TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 12, December 2014, pp. 8229 ~ 8237
DOI: 10.11591/telkomnika.v12i12.4853

A New Image Encryption Algorithm Based on Two-dimensional Coupled Chaotic Map

Li Tu*[1], Liyuan Jia[2], Chi Zhang[3], Saiqiu Guo[4]
School of Information Science and Engeering,Hunan City University,
Yiyang, Hunan 413000, China, 086-07376353128
*Corresponding author, e-mail: tulip1903@163.com[1], jsjcarol@126.com[2]

Abstract

In this paper, a kind of two-dimensional coupled chaotic transcendental map (TCCTM) was proposed. Firstly, by using the TCCTM chaotic sequences were generated,then the chaotic sequences were modified to generate chaotic key stream that is more suitable for image encryption. In the process of encryption, an original color image was decomposed into three images of red, green and blue components, and encrypted them in a different way respectively. The experimental results demonstrate that the extremely sensitive to the key, the encrypted image has random-like distribution behavior of grey values, the adjacent pixels have zero co-correlation properties. Furthermore, the algorithm shows the advantages of large key space and high speed of encryption.

Keywords: *two-dimensional coupled chaotic transcendental equation; position scrambling, sensitivity, Image encryption*

1. Introduction

Due to the characteristics of easy-understanding and attractive presentation, multimedia contents such as image and audio, have been widely transmitted in Internet and mobile communications. people can obtain, use or process digital images more frequently. Since digital media such as image, audio, and video are easy to process, copy and transfer, the emergence of powerful tools raises a series of problems. It has become essential to secure information from leakages. Many peoplehas done research of this area and obtained many achievements [1]. Some classic encryption techniques such asoptical transforms and chaotic maps have become a vital role in protecting images due to the increasing requirement for image storage and transmission [2-7].

Chaos is a particularly interesting non-linear effect. Chaos theory has been established since 1970s by many different research areas, such as physics, mathematics, engineering, and biology, etc [8]. Because of the characters of non-periodicity, non-convergence, ergodicity,and high sensitivity to initial conditions, which is related to cryptosystem, chaos is used for cryptology. Several approaches are seen in the literature that applies to concepts from the chaotic systems.

In recent years, a variety of chaos-based image cryptosystems have been studied. In [9], a hyperchaotic encryption scheme is presented. The drawbacks such as small key space and weak security of low-dimensional maps, high-dimensional chaotic systems were used in cryptosystems. To meet the requirements of modern applications with high levels of security, a kind of two-dimensional coupled chaotic transcendental map (TCCTM) is proposed in this paper, And it was used in image encryption

2. Chaos Model

2.1. Transcendental Equation

Function 2.1 is a transcendental equation, Feigenbaum has studied its bifurcation and chaotic characteristics, and made its corresponding figure.

$$x_{k+1} = a\sin(\pi s_k), k = 1,2,3,...n \tag{1}$$

Received November 19, 2013; Revised October 18, 2014; Accepted November 6, 2014

Here parameter a is a non-negative real number, from any initial value, $x_k \in [0,1]$, selected the initial values of x$_0$=0.1234 and a=3, Figure 1 is the scatter plot of a transcendental equation. Figure 1 shows that:

(1) When parameter$a \in (0.0,0.319)$, no matter what initial values we choose, the final result will be close to 0;

(2) When parameter$a \in (0.319,0.732)$, the final result will be close to A non-zero number,This is a stable single value ;

(3) When parameter$a \in (0.732,0.856)$, the function curve gets into two branches, the iterative value x falls between two fixed values, a solution of period 2;

(4) When parameter $a \in (0.856,1)$,it is a chaotic mapping;

(5) When parameter $a \geq 1$, the iterative results may fall in any sub-interval of the interval (-a,a) randomly, and it may be repeated. This is the ergodicity of chaos. With the increasing of parameter a, the map appears blank windows periodically.

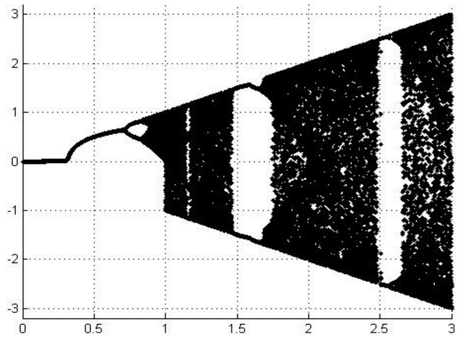


Figure 1. Bifurcation and Blank window for transcendental equation (a=0:3,x$_1$ =0.1234)

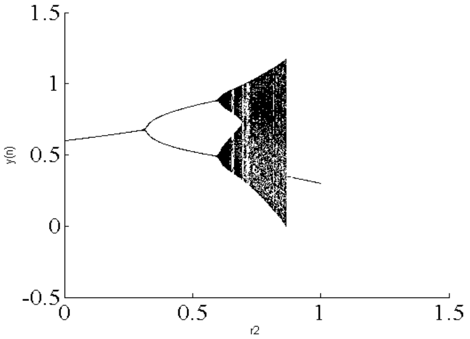


Figure 2. Bifurcation for the improved transcendental equation a=0.2, b=0.21, x$_1$=0.12, y$_1$=0.31, r$_1$= r$_2$=0:2

2.2. Improved Two-dimensional Transcendental Equation

A one-dimensional equation can generate chaotic sequence through iterative calculation, but its key space is generally small, and its security is not high. For this problem, we proposed an improved two-dimensional coupled chaotic transcendental map, its mathematical expression is:

$$\begin{cases} x_{n+1} = 3\,a\sin(\pi s_n) + r_1 y_n x_n \\ y_{n+1} = 3\,b\sin(\pi s_n) + r_2 y_n x_n \end{cases} \tag{2}$$

Where $a,b \in (0,1), r_1, r_2 \in (0,2), x,y \in (-12,12)$.Took the initial values of $x_1 = 0.12, y_1 = 0.31$ The bifurcation of the improved transcendental equation is shown in Figure 2:

(1) When parameter $a \in (0.0,0.3)$, the chaotic mapping converges to a nonzero number,it is called a fixed point, and it is a stable single value;

(2) When parameter $a \in (0.3,0.6)$, the function curve gets into two branches,it is a state of period 2;

(3) When parameter $0.6 \leq a \leq 0.8$, the chaotic mapping appear chaotic state mainly, and it appears blank windows too;

(4) When parameter $a \geq 0.8$, the chaotic mapping generates a stable single value. It doesn't have chaos characteristics.

3. Encryption Algorithm and Decryption Scheme

3.1. Encryption Algorithm

The encryption steps are as follows:

(1) Read a size of 256*256 pixels colour image, calculated its red, green, and blue components, saved its value in three two-dimensional arrays respectively, then converted them to 3 length of 256*256 one-dimensional sequence. Through iterative calculation from the improved chaotic equation, it generated two one-dimensional arrays, they are named array B(Formed from x series) and array I (Formed from y series), their length are 256*256. In order to increase the difficulty of the ciphertext, took the first, the sixth and the fifth digit of the elements in array B after the decimal point to form a three-digit number, had it on 256 remainder operation, and we got sequence L1;

(2) First we encrypted the image of the red component, had its value on array L1 remainder operation, converted it to a 2-dimensional sequence;

(3) Then we encrypted the image of the green component,built a two-dimensional matrix M1, its column length is 2, and its line length is 65536(256* 256). Put the elements of array I on the first row of the matrix P, elements of green component on the second line, these numbers 1,2,3...256*256 on the second line, the two-dimensional matrix p is also the decryption matrix. Then sorted the elements in the array I, that sort the first line of matrix P, took the second line of sorted matrix P1, we got a one-dimensional sequence D1. The position of elements in green component sequence has changed following the elements in chaotic array I;

(4) We had a double encryption on the image of the blue component,first it made a gray encryption(the method is the same as the encryption algorithm of red component),then made a position encryption(the method is the same as the encryption algorithm of green component).

3.2. Decryption Scheme

(1) Read these encryped images of the red, green and blue component, saved their value in three two-dimensional arrays respectively, then converted them to 3 length of 256*256 one-dimensional array A1, A2 and A3;

(2) The decryption sceme of the red component image was to have its value on array L1 remainder operation, then convert it to a 2-dimensional sequence;

(3) The decryption sceme of the green component image: Built a two-dimensional matrix E, put the elements of array I on the first row of the matrix P, put these numbers 1,2,3...256*256 on the second line, then sorted the elements in the array I, took the second line of sorted matrix E, we got a one-dimensional sequence Q. Built a two-dimensional matrix K, put the elements of array A2 on the first row of the matrix K,and put the elements of array Q on the second row of the matrix K, sorted the elements in the sequence Q, took the first line of sorted matrix K, converted it to a 2-dimensional matrix G, matrix G is the decrypted image of the green component;

(4) The decryption sceme of the blue component image: first we made a gray decryption (the method is the same as the decryption algorithm of red component), then we made a position decryption(the method is the same as the decryption algorithm of green component);

(5) Put these three decrypted component in a 3-dimensional matrix, composed the three components of image to a color images.

3.3. Experimental Results

In this paper we used the double encryption approach to encrypt images, and the initial value and the control parameters were: $r_1 = 0.1, r_2 = 0.2, a = 1.01, b = 0.9, x_1 = 0.22, y_1 = 0.23$. We have used the USC-SIPI image database which is referred in Reference [13] (freely available at http://sipi.usc. edu/database/). Figure 3(a) and Figure 3(b) are the color plain image and the gray plain image.

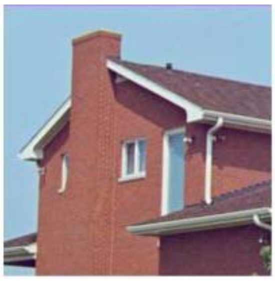


Figure 3(a). Plain image

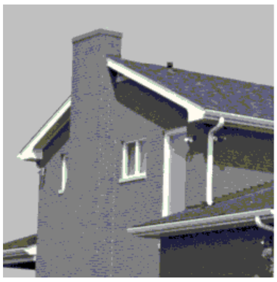
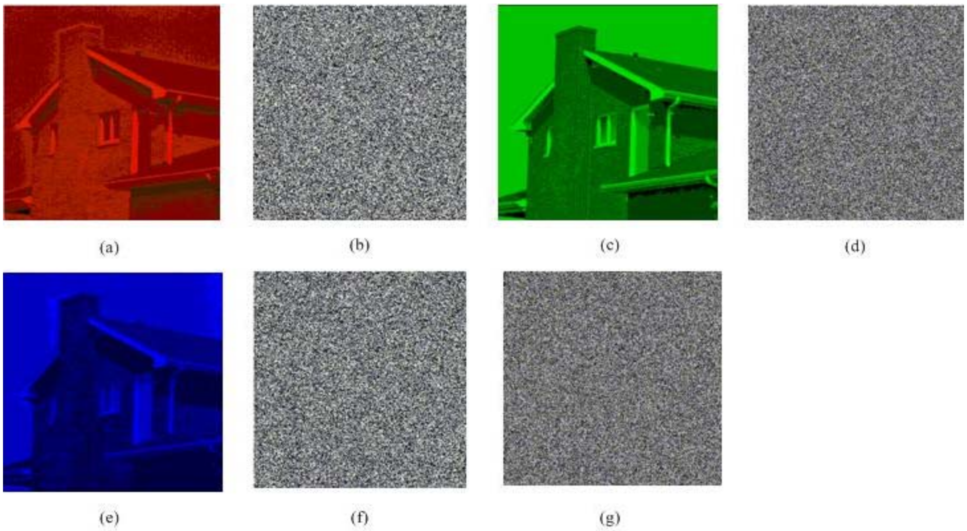


Figure 3(b). Plain gray image

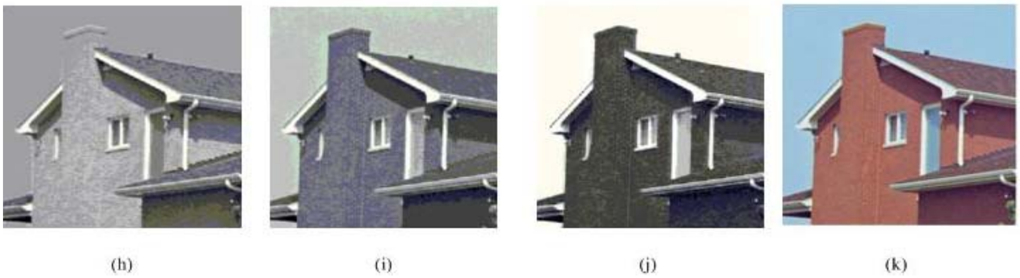
Figure 4(b, d) are the encrypted images of red and green component, Figure 4(f, g) are the encrypted images of green component.



(a) Image of the red component (b) Encryped image of the red component(c) Image of the green component (d) Encryped image of the green component(e) Image of the blue component (f) The first encryped image of the blue component (g)The second encryped image of the blue component

Figure 4. Cipher images

The decrypted images of the red, green, blue component are shown in Figure 5(h, j, k), the composited image is shown in Figure 5(k).



(h)The decrypted image of the red component (i) The decrypted image of the green component (j) The decrypted image of the blue component (k) The composited image

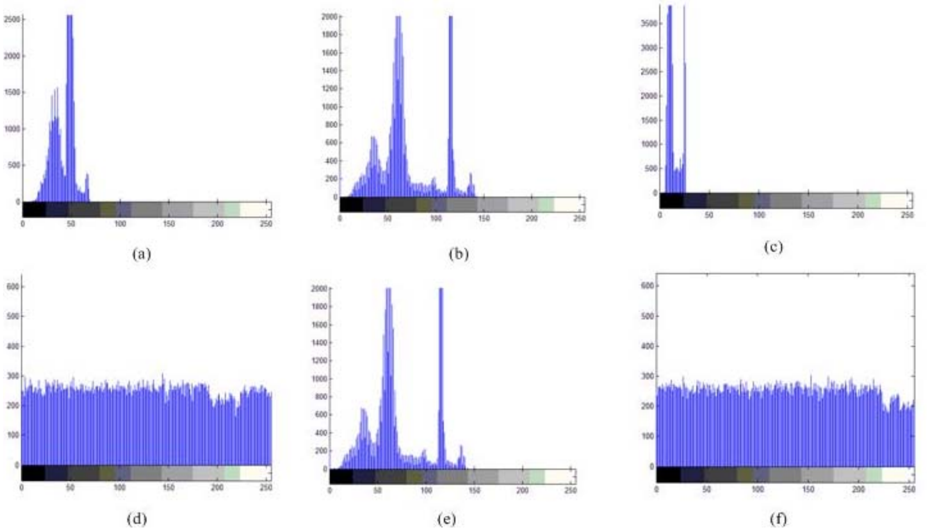
Figure 5. Decrypted images

4. Performance and Security Analysis

All the security analysis has been done on MATLAB 7.0 by Intel Pentium 64 X2 Dual Core processor 2.0GHz personal computer.

4.1. Histogram

Gray histogram is a function of grayscale, it describes the number of gray levels of pixels in an image, and it reflects the frequency of gray value in an image. Its abscissa is gray level, its ordinate is the frequency of the gray level. Figure 6 is the histogram of the three components.



(a) Histogram of the image of red component(a) Histogram of the image of green component(a) Histogram of the image of blue component(d) Histogram of the decrypted image of red component(e) Histogram of the decrypted image of green component(f) Histogram of the decrypted image of blue component

Figure 6. The histogram of the three components

Figure 6 shows, before encryption the rise and fall of the histograms are very large, the distribution is not uniform, and after encryption the histogram of the image of red component and green component are complanate, the gray value of encrypted image is in uniform distribution. This shows that in the range of (0,255), the probability of the pixel value in encrypted image is equal. The statistical characteristics of encrypted image are quite different from that of the plain image. The statistical characteristics of plain images spread to encrypted images evenly, this reduces their correlation greatly.while it only made a position encryption on the image of green component, its histogram does not change.

4.2. Correlation Analysis of Two Adjacent Pixels

The substantive characteristics of a digital image determine that there is strong correlation among adjacent pixels. This correlation makes the content of the image is easy to be identified [10]. We calculated the pixel correlation using the following formula (3) and formula (4) [11]:

$$\mathrm{cov}(x,y)=E((x-E(x))(y-E(y))) \tag{3}$$

$$R_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{4}$$

Here x and y are the gray values of two adjacent pixels in the image, E(x) is a mathematical expectation, D(x) is the variance of x, cov(x,y) is the population covariance. In order to destroy the statistical attacking,we must reduce the correlation of adjacent pixels. The lower the correlation coefficient, the better the encryption effect. In the process of calculation, we use formula (5-7).

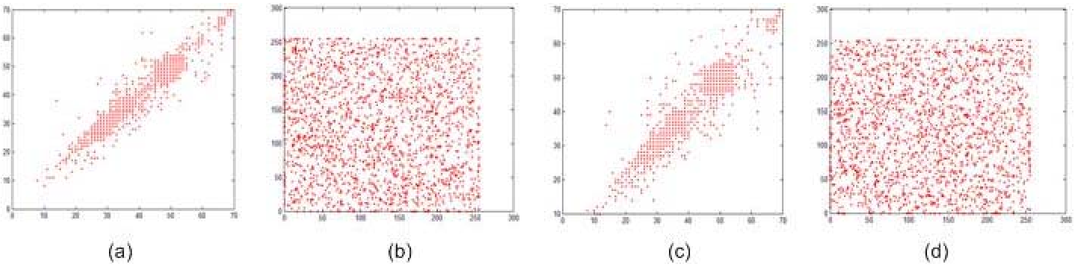
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{5}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{6}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))\cdot(y(i)-E(y)) \tag{7}$$

The following steps are performed to evaluate an image's correlation property: (1) 2000 pixels are randomly selected as samples, (2) the correlations between two adjacent pixels in horizontal, vertical or diagonal directions are calculated by the formula above. Their distribution is shown in Figure 7, Figure 8 and Figure 9.

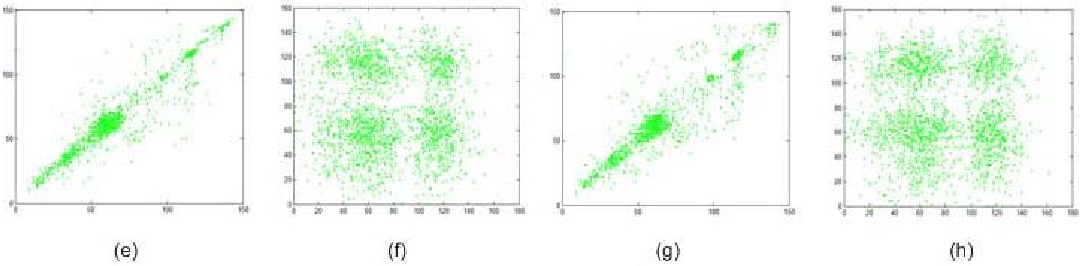
Figure 7 is the correlation of adjacent pixels of red component.



(a) Correlation of level adjacent pixels of the image of red component (b) Correlation of level adjacent pixels of the encryped image of red component (c) Correlation of diagonal adjacent pixels of the image of red component (k) Correlation of diagonal adjacent pixels of the encryped image of red component

Figure 7. Correlation of adjacent pixels of red component

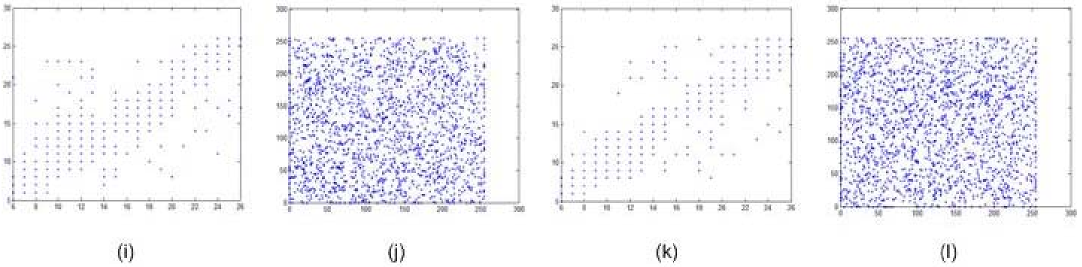
Figure 8 is the correlation of adjacent pixels of green component.



(e) Correlation of level adjacent pixels of the image of green component (f) Correlation of level adjacent pixels of the encryped image of green component (g) Correlation of diagonal adjacent pixels of the image of green component (h) Correlation of diagonal adjacent pixels of the encryped image of green component

Figure 8. Correlation of adjacent pixels of green component

Figure 7 is the correlation of adjacent pixels of blue component.



(i) Correlation of level adjacent pixels of the image of blue component (j) Correlation of level adjacent pixels of the encryped image of blue component (k) Correlation of horizontal adjacent pixels of the image of blue component (l) Correlation of horizontal adjacent pixels of the encryped image of blue component

Figure 9. Correlation of adjacent pixels of blue component

The more obvious the scrambling degree of images were, the better the effect of the encryption is. The correlation among the plain image pixels shows a linear distribution,the correlation among the encrypted image pixels is a random distribution. It can be seen from the Figures above that the degree of image scrambling is very significant.

4.3. MSE

MSE (Mean Square Error) is used to measure the performance of encryption, the bigger the the value of mean square error, the better the effect of encryption. The formula of MSE is:

$$MSE = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{i=1}^{N}[D(i,j) - P(i,j)]^{2} \qquad (8)$$

Where parameter M, N are the gray level of images, parameter D is the grayscale of the encrypted image, and parameter P is the grayscale of the plain image. Table 1 is the MSE value of the encryped image of the red, green and blue components and their plain images:

Table 1. MSE value

Image	MSE
the encryped image of the red component and the plain image of red component	12113
the encryped image of the green component and the plain image of green component	2167.6
the encryped image of the blue component and the plain image of blue component	17068
the decrypted image of red component and the plain image of red component	0
the decrypted image of green component and the plain image of green component	0
the decrypted image of blue component and the plain image of blue component	0

Table 2. MSE value

component	Entropy of information
the plain image of red component	4070662
the encryped image of red component	7.954878
the plain image of green component	5.737772
the encrypted image of green component	5.737772
the plain image of blue component	3.372893
the double encrypted image of blue component	7.993671

4.4. Information Entropy Analysis

Information entropy is one of the criteria to measure the strength of a cryptosystem, which was firstly proposed by Shannon in 1949 [11]. Information entropy of image describes the distribution of grey value [12], its formula is:

$$H(s) = -\sum_{i=1}^{2^n-1} P(S_i)\log_2[P(S_i)] \tag{9}$$

Where $P(S_j)$ is the probability of symbol S_i, 2^n is the total number of state of information source S. The information entropy is used to analyze the performance of encryption method. When the image pixel is uniformly distributed, the probabilities of grey value are basically equal, entropy can achieve the maximum, it shows that, the more dispersed the grey value, the better the performance of encryption. A 256 level of gray image has 28 kinds of possible pixel values, so its ideal information entropy should be 8. If the information entropy of a 256 level gray encrypted image is close to 8, the cipher image closes to the random distribution. The information entropy obtained from simulation experiment is shown in Table 2.

Table 2 shows that, it made a gray encryption on the image of red component, and it made a double encryption on on the image of blue component, their information entropy had changed a lot, their performance of encryption method is very good, it is hard to be decryped. And it made a position encryption on the image of green component, its information entropy did not change, this means that, position encryption only changes the position of the pixel, it does not change its information entropy.

4.5. Key Space Analysis

Key space size is the total number of different keys that can be used in the encryption [13]. There are six parameters in the improved chaotic equation, in theory, the key space of each parameter is 1014, due to the actual precision of computer, the key space of each parameter was 10^6, so, the key space of the two-dimensional coupled chaotic map is $1.0*10^{36}$. It has obvious superiority, and it is easier to implement the algorithm by using hardware. Simulation results show that, even under the condition of existing computer precision, the key space is large enough. And 1035=2117,it means that, an attacker needs a 117-bit computer to decode the algorithm. If he use the violence attack methods, $10^{36}=2^{117}/365/24/60/60/2.6G=1.2192*10^{18}$, it means, if an attacker decode the algorithm by using a 2.6GHZ frequency of computer, he needs $1.2192*10^{18}$ years.

5. Conclusion

In this work a kind of two-dimensional coupled chaotic map based on Feigenbaum transcendental equation is proposed, the behavior of this method is similar to the substitution box like encryption algorithms. The results show that the encryption algorithm is easy to realize, the pixels of encrypted image has characteristics of statistical distribution, and the algorithm is sensitive enough to the keys, The key space is large enough, the correlation of adjacent pixels of encrypted images is close to 0, the algorithm is more secure and hence more suitable for image encryption for applications. As future work, the diffusion efficiency of this algorithm needs to be improved.

Acknowledgements

This work was supported by Scientific Research Fund of Hunan Provincial Science Department under Grant (No: 2013FJ3087, 2013FJ3086, 2012FJ4329), Scientific Research Fund of Hunan Provincial Education Department under Grant (No: 12C0573).

References

[1] Liu YJ, Chen CPL, Wen GX, Tong SC. Adaptive neural output feedback tracking control for a class of uncertain discrete-time nonlinear systems. *IEEE Trans. Neural Netw.* 2011; 22: 1162–1167.

[2] Li H, Wang Y. Information security system based on iterative multiple-phase retrieval in gyrator domain. *Opt Laser Technol*. 2008; 40: 962–966.

[3] Meng XF, Cai LZ, Wang YR, Yang XL, Xu XF, Dong GY, et al. Digital image synthesis and multiple-image encryption based on parameter multiplexing and phase-shifting interferometry. *Opt Lasers Eng.* 2009; 47: 96–102.

[4] Liu ZJ, Guo Q, et al. Double image encryption by using iterative random binary encoding in gyrator domains. *Opt Express*. 2010; 18: 12033–12043.

[5] Jin J. An image encryption based on elementary cellular automata. *Opt Lasers Eng*. 2012; 50: 1836–1843.

[6] Wang Y, Wong K W, Liao X, et al.. A new chaos-based fast image encryption algorithm. *Applied Soft Computing.* 2011; 11(1): 514-522.

[7] Liu Z, Li S, Liu W, Wang Y, Liu S. Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Opt Lasers Eng*. 2013; 51: 8–14.

[8] R Brown, LO Chua. Clarifying chaos: examples and counterexamples. *Int. J. Bifurcat Chaos.* 1996; 6: 219–242.

[9] Belmouhoub I, Djemai M, Barbot JP. Cryptography by discrete-time hyperchaotic systems. *Proceedings of 42nd IEEE Conference on Decision and Control.* 2003; 2: 1902-1907.

[10] Iqtadar Hussain, Tariq Shah Muhammad Asif Gondal, Hasan Mahmood. A novel image encryption algorithm based on chaotic maps and GF(2^8) exponent transformation. *Nonlinear Dyn*. 2013; 72: 399-406.

[11] Shannon CE. Communication theory of secrecy system. *Bell Syst Tech J.* 1949; 28: 656-715.

[12] Wei Zhang, Kwok-wo Wong, Hai Yu , Zhi-liang Zhu. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Commun Nonlinear Sci Numer Simulat.*2013; 18: 2066-2080.

[13] Shubo Liu, Jing Sun, Zhengquan Xu. An Improved Image Encryption Algorithm based on Chaotic System. *Journal of Computers.* 2009; 4(11):1091-1100