Implementation of Digital Image Encryption Algorithm Based on DNA Coding and Chaos Theory

Denghui Li¹, Yanhong Wang²,3,*

¹Institute of Information Technology of GUET, Guilin, China
²Guangxi Key Lab of Wireless Wideband Communication & Signal Processing, Guilin, China
³Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) GUET, Guilin, China

*Corresponding author e-mail: 13642430@qq.com

Abstract. Because of the large amount of data and high redundancy, digital image can not be encrypted by traditional methods. The method based on DNA and chaos theory can be used for image encryption. The experimental results show that the gray value of the image after encryption is randomly and evenly distributed, which directly loses the features of the original image. The histogram is balanced, the correlation between adjacent pixels is low, and the information entropy is close to the ideal value, which shows a good anti cracking ability and can restore the image well.

1. Introduction

Dr. Adleman creatively used the idea of base complementary pairing to solve the Hamilton path problem with seven nodes in 1994, and it has started a boom in DNA computing research. The development of DNA computing has been greatly promoted by many researchers, and some remarkable achievements have been made. The basic principle of DNA computing is to code DNA sequence as the carrier of information coding. Based on the characteristics of double helix structure and complementary base pairing of DNA molecules, the problem to be solved is mapped to a specific DNA sequence, and then the solution space of the problem is generated by special operators and controllable biochemical reactions. Finally, using modern biotechnology to obtain results.

DNA computing has some significant advantages. Firstly, DNA Computing supports highly parallel computing, which can achieve large-scale parallel search, and the computing speed is very fast. Secondly, when DNA is used as the carrier of information, its storage capacity is very large, one cubic millimeter DNA solution can store 100 trillion GB of binary data. In addition, DNA computing consumes one billionth of the energy that computers use to do the same job. Because DNA computing has so many advantages, it has become the hottest research field in recent years.

DNA cryptography is a new application of DNA computing in the field of cryptography. It uses the advantages of DNA information carrier, biotechnology, high storage and high parallelism to realize cryptography functions such as encryption, authentication and signature. At present, the research of DNA cryptography has just started, but many achievements have been made. The mapping substitution method and XOR method proposed by Professor Gehani is a one-time-one-density method based on DNA, and it's considered absolutely safe in theory. But it's hard to make a large-scale DNA scrambling book that can easily separate and read data. Celland proposed a DNA based encryption algorithm for information hiding, and Rao Nini proposed encryption based on recombinant DNA.
technology, and so on. But all these methods are based on complex biological experiments, which are expensive and not practical.

2. Chaotic system

In the 1960s, when Lorenz studied the theory of air system, he found that small changes in initial conditions would lead to unpredictable results, which is the famous butterfly effect, therefore Lorenz is also known as the "father of chaos". With the development of science and technology, people's research on chaos system is gradually in-depth, and they have made remarkable achievements in theoretical research and application research. Although scholars at home and abroad have fully studied chaos, the definition of chaos is not uniform. In 1975, Li Tianyan and Yorker first proposed the mathematical definition of chaos[1]-[2]:

If the continuous self mapping \( f(x) \) on the closed interval \( I \) satisfies the following three conditions, it can be called chaotic:

1. There is no upper bound for the period of \( f(x) \):

\[
\lim_{n \to \infty} \sup |f^n(x) - f^n(y)| > 0, \forall x, y \in S, x \neq y
\]

2. There is an uncountable subset \( S \) in the closed interval \( I \), and there is no periodic point in \( S \), and

\[
\lim_{n \to \infty} \inf |f^n(x) - f^n(y)| = 0, \forall x, y \in S
\]

3. \( \forall x \in S, \forall p \in \text{Per}(f) \), and \( \lim_{n \to \infty} |f^n(x) - f^n(p)| > 0 \). where \( f^n(x) = f(f(f(\cdots f(x)))) \)

Chaotic system has its own characteristics, including initial value sensitivity, internal randomness, long-term unpredictability, boundedness and ergodicity[3]. These characteristics are inextricably related to cryptography.

3. Image Encryption Algorithm Based on DNA Coding and Chaos Theory

3.1. A subsection

The image encryption method based on DNA coding is a new image encryption method, which makes use of the advantages of DNA computing for image encryption and has a high research value. Each single strand DNA sequence consists of four bases, A, T, C and G, among which A and T, C and G are complementary base pairs[4]-[6]. If a base is represented by two bits, there are \( 4! = 24 \) coding methods, considering the complementary rules of base, only 8 methods meet the requirements, as shown in table 1.

|   | 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 | 10 | 01 | 11 | 00 | 11 | 00 | 10 | 01 |
| G | 01 | 10 | 00 | 11 | 00 | 11 | 01 | 10 |

According to the rules of bit operation, the rules of DNA addition and subtraction operation can be given as shown in Table 2 and table 3.
Table 3. The rule of DNA addition operation

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

3.2. Logistic map

Logistic map is a kind of simple chaotic map which is widely used. Its function is defined as follows:

\[ x_{n+1} = \mu x_n(1-x_n) \]  

(3)

Where \( 0 < \mu \leq 4 \) is called a branch parameter, \( x_n \in (0,1), n = \{0,1,2,3,\ldots\} \), and if \( 3.5699456 < \mu \leq 4 \), the logistic map is in chaos. In this case, the sequence generated by the initial condition \( x \) under the action of logistic map is aperiodic and non-convergent, and this sequence can be used for image encryption and decryption.

3.3. Lorenz system

Lorenz system is a continuous three-dimensional chaotic system, and its function is defined as follows:

\[
\begin{align*}
\dot{x}_1 &= \alpha (x_2 - x_1) \\
\dot{x}_2 &= \beta x_1 - x_3 (x_1 + 1) \\
\dot{x}_3 &= x_1 x_2 - \gamma x_3 
\end{align*}
\]

(4)

Where \( \alpha, \beta, \gamma \) are system parameters. When \( \alpha = 10, \beta = 28, \gamma = \frac{8}{3} \), then the system will go into chaos.

3.4. Chen hyperchaotic system

Chen hyperchaotic system is derived from Chen system, and its dynamic equation is as follows:

\[
\begin{align*}
\dot{x} &= a(y - x) \\
\dot{y} &= dx - xz + cy - h \\
\dot{z} &= xy - bz \\
\dot{h} &= x + k 
\end{align*}
\]

(5)

Where \( a, b, c, d \) and \( k \) are system control parameters, \( x, y, z, h \) are state variables. When \( a = 36, b = 3, c = 28, d = 16 \) and \( -0.7 \leq k \leq 0.7 \), then the system will go into chaos. Because that Chen hyperchaotic system has multiple positive Lyapunov, so it is more suitable for image encryption.

4. Implementation

First of all, the image should be divided into blocks, and the block size should be set to \( t \). Then adjust the size of the image, increase the number of rows and columns to the smallest integer that can be divisible by \( t \), and all added elements are added with 0.

The second step is to generate the logistic sequence according to the formula (3). In order to ensure good randomness, more random points are generated, and the previous part is removed when the value is taken. And the resulting sequence is transformed into a random matrix \( R \) of \( M \) rows and \( N \) columns.

Then four system parameters \( x, y, Z \) and \( h \) of Chen hyperchaotic system are obtained. Further using them and block number \( r \) to solve fourth order Runge-Kutta differential equations, and Obtain a Chen hyperchaotic system with good randomness. Finally the image encryption is realized by DNA coding operation on the block image. And the decryption process is an inverse process.
5. Experimental results and analysis

Using the above method, we encrypted the image of Lena, and the effect before and after encryption is shown in Figure 1. We can find that the encrypted image cannot see any intuitive information of the original image at all.

![Figure 1. Lena image before and after encryption.](image1)

Then, we draw the histogram of the original image and the encrypted image respectively, as shown in Figure 2. The results show that the histogram of the encrypted image is more balanced and has better anti statistical attack characteristics.

![Figure 2. the histogram of the original image and the encrypted image](image2)

In addition, we also analyzed the correlation of the image before and after encryption, and found that the horizontal correlation of the image before encryption was 0.98079, the vertical correlation was 0.98952, and the diagonal correlation was 0.96501; after encryption, the correlation changed greatly, which were 0.000612, 0.001991 and 0.002732. After encryption, the original image is evenly distributed to the ciphertext image. We also analyzed the information entropy of the image before and after encryption, and the information entropy of encrypted image is 7.9992, very close to the ideal
value of 8, it shows that the gray value distribution of the encrypted image is very uniform, and it can effectively resist the brute force attack.

Finally, we restore the image information from the encrypted image.

6. Conclusion

Through the experiment of encryption and decryption of Lena image, it is found that the method based on DNA and chaos theory is used to encrypt the image. After encryption, the gray value of the image is randomly and evenly distributed, which directly loses the features of the original image. The histogram is balanced, the correlation between adjacent pixels is low, and the information entropy is close to the ideal value, which shows a good anti cracking ability and can restore the image well.

7. Acknowledgments

This work was supported by Guangxi Key Lab of Wireless Wideband Communication & Signal Processing (CXKL06180105) and Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology, and Scientific research project of the Guangxi Education Office(2017KY1350), thanks for their supports.

References

[1] Zhi-Hong G, Fangjun H, Wenjie G. Chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1–3):153-157.

[2] Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos Solitons and Fractals, 2004, 21(3):749-761.

[3] Yin Y Q, Long Z M. Chosen plaintext attacking on a hyper-chaos image encryption algorithm[C]. IEEE, International Conference on Electronics Information and Emergency Communication. IEEE, 2014:144-147.

[4] Niyat A Y, Hei R M H, Jahan M V. Chaos-based image encryption using a hybrid cellular automata and a DNA sequence[C]. International Congress on Technology, Communication and Knowledge. IEEE, 2016.

[5] Xiaoling Huang, Guodong Ye. An image encryption algorithm based on hyper chaos and DNA sequence[J]. Multimed Tools Appl. DOI 10.1007/s11042-012-1331-6.

[6] Gupta, Ritu; Jain, Anchal. A New Image Encryption Algorithm based on DNA Approach[J]. International Journal of Computer Applications . Jan2014, Vol. 85, p27-31.