The application of Galois fields operation with chaos mapping in digital image encryption

Bing Liu†
Department of Public Affairs Management,
Dazhou Vocational and Technical College, Dazhou, 635001, China
E-mail: newbing@126.com
www.dzvtc.edu.cn

Qiang Chen
College of Computer and Information Science, Southwest University
Chongqing, 400715, China

A new digital image encryption method is proposed by introducing a chaos mapping combining matrix operations on Galois fields. The original image is mapped into two matrices by using chaos mapping, and then the original image matrix is processed sequentially with the two matrices over a Galois field to obtain the encrypted image. The experimental results show that the proposed method can obtain more uniform and fine scrambling effect than the traditional one, it has a stronger anti-jamming performance and faster encryption speed.

Key words: digital image; image encryption; 3D chaos mapping; Galois field operation.

1. Introduction

In order to more secure and convenient transmission of image data, researchers have been studying various image encryption technologies, and a lot of successful usages have been achieved[1-4]. Because the chaotic system has unpredictability and sensitive dependence on the initial value, if it is used to encrypt the digital image obviously can greatly improve the security and reliability of ciphertext image [5-7]. This paper introduces a 3D chaos mapping to construct a digital image encryption algorithm based on this mapping to obtain a better image encryption effect.

2. Introduce a Chaos Mapping

A chaos mapping is designed by Dr. A.S. LU[8], which is called LU mapping in this paper. The kinetic equation is shown in Eq. (1):

$$\begin{cases} \frac{dx}{dt} = a(z-y) \\ \frac{dy}{dt} = bx - dx^2 \\ \frac{dz}{dt} = kxy - cy - gz \end{cases} \quad (1)$$

In the Eq. (1), when "a = 25.6, b = 66.8, c = 39.22, d = 0.2, e = 4", there exists a typical chaotic attractor in this system.

3. Encryption Algorithm Design

3.1 *The overall process of the algorithm*

On the basis of LU mapping, the image encryption algorithm is constructed by combining Galois field operations. The process is shown in Figure 1.

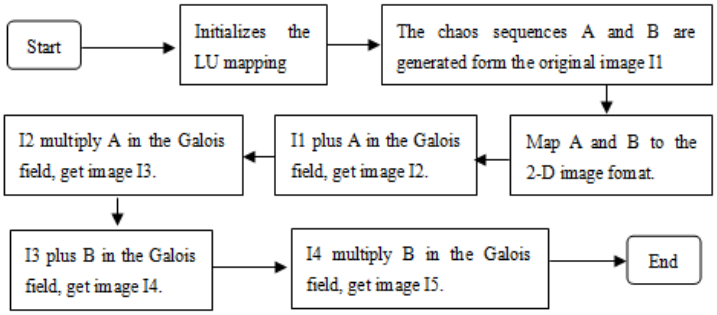


Fig.1. Encryption principle and flow chart

In Figure 1, the first few links through the LU mapping to generate the corresponding image format of the chaos sequence, the latter part of the use of Galois field operations to further enhance the complexity of the encryption process.

3.2 *Chaos scrambling processing*

In the Eq. (1), the original image I1 is substituted into x, y and z are calculated, then y and z are mapped on (0,255). The mathematical model is shown in Eq. (2).

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

In Eq. (2), A and B are y and z scaled transformation sequence, and "mod" represents a modulo operation.

The two-dimensional data sequence A and B in the Eq. (2) are converted into a two-dimensional image matrix, and the mathematical processing thereof is shown in the Eq. (3).

$$\begin{aligned} A_{M\times N} &= A \\ B_{M\times N} &= B \end{aligned} \tag{3}$$

In Eq. (3), M and N represent the width and height of the original image I1.

3.3 Galois field processing

In order to improve the complexity of the whole encryption process, matrix $A_{M\times N}$ and $B_{M\times N}$ in Eq. (3) will be further processed in the Galois field.

$$I2 = I1 \oplus A_{M\times N},\ I3 = I2 \otimes A_{M\times N} \tag{4}$$

$$I4 = I3 \oplus B_{M\times N},\ I5 = I4 \otimes B_{M\times N} \tag{5}$$

In the above equations (4) and (5), $\oplus$ denotes Galois field addition, and $\otimes$ denotes Galois field multiplication.

By the above equations, $I5$ is the final encrypted image.

3.4 *Decryption process design*

In fact, the decryption process is equivalent to the inverse of the encryption process. For the encryption algorithm designed in this paper, we still use the LU mapping and set the same initial values as the encryption side in the decryption process, and then perform various inverse operations of the encryption process on the Galois field. The flow chart is shown in Figure 2.

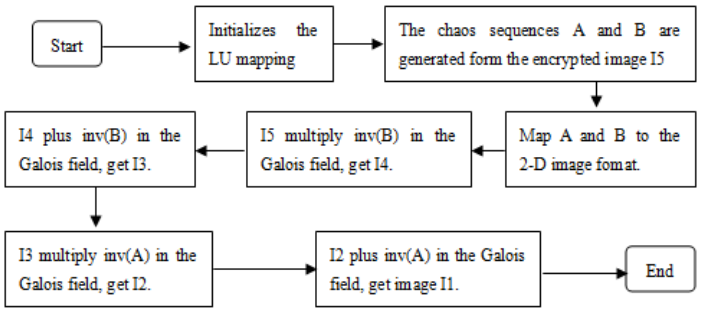
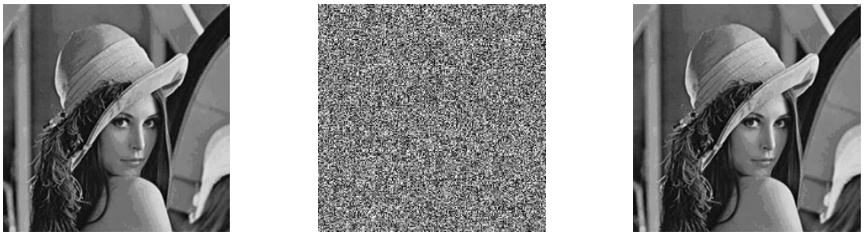


Fig. 2 Decryption principle and flow chart

4. Experimental Results and Analysis

In order to verify the effectiveness of this method, we use Lena image as the verification object. Computer hardware configuration: Core Duo, clocked at 2.0GHz CPU, 4G size of memory; computer software configuration: windows

7.0 operating system, the compiler environment for Matlab2014b. The experimental results are shown in Figure 3.



(a) Original (b) Encrypted (c) Decrypted

Fig. 3 The effect of encryption and decryption of Lena image

From the visual point of view, Figure 3 qualitative proves the effectiveness of encryption methods in this paper. After the original image is encrypted, a very good uniform scrambling effect is shown. The detailed information of the original image can not be been seen completely, and the decrypted image has no difference from the original one. We will use three methods for quantitative verification in the below.

4.1 *Information entropy analysis*

Supposing that "S" is a discrete random variable, its range R=$\{ s_1, s_2, s_3, \ldots \}$ is finite and countable. Let $p_i = P\{S = s_i\}$, then the entropy of "S" is defined as:

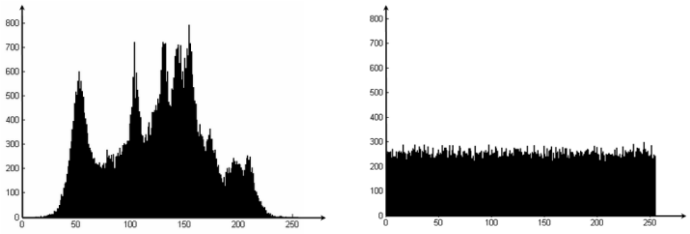
$$H(S) = -\sum_{i=1}^{n} p_i \ln p_i \qquad (\sum_{i=1}^{n} p_i = 1) \tag{6}$$

Calculating with Eq. (6): the information entropy of the Lena image is H = 7.9918, which is very close to the maximum value of the information entropy of 256 gray images. It can be seen that the gray distribution of the encrypted image is fairly uniform, so it is extremely difficult for a malicious attacker to attack the image obtained by the method in this paper.

4.2 *Histogram evaluation*

In general, after the image is encrypted, the histogram of the distribution of gray-scale histogram will be more uniform. After encrypting the Lena image with this method, the histogram effect before and after encryption is shown in Figure 4.

It can be seen from Figure 4 that the histogram distribution of the image encrypted with this method is very uniform, which proves that the encryption security is high.



(a) Original (b) Encrypted

Fig. 4 Evaluation of Gray Scale Histogram of Lena Image

4.3 *Correlation analysis*

The Equation for calculating the correlation coefficient of adjacent pixels of an image is:

$$R_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}} \tag{7}$$

In Eq. (7), x and y are the values of two adjacent pixels in the image. $\operatorname{cov}(x, y)$ and $D(x)$ are defined as follows:

$$\begin{aligned} \operatorname{cov}(x, y) &= \frac{1}{m \times n} \sum_{i=1}^{m \times n} (x_i - E(x))(y_i - E(y)) \\ D(x) &= \frac{1}{m \times n} \sum_{i=1}^{m \times n} (x_i - E(x))^2 \\ E(x) &= \frac{1}{m \times n} \sum_{i=1}^{m \times n} x_i \end{aligned} \tag{8}$$

The correlation of neighborhood pixels in this paper involves three kinds of pixel correlation. They are the adjacent pixel correlation in the horizontal, the vertical, and diagonal direction respectively. Using the above Eq. (8), the correlation coefficients of the Lena image before and after the encryption are calculated, which are shown in following table.

The table of correlation coefficients in three directions before and after encryption

Directions	Original	Encrypted
Horizontal	0.90462	0.001326
Vertical	0.92403	0.001614
Diagonal	0.91701	0.001431

As can be seen from above table, there is a strong randomness in the ciphertext generated from the proposed encryption algorithm. After an image is encrypted, the correlation of adjacent pixels has been reduced to 0.001 orders of

magnitude. Compared with the original image, the encrypted one has been significantly reduced in correlation.

5. Conclusion

The encryption algorithm proposed in this paper is a chaos scrambling one combined with Galois field operation. In the simulation experiment, Lena image is tested, analyzed and compared from three aspects: histogram, correlation and information entropy. The results show that the proposed method possesses better encryption effect, stronger anti-attack performance and excellent execution efficiency.

Acknowledgments

This work is supported by the Key Science and Technology Project of Sichuan Provincial Department of Education (14ZA0330) and Dazhou Science and Technology Project of Sichuan Province (2014-8220).

References

1. S.H. Liu, D.S. Wang, Long. Chen. Analysis of the Ambiguity Characteristic of Digital Synthesis Signals with Chaos Frequency Modulation. ACTA ELECTRONICA SINICA, China 35(9): 1784-1788(2007)
2. W. Song, J.J. Hou, Z.H. Li. A novel zero-bit watermarking algorithm based on Logistic chaos system and singular value decomposition. ACTA PHYSICA SINICA, China 58(7): 4449-089 (2009)
3. H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee. Data hiding methods based upon DNA sequences, Information Sciences, China 180 (11): 2196–2208(2010).
4. S.Banerjee. Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption. Optics Communications, China 284(9): 2278-2291(2009).
5. F. Zhao, C.M. Wu. Image Encryption Algorithm Combined Self-Encoded Theory with Super-Chaos Mapping. Journal of Computer-Aided Design & Computer Graphics, China 28(1): 119-128(2016)
6. L.P. Liu, X.F. Zhang. Image encryption algorithm based on chaos and bit operations. Journal of Computer Applications, China33 (4): 1070-1073(2013)
7. X. Zhou. A novel chaos system and its circuit simulation. Acta Physica Sinica, China 61(3): 030504(2012)
8. A.S. Lu, A New Chaos System and Its Synchronization. Journal of Henan Normal University (Natural Science), China 36(1): 66-68(2008).