encryption, but can also resist exhaustive attack, statistical attack and differential attack.

1. Introduction

Since computer networks have been widely applied, people's communications have had a revolutionary change, and transmission of digital images over the Internet has become more and more popular. However, the openness and sharing of networks exposes the security of digital images to serious threats in the process of transmission. Consequently, people have to pay more and more attention to security and confidentiality of multimedia information. Among various protection methods, the image encryption technique is one of the most efficient and common methods for the protection of image information. Traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not suitable for image encryption. So a new research method of image encryption is acquired urgently.

The chaotic system is a deterministic nonlinear system. It possesses varied characteristics, such as high sensitivity to initial conditions, determinacy and so on [1–6]. Chaotic sequences produced by chaotic maps are pseudo-random sequences; their structures are very complex and difficult to analyze and predict. In other words, chaotic systems can improve the security of encryption systems. The extant cryptography algorithms based on chaotic maps can be classified into two kinds: permutation and diffusion. In the permutation stage, the positions of pixels from the original image are changed by chaotic sequences or by some matrix transformation. The permutation algorithm has a better encryption effect, but without changing the pixel values, leading to the histogram of the encryption image and the original image being duplicates; thus its security could be threatened the statistical analysis. In the diffusion stage, the pixel values of the original image are changed by chaotic sequences. Most of these methods are directly implemented encryption by overlaying a chaotic sequence generated by a single chaotic map and the pixel grey value from the image. Compared to the permutation, diffusion may lead to higher security, but the encryption effect is not good. Thereby, in order to improve the security and the encryption effect, some researchers have combined permutation and diffusion. Pareek et al. [7] proposed an image encryption algorithm based on a one dimension chaotic map. However, a single chaotic map used to encrypt image may lead to a smaller key space and lower security, so some new ways to develop efficient image-encryption schemes have been suggested. Lian et al. [8] use the spatiotemporal chaos system to encrypt an image and performed a detailed analysis of the security of algorithms to show

* Corresponding author. Tel.: +86 41187403733; fax: +86 41187403963.
E-mail address: zhangq30@yahoo.com (Q. Zhang).

0895-7177/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.mcm.2010.06.005

their algorithms have satisfactory security with a low cost. Pisarchik et al. [9] proposed image encryption with chaotically coupled chaotic maps. Similarly, Liu, et al. [10] use multiple chaotic maps to encrypt the image. Their algorithms have larger key space, high sensitivity to keys, and have the ability of to resist traditional attacks.

In 1994, Adleman [11] did the first ever experiment on DNA computing, and initiated a new stage in the information age. In subsequent research, the characterstics of DNA computing, massive parallelism, huge storage and ultra-low power consumption had been found. From the research on DNA computing, DNA cryptography emerged as a new cryptographic field, in which DNA is used as an information carrier and modern biological technology is used as implementation tool [12]. Gehani et al. [13] presented an image encryption algorithm of one-time pad cryptography with DNA strands. They pointed out that current practical applications of cryptographic systems based on one-time pads are limited to the confines of conventional electronic media. But DNA has extraordinary information density and is very suitable to store a huge one-time pad. Their method might be effective for solving the storage problem of the one-time pad. Clelland et al. [14] successfully hid the famous "June 6 invasion: Normandy" in DNA microdots. They proposed a novel encoding method as an alternative to traditional binary encoding. Nucleotides are used as a quaternary code and each letter is denoted by three nucleotides. For example, use *CGA* to denote the letter *A*, use *CCA* to denote the letter *B*, etc. Then, the secret message is encoded into a DNA sequence for example, *AB* is expressed as *CCGCCA*. For the two DNA cryptography schemes described above, many biological experiments have to be done in the encryption and decryption step. These experiments can only be done in a well equipped lab using current technology, and it is very costly. For these reasons, the research on DNA cryptography is still much more theoretical than practical. Recently, Kang Ning [15] proposed a pseudo DNA cryptography method, which has better encryption and was not through real biological experiments. But it was only used to encrypt character information.

In order to overcome the above shortcomings from image encryption based on chaotic maps and DNA cryptography, in this paper we use the simple theory of the DNA sequence operation to encrypt image information and the combined chaotic maps and DNA sequence addition operation to implement image encryption. The paper is organized as follows. In Section 2, we introduce some theory behind the proposed algorithm. The design of the proposed image encryption scheme is proposed in the Section 3. In Section 4, some simulation results are described. In Section 5, security analysis is discussed. Section 6 gives the conclusion.

2. Basic theory of the proposed algorithm

2.1. Chaotic map

In this paper, we used 2D Logistic and 1D Logistic maps whose definitions are as follows. 2D Logistic map is described as Eq. (1) [16]:

$$\begin{cases} x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_1 y_i^2; \\ y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2(x_i^2 + x_i y_i); \end{cases} \tag{1}$$

When $2.75 < \mu_1 \le 3.4$, $2.75 < \mu_2 \le 3.45$, $0.15 < \gamma_1 \le 0.21$, $0.13 < \gamma_2 \le 0.15$, the system is in a chaotic state and can generate two chaotic sequences in the region (0,1]. Due to the system parameters γ_1 and γ_2 having a smaller value range, we set $\gamma_1 = 0.17$ and $\gamma_2 = 0.14$, the other parameters can be seen as secret keys.

1D Logistic map is an example chaotic map, it is described as follows:

$$x_{n+1} = \mu x_n(1 - x_n). \tag{2}$$

Where $\mu \in [0, 4]$, $x_n \in (0, 1)$, $n = 0, 1, 2, \ldots$ the research result shows that the system is in a chaotic state under the condition that $3.56994 < \mu \le 4$.

2.2. DNA sequence encryption

2.2.1. DNA encoding and decoding for image

A DNA sequence contains four nucleic acid bases *A* (*adenine*), *C* (*cytosine*), *G* (*guanine*), *T* (*thymine*), where *A* and *T* are complementary, and *G* and *C* are complementary. In the binary, 0 and 1 are complementary, so 00 and 11 are complementary, 01 and 10 are also complementary. In this paper, we use *C*, *A*, *T*, *G* to denote 00, 01, 10, 11, respectively. For 8 bit grey images, each pixel can be expressed a DNA sequence whose length is 4. For example: If the first pixel value of the original image is 173, convert it into a binary stream as [10101101], by using the above DNA encoding rule to encode the stream, we can get a DNA sequence [*TTGA*]. Whereas using 00, 01, 10, 11 to denote *C*, *A*, *T*, *G*, respectively, to decode the above DNA sequence, we can get a binary sequence [10101101].

2.2.2. Addition and subtraction algebraic operation for DNA sequences

With the rapid developments in DNA computing, some biology operations and algebraic operations based on the DNA sequence have been presented by researchers [17,18], such as the addition operation. The addition and subtraction operations for DNA sequences are performed according to traditional addition and subtraction in the Z_2. For example, $11 + 10 = 01$, $01 - 11 = 10$. We use 00, 01, 10, 11 to denote *C*, *A*, *T*, *G*, respectively, the details of the addition and

Table 1
Addition operation for DNA sequence.

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

Table 2
Subtraction operation for DNA sequence.

-	*T*	*A*	*C*	*G*
T	*C*	*G*	*T*	*A*
A	*A*	*C*	*G*	*T*
C	*T*	*A*	*C*	*G*
G	*G*	*T*	*A*	*C*

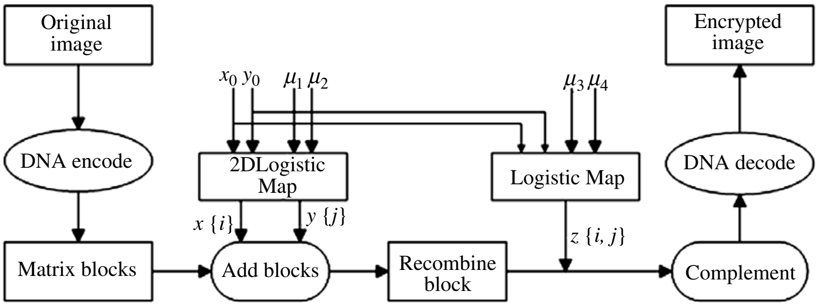

Fig. 1. Block diagram for the image encryption algorithm.

subtraction rules are shown in Tables 1 and 2. From Table 1, we can see that any two rows are complementary, and Table 2 is the same. In other words, the addition algebraic operation table is a double helix structure which satisfies the Watson–Crick complement regulation. Subtraction is the inverse operation of addition, but whose structure is not a double helix structure. However, we also can find the complement of every base in the Table 2. In this paper, we will use these wonderful addition rules to scramble the pixel values of the original image.

3. Algorithm described

In this section, we will study the procedure of image encryption based on the DNA sequence addition operation in detail. Firstly, produce secret keys. Secondly, divide the original image into blocks and add these blocks by using the DNA sequence addition operation. Thirdly, carry out the DNA sequence complement operation for the resulting added matrix using two Logistic maps. Lastly, decoding the result from the third stage, we obtain the encrypted image. The process of the proposed image encryption algorithm is shown in Fig. 1.

3.1. *Generation of the secret key*

We use the method in Ref. [19] to generate the secret key. Input an 8 bit grey image A as the original image, $A = A(a_{ij})$, $i = 1, 2, \dots, m, j = 1, 2, \dots, n$. Here, a_{ij} is the value of the image pixel, (i, j) is pixel position, and (m, n) is the size of image. Using following formulas we can calculate k_1 and k_2.

$$k_1 = \frac{1}{256}\mathrm{mod}\left(\sum_{i=1}^{\frac{m}{2}}\sum_{j=1}^{n} a_{ij}, 256\right) \tag{3}$$

$$k_2 = \frac{1}{256}\mathrm{mod}\left(\sum_{i=\frac{m}{2}}^{m}\sum_{j=1}^{n} a_{ij}, 256\right). \tag{4}$$

Then choose two initial values x_1, y_2,and four system parameters $\mu_1, \mu_2, \mu_3, \mu_4$. Use following pseudo-code to calculate x_0 and y_0. We set x_0, y_0, μ_1, μ_2 as the parameters of the 2D Logistic map and x_0, y_0, μ_3, μ_4 as the parameters of two 1D Logistic maps. Thus these parameters can be seen as secret keys. The pseudo-code is:

```
$x_0 \leftarrow x_1 + k_1$
if $x_0 > 1$ then
   $x_0 \leftarrow \mathrm{mod}(x_0, 1)$
else
   $x_0 \leftarrow x_0$
end if
```

3.2. Image encryption algorithm based on DNA sequence addition

According to Fig. 1, the proposed encryption algorithm can be divided into the following steps:

Step 1: Convert the image into a binary matrix, then carry out DNA encoding for the binary matrix according to Section 2.2.1, to obtain a coding matrix Ab, the size of Ab is $(m, n \times 4)$;

Step 2: Divide Ab into some equal blocks $Ab\{i, j\}$, $i = 1, 2, \dots, \frac{m}{4}$, $j = 1, 2, \dots, n$, where the size of blocks is 4×4;

Step 3: Generate two chaotic sequences $X = \{x_1, x_2, \dots, x_{\frac{m}{4}}\}$, $Y = \{y_1, y_2, \dots, y_n\}$, through 2$D$ Logistic map under the condition that the initial values are x_0, y_0 and system parameters are μ_1, μ_2;

Step 4: Sorting X, Y in ascending order, we get two new sequences X', Y';

Step 5: Let the location value of sequences X', Y' be row coordinates and column coordinates of $Ab\{i, j\}$, in other words, it can be expressed as $Ab\{x'_p, y'_q\}$, where $\{x'_1, x'_2, \dots, x'_p, \dots, x'_{\frac{m}{4}}\}$ and $\{y'_1, y'_2, \dots, y'_q, \dots, x'_n\}$ are the location values of sequences X', Y', respectively;

Step 6: Add $Ab\{i, j\}$ and $Ab\{x'_p, y'_q\}$ according to the rules in Section 2.2.2, obtaining the result as blocks $B\{i, j\}$.

Step 7: Recombining these blocks, $B\{i, j\}$, we will get a new sequence matrix C.

Step 8: Two chaotic sequences z_1 and z_2 are produced by two 1D Logistic maps, whose lengths are m and $n \times 4$. Reconstruct z_1 and z_2 as two matrices $Z_1(m, 1)$ and $Z_2(1, n \times 4)$. Performing the multiply operation for $Z_1(m, 1)$ and $Z_2(1, n \times 4)$, we obtain the matrix Z whose size is $m \times n \times 4$. Map the value of Z into (0,1) by $\mathrm{mod}(Z, 1)$. Then use the following threshold function $f(x)$ to get a binary sequence matrix:

$$f(x) = \begin{cases} 0, 0 < Z(i, j) \leq 0.5; \\ 1, 0.5 < Z(i, j) \leq 1; \end{cases} \tag{5}$$

Step 9: If $Z\{i, j\} = 1$, $C\{i, j\}$ is complemented, otherwise it is unchanged. After the complementing operation, we get a new coding matrix C';

Step 10: Carry out the inverse process of the step 1 for the coding matrix C', we will obtain a real value matrix D, then output image D, which is our encrypted image.

The process of decryption is an inverse process of encryption. Receivers obtain secret keys from the sender. To decrypt the encrypted image according to reverse operation of the above algorithm, the addition operation is replaced by the subtraction operation in step 6, the other steps are unchanged.

4. Simulation result and analysis

To demonstrate the security and efficiency of our algorithm, we use the standard 256 × 256 gray image Lena as the original image, use Matlab 7.1 to simulate the experiment and set parameters $x_1 = 0.62, y_1 = 0.12, \mu_1 = 3.2, \mu_2 = 3, \mu_3 = 3.9, \mu_1 = 3.85$. Fig. 2(a) shows the original image, the encrypted image is shown in Fig. 2(b). Fig. 2(c), (d) show the decrypted image under the wrong secret key and the correct key, respectively. From the result of our experiment, we can see it is difficult to recognize the original image from Fig. 2(b), Fig. 2(c) shows that we can not recover the image with the wrong secret key. It is obvious that our algorithm achieves good encryption.

5. The security analysis

A good encryption algorithm should resist all kinds of known attacks, such as exhaustive attack, statistical attack and differential attack, etc. [20–24]. In this section, we will discuss the security analysis of the proposed encryption scheme.

5.1. Resistance to exhaustive attack

5.1.1. Secret key's space analysis

In our algorithm, the initial value and the system parameter of the chaotic maps can be seemed as secret key. Thus, there are six secret keys $(x_1, y_1, \mu_1, \mu_2, \mu_3, \mu_4)$ in our algorithm. If the precision is 10^{-12}, the secret key's space is $10^{12} \times 10^{12} \times 10^{12} \times 10^{12} \times 10^{12} \times 10^{12} = 10^{72}$. The secret key's space is large enough to resist exhaustive attack.

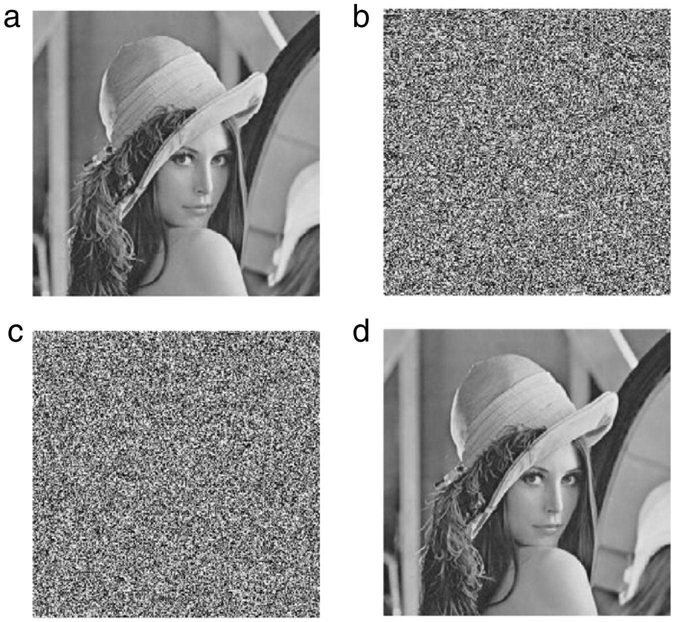

Fig. 2. Experimental result: (a) The original image (b) The encrypted image (c) The decrypted image with a different initial value (d) The decrypted image with correct parameters.

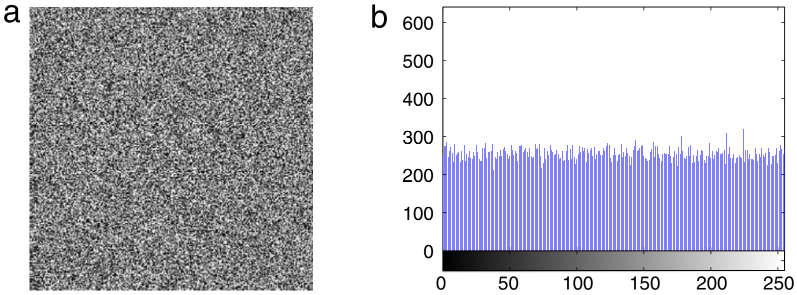

Fig. 3. The sensitivity to the secret key x_1 (a) The decrypted image whit secret key (0.62000000000001, 0.12, 3.2, 3, 3.9, 3.85) (b) The corresponding histogram.

5.1.2. Secret key's sensitivity analysis

The 2D Logistic and 1D Logistic chaotic maps are sensitive to the system parameters and initial values. If they have a slight difference, the decrypted image has no connection with the original image. Some secret key sensitivity tests are shown here. Using the secret key in the Section 4 to encrypt the original image, we have obtained the encrypted image shown Fig. 2(b) in the Section 4, next utilize the secret key (0.62000000000001, 0.12, 3.2, 3, 3.9, 3.85) to decrypt for the encrypted image. The result of decrypting is shown in Fig. 3. Fig. 3(a) shows the decrypted image and the corresponding grey histogram of the decrypted image is shown in Fig. 3(b). We can see that the histogram of the decrypted image is fairly uniform and the decrypted image is different from the original image. As the sensitivities of the other parameters are the same as for x_1, we omit examples of them here. Based on the above argument, our algorithm is sensitive to the secret key, which demonstrates it has the ability to resist exhaustive attack.

5.2. Resistance to statistical attack

5.2.1. The grey histogram analysis

Considering the statistical analysis of the original image and the encrypted image, Fig. 4(a), (b) show the grey-scale histograms of the original image and the encrypted image, respectively. Comparing the two histograms we find that the pixel grey values of the original image are concentrated on some values, but the histogram of the encrypted image is very uniform, which makes statistical attacks difficult.

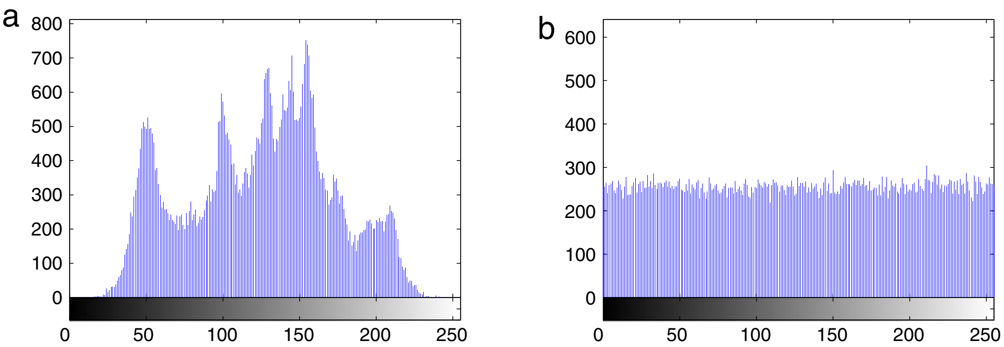

Fig. 4. The grey histogram of the original image and the encrypted image (a) The grey histogram of the original image (b) The grey histogram of the encrypted image.

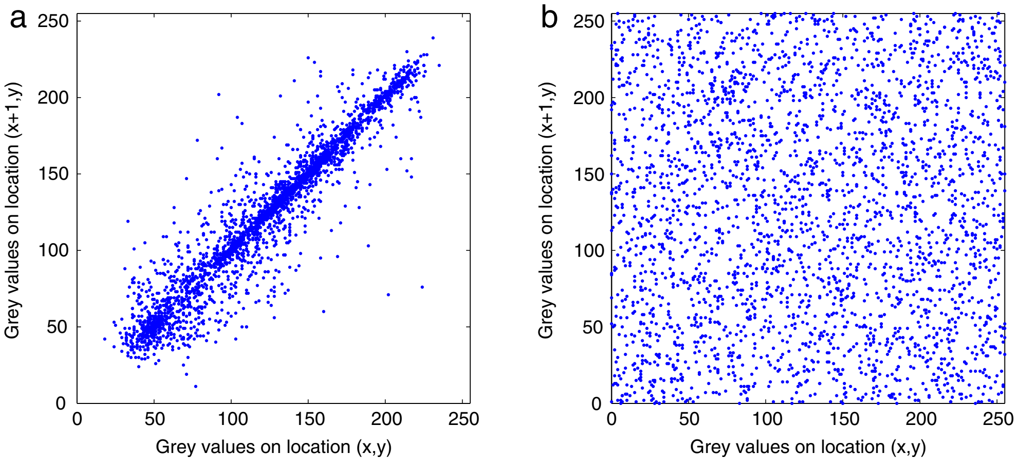

Fig. 5. Correlation of two horizontally adjacent pixels in the original image and in the encrypted image.

5.2.2. Correlation coefficient analysis

As far as we know the correlation of between adjacent pixels in the original image is very high. An effective encryption algorithm can reduce the correlation between adjacent pixels, in order to test the correlation of two adjacent pixels, we randomly select 3000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image. Using the following formulas for the correlation coefficient.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{7}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{8}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{9}$$

where x and y are the grey values of two adjacent pixels in the image, $\mathrm{cov}(x, y)$ is the covariance, $D(x)$ is the variance, and $E(x)$ is the mean.

Fig. 5(a), (b) show the correlation of two horizontally adjacent pixels in the original image "Lena" and its encrypted image, where the correlation coefficients are 0.9468 and 0.0036,respectively. Fig. 5(b) shows that the correlations of adjacent pixels in the encrypted image are greatly reduced. Similarly, other results are shown in the Table 3. From the result of Table 3, we find that the correlation coefficient of the adjacent pixels in the encrypted image is very small, which is close to 0. It can

Table 3
Correlation coefficients of two adjacent pixels in the two images.

Model	The original image	The encrypted image
Horizontal	0.9468	0.0036
Vertical	0.9697	0.0023
Diagonal	0.9153	0.0039

clearly be seen that our algorithm can destroy the relativity effectively; the proposed image encryption algorithm has a strong ability to resist statistical attack.

5.3. Resistance to differential attack

Attackers often make a slight change to the original image, and use the proposed algorithm to encrypt for the original image before and after changing, through comparing two encrypted image to find out the relationship between the original image and the encrypted image. It is called differential attack. Here, the encrypted image of Lena is called "Lena-test1", and the encrypted image after changing the first pixel grey value from Lena is called "Lena-test2". Researchers usually use *NPCR* (number of pixels change rate) and *UACI* (unified average changing intensity) as two criterions to examine the performance of resisting differential attack. Here, we use Eqs. (10)–(12) to calculate (*NPCR*) and (*UACI*) between "Lena-test1" and "Lena-test2".

$$C(i,j)=\begin{cases}0, & \text{if } T_1(i,j)=T_2(i,j);\\ 1, & \text{if } T_1(i,j)\neq T_2(i,j);\end{cases} \tag{10}$$

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}C(i,j)}{M\times N}\times 100\% \tag{11}$$

$$UACI=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|T_1(i,j)-T_2(i,j)|}{255\times M\times N}\times 100\% \tag{12}$$

where M and N are the height and width of the image, $T_1(i,j)$ and $T_2(i,j)$ denote the pixel grey value of "Lena-test1" and "Lena-test2" on the location (i,j). We obtained the result, $NPCR = 99.61\%$ and $UACI = 0.38\%$, from the simulation. This result demonstrates that our algorithm has a strong ability to resist differential attack.

5.4. Information entropy

The information entropy is defined as expressing the degree of uncertainty in the system [25]. We can also use it to express uncertainties in the image information. The information entropy can measure the distribution of grey values in the image. If the distribution of grey values is more uniform, the information entropy is greater. The information entropy is defined as follows:

$$H(m)=-\sum_{i=0}^{L}P(m_i)\log_2 P(m_i) \tag{13}$$

where m_i is the ith grey value for an L level grey image, $P(m_i)$ is the emergence probability of m_i, so $\sum_{i=0}^{L}P(m_i)=1$. For an ideal random image, the value of the information entropy is 8. An effective encryption algorithm should make the information entropy tend to 8. We obtained an information entropy $H = 7.9980$, that is very close to 8. It is can be seen that the proposed algorithm is very effective.

6. Conclusion

In this paper, we proposed a new image encryption algorithm based on DNA sequence addition. From above discussion, the pixel grey values of the original image are completely scrambled by the DNA sequence addition operation and the DNA complement operation. Through the experimental result and security analysis, we find that our algorithm has a better encryption, a larger secret key space and is highly sensitive to the secret key. Furthermore, the proposed algorithm can also resist most known attacks, such as exhaustive attacks, statistical attacks and differential attacks. All these features show that our algorithm is very suitable for image encryption.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No. 30870573) and the National High Technology Research and Development Program ("863" Program) of China (No. 2009AA01Z416).

References

[1] C. Fu, Z.L. Zhu, A chaotic image encryption scheme based on circular bit shift method, in: The 9th International Conference for Young Computer Scientists, 2008, pp. 3057–3061.
[2] Y.P. Zhang, F. Zuo, Z.J. Zhai, X.B. Cai, A new image encryption algorithm based on multiple chaos system, in: International Symposium on Electronic Commerce and Security, 2008, pp. 347–350.
[3] C.K. Huang, H.H. Nien, Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282 (2009) 2123–2127.
[4] S.G. Lian, J.S. Sun, Z.Q. Wang, A block cipher based on a suitable use of the chaotic standard map, International Journal of Chaos, Solitons and Fractals 26 (1) (2005) 117–129.
[5] S.G. Lian, A block cipher based on chaotic neural networks, Neurocomputing 72 (2009) 1296–1301.
[6] Z.H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Physics Letters A 346 (2005) 153–157.
[7] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9) (2006) 926–934.
[8] S.G. Lian, Efficient image or video encryption based on spatiotemporal chaos system, International Journal of Chaos, Solitons and Fractals 40 (15) (2009) 2509–2510.
[9] A.N. Pisarchik, M. Zanin, Image encryption with chaotically coupled chaotic maps, Physica D 237 (2008) 2638–2648.
[10] 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.
[11] Adleman, Molecular computation of solutions of combinatiorial problems, Science 266 (1994) 1021–1024.
[12] G.Z. Xiao, M.X. Lu, L. Qin, X.J. Lai, New field of cryptography: DNA cryptography, Chinese Science Bulletin 51 (12) (2006) 1413–1420.
[13] A. Gehani, T.H. LaBean, J.H. Reif, DNA-based cryptography. DIMACS series in discrete mathematics, Theoretical Computer Science 54 (2000) 233–249.
[14] C.T. Celland, V. Risca, C. Bancroft, Hiding messages in DNA microdots, Nature 399 (1999) 533–534.
[15] Kang Ning, A pseudo DNA cryptography method, arXiv:0903.2693.
[16] H.J. Liu, Z.L. Zhu, H.Y. Jiang, B.L. Wang, A novel image encryption algorithm based on improved 3D chaotic cat map, in: The 9th International Conference for Young Computer Scientists, 2009, pp. 3016–3021.
[17] P.M.J. Allen, Y. Bernard, M.P. Philip, Article for analog vector algebra computation, BioSystems 52 (1999) 175–180.
[18] W. Piotr, J.M. Jan, R.R. Witold, L. Bogdan, Adding numbers with DNA, in: International Conference on Systems, Man and Cybernetics, 2000, pp. 265–270.
[19] E.Z. Dong, Z.Q. Chen, Z.Z. Yuan, Z.P. Chen, A chaotic image encryption algorithm with the key mixing proportion factor, in: 2008 International Conference on Information Management, Innovation Management and Industrial Engineering, 2008, pp. 169–174.
[20] L. Wang, Q. Ye, Y.Q. Xiao, et al. An image encryption scheme based on cross chaotic map, in: 2008 Congress on Image and Signal Processing, 2008, pp. 22–26.
[21] J. Peng, S.Z. Jin, Y.G. Liu, et al. A novel scheme for image encryption based on piecewise linear chaotic map, in: Cybernetics and Intelligent Systems, 2008, pp. 1012–1016.
[22] M. Sabery, K.M. Yaghoobi, A new approach for image encryption using chaotic logistic map, in: 2008 International Conference on Advanced Computer Theory and Engineering, 2008, pp. 585–590.
[23] S.J. Xu, Y.L. Wang, J.Z. Wang, M. Tian, A novel image encryption scheme based on chaotic maps, in: ICSP, 9th International Conference on Signal Processing, 2008, pp. 1014–1018.
[24] S.G. Lian, J.S. Sun, Z.Q. Wang, Security analysis of a chaos-based image encryption algorithm, Physica A: Statistical and Theoretical Physics 351 (2–4) (2005) 645–661.
[25] C.E. Shannon, Communication theory of security systems, Bell System Technical Journal 28 (1949) 656–715.