2021 2nd International Conference on Computer Engineering and Intelligent Control (ICCEIC) | 978-1-6654-0212-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCEIC54227.2021.00028

Image Encryption System Based On Chaotic System And DNA Computing

Yunyi Li
School of Information Engineering
Zhengzhou University
Zhengzhou, China
qq315056127@163.com

Jiangfeng Xu
School of Information Engineering
Zhengzhou University
Zhengzhou, China
jfxu@zzu.edu.cn

***Abstract*—The misuse and arbitrary tampering of digital images by third parties pose a threat to the security and privacy of human subjects, requiring the development of good encryption techniques to meet the security needs of digital images. In this paper, we focus on the image encryption algorithm based on the combination of hyper chaotic system and DNA operation, which divides the digital image into three two-dimensional matrices by R, G and B channels, encrypts the image in blocks, and the chaotic sequence generated by the chaotic system determines the DNA coding, decoding and operation of each image block in the encryption process. The number of chaotic systems in the algorithm is increased and the encryption process is optimized to address the problems of low key space and inability to resist cropping attacks. The simulation results show that the improved encryption algorithm can resist the exhaustive key attack, the correlation of adjacent elements of the encrypted image is greatly reduced, and the encrypted image is resistant to cropping.**

Keywords-DNA coding and decoding; image encryption; chaotic systems ;

I. INTRODUCTION

The rapid development of digital technologies and communication networks has led to the generation of more and more digital data. Since images are two- or three-dimensional data, leading to a strong correlation of data between adjacent locations of images, traditional cryptosystems are not suitable for image encryption[1]. In order to enhance the resistance of encryption while adapting to the characteristics of digital images themselves, experts and scholars have successively proposed many schemes specifically for encrypting images, among which those based on chaos theory have excellent performance.

Chaotic systems have initial value sensitivity, randomness, ergodicity and certainty. The chaotic sequence generated by it is very suitable for data encryption because of its noise like and aperiodic characteristics. The designed encryption algorithm has large key capacity and high randomness, and has congenital advantages in image encryption[2]. Low-dimensional chaotic systems have low key capacity and therefore have low resistance to attack, while high-dimensional chaotic systems with high randomness and complexity have higher resistance to attack[3]. The DNA computing process has the advantages of massive parallelism, large storage capacity ultra-low power consumption, etc[4]. In this paper, we propose an image encryption system based on chaotic system with DNA computing and conduct simulation experiments and performance tests, and the experimental results show that the encryption system has large key capacity, high noise resistance, high cropping resistance, and high attack resistance.

II. COLOR IMAGE ENCRYPTION ALGORITHM

This encryption algorithm divides the color digital image into three two-dimensional matrices, performs DNA encoding and operations on each two-dimensional matrix in chunks, and then performs row and column permutations again after encryption. Three different chaotic sequences obtained by iteration of Logistic mapping, one for DNA operation with the original image, one for row permutation and one for column permutation, finally merge the three channels to get the color encrypted image. The encryption steps are as follows.

(1) The digital image I to be encrypted of size $M \times N$ is divided into three two-dimensional matrices R, G and B according to the following equation (1).

$$\begin{cases} I_1 = (:,:,1) \\ I_2 = (:,:,2) \\ I_3 = (:,:,3) \end{cases} \tag{1}$$

(2) The three two-dimensional matrices are filled with data 0 by size so that they satisfy the following equation (2). Where t is the chunk size, and each 2D matrix can be divided into $(M \times N)/t^2$ image blocks after filling 0.

$$\begin{cases} mod(M,t) = 0 \\ mod(N,t) = 0 \end{cases} \tag{2}$$

(3) Obtain the chaotic sequence: set the initial value x_0 and the parameter μ. Obtain the sequence $\{K_i\}$ by successive iterations of the Logistic mapping and set the length of the obtained sequence to $M \times N$. Where μ is set to 3.9999 and the initial value x_0 is generated according to equation (3).

$$x_0 = \frac{sum(I_1(:)) + sum(I_2(:))}{255 \times M \times N \times 2} \tag{3}$$

(4) The sequence $\{K_i\}$ is converted into a

978-1-6654-0212-5/21/$31.00 ©2021 IEEE
DOI 10.1109/ICCEIC54227.2021.00028

two-dimensional matrix of $M \times N$ according to equation (4), while the values of the matrix are transformed into the range from 0 to 255 for DNA operations with $I_i(i=1,2,3)$.

$$\begin{cases} k = mod\left(round\left(k \times 10^4\right), 256\right) \\ R = reshape(k, M, N) \end{cases} \tag{4}$$

(5) After setting the initial values and parameters, the four $(M \times N)/t^2$ sequences $\{X_i\}$, $\{Y_i\}$, $\{Z_i\}$, $\{W_i\}$ of all lengths are obtained by using the built-in Longo-Kuta function of Matlab. The four initial values $X(0)$, $Y(0)$, $Z(0)$, $W(0)$ of the Chen hyperchaotic system are calculated by equation (5).

$$\begin{cases} X_0 = sum\left(sum\left(bitand\left(I_1, 17\right)\right)\right)/17 \times M \times N \\ Y_0 = sum\left(sum\left(bitand\left(I_2, 34\right)\right)\right)/34 \times M \times N \\ Z_0 = sum\left(sum\left(bitand\left(I_3, 68\right)\right)\right)/68 \times M \times N \\ W_0 = sum\left(sum\left(bitand\left(I_1, 136\right)\right)\right)/136 \times M \times N \end{cases} \tag{5}$$

(6) The sub-blocks at the same position of I_1、I_2、I_3 use the same DNA coding method, uniformly determined by $\{X_i\}$. The DNA coding method of each sub-block of the R matrix is determined by $\{Y_i\}$. Because there are 8 ways of DNA coding, the values of sequence $\{X_i\}$ and sequence $\{Y_i\}$ need to be transformed into integers ranging from 1 to 8. The $\{X_i\}$ and $\{Y_i\}$ sequences are transformed according to equation (6).

$$\begin{cases} X = mod\left(round\left(A \times 10^4\right), 8\right) + 1 \\ Y = mod\left(round\left(B \times 10^4\right), 8\right) + 1 \end{cases} \tag{6}$$

(7) The same operator is used between the I_1、I_2、I_3 and R corresponding blocks, determined by the sequence $\{Z_i\}$ generated by the Chen hyperchaotic system. Since a total of four DNA operators are used in this algorithm, it is necessary to transform the sequence $\{Z_i\}$k into an integer in the range from 0 to 3 by transforming it according to equation (7). It is specified that if $Z_i = 0$, additive operation is used; if $Z_i = 1$, subtractive operation is used; if $Z_i = 2$, heterogeneous or operation is used; if $Z_i = 3$, homogeneous or operation is used.

$$Z = mod\left(round\left(C \times 10^4\right), 4\right) \tag{7}$$

(8) To obtain a better diffusion effect, the encryption result of the current sub-block is subjected to DNA operation with the previous sub-block again, except for the first sub-block, and the algorithm used is determined by the sequence $\{Z_i\}$. DNA decoding is performed on the matrix chunks after the DNA operation, and the sequence $\{W_i\}$ determines the DNA decoding rules of the sub-blocks after the operation.

(9) Two Logistic chaotic sequences are obtained. The chaotic sequence generation process is similar to step (3), and two chaotic sequences $\{k_x\}$ and $\{k_y\}$ of length M and N are obtained, where μ is uniformly set to 3.9999 and the two initial values x_{01} and x_{02} are generated according to equation (8).

$$\begin{cases} x_{01} = \dfrac{sum\left(I_1(:)\right) + sum\left(I_3(:)\right)}{255 \times M \times N \times 2} \\ x_{02} = \dfrac{sum\left(I_2(:)\right) + sum\left(I_3(:)\right)}{255 \times M \times N \times 2} \end{cases} \tag{8}$$

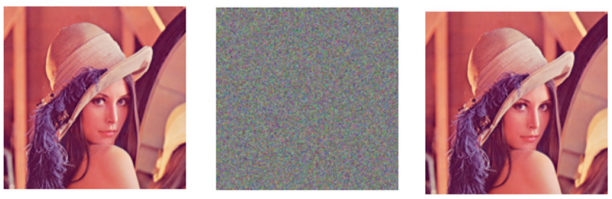
(10) The sequences $\{k_x\}$ and $\{k_y\}$ are arranged in descending order by equation (9), and the position sequences U_x and U_y before the ordering of each element in the sequences are obtained, and the row and column swap coordinates are used for the U_x and U_y sequence values and their corresponding indexes, respectively, to perform row permutation and column permutation on the matrices of the three channels after DNA decoding.

$$\begin{cases} [\sim, U_x] = sort\left(kx, 'descend'\right) \\ [\sim, U_y] = sort\left(ky, 'descend'\right) \end{cases} \tag{9}$$

(11) The three two-dimensional matrices that have been row-wise permuted are combined into one three-dimensional matrix to obtain the cipher-text image.

III. EXPERIMENTAL ANALYSIS

The simulation platform for this experiment is Matlab R2018a, and the size of "Lena" is 512×512 for the test simulation. Figure 1 shows the plain-text, cipher-text and decrypted images. From the visual point of view, there is no correlation between the cipher-text image and the original image, and after comparing the data, it is found that all the data of R, G and B channels are identical before and after encryption, so the encryption effect is excellent.



(a)Plain-text image (b)Cipher-text image (c)Decrypt image

Figure 1 Plain-text , Cipher-text and Decrypt images

A. Histogram analysis

Figure 2 shows the histograms of the plain-text and cipher-text images. The histogram comparison shows that the cipher-text image pixels have been nearly uniformly distributed with pseudo-randomness, which can hide the statistical properties of the original image and thus can effectively resist large-scale histogram-based statistical attacks against the image.

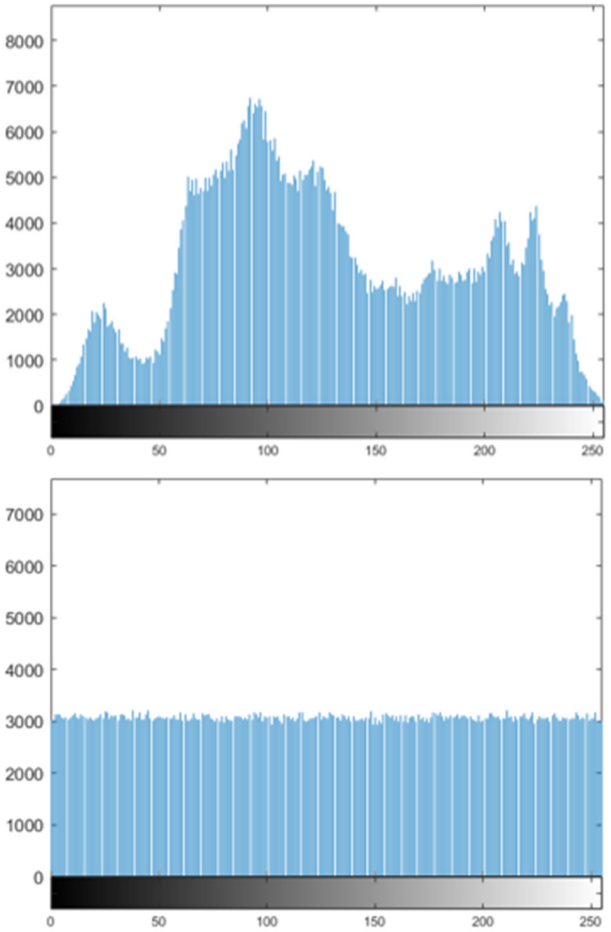


Figure 2 Histogram of plain-text and cipher-text

B. Correlation analysis of adjacent pixels

The ability of an image to resist an attack is inversely related to the correlation of its neighboring pixels. To test the resistance of the image to attack, 5000 pairs of pixel points adjacent to the image in horizontal, vertical and diagonal directions were randomly selected for analysis, respectively. The correlation coefficient is calculated as shown in equation (10).

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{10}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{11}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \tag{13}$$

Table 1 shows the results of the correlation calculations between the plain-text and cipher-text images in the R, G, and B components of the adjacent pixels and the comparison with other literature. From Table 1, it can be seen that the absolute values of the correlation coefficients of the neighboring pixels of the plain-text images are all close to with 1, indicating that the neighboring pixels of the plain-text are highly correlated with each other; while the absolute values of the correlation coefficients of the cipher-text images are all close to 0, indicating that the pixel distribution of the cipher-text images has good randomness.

Table 1 Comparison of correlation coefficients of adjacent pixels

	Horizontal direction	Vertical Direction	Diagonal direction
Plaintext Image	0.9613	0.9765	0.9491
Ciphertext Image	0.0029	-0.0030	-0.0019
Literature[1]	-0.0016	-0.0033	0.0130
Literature[5]	0.0017	0.0007	0.0008
Literature[6]	-0.0381	-0.0291	0.0027

C. Information entropy analysis

The specific mathematical definition of information entropy is shown in equation (14), which is an important indicator of the randomness of the grayscale value of an image.

$$H(x) = -\sum_{i=0}^{2^N-1} p(x_i)\log_2 p(x_i) \tag{14}$$

From Table 2, we can see that the information entropy of the three channels of the cipher image R, G, and B are close to the ideal value.8 It means that after encryption by this encryption algorithm, the confusion of the cipher image is close to the theoretical limit value, and by comparing with the literature, we can find that the information entropy performance of the algorithm in this paper is better and can effectively resist the information entropy attack.

Table 2 Comparison of information entropy			
Raw information entropy	Algorithm of this paper	Literature[1]	Literature[5]
7.7502	7.9998	7.9997	7.9992

D. Key Capacity

In this paper, the algorithm uses three Logistic chaotic systems, which use the same parameters μ, but their respective initial values x_0, x_{01} and x_{02} are different. μ and x_0, x_{01}, x_{02} and the four initial values $X(0)$, $Y(0)$, $Z(0)$, $W(0)$ of Chen hyperchaotic system can be used as the system key. 64-bit computers have an arithmetic precision of 10^{-15}, then the key space of this algorithm is about 10^{120}, and the key capacity space is huge, which can The key space of this algorithm is about 120, which has a large key capacity and can effectively resist exhaustive attacks. In addition, the parameter μ of the three Logistic chaotic systems can be set to different values, which can further expand the key capacity.

E. Key sensitivity analysis

Change the amount of one of the keys,x_0=0.4953 , to $+10^{-10}$, and keep the other keys unchanged. From the incorrectly decrypted image, we can see that no plaintext information can be seen in the incorrectly decrypted image. The verification of the other keys still yields the wrong decrypted image, which shows that this algorithm has a very high key sensitivity.

F. Analysis of anti-differential attacks

The experiments introduce the pixel change rate (NPCR), and the average change intensity (UACI) as two metrics to evaluate the ability of the algorithm in this paper to resist differential attacks.The expected values of NPCR and UACI are 99.6094% and 33.4635%. Table 3 shows the comparison of the NPCR and UACI test values of two ciphertexts before and after randomly changing a pixel value of the plaintext with other literature. The comparison shows that the algorithm proposed in this paper has higher plaintext sensitivity and high effectiveness against differential attacks.

Table 3 Analysis of anti-differential attacks		
Algorithm	NPCR	UACI
Algorithm of this paper	99.6131	33.4598
Literature[5]	99.6289	33.5420
Literature[6]	99.6114	33.4523

G. Analysis of shearing resistance

When the ciphertext image is subjected to cropping attack, for images with detail information, such as those containing some text, it is necessary to retain its detail information to the maximum extent to minimize the impact of cropping on the image as a whole. Here we crop the cipher image according to 1/16, 1/4 and 1/2 of the original image, and decrypt the cipher image after the crop attack, the specific simulation results are shown in Figure 3.

As can be seen from Figure 3, although the encrypted image is corrupted by different degrees of cropping, this algorithm spreads the impact on the cropped part to the whole image, and even when half of the information is lost, some features can still be obtained, which proves that this algorithm has a strong performance against cropping attacks.

Figure 3 Analysis of shearing resistance

IV. CONCLUSION

In this paper, we propose a color digital image encryption algorithm that is based on a combination of chaotic systems and DNA operations. The experimental analysis shows that the proposed algorithm has a simple encryption process, large key space, and can effectively resist exhaustive attack, statistical characteristic attack, differential attack, and cropping attack. Therefore, the proposed algorithm is of good use in the encryption of digital images.

REFERENCES

[1] Chai X , Gan Z , Yang K , et al. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations[J]. Signal Processing Image Communication, 2017, 52:6-19.

[2] Lian S , Sun J , Wang Z . Security Analysis of A Chaos-based Image Encryption Algorithm[J]. Physica A Statistical Mechanics & Its Applications, 2005, 351(2-4):645-661.

[3] Wang Ke. Research on image encryption algorithm based on chaotic system [D]. Anhui University, 2017.

[4] Wang X Y , Li P , Zhang Y Q , et al. A novel color image encryption scheme using DNA permutation based on the Lorenz system[J]. Multimedia Tools and Applications, 2018.

[5] Nematzadeh H , Enayatifar R , Yadollahi M , et al . Binary Search Tree Image encryption with DNA[J] . Optik , 2020 , 202 : 163505.

[6] Zhou M , Wang C . A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks[J]. Signal Processing, 2020, 171:107484