Optik 124 (2013) 3596–3600

Contents lists available at SciVerse ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system

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 12 June 2012
Accepted 2 November 2012

Keywords:
Image encryption
DNA sequence
XOR operation
Chen's hyper-chaotic
Security

ABSTRACT

A new image fusion encryption algorithm based on image fusion and DNA sequence operation and hyper-chaotic system is presented. Firstly, two DNA sequences matrices are obtained by encoding the original image and the key image. Secondly, using the chaotic sequences generated by Chen's hyper-chaotic maps to scramble the locations of elements from the DNA sequence matrix which generated form original image. Thirdly, XOR the scrambled DNA matrix and the random DNA matrix by using DNA sequence addition operation. At last, decoding the DNA sequence matrix, we will get the encrypted image. The simulation experimental results and security analysis show that our algorithm not only has good encryption effect, but also has the ability of resisting exhaustive attack and statistical attack.

1. Introduction

With the fast development of network technology, the communications have been greatly changed. Transmission for multimedia content over Internet has become more and more frequently. However, the security of digital image has a serious threat in the process of transmission due to the openness and sharing of networks. So people have to take more and more attention on security and confidentiality of multimedia information. Among various protecting methods, image encryption technique is one of the most efficient and commonly methods for image information protection. Because of the special storage format of an image, the traditional block cipher algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not very suitable for image encryption. Now, more and more new methods are proposed for image encryption, which aims to reduce image content's redundancy by special operations, e.g., the chaos-based ciphers [1–3] and DNA based encryption operations [4].

The chaos system possesses of a variety of characteristics, such as high sensitivity to initial conditions, determinacy, ergodicity and so on. Chaotic sequences produced by chaotic maps are often pseudo-random sequences, and their structures are very complex and difficult to be analyzed and predicted [5–9]. The typical ciphers based on chaotic map can be partitioned into two stages: permutation and diffusion. In practice, researchers often combine permutation and diffusion to get high computational security. Lian et al. [10] proposed an image encryption with chaotic standard map. The algorithm has large key space and high sensitive, but their security is not high enough. Recently, due to hyper-chaos has more than one positive Lyapunov exponent, larger key space, better sensitivity and more complex dynamical characteristics, it may be more valuable to study the application of hyper-chaos in image encryption algorithms. Some researchers have investigated encrypting image based on hyper-chaos, such as Gao and Chen [11] propose an image encryption algorithm based on hyper-chaos, the algorithm has large key space, high sensitivity to key, and high security.

In addition to the image encryption algorithm based on chaotic map, some researchers also have proposed some image encryption algorithms based on graphics fusion technique. Zhang and Chen [12] proposed a new chaotic algorithm for image encryption, and got a good effect. Recently, Xue and Zhangh proposed an image fusion encryption algorithm based on multi-chaotic maps [13]. The algorithm has good encrypted effect and high security. Unfortunately, the fusion function is difficult to control the fusion parameter, when the fusion parameter is close to 0, the original image can be recurred. And when the fusion parameter is close to 1, the key image can be recurred. It is obvious that these fusion algorithms are not security and easy to be identified the original image.

With the research of DNA computing, DNA cryptography is born as a new cryptographic field emerged, in which DNA is used as information carrier and the modern biological technology is used as implementation tool [14]. Clelland et al. [15] successfully hid the famous "June 6 invasion: Normandy" in DNA microdots. They proposed a novel encoding method which is instead of the

* Corresponding author.
E-mail address: zhangq30@yahoo.com (Q. Zhang).

0030-4026/$ – see front matter © 2012 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2012.11.018

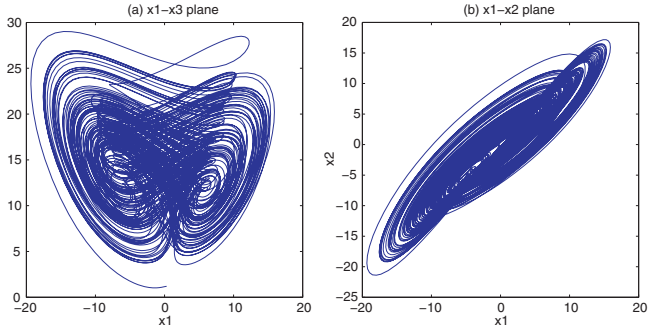

Fig. 1. Hyper-chaos attractors of Chen's hyper-chaotic system with $k = 0.2$.

traditional binary encoding. Nucleotides are used as quaternary code and each letter is denoted by three nucleotides. Ailenberg and Rotstein [16] proposed an improved Huffman coding method in DNA and encrypted an image successfully. Shyam et al. [17] proposed a novel encryption scheme based on DNA computing, they used the nature DNA sequences to encoding the information and encrypted an image by using the XOR logic operation. Such experiments can only be done in a well equipped lab using current technology, and it need high cost. For these reasons, the researches of DNA cryptography are still much more theory than practicality. Recently, Zhang and Guo [18] proposed a new image encryption algorithm based on DNA sequence addition operation, it has good encryption effect and not through real biological experiments. In order to overcome above shortcomings from the image encryption based on chaotic map and DNA cryptography. In this paper, we use the simple theory of pseudo DNA sequence operation to encrypt for image information and combined hyper-chaotic maps, image fusion operation and DNA sequence XOR operation to implement image encryption. This paper is organized as follows. In Section 2, we introduce some basic theories of 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. Related work

2.1. Chen's hyper-chaotic system

In our proposed encryption scheme, we used hyper-chaotic sequences which generated from Chen's hyper-chaotic system to encrypt image. Chen's hyper-chaotic system is described as Eq. (1):

$$\begin{cases} \dot{x} = a(y - x) & ; \\ \dot{y} = -xz + dx + cy - q & ; \\ \dot{z} = xy - bz & ; \\ \dot{q} = x + k & ; \end{cases} \tag{1}$$

In Eq. (1), a, b, c, d, k are the system parameters, when $a = 36$, $b = 3$, $c = 28$, $d = 16$ and $-0.7 \leq k \leq 0.7$ the Chen's hyper-chaotic system is in hyper-chaotic state and can generate four chaotic sequences. In this paper, with the parameters $a = 36$, $b = 3$, $c = 28$, $d = 16$ and $k = 0.2$, we got its Lyapunov exponents are $\lambda_1 = 1.552$, $\lambda_2 = 0.023$, $\lambda_3 = 0$, $\lambda_4 = -12.573$ [19] and the hyper-chaos attractors are shown in Fig. 1. Because the hyper-chaos has two positive Lyapunov exponents, so a hyper-chaotic system's prediction time is shorter than that of a chaotic system, as a result, it is safer than chaos in security algorithm [20]. We take the four-order Runge–Kutta method to solve the equations got sequences x, y, z, q. In order to get the better effect, we reserve the part of decimal and remove the part of integer of the element from hyper-chaotic sequences, so we get new four sequences which have better randomness.

Table 1
Eight kinds of schemes encoding and decoding map rule of DNA sequence.

	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

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, *G* and *C* are complementary [21]. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases *A*, *C*, *G* and *T* to encode 00, 01, 10 and 11, there are 24 kinds of coding schemes. But there are only eight kinds of coding schemes satisfy the Watson-Crick complement rule, which are shown in Table 1.

In this paper, we use the DNA code to encode the color image. A color image can be divided into three channels: Red channel, Green channel and Blue channel. For the 8 bit single channel image, each pixel can be expressed as a DNA sequence whose length is 4 (its binary sequence's length is 8). For example: If the first pixel value of the Red channel image is 173, convert it into a binary sequence is [10101101], by using above DNA encoding rule 1 to encode it, we can get the DNA sequence [*CCTG*]. Whereas use DNA encoding rule 1 to decode the above DNA sequence, we can get a binary sequence [10101101], but if we use DNA encoding rule 2 to decode the same DNA sequence, we get another binary sequence [01011110]. Obviously, it is also a simple way of encryption.

2.2.2. XOR algebraic operation for DNA sequences

With the rapid developments of DNA computing, some biology operations and algebraic operations based on DNA sequence are presented by researchers [22,23], such as XOR operation. XOR operation for DNA sequences is performed according to traditional XOR in the binary. Corresponding to eight kinds of DNA encoding schemes, there also exist eight kinds of DNA XOR rules.

In this paper, we used the XOR operation to fusion the original image and the key image. For example, there are two DNA sequences [*AGCT*] and [*CTGA*], we adopt one type of XOR operation which is shown in Table 2 to XOR them and we get a sequence [*CCTT*] as the result. The XOR operation is reflexive. So, we also can get the sequence [*AGCT*] by sequence [*CATT*] XOR sequence [*CTGA*] under the XOR operation. From Table 2, we can see that any one base in every row or column is unique, in other words, the results of XOR operation is one and only. In this paper, we will use this XOR operation rule to scramble the pixel values of the original image.

Table 2
One type of XOR operation for DNA sequences.

XOR	*A*	*G*	*C*	*T*
A	*A*	*G*	*C*	*T*
G	*G*	*A*	*T*	*C*
C	*C*	*T*	*A*	*G*
T	*T*	*C*	*G*	*A*

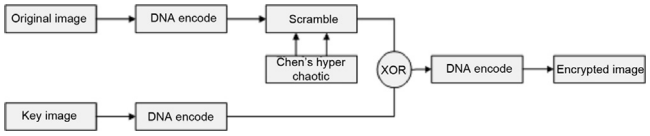

Fig. 2. Block diagram for the image encryption algorithm.

3. The proposed image encryption scheme

3.1. Key image generation

In this paper, the key image is a random image which generated by a random sequence generator. We use the random function *randint*(256, 256, [0, 255]) to generate 256×256 matrix of random integers. Because the key image is a random matrix, the correlation of key image is relatively low. It's more suitable for the key image than the average template image.

3.2. Image encryption

The proposed encryption algorithm includes three parts. Firstly, the original image and the key image are encoded into two DNA sequences matrices. Secondly, the first DNA matrix is permutated under the Chen's hyper chaos system. Thirdly, carry out DNA sequence XOR operation to XOR the two DNA sequences matrices. At last, decode the result from the third part, we will gain the encrypted image. The schematic block diagram is shown in Fig. 2.

According to Fig. 2, the encryption processes is given as follows in detail:

Step 1: Input two 8 bit grey image $O(m\,;n)$, $K(m\,;n)$ as the original image and the key image, where m, n is rows and columns of images;

Step 2: Convert image O, K into binary matrices, then carry out the third DNA encoding for these two binary matrices according to Section 2.2.1, we will gain two coding matrices Oe, Ke;

Step 3: Generate two chaotic sequences $x = (x_1, x_2, \ldots, x_{4n})$, $y = (y_1, y_2, \ldots, y_{4n})$, through Chen' hyper-chaotic system under the condition that initial values are x_1, y_1, z_1 and q_1 and system parameters are a, b, c, d, k, where x_1, y_1, z_1, q_1 and k are gained by Section 2.1;

Step 4: Prepare the chaotic sequences x, y as follows:

$$\begin{cases} [lx, fx] = \mathrm{sort}(x) \quad ; \\ [ly, fy] = \mathrm{sort}(y) \quad ; \end{cases} \tag{2}$$

where $[\bullet, \bullet] = \mathrm{sort}(\bullet)$ is the sequencing index function, fx is the new sequence after ascending to x, lx is the index value of fx. ly is the same as lx.

Step 5: Select the combination (lx, ly) to scramble Oe according to following formulas:

$$Oe(i,j) \leftrightarrow Oe(lx(i), ly(j)); i = 1, 2, \ldots, m; j = 1, 2, \ldots, n \times 4; \tag{3}$$

$R(i, j)$ is the pixel value of the position (i, j) from R channel; $G(i, j)$ and $B(i, j)$ are similar as $R(i, j)$.

Step 6: According to DNA XOR operation described in Section 2.2.2, XOR the matrices Oe and Ke by using the following formulas:

$$Oe\{i,j\} \leftarrow Oe\{i,j\} XOR\, Ke\{lx(i), ly(j)\}; i = 1, 2, \ldots, \frac{m}{4}; j = 1, 2, \ldots, n; \tag{4}$$

Step 7: Carry out the fourth DNA decoding rule to decode the matrix Oe according to Section 2.2.1, we will gain a binary matrix E.E is the encrypted image.

The process of decryption is an inverse process of encryption. Receivers obtain secret keys from sender. To decrypt the encrypted image according to contrary operation of above algorithm, where the addition operation is replaced by subtraction operation in the step 7, other steps is unchanged.

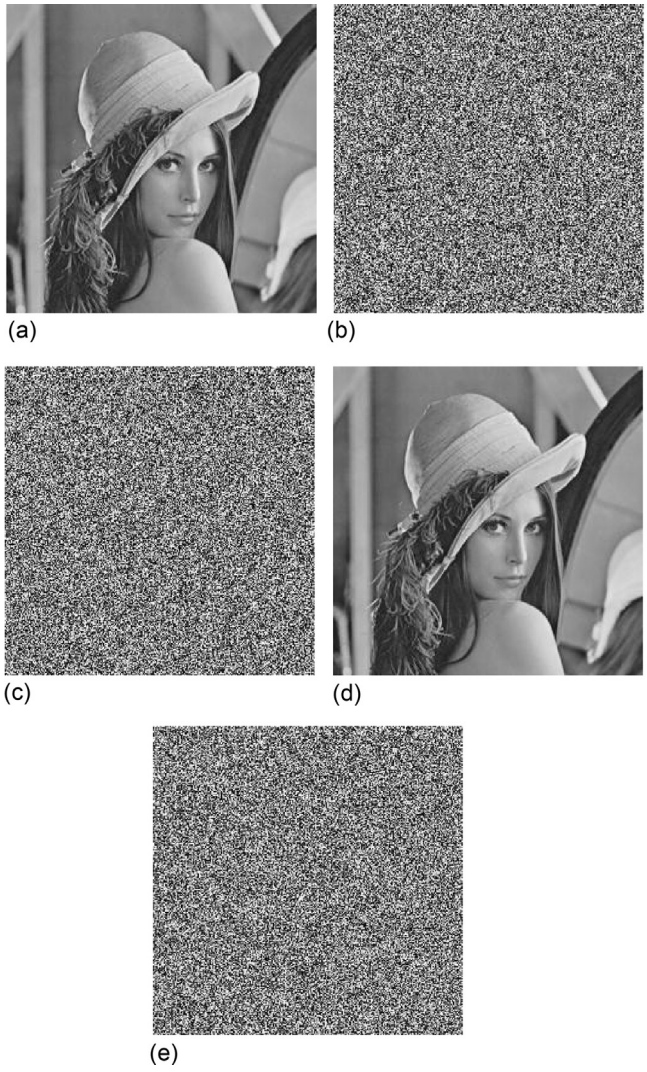

Fig. 3. Experimental results: (a) the original image (b) the key image, (c) the encrypted image, (d) the decrypted image, (e) The decrypted image under a wrong key image.

4. Simulation result and analysis

In this paper, we use standard 256×256 grey images "Lena" shown in Fig. 3(a) as the input image for the proposed encryption scheme, and key image which generated by a random function is shown in Fig. 3(b). We utilize Matlab 7.1 to simulate the experiment and set parameter $k = 0.2$, $x_1 = 0.3$, $y_1 = -0.4$, $z_1 = 1.2$, $q_1 = 1$. The encrypted image is shown in Fig. 3(c) and the decrypted image is shown in Fig. 3(d) and (e) is the decrypted image under another key image which is different from Fig. 3(b). From the visual point of view, there is no relationship between the original image and encryption images. It shows that our algorithm can get good encryption effect.

5. The security analysis

As a image encryption algorithm, it should resist known attacks such as exhaustive attack and statistical attack, it also should be sensitive to the secret keys, and the key space should be large

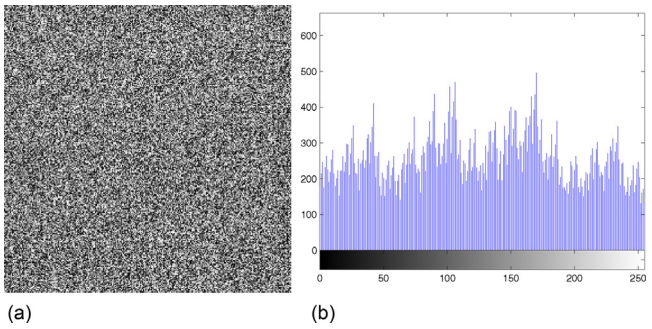

Fig. 4. Experimental result of secret key's sensitivity (a) the decrypted image with x_1 add 0.00000000000001 (b) is the histograms of (a).

enough to resist brute-force attacks [24–29]. In this section, we will discuss the security analysis on the proposed encryption scheme.

5.1. Secret key's space analysis

In this algorithm, the initial values of Chen's system can be seen as the secret keys, so there are five secret keys (x_1, y_1, z_1, q_1, k). If the precision is 10^{-14}, the secret key's space is $10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{70} \approx 2^{233}$. The secret key's space is large enough to resist exhaustive attack.

By the way, the key image can also be used as a secret key, we can periodically change the key image, and then transmission the key image and the secret keys secure to the decryption side.

5.2. Secret key's sensitivity analysis

The Chen's system is sensitive to the system parameters and initial values. It means that, the decrypted image will have no connection with the original image if the initial values have a slight difference. Some secret key sensitivity tests are shown at here. Using the secret key in the Section 4 to encrypt the original image, we have obtained the encrypted image shown Fig. 4(b) in the Section 4, then employ the secret key x_1 added 0.00000000000001 to decrypt the encrypted image. The result of decryption is shown in Fig. 4. Fig. 4(a) shows the decrypted image and Fig. 4(b) is the corresponding histograms of the decrypted image. We can see that the histograms of the decrypted image are more uniform than the original image and the decrypted image is different from the original image. The sensitivity of the other parameters are same as x_1, we omit it. Based on the above argument, our algorithm is sensitivity to the secret keys which demonstrates it has ability of resisting exhaustive attack.

5.3. Resist statistical attack

5.3.1. The grey histogram analysis

We compare the grey histogram of the image before and after encryption to analyze the statistical performance. The Fig. 5(a) shows the grey histogram of the original image and Fig. 5(b) shows the grey histogram of the encrypted image. From the two Figures, we can see that the primitive pixel grey values are concentrated on some value, but the pixel grey values after the encryption are scattering in the entire pixel value space, namely two images have lower similarity. Clearly, it is difficult to use the statistical performance of the pixel grey value to recover the original image. Thereby, our algorithm has strong ability of resisting statistical attack.

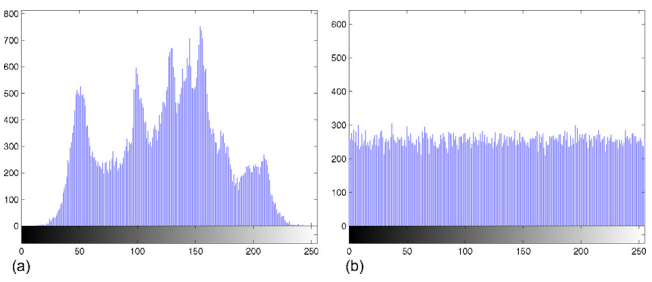

Fig. 5. Histograms of the original image and the encrypted image.

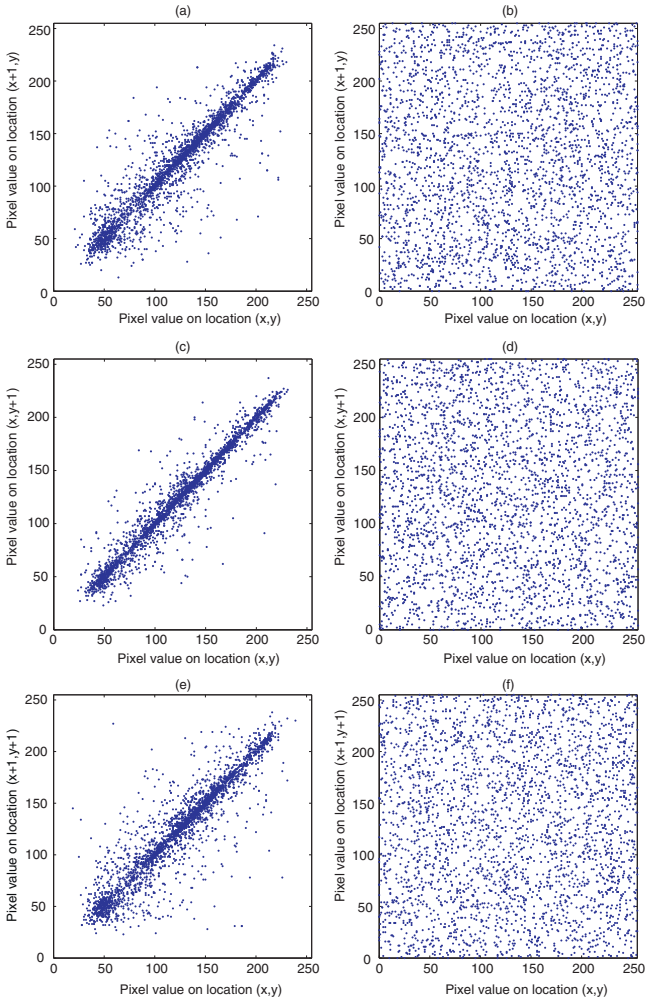

Fig. 6. Correlation of adjacent pixels in the original image and in the encrypted image.

5.3.2. Correlation coefficient analysis

It is well known that the less correlation coefficient of two adjacent pixels the stronger ability of resisting statistical attack. In this section, correlation coefficient of two adjacent pixels in original image and encrypted image is studied. In order to test the correlation of between 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 to calculate the correlation coefficient.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{6}$$

Table 3
Correlation coefficients of two adjacent pixels in original image and encrypted image.

Model	The original image	The encrypted image
Horizontal	0.9707	0.0012
Vertical	0.9733	0.0026
Diagonal	0.9122	0.0021

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{7}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{8}$$

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

Fig. 6(a), (c) and (e) shows the correlation of two adjacent pixels from horizontally vertical diagonal of the original image, respectively and Fig. 6(b), (d) and (f) shows the correlation of two adjacent pixels from horizontally vertical diagonal of the encrypted image, respectively. The correlation coefficients are shown in the Table 3. Fig. 6(b), (d) and (f) shows that the correlations of adjacent pixels in the encrypted image are greatly reduced. And from the result of Table 3, we can see that the correlation coefficient of the adjacent pixels of encrypted image is close to 0. In other words, the proposed image encryption algorithm has strong ability of resisting statistical attack.

5.4. Information entropy

The information entropy is defined to express the degree of uncertainties in the system [30]. We can also use it to express uncertainties of the image information. The information entropy can measure the distribution of grey value in the image, the results show that the greater information entropy the more uniform of the distribution of grey value. The information entropy is defined as follows:

$$H(m)=-\sum_{i=0}^{L}P(m_i)\log_2 P(m_i) \tag{9}$$

where m_i is the ith grey value for 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 idea random image, the value of the information entropy is 8. An effective encryption algorithm should make the information entropy tend to 8. We obtain information entropy $H=7:9968$ that is very close to 8. It is can be seen the proposed algorithm is very effective.

6. Conclusion

In this paper, we proposed a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. From above discussing, the positions of pixels are scrambled by Chen's hyper-chaotic system and the pixel grey values of the original image are scrambled by DNA sequence XOR operation with the key image. Through the experiment result and security analysis, we find that our algorithm has good encryption effect, larger secret key space and high sensitive to the secret key. Furthermore, the proposed algorithm also can resist most known attacks, such as statistical analysis and exhaustive attacks. All these features show that our algorithm is very suitable for digital image encryption.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 31170797), Program for Changjiang Scholars and Innovative Research Team in University (No. IRT1109) and by the Program for Liaoning Innovative Research Team in University (No. LT2011018).

References

[1] S.G. Lian, Multimedia Content Encryption: Techniques and Applications, ISBN: 1420065270, Auerbach Publication Taylor & Francis Group, Boca Raton, 2008.
[2] K. Wong, B. Kwok, W. Law, A fast image encryption scheme based on chaotic standard map, Phys. Lett. A 372 (2008) 2645–2652.
[3] Y. Wang, K. Wong, X. Liao, T. Xiang, G. Chen, A chaos-based image encryption algorithm with variable control parameters, Chaos Solitons Fractals 41 (2009) 1773–1783.
[4] A. Gehani, T.H. LaBean, J.H. Reif, DNA-based cryptography, DIMACS 54 (2000) 233249.
[5] S.G. Lian, A block cipher based on chaotic neural networks, Neurocomputing 72 (2009) 1296–C1301.
[6] Z.H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Phys. Lett. A 346 (2005) 153–157.
[7] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926–934.
[8] S.G. Lian, Efficient image or video encryption based on spatiotemporal chaos system, Int. J. Chaos Solitons Fractals (Elsevier) 40 (15) (2009) 2509–2510.
[9] 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.
[10] S.G. Lian, J.S. Sun, Z.Q. Wang, A block cipher based on a suitable use of the chaotic standard map, Int. J. Chaos Solitons Fractals 26 (2005) 117–129.
[11] T.G. Gao, Z.Q. Chen, A new image encryption algorithm based on hyper-chaos, Phys. Lett. A 372 (2008) 394–C400.
[12] X. Zhang, W.B. Chen, A new chaotic algorithm for image encryption, in: ICALIP 2008, 2008, pp. 889–892.
[13] X.L. Xue, Q. Zhang, An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps, J. Comput. Theor. Nanosci. 7 (2) (2010) 397–403.
[14] G.Z. Xiao, M.X. Lu, L. Qin, X.J. Lai, New field of cryptography: DNA cryptography, Chin. Sci. Bull. 51 (12) (2006) 1413–1420.
[15] C.T. Celland, V. Risca, C. Bancroft, Hiding messages in DNA microdots, Nature 399 (1999) 533–534.
[16] M. Ailenberg, O.D. Rotstein, An improved Huffman coding method for archiving text, images, and music characters in DNA, BioTechniques 47 (2009) 747–754.
[17] M. Shyam, N. Kiran, V. Maheswaran, A novel encryption scheme based on DNA computing, in: HIPC2007, 2007.
[18] Q. Zhang, L. Guo, An image encryption algorithm based on DNA sequence addition operation, in: BIC-TA, 2009, pp. 75–79.
[19] T.G. Gao, Z.Q. Chen, Z.Y. Yuan, G. Chen, Hyperchaos generated from Chen's system, Int. J. Mod. Phys. C 17 (2006) 471.
[20] S. Yanchuk, T. Kapitaniak, Chaos-hyperchaos transition in coupled Rössler systems, Phys. Rev. E 64 (2001) 056235.
[21] J.D. Watson, F.H.C. Crick, A structure for deoxyribose nucleic acid, Nature 171 (4356) (1953) 737–738.
[22] P. Gaborit, O.D. King, Linear constructions for DNA codes, Theor. Comput. Sci. 334 (2005) 99–113.
[23] O.D. King, P. Gaborit, Binary templates for comma-free DNA codes, Discrete Appl. Math. 155 (2007) 831–839.
[24] E.B. Baum, DNA sequences useful for computation, in: Proceedings of 2nd DIMACS Workshop on DNA Based Computers, 1996, pp. 122–127.
[25] 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.
[26] 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.
[27] J. Peng, S.Z. Jin, Y.G. Liu, et al., A novel scheme for image encryption based on piecewise linear chaotic map, in: 2008 IEEE Conference on Cybernetics Intelligent Systems, 2008, pp. 1012–1016.
[28] M.K. Sabery, 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.
[29] S.G. Lian, J.S. Sun, Z.Q. Wang, Security analysis of a chaos-based image encryption algorithm, Phys. A: Stat. Theor. Phys. 351 (2–4) (2005) 645–661.
[30] C.E. Shannon, Communication theory of security systems, Bell Syst. Tech. J. 28 (1949) 656715.