International Journal of Hybrid Information Technology
Vol. 9, No.10 (2016), pp. 281-288
http://dx.doi.org/10.14257/ijhit.2016.9.10.28

Research on Image Encryption Based on Lorenz Chaotic Mapping in Finite Field

Fangtao Liu [1] and Yu Liu [1, 2]

[1]. *Chongqing Vocational Institute of Engineering,Chongqing 402260, China*
[2]. *State Key Laboratory of Coal Mine Disaster Dynamics and Control, Chongqing University, Chongqing 400044, China*
8551756@qq.com

Abstract

An image encryption method was built based on Lorenz chaotic mapping and finite field theory. First, original image information was divided into two image matrix by using Lorenz chaotic mapping. Second, five step calculations were finished about these two image matrix in the finite field. By combination of chaotic mapping and computing in the finite field, the new encryption method has a good effect and a fast speed. And the new encryption method realize the balance of speed and effect. Experimental results show that the proposed method has good encryption effect, attack resistance, the ideal speed of execution.

Keywords*: image encryption, finite field, Lorenz mapping, chaotic encryption*

1. Introduction

With the rapid development of communication technology, the demand of large data file transmission is growing up. Among them, image file transmission is a very common communication needs [1]. In the process of image data transmission, people have high demands on the security of image information, that promotes the rapid development of image encryption technology [2]. Image encryption is a method which can map original image information into cipher image information by using all kinds of encryption methods. Image encryption can make the attacker and the translator not obtain the original image information. At the beginning of the image encryption technology development, stream cipher and matrix scrambling were used more[3-4]. But these encryption methods are so simple that decryption process is vulnerable to decode by attacker. This makes more complex encryption processing technology be introduced into image encryption field. Image encryption technology based on chaotic theory had been applied in recent years because chaotic mapping has a complex process and is sensitive to initial value. These factors make encryption safety greatly improved. Raiput used chaotic mapping to reschedule and layout the original image information, and built a new image encryption algorithm by using special treatment of initial sensitivity. This new encryption algorithm got a good encryption effect [5]. Chen set up a dynamic vector update mechanism to the process of image encryption based on chaotic mapping, in order to achieve the purpose which can improved the speed of image encryption and decryption[6]. Wen built a image encryption method that its security is very high. He combined Tent mapping with Hyper mapping, and further strengthen anti-attack performance of chaotic encryption. The safety performance of this method had been verified by 6^{th} CNN attacking performance test [7]. Rohith used logistic to further dispose the key of encryption algorithm, and set up a linear transformation mechanism to further improve its security for image encryption algorithm based on chaotic theory [8].

ISSN: 1738-9968 IJHIT

Image encryption method based on chaotic theory has a strong advantage on the security, but its speed is generally slower. Therefore, a new image encryption method was built by combining finite field theory with chaotic theory.

2. The Proposed Algorithm

2.1. Encryption Process Design

The image encryption algorithm has built in this paper. It is combined the binary arithmetic on the finite field with chaotic encryption, and it can give full play to the advantages. That is, security and rapidity can be highlighted for image encryption at the same time. For this reason, the encryption process of the encryption method is presented as shown in Figure 1.

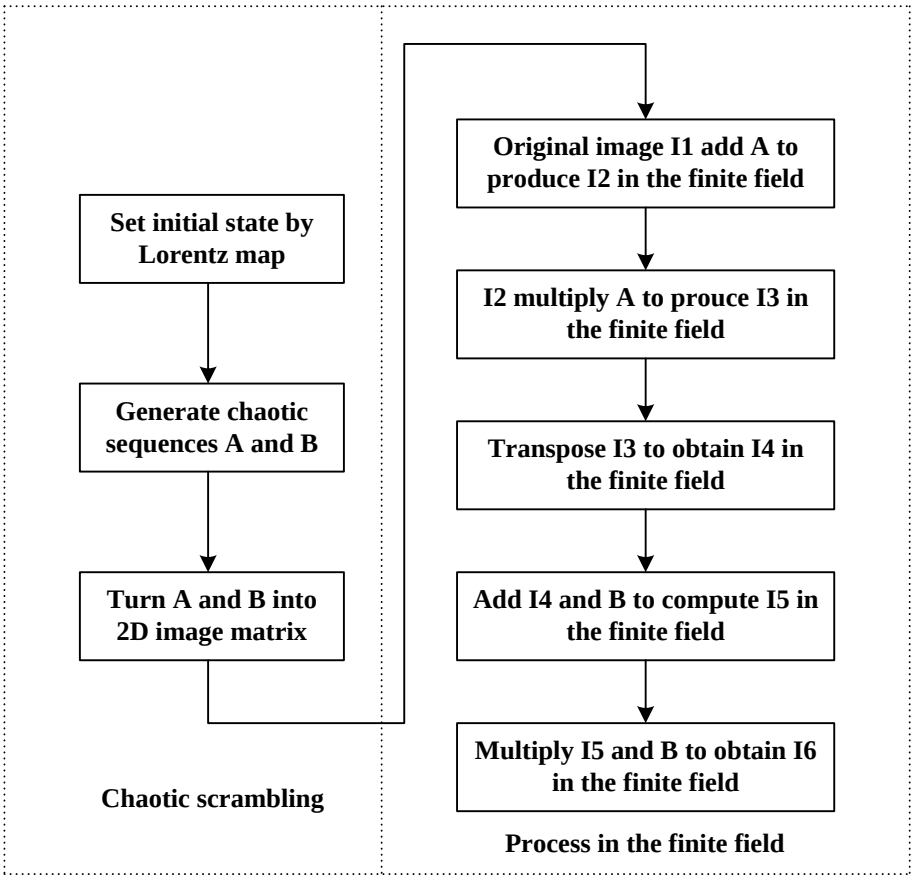


Figure 1. Encryption Principle and Encryption Process

2.2. Chaotic Scrambling Process

In the processing of the chaotic scrambling disposal, simple and effective chaotic mapping was used in order to accelerate the speed of encryption. Here, Lorenz chaotic mapping was used and it was shown in formula (1).

$$\begin{cases} x_1 = 10(x_2 - x_1) \\ x_2 = 28x_1 - x_2 + x_4 - x_1 x_3 \\ x_3 = -\frac{8}{3}x_3 + x_1 x_2 \\ x_4 = -\frac{28}{3}x_1 + x_2 \end{cases} \quad (1)$$

Here, we put the original image information as x_1 into the formula (1), and generate other three variables x_2, x_3, x_4 by using Lorenz chaotic mapping.

We dispose x_3 and x_4 to make it just map between 0-255, in order to satisfy the demand of numerical range of digital images. Specific treatment method is shown in formula (2).

$$\begin{cases} A = (x_3 * 1000) \bmod 256 \\ B = (x_4 * 1000) \bmod 256 \end{cases} \quad (2)$$

By above process, A and B had become an one-dimensional sequence data. In order to satisfy the requirement of the matrix operations on the finite field, A and B will map into image matrix, shown as in formula (3).

$$\begin{aligned} A_{M \times N} &= A_n \\ B_{M \times N} &= B_n \end{aligned} \quad (3)$$

2.3. Finite Field Process

Use I1 to express the original image, respectively execute additive operation and multiplication operation with A on the finite field. Then new image I2 and I3 will be obtained as follows:

$$I2 = I1 \oplus A \quad (4)$$

$$I3 = I2 \bullet A \quad (5)$$

Where, "$\oplus$"express addition on finite field, "$\bullet$" express multiplication on finite field.

Use transposition operation to obtain the new image I3, as shown in formula (6).

$$I4 = I3' \quad (6)$$

Image I4 was respectively executed addition operation and multiplication operation with B on the finite field, new image I5 and I6 is obtained as follows.

$$I5 = I4 \oplus B \quad (7)$$

$$I6 = I5 \bullet B \quad (8)$$

2.4. Decryption Process Design

On the receiver of encryption image transmission, you need to use the decryption algorithm to get the original image information. Here, receiver need to use the same Lorenz chaotic mapping function and the state of initial value with encryption end, and corresponding chaotic sequence to complete decryption. Rest of steps are equal to the inverse transformation of encryption process.

The first step, set the initial state according to the Lorentz mapping.

The second step, generate chaotic sequence A and B according to the Lorentz mapping and the original image information.

The third step, converts A and B to 2D image matrix.

The fourth step, make image I6 and B to execute the inverse operation of multiplication on finite field to get image I5.

The fifth step, make image I5 and B to execute the inverse operation of addition on finite field to get image I4.

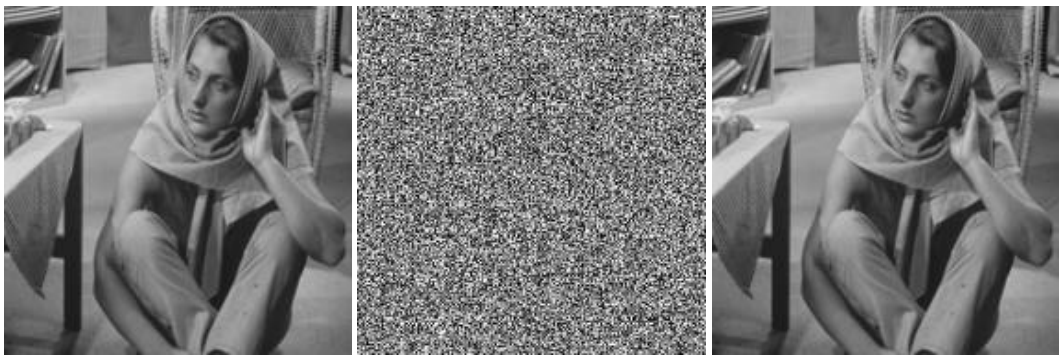
The sixth step, make the image I4 to execute transposition process to get image I3.

The seventh step, make image I3 and A to execute the inverse operation of multiplication on finite field to get image I2.

The eighth step, make image I2 and A to execute the inverse operation of addition on finite field to get image I1.

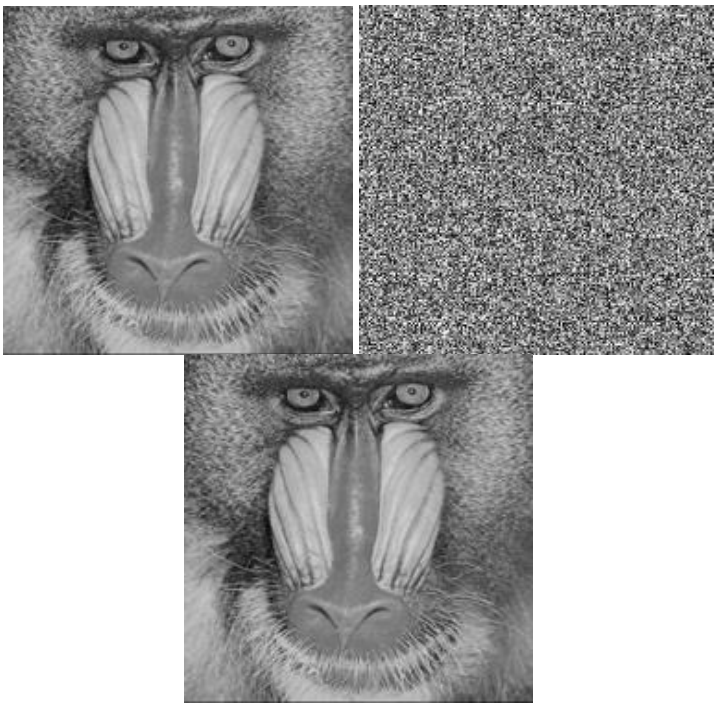
3. Experimental Results and Analysis

In order to verify the effectiveness of image encryption method based on fusion of chaotic scrambling and finite field, test and analysis is executed on encryption effect. Barbara image and Bahoon image is selected as experimental image, experimental results are shown in Figure 2 and Figure 3.



a) original image b) encryption image c) decryption image

Figure 2. Encryption Effect of Barbara Image

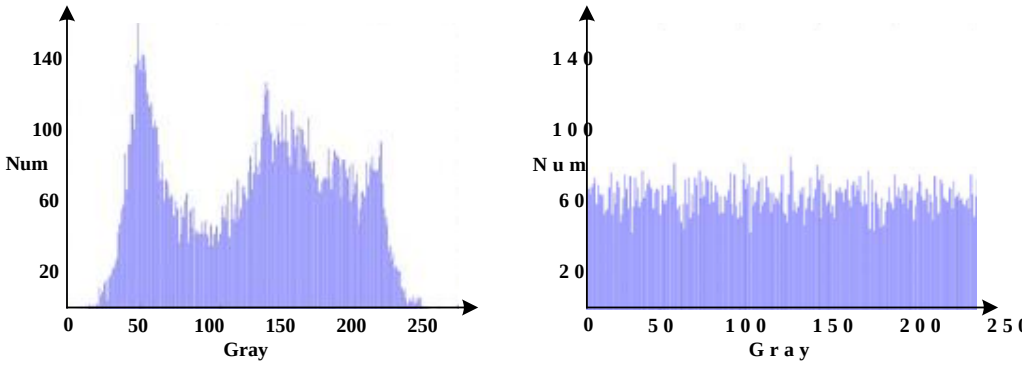


a) original image b) encryption image c) decryption image

Figure 3. Encryption Effect of Bahoon Image

3.1. Gray Histogram Evaluation

Observe gray histogram original image and encryption image, it is also an effective safety evaluation method. In general, image texture feature is more obvious, the gray scale distribution is more concentrated. After encryption process, the distribution of gray histogram is more homogeneous. The better Homogeneity is, the better encryption effect is. Histogram effect of Barbara original image and encryption image is shown as Figure 4.



a) Original image **b) Encryption image**

Figure 4. Gray Histogram Evaluation

From Figure.4, we can see that gray histogram distribution of encryption image is getting very uniform. So it can prove that encryption security of the proposed method is higher.

3.2. Three-Way Correlation Evaluation

Three-way correlation refers to the correlation of image pixels among the horizontal direction, vertical direction, and diagonal direction. The correlation no matter which direction is high, it will make image date easily to decode. Therefore, to measure encryption performance is good or not, the most direct way is evaluating the correlation of these three directions. When the correlation is calculated, statistical formula are generally used as follows.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{10}$$

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

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{12}$$

By using above formula, three directions correlation coefficient are calculated on Barbara image, and results are shown in Table 1

Table 1. Correlation Results

correlation coefficient	Barbara original image	Barbara encryption image
The correlation coefficient of horizontal direction	0.9250	0.0021
The correlation coefficient of vertical direction	0.9550	0.0016
The correlation coefficient of diagonal direction	0.8890	0.0017

From Table 1, we can see that correlation coefficient of three directions are very low. The results show that the proposed method has a high safety.

3.3. Execution Time Analysis

For Barbara and Bahoon images, the execution time of the proposed method are shown as in Table 2.

Table 2. Execution Time

Image size	Encryption time (second)	Decryption time(second)
Barbara image	0.084	0.079
Bahoon image	0.092	0.085

4. Conclusions

In order to get better image encryption effect and encryption speed, a new image encryption was built based on the finite field and Lorenz chaotic mapping. In this method, original image information was mapped into two matrices, and final encryption result can be obtained by all kinds of operation on the finite field. In the test experiment, we analyzed the encryption effect, histogram evaluation effect, three-way correlation effect, and execution time of this method. The experimental results show that the encryption effect is good, anti-attack performance is strong, and the execution time is fast. The proposed method gives full play to the characteristics which the chaotic encryption effect is good and the operation speed is fast on finite field.

References

[1] D. Maluenda, A. Carnicer, R. Martnez-Herrero, I. Juvells and B. Javidi, "Optical encryption using photon-counting polarimetric imaging", *Optics Express*, vol. 23, **(2015)**, pp. 655-666.
[2] N.F. Elabady, H.M. Abdalkader, M.I. Moussa and S.F. Sabbeh, "Image encryption based on new one-dimensional chaotic map", *ICET 2014-2nd International Conference on Engineering and Technology*, **(2015)**, pp. 851-892.
[3] H. Singh, A.K. Yadav, S. Vashisth and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane", *Optics and Lasers in Engineering*, vol. 67, **(2015)**, pp.145-156.
[4] Y. Morales, L. Daz and C. Torres Radia, "Hilbert transform in terms of the fourier transform applied to image encryption", *Journal of Physics Conference Series*, vol. 1, **(2015)**, pp. 582-590.
[5] R. A. Singh and S. Mansi, "A novel image encryption and authentication scheme using chaotic maps", *Advances in Intellgent Systems and Computing*, **(2015)**, pp. 277-286
[6] J.X. Chen, Z.L. Zhu, C. Fu and H. Yu, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism", *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, **(2015)**, pp.846-860.
[7] W. Wen, "Security analysis of a color image encryption scheme based on skew tent map and hyper chaotic system of 6-order CNN against chosen plaintext attack", *Multimedia Tools and Applications*, 2015, vol. 6, **(2015)**, pp.224-235.
[8] S. Rohith, K.N. Bhat, S. Hari and A. Nandini, "Image encryption and decryption using chaotic key sequence generate by sequence of logistic map and sequence of states of Linear Feedback Shift Register", *International Conference on Advances in Electronic, Computers and Communications*, vol. 6, **(2015)**, pp.1124-1130.

Authors

Fangtao Liu, he is an Engineer , School of Information Engineering, Chongqing Vocational Institute of Engineering, Chongqing 402260, China;Tel: +86-023-61065852;Email: 8551756@qq.com

Yu Liu, he is a Professor, School of Information Engineering,Chongqing Vocational Institute of Engineering, Chongqing 402260, China; Tel: +86-023-65208186; Email:16619054@qq.com

