A Color Image Encryption Scheme Based on Chaos

Jing Li [a], Fei Xiang [b], Junpeng Zhang [c, *]

Electrical Engineering College, Henan University of Science and Technology, Luoyang 471023, China.

[*]Corresponding author: 1275668527@qq.com

[b]fayexiang @163.com

[c]1305783952@qq.com

Keywords: Chaotic System; Color Image; Logistic Map; Encryption.

Abstract: In order to improve the security of color image information, a two-dimensional Logistic system is combined with a newl discrete system to propose an image encryption scheme that can greatly expand the key space and enhance security. Firstly, the plaintext digital image is preprocessed, and its R, G, and B components are extracted and converted into a one-dimensional array, and the pseudo-random chaotic sequence generated by the two dimensional Logistic map is mathematically operated. Secondly, using the new two-dimensional discrete chaotic system based on the modified Marotto theorem and the corresponding one-time ciphertext XOR, get three one-dimensional arrays. Finally, convert to a three-dimensional array to get the final ciphertext image. The experimental results show that compared with the traditional chaotic encryption algorithm, it has the advantages of easy implementation, sensitivity to initial conditional disturbance, and large key space.

1. Introduction

Digital image and video information become an indispensable part of people's communication and work, Multimedia information security has become the focus of people's attention, especially in the military, commercial, medical engineering and other fields have higher requirements [1,2]. Chaotic system is one of the commonly used encryption techniques in the whole field of multimedia information [3-7].

Chaos is a kind of seemingly random and random complex motion [8], which is suitable for the encryption of digital information due to its ergodicity, sensitivity to initial conditions, and instability of orbits. Currently, there are several commonly used chaotic encryption algorithms: [10] used two Logistic system to generate two random sequences, one for diffusion and the other for permutation; In [11], two Lorenz system are coupled to form a 6-dimensional chaotic system, and impulse interference is introduced to make the encryption algorithm more efficient; [12] proposed the multi-chaotic encryption algorithm, which regarded the chaotic sequence and pixel of color map produced by the chaotic system as two spatial points, generated the encryption factor by the distance formula between the point and the point, and obtained the encrypted image by the corresponding calculation with the pixel value of the image.[13] proposed a chaotic encryption algorithm combining Logistic mapping and Sine mapping.

Inspired by the pseudo-random number generator [15], In this paper, a two-dimensional discrete chaotic map based on Logistic mapping and modified Marotto theorem is proposed, which is optimized to be a random sequence, generating better encryption sequence and image pixel value operation, and realizing double encryption of images.

2. Principle of chaotic system

2.1 Logistic System

Logistic system is a typical chaotic dynamic system, also known as bug mapping. It has simple

  DOI: 10.25236/icscbd.2018.023

structure and higher operation efficiency than other systems. The mathematical model of this mapping is a one-dimensional nonlinear iterative equation, which can be expressed as:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

Where $x_n \in (0,1), n = 0,1,2...$

$$\begin{cases} x_{n+1} = \mu x_n \left(1 - x_{n+1} + 0.01 y_n\right) \\ y_{n+1} = 0.1 y_n + x_n \end{cases} \tag{2}$$

When $3.81 \le \mu \le 3.815$ its largest Lyapunov index is around 2.2, and the state of the system is chaotic.

2.2 Discrete Chaotic System based on Modified Marotto Theorem

Based on theorem Modified Marotto Theorem, the two-dimensional chaotic system constructed in literature [15] is defined as follows:

$$\begin{cases} x_{n+1} = a \sin y_n \cos y_n - bc \sin x_n / a \\ y_{n+1} = b x_n + c \sin y_n \cos x_n \end{cases} \tag{3}$$

Where, a, b and c are all parameters greater than zero.

3. Encryption scheme

3.1 Encryption based on Logistic Mapping

Step 1: Read the color image P, whose size is $M \times N$, in which the gray-scale images of three R, G and B components are a monochrome image with 256 gray levels, and extract the RGB component matrix.

Step 2: Two-dimensional Logistic system is equation (2). Given the initial value of the system X_0, Y_0 and other parameter values, an iteration $1000 + M \times N$ times is performed. In order to obtain the chaotic sequence with better experimental results, the first 1000 values of the sequence are omitted to obtain the new pseudo-random chaotic sequence $X_0^{'}$ and $Y_0^{'}$.

Step 3: The generated sequences X_1 and Y_1 are optimized by the formula (4-5), so that their value range is [0,255], and new chaotic sequences X_n, Y_n, X_n, Y_n are obtained. Then, the sequence L is obtained by transforming the formula (6).

$$S(i) = 10^{15} S(i) - floor(10^{15} S(i)) \tag{4}$$

$$S(i) = round(\mathrm{mod}((S(i) + 0.5) \times 10^6, L)) \tag{5}$$

$$L = X_n \oplus Y_n \tag{6}$$

Where S is the chaotic sequence X_n or Y_n to be optimized , L equals 256.

Step 4: transform the three components of R, G and B into a one-dimensional array, and get the corresponding array $R1, G1$ and $R1$.

$$\begin{cases} R_c = X_n(i) \oplus R1(i) \\ G_c = Y_n(i) \oplus G1(i) \\ B_c = L(i) \oplus B1(i) \end{cases} \tag{7}$$

Where R_C, G_C, B_C are the pixel values after one encryption, $i \in (1, M \times N)$.

3.2 Based on the New Two-dimensional Discrete Chaotic Map Encryption

Step 1: Given the initial values of two-dimensional discrete system X_1, Y_1, and the values of

parameters a, b, and c, the iterations and omissions are the same as in Step 2 of 2.1, and the resulting sequence is $X_1^{'}$, $Y_1^{'}$.

Step 2: Transform the chaotic sequence generated by step 1 as follows.

$$\begin{aligned} Q(X_i) &= floor(\mathrm{mod}((\frac{10^{15}\times(Y_i-\min(X_i))}{\max(Y_i)-\min(X_i)}),\ L)) \\ Q(Y_i) &= floor(\mathrm{mod}((\frac{10^{15}\times(X_i-\min(Y_i))}{\max(X_i)-\min(Y_i)}),\ L)) \end{aligned} \tag{8}$$

Where $X_i = X_i(k) Y_i = Y_i(k)(k=1,2,...,M\times N, i=1,2)$, $floor(\ )$ means to take the integer down.

The remainder of 256 is obtained after adding $T(Y_i)$ and $T(Y_i)$ of the two generated sequences.

$$Q' = \mathrm{mod}(Q(X_1)+Q(Y_1), L) \tag{9}$$

Step 3: R_C, G_C, and B_C are one-dimensional arrays obtained in the two-dimensional Logistic system encryption algorithm are encrypted by algebraic operation through the following formula.

$$\begin{cases} R_{cn} = \mathrm{mod}(Q'\oplus R_c + Q(X_1), L) \\ G_{cn} = \mathrm{mod}(Q'\oplus G_c + R_{cn}, L) \\ B_{cn} = \mathrm{mod}(Q'\oplus B_c + G_{cn}, L) \end{cases} \tag{10}$$

Where, R_{C_n}, G_{C_n} and B_{C_n} are the final pixel values after encryption.

Step 4: Convert all three one-dimensional arrays obtained from step 3 into three-dimensional arrays to obtain encrypted images.

Decryption and encryption are the inverse processes.The encryption process in this article is shown in Fig.1.

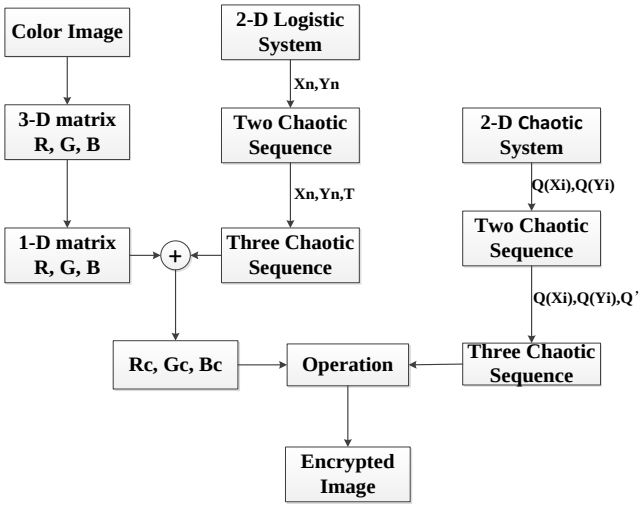


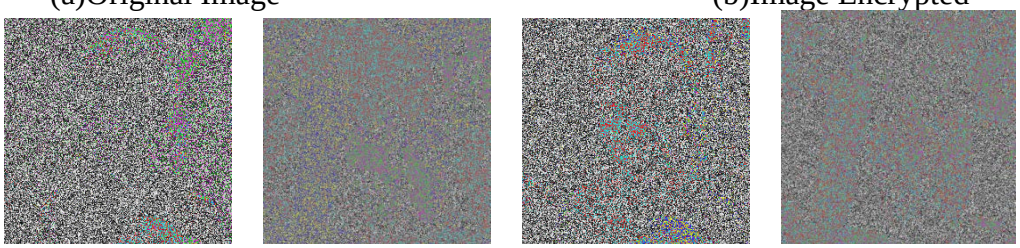
Figure 1. Encryption Flow Chart

4. Experimental simulation and performance analysis

4.1 The simulation results

We chose two images to do the simulation experiment, The initial value of two-dimensional Logistic system was[0.43501, 0.52702], and the parameter μ was 3.81003; The initial value of the two-dimensional new discrete chaotic system is [0.706, 0.231], and the parameters a, b and c are respectively 5,8,0.1,.The encryption results are shown in Fig.2.

(a)Original Image (b)Image Encrypted



(c)The Encrypted Images of the Algorithm in [14](d)The Encrypted Images of the Algorithm in [15]

Figure 2. Image Encryption Results

4.2 Safety analysis

4.2.1 The Key Analysis

Spatial analysis:This encryption system uses two improved two-dimensional chaotic maps, with four initial values, four branch parameters and a total of 8 keys, all of which are double precision floating point Numbers. The key space in this article is 10^{128}.It can be seen from Table 1 that the key space of this encryption system is large enough and larger than that of literature [14],[15] scheme, which can better resist the key exhaustion attack.

Sensitivity analysis: another important indicator to evaluate the performance of encryption algorithms is the sensitivity of keys. A higher sensitivity means that it is more difficult for an attacker to derive the plaintext and key information from the ciphertext changes.

In order to test whether the sensitivity performance in the scheme in this paper is good, only one of the key value values is slightly changed, $Y_1 = 0.231 \text{to} Y_1 = 0.231000000001$, then the error decryption result is shown in Fig.3. (b), then Fig. 3 (a) is the correct decryption result. It can be seen from the results that when the decryption key and the correct key have a very small error, finally will not be able to crack the clear text of any information.

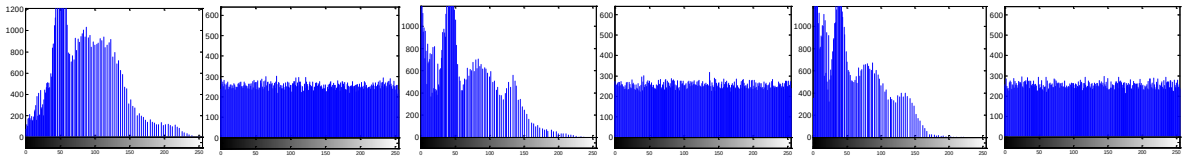
(a)Correct Decryption Image (b) Error Decryption Image

Figure 3. Image Decryption Results

4.2.2 Statistical Analysis

Histogram analysis: the gray histogram is the statistics of the gray level distribution in the image, and the frequency of its occurrence is counted, which can show the proportion of each gray level in the image.

Correlation analysis: there is a strong correlation between adjacent pixels in plaintext, and one of the purposes of encryption is to break this feature between them, that is, the adjacent pixel distribution of ciphertext image in horizontal, vertical and diagonal directions is balanced. Here, we use the correlation [16] to measure the encryption effect of the encryption scheme.



(a) (b) (c) (d) (e) (f)

Figure 4. Histograms of Original Image and Encrypted Image: (a), (b), (c) are Histograms of R, G, B from Original the first image. (d), (e) and (f) are histograms of R, G, B from encrypted the first image histogram analysis

$$\begin{cases} r(x,y)=\dfrac{\left|\operatorname{cov}(x,y)\right|}{\sqrt{D(x)\sqrt{D(y)}}} \\ E(x)=\dfrac{1}{N}\sum_{k=1}^{N}x_k \\ D(x)=\dfrac{1}{N}\sum_{k=1}^{N}(x_k-E(x)) \\ \operatorname{cov}(x,y)=\dfrac{1}{N}\sum_{k=1}^{N}(x_k-E(x))(y_k-E(y)) \end{cases} \tag{11}$$

The pixel points of the original image and the encrypted image are randomly selected as reference points, and the correlation distribution diagram of horizontal, vertical and diagonal lines is drawn respectively, as shown in Fig. 5 to Fig.7.

TABLE 1. Correlation Coefficients of Adjacent pixel

Correlation	Original image	Encrypted image	Encrypted image in reference[17]
Horizontal	0.9637	0.0073	0.0286
Vertical	0.9621	-0.0015	0.0751
Diagonal	0.9540	-0.0028	0.0039

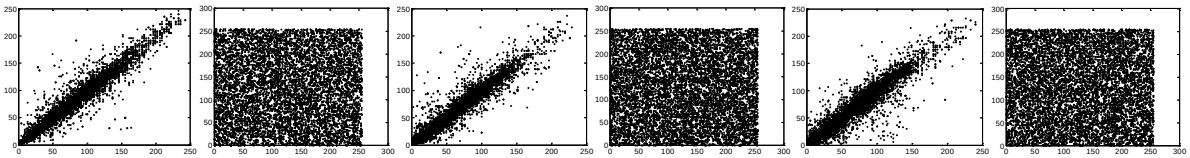


Figure 5. Horizontal Direction Figure 6. Vertical Direction Figure 7. Diagonal Direction

3.2.3 Statistical Analysis

After adding noise to the finally obtained ciphertext image, the decryption scheme described in the paper is used for decryption. The decryption images obtained are shown in Fig.8.

It can be clearly seen from the two decrypted images in Fig.8 that, compared with the plain text image, the image quality restored by Fig.8 (b) is better than Fig.8 (a).

(a) [14] Decrypts Dmage (b) Decrypt the Image in This Paper

Figure 8. Decryption Images with Noise

5. Conclusion

In this paper, a scheme of image information security is proposed by combining Logistic system and discrete chaotic system based on Marroto theorem. Through simulation experiment, this paper, security is higher than the other two kinds of schemes, such as using only one of them, the results clearly show that you can see from the two kinds of schemes of cipher text clear outline, but this article scheme of cipher text and are a far cry from a clear, relevance is very small, the naked eye can not see the outline of the original image or other plain text, and the key space range is larger.It can be seen that this scheme has good security, is easy to implement, and has superior performance such as large key space, strong key sensitivity and high security.

Acknowledgments

The work was sponsored by National Natural Science Foundation of China Grant No.61772174, and Plan for Scientific Innovation Talent of Henan Province Grant No.174200510011.

References

[1] Bakhshandeh A, Eslami Z. An authenticated image encryption scheme based on chaotic maps and memory cellular automata [J]. Optics & Lasers in Engineering, 2013, 51(6):665-673.

[2] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique [J]. Optics & Lasers in Engineering, 2015, 66(66):10-18.

[3] Wang X, Xu D. A novel image encryption scheme based on Brownian motion and PWLCM chaotic system [J]. Nonlinear Dynamics, 2014, 75(1-2):345-353.

[4] Chua L. Memristor, Hodgkin-Huxley, and edge of chaos.[J]. Nanotechnology, 2013, 24(38):383001.

[5] Junsangsri P, Lombardi F. Design of a Hybrid Memory Cell Using Memristance and Ambipolarity[J]. IEEE Transactions on Nanotechnology, 2013, 12(1):71-80.

[6] Zhen P, Zhao G, Min L, et al. Chaos-based image encryption scheme combining DNA coding and entropy[J]. Multimedia Tools & Applications, 2016, 75(11):6303-6319.

[7] Xiang Fei, Zhao Changwei,Wang Jian, et al. One-way hash function based on cascade chaos. Open Cybernetics and Systemics Journal , 2015, 9 (1): 573-580.

[8] Liu G, Zhang H. An image encryption algorithm based on chaotic map and Hash function[J]. Journal of Guilin University of Electronic Technology, 2016.

[9] Chen X, Xiang F, Zhang L. Optimal design of double-precision chaotic signal generators based on IEEE-754 standard[C] IEEE International Conference on Automation and Logistics. IEEE, 2012:466-469.

[10] Chen C, Jing L I, Deng H. Chaotic encryption algorithm based on image pixel values change and position scrambling[J]. Journal of Computer Applications, 2015.

[11] Kadir A, Aili M, Sattar M. Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections[J]. Optik - International Journal for Light and Electron Optics, 2017, 129:231-238.

[12] Zhao P, Liu G, Wang M, et al. An image encryption algorithm based on multi-scroll chaotic map[C] International Conference on Biomedical Engineering and Informatics. IEEE, 2013:186-189.

[13] Zhang T, Zhou Y, Chen C L P. A new combined chaotic system for image encryption[C] IEEE International Conference on Computer Science and Automation Engineering. IEEE, 2012:69-73.

[14] Huang S. A color image encryption algorithm based on improved Logistic chaotic map[J].

Journal of Henan Institute of Engineering, 2015.

[15] Xu H, Tong X, Meng X. An efficient chaos pseudo-random number generator applied to video encryption[J]. Optik - International Journal for Light and Electron Optics, 2016, 127(20):9305-9319.

[16] Wang J Y. Research on Tracking Algorithm Based on Correlation Coefficient[J]. Journal of Shandong Agricultural University, 2017.

[17] Feng-Ying W , Xiao-Li H , Guo-Wei C . An Improved Image Encryption Algorithm Based on Chaotic Logistic Map[C] Fifth International Symposium on Computational Intelligence & Design. IEEE, 2013.