ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 313-317
doi: 10.18178/wcse.2017.06.054

Research on Image Encryption Algorithm Based on Rubik's Cube Mechanism

Cong Ma [1] and Shuwen Wang [1 +]
[1] College of electrical engineering, Northwest Minzu University, Lanzhou, China

Abstract: Traditional digital image encryption is easily to be attacked, which is caused by single encryption approaches and lesser key space. The key idea of our approach is that secret image is double encrypted by our model, which are divided into two steps. The first step is that expand the key space according to the mechanism of Rubik's cube mapping. Subsequently, the second step is to embed the secret image of disrupting into a public image, enhancing the concealment. The combination of two-step's greatly contributes to improve the security of information transmission and then Cube encryption technology is get better promotion.

Keywords: Rubik's cube encryption; Watermark; Safe transmission

1. Introduction

Information deciphering technology has been greatly improved with the rapid development of computer technology. Asymptotically information security issues have become a common concern of researchers. The application of information security has been paid more and more attention. People have come to realize that with excellent pseudo-randomness, statistics and topology characteristics can be used as a good encryption system. So the Rubik's cube is dug out by researchers. Then the combination of Rubik's cube and encryption image has gradually become a hot topic [1].

Scrambling the image pixels so that the image becomes garbled state cannot distinguish the secret image haves already been the commonly used digital image encryption method. The current mainly methods are as follows: Arnold transform, FASS curve, Gray code transformation, Conway game, IFS model, Tang ram algorithm, magic square transformation, Hibert curve, elliptic curve, generalized Gray code transformation [2-3]. In this paper, a digital image encryption algorithm based on Lorenz chaotic system is proposed in [4], and the encryption effect can be obtained by applying this method. However, because the encryption process of this method is only the encryption of the image pixels, its security still need to be further improved. Gilani [5] proposed a block-based enhanced image scrambling algorithm. Sabery [6] uses the chaotic sequence to control the scrambling of the image in the improved algorithm. In summary, a digital image encryption technology based on the improved Rubik's cube theory, which is an encryption technology based on Rubik's cube Principle have proposed in this paper. This technique has the characteristics of similar noise, complex structure and extremely sensitive to the initial conditions. Therefore, it can get it with good robustness and security of digital image encryption algorithm.

2. Rubik's Cube Mechanism Introduction

Rubik's cube is a three-dimensional cube. Each sub-block is relatively flexible and each rows and columns can be free to turn. You can turn into not only the specified pattern, but also the disrupting pattern.

[+] Corresponding author. Tel.: +8613659320028
E-mail address: shuwenwang@163.com

According the above principles, the Rubik's cube can be regarded as a two-dimensional digital image, which each block is a pixel of a digital image. Rubik's cube printed on a specific pattern, the original pixel sequence of the image is disturbed based on the own disengaged idea in process of information transmission for improving the security and safety [7].

3. Encryption Technology

3.1 Rubik's cube map

In this paper, a new technology encrypting the secret image from the controlled Rubik's cube and generated a sequence is proposed. According to the rules of the cube toy, the rows and the columns of the pixel matrix x_0 of the digital image are rotated. Taking into account the two-dimensional features of the image matrix and introducing the idea of cyclic shift [8].

Rotated a line I_k can be seen as the line in a direction to move h_k bit. For more convenience, h_k is the shift parameter, and h_k can be determined by a specific algorithm. The columns of the image matrix can be processed in the same way. A new image $I'_{M\times N}$, $I'_{M\times N} = P_0(I_{M\times N})$, and P_0 is obtained from the $I_{M\times N}$ to $I'_{M\times N}$. The input x_0 and P_0 together from the key. We refer to this transformation as a Rubik's cube map. In fact, multiple iterations can be performed as described above to achieve the desired encryption effect.

Encryption steps:

Step 1: Read a digital image x_0;

Step 2: Create the initial key P_0, generate a long enough chaotic sequence;

Step 3: Determine the order and number of rows, columns, or diagonal rotation based on the initial key P_0;

Step 4: For each of the rotating surfaces generated in step 3 operating on each rotating surface until all the swivel faces are processed to obtain a disrupted image.

Decryption process:

Step 1: Read a digital image x_0;

Step 2: Create the initial key P_0, generate a long enough chaotic sequence;

Step 3: Determine the order and number of rows, columns, or diagonal rotation based on the initial key P_0;

Step 4: For each of the rotating surfaces generated in step 3 operating on each rotating surface until all the swivel faces are processed to obtain a scrambled image.

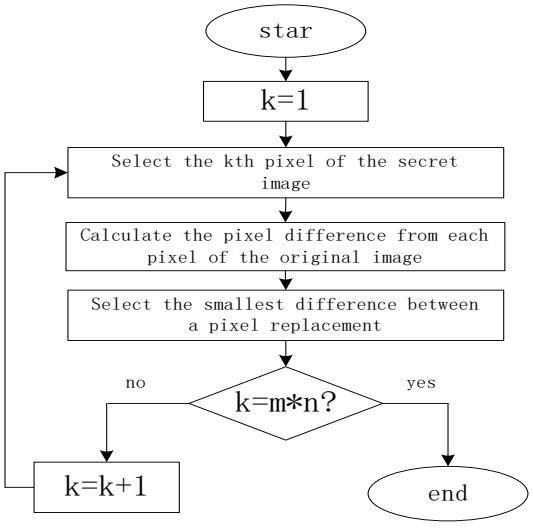


Fig. 1: Embedded flow chart

3.2 Digital watermarking technology

In order to improve the security of the information, watermarking technology is as an effective means of digital image encryption. Selecting an embedded location according to the principle of the Figure 1, and makes the watermark information embedded. Finally, the embedded watermark image as is a public image. The similarity between the extraction algorithm and the embedding algorithm lie in the key that embeds the watermark information is inverse transformed and no need the original image [9].

4. Analysis of Experimental Results

Selecting an image with a pixel of 54×54 as shown in Figure 2a, the figure 2b is by Rubik's cube map disrupted. The encrypted image cannot get any valuable information, and the pixel value and the pixel expansion of the picture will not be affected in process of the encryption.

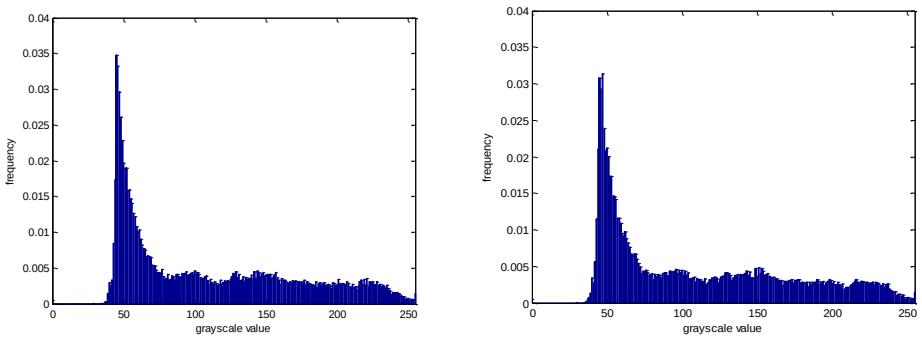
(a) Secret image (b) Encrypted image

Fig. 2 Embedded image

Figure 3a is a 216×216 pixels image without embedding information. Figure 3b is a public image that has been embedded in a secret image. It is certain that the embedding algorithm of the system could be able to ideal presented the security of the information according to the different between above two picture by our naked-eye.

(a) Original image (b) Embed ciphertext image

Fig. 3 Public image



(a) Original histogram (b) Embedded ciphertext image histogram

Fig. 4 Public image histogram

The system embedded algorithm is only embedded in the gray value of similar pixel values. It cannot change significantly the gray value of original image as shown in Figure 4. Figure 4a is a histogram of original image. Figure 4b is a histogram of embedded the secret image. From the analysis of the histogram of two images, the published image has almost the same gray histogram as the original image. Therefore, the attacker cannot judge whether there is any value information from the analysis histogram method. So it does not enhance the security of encryption, on the contrary, it will increase the concealment of secret image.

5. Security Analysis

The encrypted image should effectively remove the correlation between adjacent pixels. In this paper, the correlation coefficient of adjacent pixels was used to measure the correlation ability of original and the encrypted images. The definition is as follows:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \tag{1}$$

$$\operatorname{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{2}$$

Where x and y are the gray values of two adjacent pixels, $\operatorname{cov}(x, y)$ is the covariance of x and y, $D(x)$ and $D(y)$ are the variance of x and y,

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \ , \ D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \tag{3}$$

In the experiment, 1 000 adjacent pixel pairs in horizontal, vertical and diagonal directions were randomly selected for the original and the encrypted images. The correlation coefficients calculated using the above formula are shown in Table 1

Table I: Correlation between Adjacent Pixels

Image	horizontal direction	Vertical direction	Diagonal direction
Original image	0.9891	0.9663	0.9122
Encrypted image	0.0021	0.0076	0.0078

The eavesdropper would not get the information to pass as shown in Figure 5 when the key is not completely accurate or completely incorrect. Cracking the key is also a very difficult thing due to restoration of disrupt Rubik's cube is difficult and there is a large number of combinations[10]. The number of combinations can be calculated as follows: 8 corner blocks can be interchangeable, so there are $8!$ kinds of combinations. It can be reversed and get 37. Every corner block has three kinds of spatial position. Every corner block can not flip lonely, so it needs to divide by 3. There are $8! \times 37$ kinds of combinations. Thus, we can get $12!$ kinds of combinations for 12 edge blocks can be interchangeable position. And then it can be reversed and get 212, but due to you cannot flip a single piece of a single block and cannot be exchanged for any two positions of the two prism, so we need to be divided by 2, finally we get the combinations form as: $12! \times 212 \div (2 \times 2)$.

In summary, the all possible permutations of the cube are showed as follows:

$$8! \times 37 \times 12! \times 212 \div (2 \times 2) = 43,252,003,274,489,856,000 \approx 4.33 \times 10^{19} \tag{4}$$

Fig. 5: Error key output cipher

6. Conclusion

This paper improves the digital image encryption technology based on Rubik's cube. By analyzing the Rubik's cube map mechanism and its recovery difficulty, we find that the pixels are easy to be disrupted and difficult to restore the original pixel position in the process of encryption, and can be better applied in the field. This encryption method is more optimized and has larger key space than the classical algorithm in security performance. From the simulation results in the previous section, it is shown that our algorithm able to accurately capture the reliability and security of the information.

7. Acknowledge

This work is supported by the National Natural Science Foundation of China (No.61261042) .This project is supported by the key technology research of the Northwest University for Nationalities.

8. References

[1] Gilani SAN, Bangash Ma. Enhanced Block Based color Image Encryption technique with confusion [C] / / Multitopic Conference. INMIC2008. IEEE International 23-24 Dec. 2008: 200-206.

[2] H. Dong, P .Lu, B. Zhong. Image encryption algorithm based on Hénon mapping and Rubik's cube transform [J]. Journal of Computer Applications and Software, 2014 (5): 291-294.

[3] M. Li. A hidden encryption method for digitized image information based on superchaos [J]. Science Technology and Engineering, 2009, 9 (4): 905-910.

[4] Zhang Yong-Hong, Kang Bao-Sheng, Zhang Xue-Feng. Image encryption algorithm based on chaotic sequence[C]. IEEE Computer Society,2006.

[5] Gilani SAN, Bangash Ma. Enhanced Block Based color Image Encryption technique with confusion [C] / / Multitopic Conference. INMIC 2008. IEEE International 23-24 Dec. 2008: 200-206.

[6] Sabery MK, Yahoobi Ma. New Approach for Image Encryption Using Chaotic Logistic Map [C] / / Advanced Computer Theory and Engineering, 2008, ICACTE'08. International Conference on 20-22 Dec. 2008:585-590.

[7] G .Ye. A block image encryption algorithm based on wave transmission and chaotic systems [J]. Nonlinear Dynamics, 2014, 75 (1): 319-330.

[8] L .Sun, Z. Huang, W. Fu. Research on image encryption algorithm based on time delay and superchaos Chen system [J]. Science and Technology and Engineering, 2013,13 (35): 10521-10528.

[9] Hermassi H, Rhouma R, Belghith S. Improvement of an image encryption algorithm based on hyper-chaos [J]. Optik –International Journal for Light and Electron Optics, 2013, 124 (18): 3596-3600.

[10] Y. Wang, N. Liu, D. Zhu. Novel semi-fragile watermarking algorithm for image content authentication [J]. Journal of Zhejiang University (Engineering Science), 2013, 6 (6): 969-976.