2010 International Conference on Multimedia Information Networking and Security

Image Encryption Algorithm Based on DNA Sequences for the Big Image

Shihua Zhou
[1]*School of Mechanical Engineering*
Dalian University of Technology
Dalian, P.R.China
[2]*Key Laboratory of Advanced*
Design and Intelligent Computing
(Dalian University)
Ministry of Education
Dalian, P.R.China
shihuajo@gmail.com

Qiang Zhang
[1]*Key Laboratory of Advanced*
Design and Intelligent Computing
(Dalian University)
Ministry of Education
Dalian, P.R.China
zhangq@dlu.edu.cn

Xiaopeng Wei
[1]*School of Mechanical Engineering*
Dalian University of Technology
Dalian, P.R.China
[2]*Key Laboratory of Advanced*
Design and Intelligent Computing
(Dalian University)
Ministry of Education
Dalian, P.R.China
weixp@dlu.edu.cn

***Abstract*—With the fast development of Internet technology and information processing technology, the image is commonly transmitted via the Internet. People enjoy the convenience and shortcut, but people have to face to the obsession that the important image information in transmission is easily intercepted by unknown persons or hackers. In order to enhance the image information security, image encryption becomes an important research direction. An image encryption algorithm based on DNA sequences for the big image is presented in this paper. The main purpose of this algorithm is to reduce the big image encryption time. This algorithm is implemented by using the natural DNA sequences as main keys. The first part is the process of pixel scrambling. The original image is confused in the light of the scrambling sequence is generated by the DNA sequence. The second part is the process of pixel replacement. The pixel gray values of the new image and the one of the three encryption templates are generated by the other DNA sequence are XORed bit-by-bit in turn. The experimental result demonstrates that the image encryption algorithm is feasible and simple. Through performance analysis, this algorithm is robust against all kinds of attacks and owns higher security.**

***Keywords*-image encryption; DNA sequences; the big image;**

I. INTRODUCTION

The important image information in transmission is easily intercepted by unknown persons or hackers via the Internet. Hence, the problem of image information security has become more and more important. Image encryption [1-3] is usually used to prevent the important information from disclosing when they are transmitted over an insecure channel. At the sending end, the people first selects a secret key and uses a specifically method to encrypt the original image into the encrypted image. At the receiving end, Only the authorized receiver could decrypt the encrypted image with the secret key to obtain the original image. According to the effect, the image encryption algorithms mainly include three types [4, 5]: 1) pixel scrambling; 2) pixel replacement; 3) the compound of scrambling and replacement.

At present, the hottest encryption methods are chaos-based image encryption and DNA cryptography-based image encryption and so on. The principle of chaos-based image encryption [6-9] is as follow. Firstly, the sender first selects a secret key and uses a specifically chaotic sign generator to generate a chaotic signal sequence stream. Then, the original image information is confused or diffused in the light of the chaotic sequence and the encrypted image becomes similar to the random noise is generated. Decryption is basically the same as encryption. Only the authorized receiver could use the same chaotic sign generator to generate the chaotic signal sequence stream with the secret key. Then, the encrypted image is decrypted in the light of the chaotic sequence, and the original image is gained. According to the chaotic dimension, the chaos-based image encryption algorithms mainly include three types [10-13]: 1) low-dimensional chaos-based image encryption algorithm; 2) Hyper-chaos image encryption algorithm; 3) the image encryption based on the compound of the other encryption algorithm and chaos. For example, the hyper-chaotic cellular neural network system is used in a digital image encryption algorithm [13]. In this algorithm, the hyper-chaos is employed to achieve a more sophisticated chaotic sequence to be used for encrypting the original image.

DNA cryptography [14] is a new born cryptography, in which DNA is used as information carrier and the modern biological technology is used as implementation tool, and the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, signature, and so on. The study of DNA cryptography-based image encryption algorithms [15,16] has become a hot direction. The main security basis depends on the restriction of biotechnology, which has nothing to do with computing power. For example, a image encryption method based DNA chip [16] is proposed. In the encryption, a mass of probes are arranged in a square area less than one square inch on glass or silicon matrix. The receiver uses numerous strands contain the fluorescent label to anneal

978-0-7695-4258-4/10 $26.00 © 2010 IEEE
DOI 10.1109/MINES.2010.188

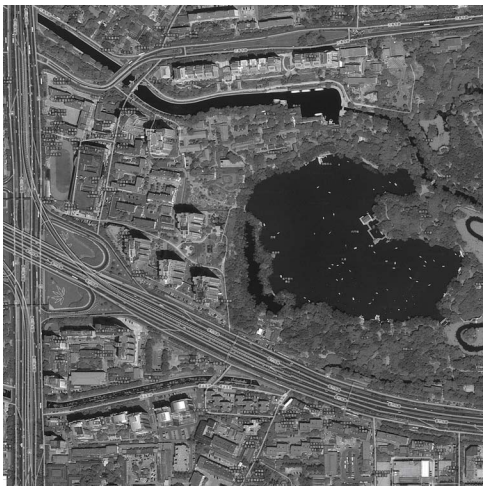

Figure 1. A Big Image Example (Map.bmp)

with probes which correspond to the secret information on the chip, and get the secret information by the fluorescence reaction.

An image encryption algorithm based on DNA sequences for the big image is presented in this paper. We don't use DNA biological operation to implement image encryption, yet the first DNA sequence is used to generate the scrambling sequence to accomplish pixel scrambling, and the second DNA sequence is used to generate the three DNA templates to accomplish pixel replacement. This algorithm is further fit for encrypting the big image as a result of its principle. Since the main keys are the natural DNA sequences, this algorithm has higher security and is robust against all kinds of attacks.

II. Image Encryption Algorithm

A. The Introduction of Algorithm

Although a lot of more mature encryption algorithms have been proposed, they are hardly fit for encrypting the big image. In the practice, there are many big images that need been transmitted via the Internet and can not be compressed arbitrarily, such as the map (Fig.1). This map is 2000×2000 in size. If it is compressed, a lot of important information will be incapable of identification. So an image encryption algorithm for the big image that owns the low encryption time and the high security is necessary.

At present, the pixel scrambling methods mainly include two types. The one is all pixels scrambling, and the other is ranks compound scrambling. It is obvious that the first type is more secure than the second one. But the first type need more encryption time, when the image is the big scale in particular. For the map.bmp (Fig.1), the encryption time of the first type is considerable, and the sender is not able to accept. The encryption time of the second type is far lower than the first one. However, Fig.2 shows the effect of this type, and the results are not satisfactory.

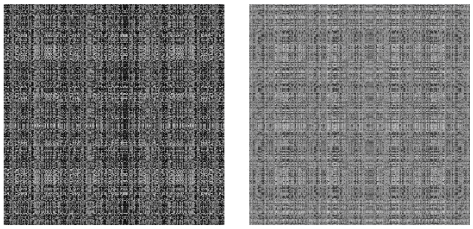

Figure 2. Ranks scrambling Results

In this paper, we use ranks compound scrambling to confuse the original image in the light of the scrambling sequence are generated by the natural DNA sequence, and the new image and three DNA templates that are generated by the second DNA sequence and the rules of Fig.3 are XORed in turn.

B. The Flow of the Encryption Algorithm

In this paper, the original image is confused in the light of the scrambling sequence that is generated by using the natural DNA sequence. Then, the new image and the three DNA templates that are generated according to the other DNA sequence are XORed in turn. Fig.4 is the flow chart of this algorithm. The image encryption algorithm is as follow:

Step1: Input the original image A_0 is $m \times n$ in size, where m and n are rows and columns of the image respectively.

Step2: Gain the image A_1 by confusing the original image A_0 in the light of the scrambling sequence which is gained according to the first natural DNA sequence. The information of the first DNA sequence is the part of the secret key information.

Step3: The DNA template B_1 is generated by the second DNA sequence.Then, the DNA template B_1 and the image A_1 are XORed, and the image A_2 is generated. In this algorithm, we design that a gray value is made up of four bases. One base represents two binary digits, in which A, C, G and T are replaced by 00, 01, 10 and 11. For instance, the binary string of DNA sequence is CAGT is 01001011, and the corresponding pixel gray value is 75. The second DNA sequence D_2 is used to gain the DNA template, where $D_2 = \{d_{2k}\}$, $1 \leq k \leq l$, $d_{2k} \in \{A, C, G, T\}$. The information of the second DNA sequence is the other part of the secret key information.

Step4: According to Fig.3 (b) and Step3, the DNA template B_2 is generated by the DNA template B_1 and the image A_2 are XORed, and the image A_3 is generated.

Step5: According to Fig.3 (c) and Step3, the DNA template B_3 is generated by the DNA template B_2 and the image A_3 are XORed, and the image A_4 is generated.

Step6: Gain the encrypted image A^1, where $A^1 = A_4$.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

(a)

1	6	11	16	21
2	7	12	17	22
3	8	13	18	23
4	9	14	19	24
5	10	15	20	25

(b)

25	24	23	22	21
20	19	18	17	16
15	14	13	12	11
10	9	8	7	6
5	4	3	2	1

(c)

Figure 3. The Matrices of the Location

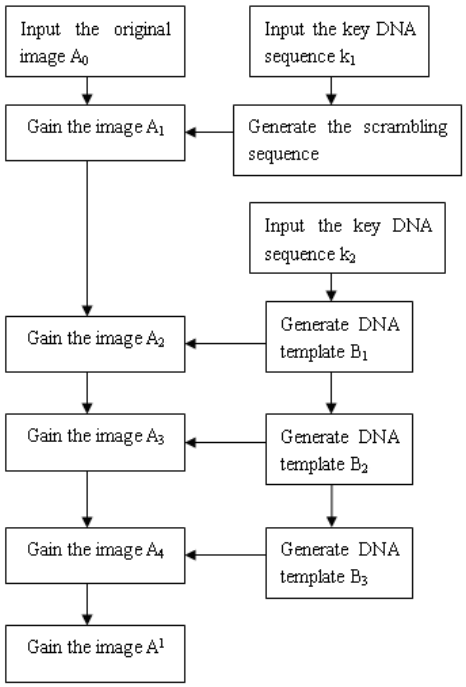

Figure 4. The Flow Chart

III. Experimental Results

In this paper, for the original gray image Map.bmp that is 2000×2000 in size, we use Matlab7.1 to simulate the experiment on the condition that we set the encryption keys are (Escherichia coli HS, 72, 120, Mycobacterium marinum M, 101, 319).

Fig.5 is the experimental result shows the encrypted image and decrypted image. Fig.5 (a) shows the original image, and

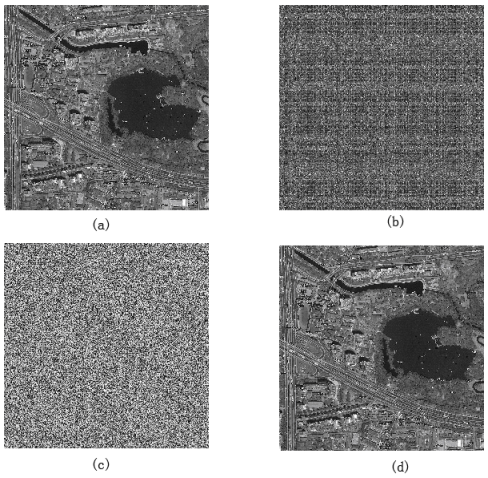

Figure 5. Experimental Results

Fig.5 (b) is the scrambling image is gained by the scrambling process that the DNA sequence is used to generate the scrambling sequence in the light of the DNA sequence representation and the original image is confused by ranks location translation. Fig.5 (c) is the encrypted image that is different from the original image absolutely. The encryption processes contain three XOR operation. The decryption processes are similar to the encryption ones. If and only if the true keys are obtained, the encrypted image is executed on the basis of the decryption algorithm and the decrypted image (Fig.5 (d)) is gained. From the experimental results, the image encryption algorithm is feasible and satisfactory.

IV. Algorithm Performance Analysis

A image encryption algorithm is satisfactory only when it is robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analysis has been performed on the proposed one, including some important ones like key space analysis, statistical analysis, etc. The security analysis demonstrates that the algorithm owns the high security.

A. Key's Security Analysis

A large key space is very important, since we must be assumed that everything is known by the attacker except the keys in the light of the hypothesis is proposed by Kerckhoff. So it could repel the exhaustive attacks only when the key space is large enough. In this paper, we use the natural DNA sequences as main keys. In the nature, DNA sequences are various, and the length has the considerable difference. In case of the same DNA sequence, since the difference of the length and the initial position, a segment is quite different from others. Therefore, the key space is large enough to resist exhaustive attacks.

In order to further analyze sensitivity, We test the algorithm under the worry decryption keys . If key values

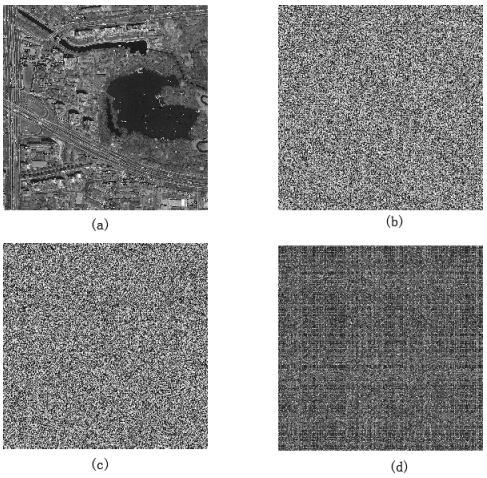

Figure 6. The Experimental Results of the Wrong Keys

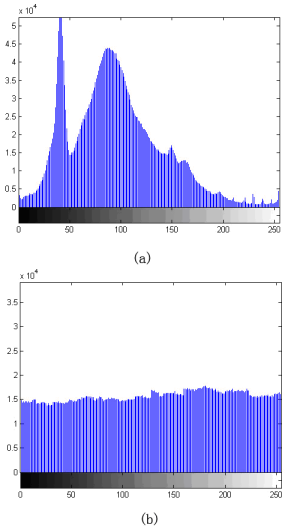

Figure 7. The Gray Histograms of the Image before and after Encryption

have slight change, for example, the decryption keys are (Escherichia coli SE11, 72, 120, Mycobacterium marinum M, 101, 319) and ((Escherichia coli HS, 72, 120, Mycobacterium marinum M, 102, 319) respectively, the decrypted images are different from the original image. Fig.6 shows the experimental results. Fig.6 (c) and Fig.6 (d) are the decrypted images under the wrong key1 and key2 respectively. We barely distinguish any information of the original image.

B. The Gray Histogram Analysis

An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. If the gray histograms of the image before and after are little or no statistical similar, it could better prevent the leakage of information by statistical attacks.

We compare the gray histograms of the Map.bmp before and after encryption (Fig.7) to analyze the statistical performance, and we can see that the gray histogram of the encrypted image (Fig.7 (b)) is fairly uniform and significantly different from the one of the original image (Fig.7 (a)). Hence, The gray histogram does not provide any clue to use any statistical attack on the presented image encryption image and to recover the original image.

C. Correlation Coefficient Analysis

The correlation of the adjacent pixels in the original image is very high, and an effective encryption algorithm can reduce the correlation of between adjacent pixels. Here, to test the correlation between two adjacent pixels of Map.bmp before and after encryption, we select 3000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image at random, then by using the following formulas to calculate the correlation coefficient.

Fig.8 shows the correlation of two horizontal adjacent pixels of Map.bmp before and after encryption. Fig.8 (a) shows the correlation of the original image, and Fig.8 (b) shows the one of the encrypted image, where the correlation coefficients are 0.8562 and 0.0105 respectively. The other two groups are (0.9475,0.0024) and (0.8187, -0.0026) respectively. From experimental results, we can see that the correlation coefficient of the adjacent pixels in the encrypted image is far lower than the one in the original image, and it is obvious that the image encryption algorithm can strongly resist statistical attack.

V. Conclusion

This paper presents a image encryption algorithm for the big image that is to use the DNA sequences to generate the scrambling sequence and encryption template so that the encryption time of the big image is reduced to a great extent. The main keys are the natural DNA sequences in this paper, so the key space is large enough to resist exhaustive attacks. The analysis demonstrates that the image encryption algorithm is efficient and highly secure. This algorithm can effectively resist attacks.

Acknowledgment

This work is supported by National High Technology Research and Development Program (”863” Program) of China (No. 2009AA01Z416).

References

[1] G. D. Ye, ”Image Scrambling Encryption Algorithm of Pixel Bit Based on Chaos Map” Pattern Recognition Letters, vol. 31, pp. 347-354, 2009.

[2] M. Zeghid, M. Machout, L. Khriji, A. Baganne and R. Tourkil, ”A modified AES Based Algorithm for Image Encryption” International Journal of Computer Science and Engineering, vol.1, pp. 70-75, 2007.

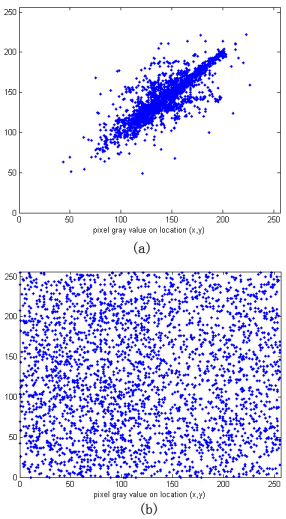

Figure 8. Correlation of Two Horizontal Adjacent Pixels

[3] S. G. Lian, "Efficient Image or Video Encryption Based on Spatiotemporal Chaos System" Chaos, Solitons and Fractals, vol. 40, pp. 2509-2519, 2009.

[4] Y. Wang, K. W. Wong, X. F. Liao, T. Xiang and G. R. Chen, "A Chaos-based Image Encryption Algorithm with Varialbe Control Parameters" Chaos, Solitons and Fractals, vol.41, pp.1773-1783, 2009.

[5] X. J. Tong, M. G. Cui, and Z. Wang, "A New Feedback Image Encryption Scheme Based on Perturbation with Dynamical Compound Chaotic Sequence Cipher Generator" Optics Communications, vol.282, pp.2722-2728, 2009.

[6] F. Y. Sun, S. T. Liu, Z. Q. Li and Z. W. L, "A Novel Image Encryption Scheme Based on Spatial Chaos Map" Chaos, Solitons and Fractals, vol.38. pp.631-640, 2008.

[7] T. G. Gao and Z. Q. Chen, "A New Image Encryption Algorithm Based on Hyper-chaos" Physics Letters A, vol.372, pp. 394-4002008.

[8] K. M. Faraoun, "A Novel Chaotic Ciphering System for Color Digital Image" Journal of Computer Science, vol. 22, pp.85-98, 2009.

[9] J. Fridrich, "Image Encryption Based Chaotic Maps" Systems, Man and Cybernetics Computational Cybernetics and Simulation, vol.2, pp.1105-1110, 1997.

[10] K. M. Faraoun, "A Novel Chaotic Ciphering System for Color Digital Image" Journal of Computer Science, vol.22, pp.85-98, 2009.

[11] S. J. Xu, J. Z. Wang and S. X. Yang, "An Improved Image Encryption Algorithm Based on Chaotic Maps" Chinesse Physics B, vol.17, pp. 4027-4032, 2008.

[12] X. J. Tong and M. G. Cui, "Image Encryption Scheme Based on 3D Baker with Dynamical Compound Chaotic Sequence Cipher Generator" Signal Processing, vol. 89, pp. 480-491, 2009.

[13] J. Peng, "A Digital Image Encryption Algorithm Based on Hyper-chaotic Cellular Neural Network" Fundamenta Informaticae , vol.90, pp. 269-282, 2009.

[14] G. Z. Xiao, M. X. Lu, L. Qin and X. J. Lai, "New field of cryptography: DNA cryptography" Chinese Science Bulletin, vol, 51, pp.1413-1420, 2006.

[15] P. C. Wong, K. K. Wong and F. Harlan, "Organic Data Memory Using the DNA Approach" Communications of the ACM, vol. 46, pp. 95-98, 2003.

[16] A Gehani, T. H. LaBean and J. H. Reif. "DNA-based Cryptography" Dimacs Series in Discrete Mathematics and Theoretical Computer Science. vol. 54, pp. 233-249, 2000.