ENCRYPTION OF DIGITAL IMAGE BASED ON CHAOS SYSTEM

Jingtao Jian [1] , Yan Shi [2] , Caiqi Hu [1] , Qin Ma [3,*] , Junlong Li [4]

[1] *College of Mechanical and Electrical Engineering, Qingdao Agricultrual University, Qingdao, China, 266109; Email: jjtao_2518@163.com*

[2] *Foodstuff Science and Engineering college, Qingdao Agricultural University, Qingdao, China, 266109;*

[3] *College of Information and Electrical Engineering, China Agricultural University, Beijing, China, 100083*

[4] *Office of Agricultural Machine,Laixi, China,266600*

[*] *Corresponding author, Address: College of Information and Electrical Engineering, China Agricultural University, 17 Tsinghua East Road, Beijing, 100083, P. R. China, Tel:+86-10-62736973, Email: mei6668@163.com*

Abstract: In this paper, four kinds of chaos mapping equations such as Logistic, Henon, Quadratic and MacKeyGlass were discussed, and the numerical characteristics of those chaos mapping equations were analyzed and compared by histogram and correlation coefficient. Then the better chaos encryption system was selected according to analyzing result, and the encryption method of poor chaos encryption systems were modified. So the good performance of encryption was obtained, the degree of image scrambling transformation was improved greatly, and good effect of image encryption was gained.

Key words: Chaos encryption system; Digital image; Histogram; Correlation coefficient

1. INTRODUCTION

In recent years, with rapid development of the internet and the computer communications technique, the information transmission security becomes a hot subject of research currently subject of research. The chaos map equations have the property that a tiny fluctuation of the initial value can change the corresponding chaos code greatly, and so it is very difficult to

decrypt the chao coding file. Therefore, the chaos code are often used to encript the sound and image information. (Mei shuli et al., 2006; Yang wei et al., 2005; Yin xiandong et al., 2005) Different chaos codes can derived from different iterative equations such as Logistic, Henon, Quadratic, Mackeyglass and so on. But most researchers pay their attention on the Logistic chaos coding, in fact, each chaos code serial has its different value range and distribution from others. These two parameters impact the encrypt effect directly, and they are correlative to other parameters an the initial values in the chaos map equation. The object of this paper is to analyze the numerical properties of each chaos signal and find the optimal value range of each parameter in image encryption.

2. COMPARISON OF FOUR COMMON CHAOS CODE SERIES

2.1 Fundamental theory of image chaos encryption

Consider four common chaos code series such as the Logistic, the Henon, the Quadratic and the MackeyGlass, the corresponding map equations are

$$X_i = a \times X_{i-1} \times \left(1 - X_{i-1}\right), \quad \text{where a} = 4, \quad X_0 = 0.39 \tag{1}$$

$$\begin{cases} X_i = 1 - a \times \left(X_{i-1}\right)^2 + Y_{i-1} \\ Y_i = b \times X_{i-1} \end{cases}, \text{ where } \begin{cases} X_0 = 0.1, a = 1.4 \\ Y_0 = 0.1, b = 0.3 \end{cases} \tag{2}$$

$$X_i = a - \left(X_{i-1}\right)^2, \quad \text{where } X_0 = 0.1, a = 1.95 \tag{3}$$

$$X_i = X_{i-1} + \frac{a \times X_{i-s}}{1 + \left(X_{i-s}\right)^{10}} - b \times X_{i-1}, \tag{4}$$

where $X_0 = 0.1, a = 0.2, b = 0.1, s = 17$

The secret communication technique based on the chaos theory has four methods: the chaos spread spectrum, the chaos shift keying, the chaotic parameter modulation and chaotic masking. In these methods, the chaotic parameter modulation is applied widely being simple and mature. The chaos encryption principle based on the modulation technique and the chaos map method is shown in figure 1 (Mei shuli et al., 2006)., where s(n) is the wavelet transform series of the original signal，e(n) is the encryption signal which will be transmit to the receiving end, and $\hat{s}$ (n) is the final response

series, that is the decryption signal series. The corresponding chaos encryption result is shown in Fig.2.

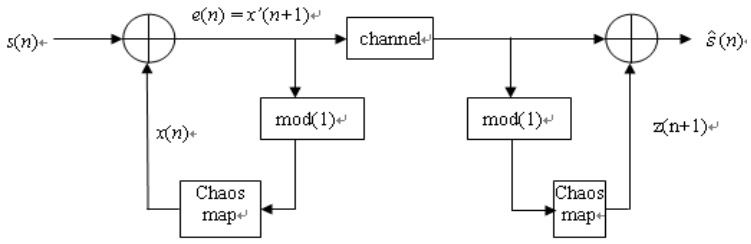


Fig.1. Chaos encryption theory

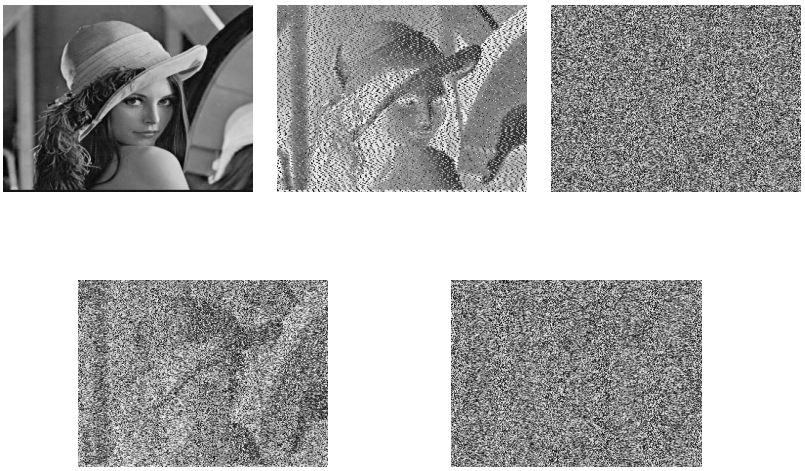
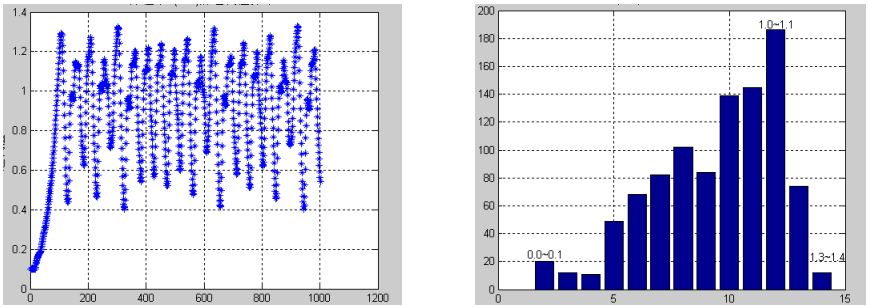


Fig.2. Encryption image based on different chaos series

（1） MacKeyGlass map equation

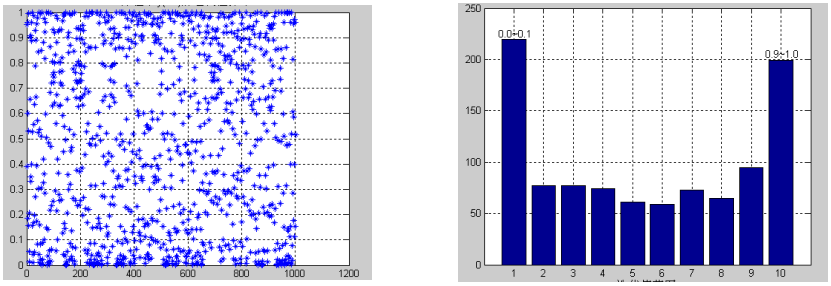


（a）chaos series distribution （b）statistic result

Fig. 3. MacKeyGlass series and its statistic result

The iterative value distribution of the MackeyGlass map equation is shown in figure 3. It is easy to see that the value range of the MacKeyGlass map equation is (0 ~ 1.4), and the distribution of the iterative value is uneven, the most of the iterative value is focus on the range (1.0~1.1).

（2） Logistic map equation

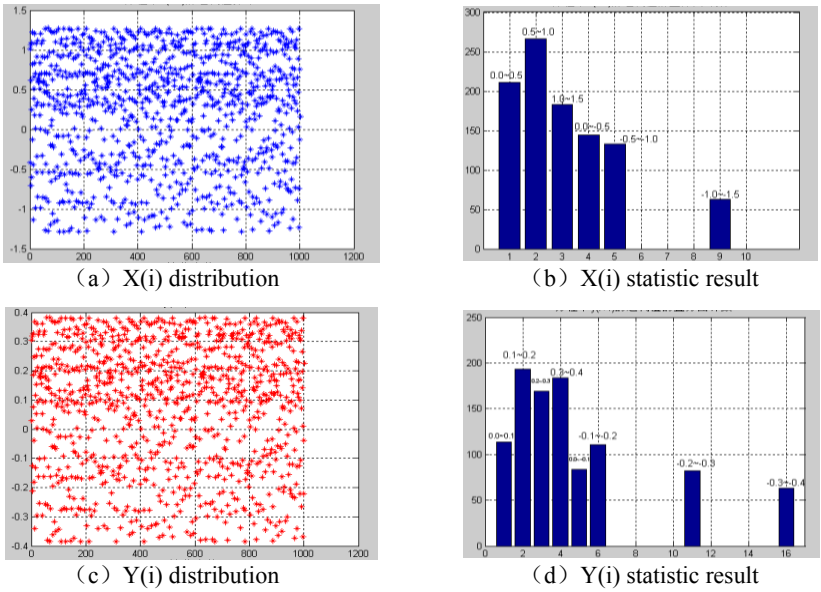


（a）chaos series distribution （b）statistic result

Fig.4. Logistic series and its statistic result

The iterative value distribution of the Logistics map equation is shown in Fig.4, the corresponding value range is (0~1.0). Apart from the range (0~0.1) and the range (0.9~1.0) where focus on a lot of iterative value, the value distribution is relative even in other range.

（3） Henon map equation



（a）X(i) distribution （b）X(i) statistic result

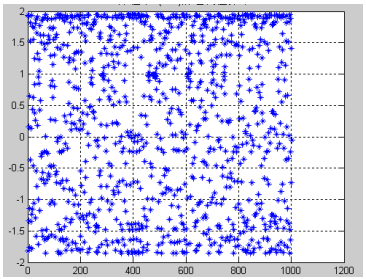
（c）Y(i) distribution （d）Y(i) statistic result

Fig.5 Henon series distribution and corresponding statistic result

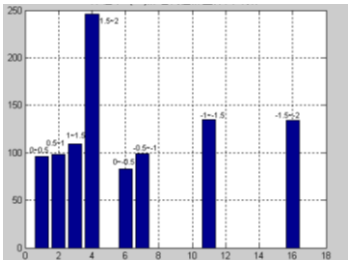
The solution x[i] of the Henon map equation is shown in Fig.(a) and (b), from which we know that the value range of x[i] is （-1.5 ~ 1.5）, and the most of the values fall in the range （-1.5 ~ 0.25）and the range （0.25 ~ 1.5）.

The soulution y[i] of the Henon map equation is shown in Fig.5(c) and (d), it is clear that the value range of y[i] is （-0.4 ~ 0.4）, and the most of the values fall in the range （0.1~0.4）and the range (-0.4~0.1).

（4） Quadratic map equation



（a）Chaos series distribution



（b）statistic result

Fig.6 Quadratic series distribution and the corresponding statistic result

The iterative value distribution is shown in Fig. 6. It is easy to see that the value range of this map equation is （-2~2）, and most of the values are distributed in the domains (1.5~2) and (-2~2.5). It should be noted that the value distribution in the domain (-2~1.5) is even in some degree.

It is easy to see that the distribution of the Logistic chaos series is even relatively, and the corresponding encryption effect is better. In fact, it could be concluded that the encryption effect is correlative with the evenness of the chaos series. And so we can improve the encryption algorithm by building a map function which can turn the uneven chaos series into the relative even ones.

3. OPTIMIZATION OF THE CHAOS SERIES

（1）Most of the iterative values obtained by the MacKeyGlass map equation are focus on the range（1.0~1.1）, the rest iterative values distributed in other range are not even in some extent.

Leaving all the iterative value falled in the range（1.0~1.1）and throwing off other ones, that is, only the values falled in the domain（1.0~1.1）are taken as the useful chaos series.

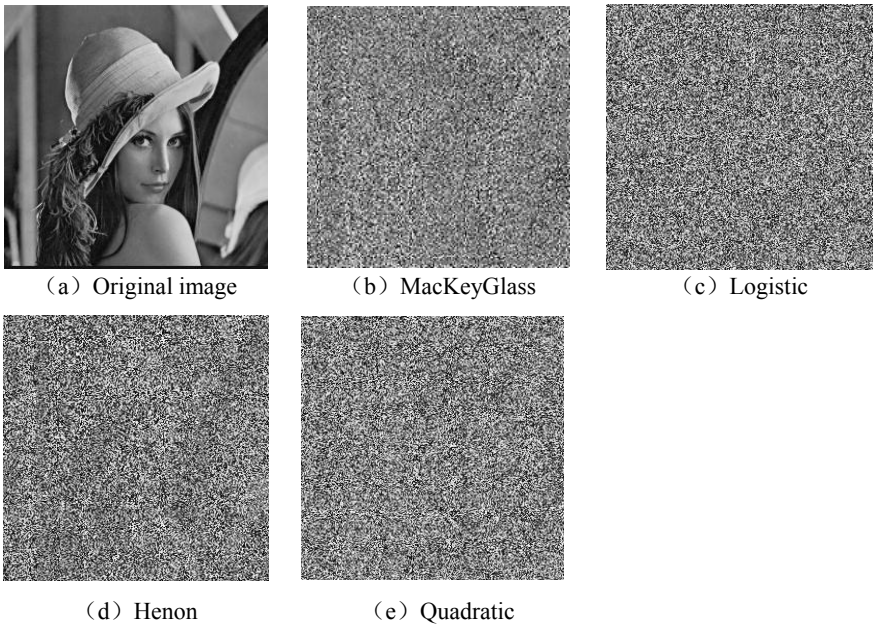
（2）Apart from the domains （0~0.1）and （0.9~1.0）, the iterative value derived from the Logistics map equation distributed in the domain

(0.1~0.9) evenly. So, we can abandon the values falled in the domains (0~0.1) and (0.9~1.0) and remain the ones falled in other domains.

（3） The iterative values derived from the Henone equation can be devided into two parts: x[i] and y[i] . Most values of the x[i] fall in the domains（-1.5~0.25）and（0.25~1.5）. Most values of the y[i] fall in the domains（0.1~0.4）and (-0.4~0.1).

Obviously, the values fall in the domains (-1.5~ 0.25) and (0.25 ~ 1.5) are taken as the useful chaos series of x[i], and the values fall in the domains （0.1~0.4）and (-0.4~0.1) are taken as the useful chaos series of y[i].

（4）Quadratic is the same as above, Apart from the values fall in the domain （1.5 ~ 2）, most of the iterative values falling in other domain are even relatively. So, the values in the domain (1.5 ~ 2) should be thrown off from the useful chaos series.



（a）Original image （b）MacKeyGlass （c）Logistic

（d）Henon （e）Quadratic

Fig.*7* Improved chaos series image encryption

4. CONCLUSION

The image encryption properties based on different chaos series were discussed in this paper. And then, an new improved method was proposed. In this new method, the encryption properties was improved by optimizing the distribution of the chaos series. In fact, the amount of the chaos map equation is more than 10, analyzing their properties and screening out the

best chaos series for the digital image encryption is very useful in net communications.

ACKNOWLEDGEMENTS

The project is supported by the national natural science fundation of China(No.60772038)

REFERENCES

Mei shuli, Gao wanlin. Image Chaos Encryption Technology Based on Interval Wavelet Coding [J]. Computer engineering, 2006, 32(16): 203-204,234

Wang Ying, Zheng Deling, Ju Lei. Digital Image Encryption Algorithm Based on Three-Dimension Lorenz Chaos System [J]. Journal of University of Science and Technology Beijing, 2004,26 (6)

Xu Quansheng,Li Zhen,Du Xuqiang. An Image Encryption Algorithm Based on Chaotic Sequences [J]. Journal of Chinese Computer Systems, 2006, 27 (9)

Yang wei, Chen Xiyou. Image Encryption Algorithm Based on Chaotic Mapping [J]. Techniques of Automation and Applications, 2005, 24(7)

Yi Kaixiang, Sun Xin, Shi Jiaoying. An Image Encryption Algorithm Based on Chaotic Sequences [J]. Journal of Chinese Computer Systems,2002,12(9)

Yin xiandong, Yao jun,Tang dan. Image Encryption Technology Based on DWT Domain[J]. Techniques of Automation and Applications, 2005, 3(1): 1-5