An Image Encryption Algorithm Based on Chaos System and DNA Strand Displacement Model

Ze-jun ZHANG, Bo-xiang XIAO, Xue-dong ZHENG and Chang-jun ZHOU*

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

Keywords: Image encryption, Chaos system, DNA strand displacement, XOR operation.

Abstract. In this paper, we proposed a novel algorithm for image encryption. In the scheme, three chaotic sequences are generated by Lorenz chaos system. These chaotic sequences are used to permutation and diffusion the digital image. Furthermore, the algorithm introduce the DNA strand displacement reaction model to extract the secret key and then encrypt the image with a combination of XOR operation. The simulation results and security analysis show that our algorithm can successfully encrypts and decrypts the input image and gets a better encryption performance. Meanwhile, the method also has a good ability of resisting attacks.

Introduction

In recent years, with the rapid development of the Internet, digital images are more and more frequently used by people. However, due to the openness of the network, the sharing of information and the continuous development of hacker technology, attack on image information may harm the business interests and privacy of individuals or organizations. Therefore, scholars have taken a series of measures to ensure the security of image transmission, in which image encryption is one of the most effective way. Because of the redundancy and special storage format of an image, the traditional block ciphers are not very suitable for image encryption. Therefore, a variety of new encryption algorithms been proposed to solve the problem of digital image encryption, such as image encryption algorithm based on modern cryptography, image encryption algorithm based on matrix transformation, image encryption algorithm based on chaos, image encryption algorithm based on secret sharing[1]. However, with the rapid increase of computer hardware and the continuous development of some new computer studies, these algorithms are more easily cracked.

In the chaos theory, when the initial conditions have a little changes, the future state of system can be caused extremely large difference through the continuous amplification. In numerous continuous chaotic system, Lorenz chaotic system are heavily used in encryption algorithms[2]. However, using chaotic system alone will have some problems like slow encryption speed, too large storage space and vulnerable to suffered the static attacks.

Adleman first proposed DNA computation in 1994, and used molecular computation of solutions to combinatorial problems to solve the Hamilton path problem[3]. After the advent of DNA computing and coding techniques, it was focused on by some researchers in the field of image encryption because of its high parallelism and massive storage capacity. DNA strand displacement is the latest developed technology of DNA computing. In the DNA strand displacement reaction, information can be hidden into single strand DNA after complied. Each short DNA single strand(20-80nt) represent a logical signal, change the sequence and length of a single DNA strand can represent an another information, it is easy to encrypt the information. So, we try to use the DNA strand displacement model into image encryption and look forward to get better encryption effect.
The Proposed Image Encryption Scheme

The Algorithm Ideas

In the paper, a novel image encryption algorithm based on the chaos system and DNA strand displacement model be proposed. First of all, code the original image according to the DNA encoding rules[4]. DNA encoding and decoding method can converts the binary pixel matrix to the DNA matrix of four bases A, G, C and T. Then use two chaotic sequences which generated from the Lorenz chaos system to scramble the DNA pixel matrix[5,6]. Lorenz chaos system is a classical high-dimensional chaotic system, it shows great sensitivity to the initial conditions. Secondly, diffuse the values according to the secret key generated by DNA strand displacement model, chaos sequences and the XOR operation which is widely used in encryption algorithms for its reflexive[1]. Then scramble the matrix again. At the end, we use the rest of chaotic sequences to diffuse the matrix. After DNA decoding for DNA matrix, the encrypted image is obtained. When the users receive the encrypted image, decoding the image by reverse order of the encryption process to get the completed original image information.

DNA Strand Displacement Model

DNA strand displacement is a new technique developed in recent years. In 2011, professor Winfree using four neurons achieved a game of "read your mind" based on DNA strand displacement[7]. In 2013, Zhang proposed a calculation model of logical gate and logical OR gate and introduced the concept single polar and bipolar[8].

DNA strand displacement model is introduced into image encryption process in the algorithm. The mechanism of DNA strand displacement reaction is: The longer DNA strand have more favorable trends to hybridize than that of short strands, control or induce the downstream displacement reaction by change the length and sequence of input signal molecules. The specific steps are shown below:

1) Two complementary strands of DNA bind together(strand A is longer than B);
2) At room temperature, single strand C(sequence is completely complementary with A) combine the single strand of A in specific identification area.
3) Strand C gradually occupy binding site between A and B, strand A and B gradually separate, slowly reach the most steady state.
4) At the last, strand C and A completely complementary, strand B and A separate completely.

Generation of the Secret Key and Application of DSD Model

The secret key of algorithm consist of two parts: the first part is three chaotic sequences and the original value for chaotic system. The other part, the secret key generated by DNA strand displacement model. Lorenz chaotic system is shown in above, the initial value of the chaotic equation is chosen with the same value as the reference [2]. System enter chaos state and generate three random and ruleless chaotic sequences which can be used in encryption process.

DSD model based on the reaction of DNA strand displacement, used for generate the secret key. Its operate object is pixel matrix which encoded by DNA, each pixel site is a DNA sequence containing four bases. For convenience, we divide DNA matrix into equal blocks, the size of each block is 4*2. For each be encrypted block, to find the corresponding secret block according to two chaotic sequences, then extract the secret key by DSD model. Each line of secret block contain 8 bases, the line is viewed as a strand of DNA, this strand bind with a short DNA strand containing 3 bases. According to the DSD model, put one long DNA strand to permute the short strand that complementary with three bases on the mother strand. The short strand is our secret key, we get four DNA short strands in total because the secret block has four rows. The four DNA sequences are regard as the secret key to encrypt the corresponding block. The process of generate secret key is shown as Figure. Encrypted block has two parts in the each line, each part contains four bases. The first three bases of the each part do XOR operation with the secret key generated in the last step, then replace the three bases with the result.
Encryption Process

The encryption algorithm mainly consists of three parts: pixel permutation, encrypted by DNA strand displacement model, diffusion the pixel value. The pixel scrambling was used two times, respectively before using the DSD model and diffuse the pixel values. In this paper, we use chaotic sequences x, y in position scrambling, use x, z in DSD encryption model and use y, z in diffuse the pixel values. The schematic block diagram is shown in Figure 2.

The major steps of the algorithm are described as follows:

Step 1: Convert the input image whose row is m and column is n into a binary matrix, then encode the binary matrix by the second DNA coding rule described in this paper. We get a DNA matrix DA whose size is (m, n), each site is a DNA sequences that contain four bases;

Step 2: Generate three chaotic sequences $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n), z = (z_1, z_2, ..., z_n)$ from Lorenz chaos system under the condition that initial values are $x_1, y_1, z_1$ and system parameters are $\sigma, \rho, \beta$;

Step 3: Integer the chaotic sequences $x, y$ as follows:

$$
\begin{align*}
  x(i) &= \text{floor}(m \times x(i)) \quad i = 1, 2, ..., m \\
  y(j) &= \text{floor}(n \times y(j)) \quad j = 1, 2, ..., n
\end{align*}
$$

Where $x(i)$ is the value of the position $i$ from chaotic sequence $x$, $m$ is the value of rows for pixel matrix, $n$ is the value of column for pixel matrix, $y(j)$ is the same with $x(i)$. Use the new chaotic sequences to scramble DA, we can get the new matrix CA, the equation as follows:

$$
DA(i, j) \leftrightarrow DA(x(i), y(j)); \quad i = 1, 2, ..., m, j = 1, 2, ..., n
$$

Step 4: Divide CA into equal blocks $bR\{i, j\}$, in the bR, each size of block is 4*2. Integer the sequences $(y, z)$ according to the step 3, the maximum of the new sequences value is rows and column of the block matrix. Diffuse the values of block matrix according to the applications of the DNA strand displacement, the specific process refer above in this paper, get sequence matrix HA via restructuring the blocks $bR\{i, j\}$;

Step 5: Repeat the step 3, scramble the NA again by the chaotic sequences $(x, z)$, we get the new matrix MA;

Step 6: Divide the MA as step 4 and integer the chaotic sequences $(y, z)$ according to step 3. Diffuse the values of MA by the new chaotic sequences and XOR operations proposed in this paper, using the following method:

$$
bR(i, j) \leftarrow bR(i, j) \ XOR bR(y1(i), z1(j)) \quad i = 1, 2, ..., m/2, j = 1, 2, ..., n/4
$$

Restructuring the block matrix, we get the new DNA sequence matrix HA;
Step 7: Decoding the HA by the third DNA coding rules described in this paper, result is a binary matrix and then transform it to decimal matrix for output.

The decryption process is the reverse order of the encryption process. After the customer receive the secret key from sender, the correct decryption image can be obtained according to the decryption process.

Simulation Result and Security Analysis

Simulation Result

The input image is standard 256*256 gray image "Lena" shown in Fig 4(a). We utilize Matlab 7.1 to simulate the algorithm and set parameters x=2.4932, y=3.1311, z=4.9843. The encryption image is shown in Figure 3(b) and decryption image is Figure 3(c). As we can see, there is no relationship between the input image and encrypted image, the encryption is a snow figure without any valuable information. It shows that our algorithm has completed the encryption of the input image and achieved the desired effect.

![Image](image.png)

(a) The original image (b) The encrypted image (c) The decrypted image

**Figure 3.** The original image and the encrypted image and the decrypted image.

Key Space Analysis

In the proposed encryption scheme, the key space can be wide because the Lorenz chaotic system is sensitive to the initial values and parameters. The three initial values x,y,z can be use as the secret key. If the computing precision is $10^{-14}$, the key space is $10^{14} \times 10^{14} \times 10^{14} = 10^{42} \approx 2^{140}$. The key space is large enough to resist exhaustive attack.

Sensitive Analysis

Large key space and high sensitive are necessary conditions for a security image encryption algorithm. The Lorenz chaos system we used in this paper is sensitive to the initial values and system parameters, therefore, only completely correct secret key can decrypt the correct image. The decryption image will have a huge difference with the original image even if the secret key is only changed a little[9]. To test the key sensitivity of composed encryption scheme, we use one correct key and three wrong key as contrast experiment. The correct key is K=[2.4932,3.1311,4.9834], the wrong key K1 = [2.4932, 3.131072, 4.98339], K2 = [2.49315, 3.13, 4.98339], K3 = [2.49315, 3.131072, 4.984]. The image generated by the wrong keys is completely different with the original image. The result indicate that the algorithm we proposed is extremely sensitive to the secret key.

The Gray Histogram Analysis

The gray histogram is the static of gray value distribution in the image. The horizontal axis shows the range of gray value and vertical axis shows frequency of one gray value. As an important index to evaluate the security of encryption algorithm, the larger the change between the original image and encrypted image, the better encryption effect for the algorithm[10]. The gray histogram of the original image is shown in Fig 4, there are multiple peaks and valleys, it shows that the distribution of pixel
value is very uneven. The Figure 5 is gray histogram of encrypted image, the histogram is fairly uniform. An attacker cannot get any useful information from the encrypted image.

![Figure 4. The gray histogram of original image.](image1)

![Figure 5. The gray histogram of encrypted image.](image2)

**Correlation Coefficient Analysis**

The gray histogram can shows the distribution of gray values, but cannot reflect the position information of pixels. Therefore, we use correlation coefficient present the relationship of two adjacent pixel. To calculate the correlation coefficient of the original image and encrypted image, we randomly select 3000 pairs of adjacent pixels from the horizontal, vertical and diagonal direction. Computational process refer with [11].

After calculation, the correlation coefficient of adjacent pixels from encrypted image at the horizontal, vertical and diagonal direction are 0.0025, 0.0014 and 0.0013. They are far less than original image very closed to 0, therefore the correlation coefficient of image fully decreased by proposed encryption algorithm. Simulate results of the correlation coefficient of adjacent pixels are shown in Figure 6 and 7. As we can see from the image, there is a weak correlation in encrypted image because the values of adjacent pixel distribute very dispersive.

![Figure 6. Correlation for the original image.](image3)

![Figure 7. Correlation for the encrypted image.](image4)

**Information Entropy**

In information theory, information entropy is used to measure the expected value of a random variable appearing. It also be represented uncertainly degree of image information and gray value distribution of image. The formulas of compute information entropy is follows:

\[
H(X) = -\sum_{i=0}^{2^8} P(x_i) \log_2 P(x_i)
\]  

(4)

For a standard 256*256 gray image, its ideal value is 8[12]. Information entropy of the encrypted image in our paper is 7.9973, very closed to 8, indicate that our algorithm has a good encryption effect.
Conclusion

In this paper, a gray image encryption scheme based on Lorenz chaos system and DNA strand displacement model be proposed. The simulate result prove this encryption algorithm has a better cipher capacity than some traditional methods. Furthermore, the proposed scheme also can strongly resist kinds of statistical analysis and exhaustive attacks. The innovation point of this paper is to introduce the DNA strand displacement model into the field of image encryption. The future direction of work is to express the algorithm with real biochemical reactions.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Nos. 61370005, 61672121, 61572093, 61402066, 61402067), and the Program for Liaoning Key Lab of Intelligent Information Processing and Network Technology in University.

References