Image Encryption Implementation Based on Fractional-order Chen System

Hongyan Jia
Department of Automation, Tianjin University of Science and Technology,
1038 Dagunanlu Road, Hexi District, Tianjin300222, PR China

Qinghe Wang
Department of Automation, Tianjin University of Science and Technology,
1038 Dagunanlu Road, Hexi District, Tianjin 300222, PR China
E-mail: jiahy@tust.edu.cn
www.tust.edu.cn

Abstract

In this paper, based on the fractional-order Chen system, a kind of double encryption algorithm method is adopted to realize the image encryption. The method mainly refers to the transformation of the pixel position and the transformation of pixel value. The effectiveness of the double encryption method is verified by encryption and decryption of some typical images. The experimental results show that this method not only has the ideal effect of image encryption and decryption, but also possesses a better guarantee on the image security. That is, this encryption method is practical and feasible.

Keywords: fractional-order; Chen system; pixel; image encryption

1. Introduction

With the rapid development of information technology, the issue on network information security has attracted more and more attention in recent years. Especially for images, a kind of important information carrier, it would be very necessary to store and transmit with a high degree of security [1]. Therefore, image encryption technology has increasingly become one of research focus in the field of information security [2].

Image encryption technology is an effective method to protect the transmission of digital images [3]. So far, many kinds of image encryption technology have been reported, such as text encryption technology [4], quad-tree image encryption technology [5], chaotic encryption technology [6], and image encryption technology based on DNA [7], and so on. As one of Image encryption technology, chaotic encryption technology has increasingly highlighted its advantage because of the development of chaos theory.

In this paper, a kind of double encryption algorithm is adopted to realize the image encryption. The algorithm will be achieved as follows. Step 1, encrypts the image by transforming the pixel position; Step 2, encrypts the image by transforming the pixel value; Step 3, decrypts the image by corresponding inverse transformation. All these transform are done by utilizing chaotic sequence from fractional-order Chen system. That is, a three-dimension chaotic sequence is firstly obtained by analyzing and computing fractional-order Chen system. Then any one of the three sequences can be selected as a position transform sequence in step 1, and subsequently all the three sequences will be selected as value transform sequences in step 2. And thus some encryption sequences for an image are gained by utilizing these chaotic sequences. Next, based on the corresponding inverse transformation, the image will be also decrypted by these chaotic sequences. At last, this encryption method is verified to be valid by encrypting and decrypting some images. All the experimental results show this method is effective and practical.

2. Fractional-order Chen system

The fractional-order Chen system is described as follows:

$$\begin{cases} \frac{d^{\alpha}x}{dt^{\alpha}} = a(y-x) \\ \frac{d^{\alpha}y}{dt^{\alpha}} = (c-a)x - xz + cy \\ \frac{d^{\alpha}z}{dt^{\alpha}} = xy - bz \end{cases} \quad (1)$$

where system parameters $a,b,c \in R$, $0 < \alpha < 1$ refer to the fractional order. When fixing $\alpha = 0.9$, $a = 35, b = 3$, $c = 28$, the system will show a typical chaotic attractor. Under the above conditions, setting an initial value of the system, a three-dimension chaotic sequence can be obtained when utilizing four-order Runge-Kutta algorithm to solve the system. Here, system parameters, the fractional order, and initial value are all used as keys.

3. Image Encryption Algorithm

3.1 Pixel position scrambling

In this paper, the sequence x in three-dimension chaotic sequence is used as the pixel position transform sequence. The sequence x is firstly sorted by ascending order. Generally speaking, the image matrix stored in computer includes three components, R component, G component and B component. These components are all $m * n$ matrix. Therefore, in order to complete encryption operation, R component, G component and B component of the image matrix need to be converted into one-dimension array, R-value, G-value and B-value, respectively. Then, the sort operations for R-value are carried out by using the sorted sequence x, and subsequently scrambling encrypted image for R component can be obtained. With the same method, the scrambling encrypted image for G component or B component can also be obtained.

3.2 Pixel value transform

Although the length of chaotic sequence can be selected to be same as each component of the image, every value of chaotic sequence is not consistent with the image storage value. In general, the storage value of image is an integer between 0 and 255. So it is necessary for the chaotic sequences used in encryption to carry out numerical transformation such as numerical expansion and limitation domain. After completing the corresponding transformation, the value results of chaotic sequences are consistent with those of the image. Then the numerical encryption algorithm using XOR is used to encrypt the pixel value after image scrambling. And thus three components of the encrypted image can be obtained. Finally, three components of the encrypted image is combined together, and getting the encrypted image information.

4. Experimental Results

This paper selects two color images named Lena and Xuexiao as the research object. The size of image Lena is $512 * 512$, and the size of image Xuexiao is $256 * 256$. The experiments have been done by MATLAB 2012, with the initial values of state variables being $(0.1,0.2,0.3)$. The image of Lena and its three component diagrams of R, G, B are shown in Fig.1 (a), (b), (c), and (d), respectively. The encrypted images of tricolor component after the pixel scrambling operation are shown in Fig.2 (a), (b), and (c), respectively. The encrypted image of Lena after pixel scrambling and the encrypted image of Lena after pixel value transform are given in Fig.3(a) and (b) , respectively. The decrypted images of Lena are shown in Fig.4 (a), (b), and (c), respectively. The encrypted image of Xuexiao and the decrypted image of Xuexiao are shown in Fig.5 and Fig.6, respectively. The experimental results show that the encrypted image is completely different from the original image, while the decrypted image and the original image are identical. It shows that the encryption method is practical and effective, and has good encryption effect.

5. Performance Analysis

5.1 Histogram analysis

Generally speaking, histogram can clearly reflect the distribution of the quality characteristics of the image [8], so it is convenient for people to correctly evaluate the overall quality condition of image. Here because the histogram of Lena image is same as one of Xuexiao image, the histogram of Lena image is selected to illustrate the pixel distribution at each color of the image. Histograms for R components, G components, and B components, before and after encryption of Lena are shown in Fig.7 (a), (b), and (c), respectively. It can be seen that the distribution of the encrypted histogram

is very uniform, which indicates that the ability to resist statistical attack for the encryption method is good.

Fig.1 Image Lena and its three component diagrams

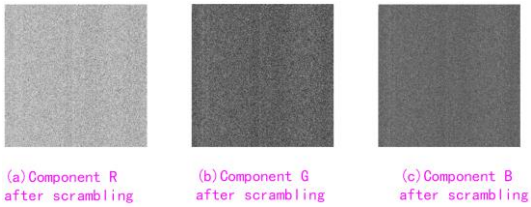

Fig.2 The encrypted images of tricolor component after the pixel scrambling operation

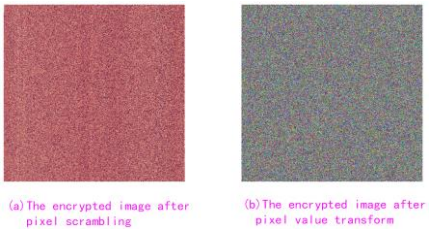

Fig.3 The encrypted image of Lena

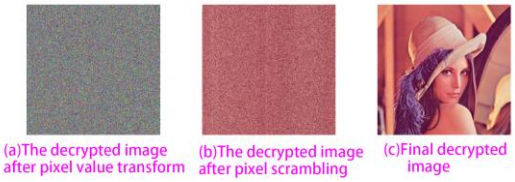

Fig.4 The decrypted image of Lena

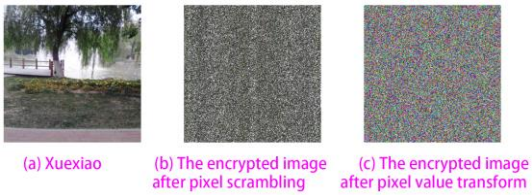

Fig.5 The encrypted image of Xuexiao

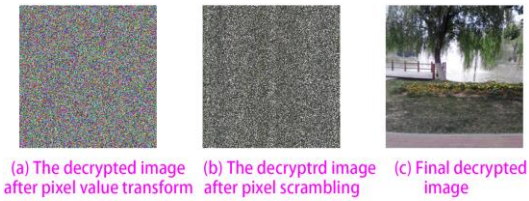

Fig.6 The decrypted image of Xuexiao

5.2 Correlation analysis

In this paper, the correlation coefficient among adjacent pixels of the image is shown in Table 1. As can be seen from the table, the correlation coefficient of the original image is close to one, which indicates that the adjacent pixels are highly correlated; The correlation coefficient of the encrypted image is close to zero, which illustrates there is little correlation among adjacent pixels. All these show the pixels of the encrypted image are randomly distributed. The encrypted image can effectively resist the attacks of the relevant statistical techniques, and its security is good.

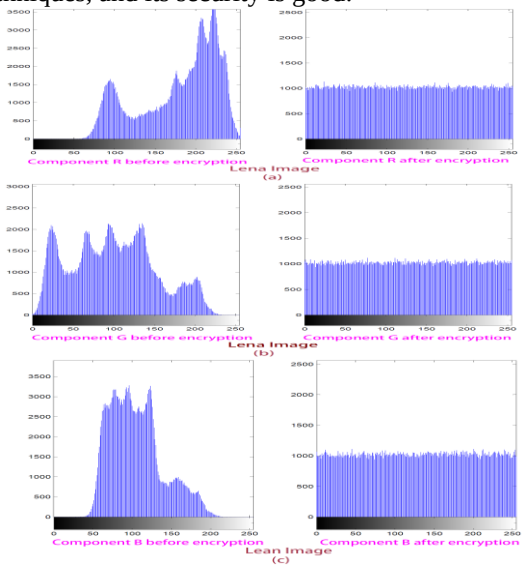

Fig.7 Histogram before and after encryption

Table 1 Correlation Coefficient

	Lena		Xuexiao	
	Original Image	Encrypted Image	Original Image	Encrypted Image
R	0.98663	0.00077537	0.91771	0.00020332
G	0.985	0.0012447	0.91698	0.0057597
B	0.9687	0.00068893	0.93997	0.0036447

6. Conclusion

This paper adopts an effective method to implement the image encryption operation. The method is based on the chaotic sequence generated by the fractional–order Chen system, and combines the double encrypted technique including the pixels position scrambling of image and the pixels value transform of image. The experimental results and performance analysis show that this method not only has good encryption effect, but also has high security.

Acknowledgements

This work was supported in part by the Young Scientists Fund of the National Natural Science Foundation of China (Grant No. 11202148), the Natural Science Foundation of China(Grant No. 61174094).

References

1. Dong W, Zhang L, Shi G, Li X, Non-Locally centralized sparse representation for image restoration, *IEEE Transactions on Image Processing*. 22(4) (2013) 1620-1630.
2. Liao X, Lai S, Zhou Q, A novel image encryption algorithm based on self-adaptive wave transmission, *Signal Processing*. 90(9) (2010) 2714-2722.
3. Jin Bing, Qi Lilei, JIA Yuzhen, Research of chaos cross-encryption algorithm based on Logistic mapping, *Computer & Digital Engineering*. 39(1) (2011) 93-94.
4. Wang Xiao, Zhao Dong. Double image encryption method with resistance against the specific attack based on asymmetric algorithm, *Optics Express*. 20(11) (2012) 11994-12003.
5. ZHANG Xiaoyan, WANG Chao, SUN Zhiren, et al. An image encryption scheme based on sequential CA, *Optics and Precision Engineering*. 16(9) (2008) 1781-1786.
6. Nooshin B, Youset F, Karim A, A robust hybrid method for image encryption based on Hopfield neural network, *Computer & Electrical Engineering*. 38(2) (2012) 356-369.
7. Liu Lili, Zhang Qiang, Wei Xiaopeng, A RGB image encryption algorithm based on DNA encoding and chaos map, *Computer and Electrical Engineering*. 38(5) (2012) 1240-1248.
8. Zhang Yonghong, Zhang Bo, Algorithm of image encrypting based on logistic chaotic system, *application research of Computer*. 32(6) (2015) 1770-1773
9. Zhang Jian, Fang Dongxin, Image encryption technology applied chaotic maps index and DNA coding, *Computer Engineering and Design*. 36(3) (2015) 613-618.