MANTECH Publications

Journal of Digital Image Processing and Computer Vision
Volume 2 Issue 2

Image Encryption Using DNA and Hyper Chaotic Sequence

Vishakha Mishra[1], Rupali Gupta[2], Anshul Bhatia[3], Sankalp Malhotra[4], Krishan Kumar

Department of Information Technology

Inderprastha Engineering College, APJ Abdul Kalam Technical University

Corresponding Authors: *vishakhamishra.it@gmail.com[1], rupali1394@gmail.com[2], bhatia.anshul4@gmail.com[3], sankalp.malhotra77@gmail.com[4], krishankumar@ipec.org.in[5]*

Abstract

A new color image encryption algorithm based on DNA (Deoxyribonucleic acid) sequence addition operation is presented. Firstly, three DNA sequence matrices are obtained by encoding the original color image which can be converted into three matrices R, G and B. Secondly, we use the chaotic sequences generated by Chen's hyper-chaotic maps to scramble the locations of elements from three DNA sequence matrices, and then divide three DNA sequence matrices into some equal blocks respectively. Thirdly, we add these blocks by using DNA sequence addition operation and Chen's hyper-chaotic maps. At last, by decoding the DNA sequence matrices and recombining the three channels R, G and B, we get the encrypted color image. The simulation results and security analysis show that our algorithm not only has good encryption effect, but also has the ability of resisting exhaustive attack, statistical attack and differential attack.

Keywords: *Color image encryption DNA sequence Addition operation Chen's hyper-chaotic Security*

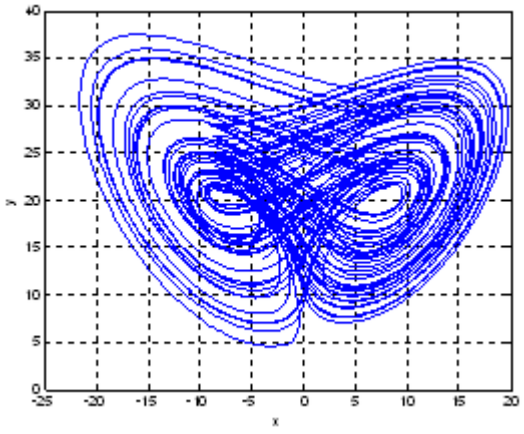
1. INTRODUCTION

Image encryption technique is one of the most efficient and common methods for image information protection. Because of the redundancy and special storage format of an image, the traditional block ciphers,

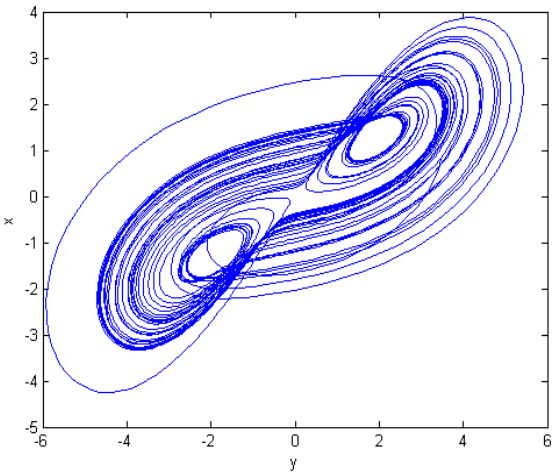
such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) are not very suitable for image encryption. The chaotic system is a nonlinearity determinate system. The typical ciphers based on chaotic map can be partitioned into two stages i.e., permutation and diffusion. In the permutation stage, the positions of pixels from original image are changed by chaotic sequences or by some matrix transformations. The permutation algorithm have certain encryption effect, but due to without changing the pixel value, the histogram of the encrypted image and the original image is duplicate, so its security is threatened by the statistical analysis. In the diffusion stage, the pixel values of original image are changed by chaotic sequences. Most of these diffusion methods directly implement encryption by overlaying a chaotic sequence generated by a single chaotic map and the pixel grey value from the image.

2. LITERATURE SURVEY

Some researchers have investigated image encryption based on hyper-chaos, for example, an image encryption algorithm based on hyper-chaos, which has large key space, high sensitivity to key, and high security. In the subsequent researches, some researchers have found lots of good characteristics of DNA computing such as massive parallelism, huge storage and ultra-low power consumption.



1(a)



1(b)

Fig1 (a) and (b): The attractors of Chen s hyper chaos system

Nucleotides are used as quaternary code and each letter is denoted by three nucleotides.

This scheme uses the simple theory of pseudo DNA sequence to transform image information, and combines hyperchaotic maps and DNA sequence addition operation to implement image encryption. The rest of the paper is organized as follows. In Section 2, the related work is introduced. The proposed image encryption scheme is presented in Section 3. In Section 4, some simulation results are given, and the security analysis and evaluation are presented in Section 5. Finally, in Section 6, some conclusions are drawn.

3. OBJECTIVE

Basically, hyper chaotic sequences and encryption techniques have been used to provide security to the original image from the sender to the receiver end. This procedure is being accomplished in two stages Permutation and Diffusion.

4. METHODOLOGY

Permutation

In the permutation stage, the positions of pixels from original image are changed by chaotic sequences or by some matrix transformations.

Diffusion

In the diffusion stage, the pixel values of original image are changed by chaotic sequences.

Chaotic Sequences

These are equations which are used to solve the maps/histograms or other equation values whose values cannot be determined.

DNA Addition and Subtraction

MAT-LAB

5. PROPOSED WORK

5.1. Chen's hyper-chaotic system

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

$$x^{\cdot} = a(y - x);$$

$$y^{\cdot} = -xz + dx + cy - q; \quad (1)$$

$$z^{\cdot} = xy - bz; \; q^{\cdot} = x + k;$$

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 the 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 1 = 1.552, 2 = 0.023, 3 = 0, 4 = −12.573 and the hyper-chaos attractors are shown in Fig. 1. Because the hyper-chaos has two positive Lyapunov exponents, a Lyapunov exponents, a hyper-chaotic system's prediction time s often shorter than that of a chaotic system. Here, we take the four-order Runge–Kutta method to solve the equations and get the sequences x, y, z, q. In our implementation, in order to get better effects, we reserve the decimal part and remove the integer part of the element from hyper-chaotic sequences.

Table 1 Addition operation for 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
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

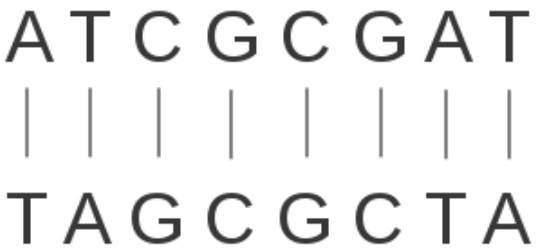


Fig. 2 A pair of DNA sequences.

5.2. DNA sequence operations

5.2.1. DNA encoding and decoding for images

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. 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 8 kinds of coding schemes 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].

Taking two DNA sequences [AGCT] and [CTGA] for example, we adopt one type of addition operation shown in Table 2 to

add them and we get a sequence [CATT]. Similarly, we can also get the sequence [AGCT] by subtracting the sequence [CTGA] from [CATT]. The subtraction operation is shown in Table 3. In other words, the results of addition operation and subtraction operation are unique. In this paper, we will use these addition or subtraction rules to scramble images' pixel values.

Table 2 Addition operation for DNA sequences

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

Table 3 Subtraction operation for DNA sequences

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

5.3 The proposed image encryption scheme

5. 3.1. Generation of the secret key

In Chen's hyper-chaotic system, the initial values x1, y1, z1 and q1 can be seen as the secret keys. After encoding the image with DNA encoding rules, we can get three Hamming distances for color image's channels. In this paper, we transform three Hamming distances (H) into three decimal numbers, add them to three initial values of Chen's hyper-chaotic system one by one, and finally, get three new initial values of Chen's hyper-chaotic system. Pseudocode of generating one new initial value x1 of Chen' system is shown as follows:

if H > 1 then

H←H/10

else x1 ←x1 + H

end if

5.3.2. Image encryption

The proposed encryption algorithm is composed of two parts, i.e., permutation and diffusion. In the algorithm, there are four chaotic sequences x, y, z and q generated by Chen's hyper-chaotic system. In this paper, we use sequences x, y, z in position scrambling and use sequences x, y, q in block addition by the DNA addition operation. The architecture of the proposed image encryption algorithm is shown in Fig. 3. Here, Fig. 3(a) shows the steps of image encryption, while Fig. 3(b) shows the permutation and diffusion operations. According to Fig. 3, the encryption steps are described as follows:

Step 1: Convert the color image O(m, n, 3) into three matrixes R(m, n), G(m, n), B(m, n).

Step 2: Convert R, G and B into binary matrices, then carry out the third DNA encoding rule to encode the binary matrixes according to Section 2.1, and finally, we get the three transformed coding matrixes R, G and B, with the size (m, n × 4)

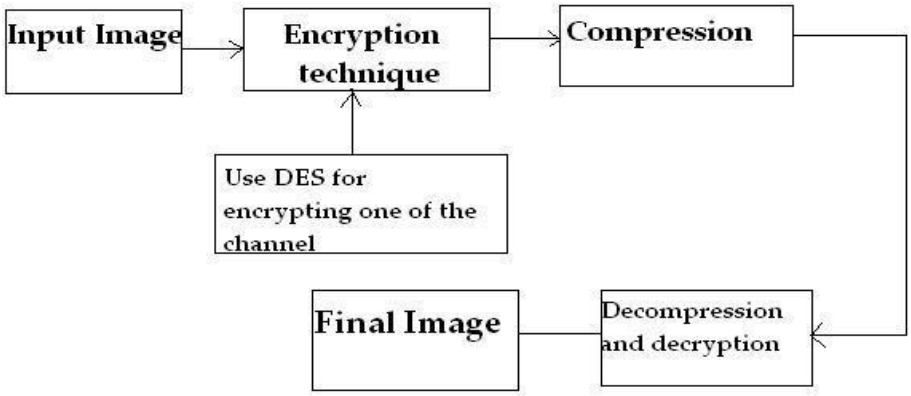
Step 3: Generate four chaotic sequences x = (x1, x2,. . ., x4n), y = (y1, y2,. . ., y4n), z = (z1, z2,. . ., z4n), q = (q1, q2,. . ., q4n), through Chen's hyper-chaotic system under the condition that initial values are x1, y1, z1 and q1 and system parameters are a, b, c, d, k, where x1, y1, z1, q1 and k are gained by Section 3(a) and 3(b).

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

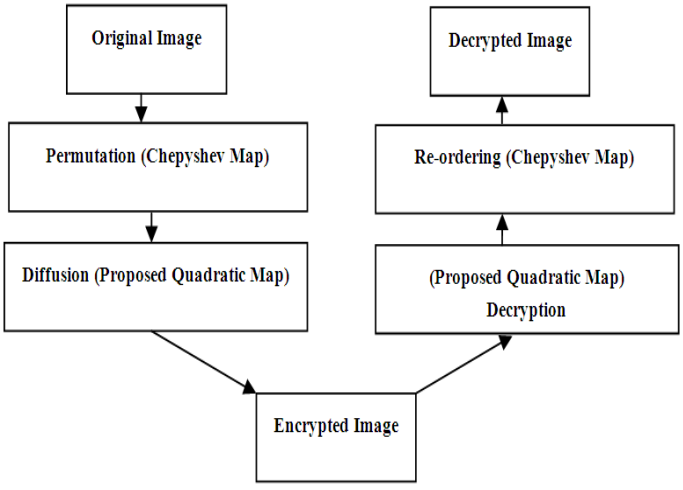
$$\begin{aligned} &[lx,fx] = sort(x);\\ &[ly,fy] = sort(y);\\ &[lz,fz] = sort(z);\\ &[lq,fq] = sort(q); \end{aligned} \qquad (2)$$

where [•, •] = sort(•) is the sequencing index function, fx is the new sequence after ascending to x, lx, ly, lz and lq are the index value of fx, fy, fz, and fq respectively.

Step 5: Select the combination (x, y, z)to scramble



3(a)



3 (b)

Fig. 3(a) Steps of image encryption;3 (b) the permutation and diffusion operations

R, G, B according to:

$$R(i,j) \leftrightarrow R(lx(i),ly(j));$$

$$G(i,j) \leftrightarrow G(lx(i),lz(j)); \quad (3)$$

$$B(i,j) \leftrightarrow B(ly(i),lz(j));$$

where i = 1, 2,. . ., m; j = 1,2,. . ., n × 4. R(i; j), G(i; j) and B(i; j) are the pixel value ofthe position (i;j) from R,G and B channel, respectively.

Step 6: We divide scrambled R, G, B into equal blocks, Rb{i, j}, Gb{i, j}, Gb{i, j}, i = 1, 2,. . ., m/4, j = 1, 2,. . ., n, where the size of block is 4 × 4.

Step 7: According to DNA addition described in Section 5.2.3, add the blocks of Rb, Gb, Bb by using the following method:

$$Rb\{i,j\} \leftarrow Rb\{i,j\} + Rb\{lx(i),ly(j)\};$$

$$Gb\{i,j\} \leftarrow Gb\{i,j\} + Gb\{lx(i),lq(j)\}; \quad (4)$$

$$Bb\{i,j\} \leftarrow Bb\{i,j\} + Rb\{ly(i),lq(j)\};$$

where i = 1, 2,. . ., m/4; j = 1, 2,. . ., n.

Step 8: Recombine these blocks Rb{i, j}, Gb{i, j} and Bb{i, j}, and get three new DNA sequence matrices R' , G' and B .

Step 9: Carry out the fourth DNA decoding rule to decode the matrices R' , G' and B' according to Section 5.1, we will gain three binary matrixes, then we recombine them into color image E. E is the encrypted image.

5.3.3. Image decryption

The process of decryption is an inverse process of encryption.

Step 1: Convert the encrypted color image E(m, n, 3) into three matrixes R'(m, n), G' (m, n), B' (m, n).

Step 2: Convert R', G' and B' into binary matrices, then carry out the fourth DNA encoding rule to encode the binary matrixes according to Section 5.3.2, and finally, we get the three transformed coding matrixes R' , G' and B' , with the size is (m, n × 4);

Step 3: Generate four chaotic sequences x = (x1, x2,. . ., x4n), y = (y1, y2,. . ., y4n), z = (z1, z2,. . ., z4n), q = (q1, q2,. . ., q4n), through Chen's hyper-chaotic system under the condition that initial values are x1, y1, z1 and q1 and system parameters are a, b, c, d, k, where x1, y1, z1, q1 and k are gained by Section 5.1.

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

[lx,fx] = sort(x);

[ly,fy] = sort(y); (5)

[lz,fz] = sort(z);

[lq,fq] = sort(q);

where [•, •] = sort(•) is the sequencing index function, fx is the new sequence after ascending to x, lx, ly, lz and lq are the index value of fx, fy, fz, and fq, respectively.

Step 5: We divide R', G', B' into equal blocks, Rb'{i, j}, Gb{i, j}, Gb {i, j}, i = 1, 2,. . ., m/4, j = 1, 2,. . ., n, where the size of block is 4 × 4.

Step 6: According to DNA subtraction described in Section 5.2.1, subtract the blocks of Rb', Gb', Bb'

by using the following method:

$$Rb\{i,j\} \leftarrow Rb\{i,j\} - Rb\{lx(i),ly(j)\};$$

$$Gb\{i,j\} \leftarrow Gb\{i,j\} - Gb\{lx(i),lq(j)\}; \quad (6)$$

where i = m/4,. . ., 2, 1; j = n,. . ., 2, 1.

Step 7: Recombine these blocks Rb' {i, j}, Gb' {i, j} and Bb' {i, j}, and get three new DNA sequence matrices R, G and B.

Step 8: Select the combination (x, y, z)to scramble R, G, B according to:

$$R(i,j) \leftrightarrow R(lx(i),ly(j));$$

$$G(i,j) \leftrightarrow G(lx(i),lz(j)); \quad (7)$$

$$B(i,j) \leftrightarrow B(ly(i),lz(j));$$

where i = m,. . ., 2, 1; j = n × 4,. . ., 2, 1. R(i; j), G(i; j) and B(i; j) are the pixel value ofthe position (i;j)from R,G and B channel, respectively.

Step 9: Carry out the third DNA decoding rule to decode the matrices R, G and B according to Section 5.1, we will gain three binary matrixes, then we recombine them into color image D. D is the decrypted image.

RESULTS

In this paper, we use the standard 256 × 256 × 3 color images "Lena", "Baboon" and "Cameraman" shown in Fig. 4(a),(d) and (g) as the input images, respectively. Utilize Matlab 7.1 to simulate the encryption and decryption operations and set parameters k = 0.2,x1 = 0.3, y1 = −0.4, z1 = 1.2, q1 = 1. The encrypted images are shown in Fig. 4(b) and (e), the decrypted images are shown in Fig. 4(c) and (f). It can be seen from the images that there are no relationship between the original images and encrypted images. It shows that our algorithm can get good encryption effect.

CONCLUSION AND DISCUSSION

In this paper, we proposed a color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. In this algorithm, 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 addition operation. Secret keys are generated in order to improve the ability of resisting differential attack. Through the experimental results 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 exhaustive attack and statistical attack. All these features show that our algorithm is very suitable for color image encryption.

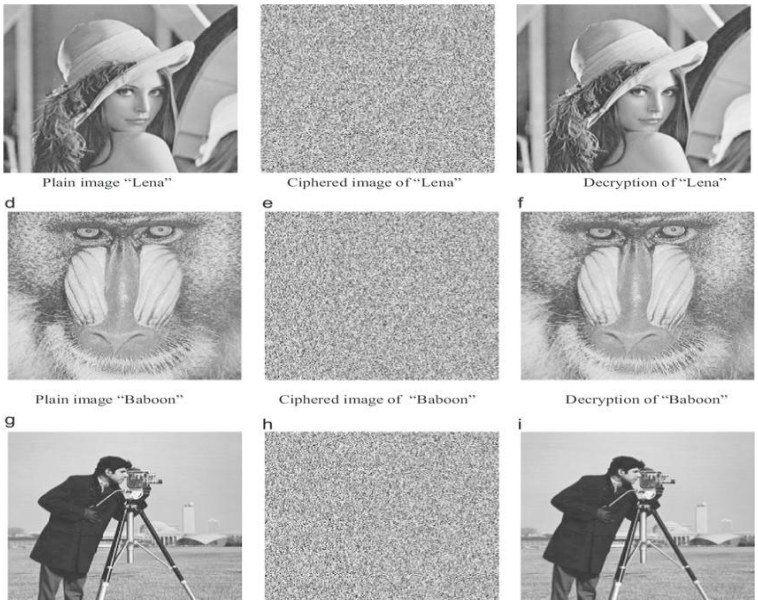


Fig. 4. Experimental results: (a) Original image of "Lena". (b) Encrypted image of "Lena". (c) Decrypted image of "Lena". (d) Original image of "Baboon". (e) Encrypted image of "Baboon". (f) Decrypted image of "Baboon". : (g) Original image of "Cameraman". (h) Encrypted image of "Cameraman". (i) Decrypted image of "Cameraman".

FUTURE WORK

As a good encryption algorithm, it should resist all kinds of known attacks such as differential attacks and statistical attacks.

Differential Attack

Attackers often make a slight change for the original image, use the proposed algorithm to encrypt the original image before and after changing, and through comparing two encrypted images to find out the relationship between the original image and the encrypted image. This kind of attack is called differential attack.

Statistical Attack

Considering the statistical analysis of the original image and the encrypted image, the histograms of R, G and B channels from original image and the histograms of R, G and B channels from encrypted image, we find that pixel values of R, G and B channels from original image concentrate some values, but the corresponding histograms of R, G and B channels from encrypted image are very uniform as shown in fig 5, which make statistical attacks difficult.

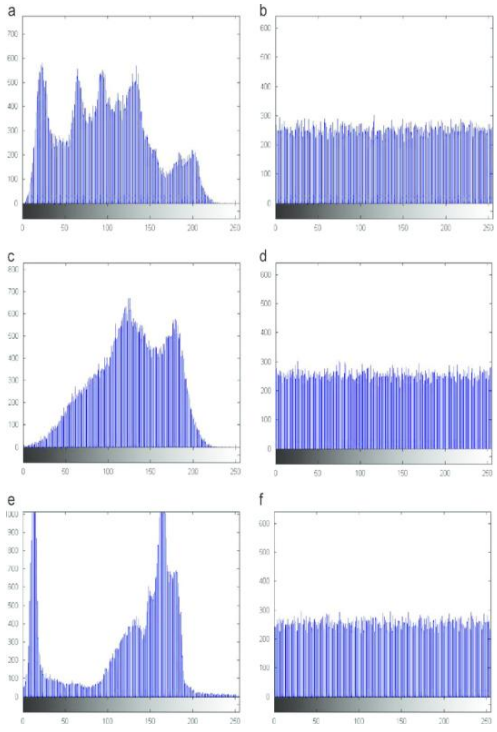


Fig.5.Histogram(a,c,e) of original R,G,B image and histogram(b,d,f) of encrypted R,G,B image.

There is no relation between thehistogram obtained before and after the image .

ACKNOWLEDGMENT

This research paper was partially supported by Lipton's techniques and some review papers.We thank our colleagues who provided insight and expertise that greatly assisted the research,although they may not agree with all the interpretations/conclusions of this paper.

REFERENCES

1) R. J. Lipton, Using DNA to solve NP complete problems Science, Vol. 268, pp. 542-545, 1995

2) Gao, T.G., Chen, Z.Q., Yuan, Z.Y., Chen, G., 2006. Hyperchaos generated from Chen's system. International Journal of Modern Physics

3) Gehani, A., LaBean, T.H., Reif, J.H., 2000. DNA-based cryptography. Dimacs Series in Discrete Mathematics and Theoretical Computer Science .

4) Hermassil, H., Rhoumal, R., Belghith, S., 2009. A modified hyperchaos based image

5) D.Prabhu, M.Adimoolam Lecturer, Bi-serial.

6) Pisarchik, A.N., Zanin, M., 2008. Image encryption with chaotically coupled chaotic maps. Physica D 237, 2638C2648.

7) Rhouma, R., Belghith, S., 2008. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Physics Letters A 372, 5973–5978.

8) SaberyK, M., Yaghoobi, M., 2008. A new approach for image encryption using chaotic logistic map. In: 2008 International Conference on Advanced Computer Theory and Engineering, pp. 585–590.

9) Shannon, C.E., 1949. Communication theory of security systems. The Bell System Technical Journal 28, 656715.

10) Sun, F.Y., Liu, S.T., Li, Z.Q., Lu, Z.W., 2008. A novel image encryption scheme based on spatial chaos map. Chaos, Solitons and Fractals 38, 631–640.

11) Wang, L., Ye, Q., Xiao, Y.Q., et al., 2008. An image encryption scheme based on cross chaotic map. In: 2008 Congress on Image and Signal Processing, pp. 22–26.

12) Watson, J.D., Crick, F.H.C., 1953. A structure for deoxyribose nucleic acid. Nature 171(4356), 737–738.

13) Wong, K., Kwok, B., Law, W., 2008. A fast image encryption scheme based on chaotic standard map. Physics Letters A 372, 2645–2652.

14) Xiao, G.Z., Lu, M.X., Qin, L., Lai, X.J., 2006. New field of cryptography: DNA cryptography. Chinese Science Bulletin 51 (12), 141311420.

15) Ling Guo is a graduate student at Dalian University, Dalian, China. His research areas include DNA Computing and DNA Cryptography.

16) Jianxin Zhang is a lecturer at Dalian University, Dalian, China. His research interests are computer animation, intelligent computing. So far, he has (co-) authored 12 papers published.