Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(6):2583-2592

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Secure transmission of encrypted biological image based on improved transcendental equation

Li Tu[1], Xuehua Huang[1*], Liyuan Jia[1] and Chuan Xie[2]

[1]School of Information Science and Engineering, Hunan City University, Yiyang, Hunan, China
[2]Department of Fundamental Medical and Clinial Loboratory, Yiyang Medical College, Yiyang, Hunan, China

ABSTRACT

An improved transcendental equation and new image encryption algorithm is proposed. Compared with the logistic mapping and the transcendental equation, the modified chaotic equation has larger key space, and the generated chaotic sequences has excellent performance such as cross correlation and sensitivity. The modified transcendental equation was used in biological image encryption, and the encryped image was embedded in a carrier image using the LSB(least significant bit) algorithm. Theoretical analyses and experimental results show that the equation and the algorithm has more efficiency and security, it can resist violence attack, known-plaintext attack and statistical analysis effectively.

Keywords: Chaos, Transcendental Equation, Image encryption

INTRODUCTION

Biology is a kind of science to study the structure, function, behavior, development and evolution of biological and the relationship between organisms and their environment of all levels in life system. The basic unit of life is cell, it is composed of proteins, nucleic acids, lipids and other biological macromolecules, the phenomenon of life is the movement and transfer of material, energy and information in the complex system. Life system has many characteristics that non living things do not have. For example,the organism can produce a variety of organic compounds at ordinary temperatures and pressures, including complex biological macromolecular; it can store and transfer information with great efficiency; it has the function of self-adjustment and the ability of self replication;it performs ontogenesis and the evolution of species in irreversible ways[1]. Biology has wide application prospects and potential economic value.

With the rapid development in digital image processing and network communica- tions,biological image data is transmitted over all kinds of wired and wireless channels more and more frequently. For example, Chinese government implements one-child policy, non-medical uses of identifying the sex of the fetus is prohibited, it would result in sexism and worsening sex ratio. How to protect the biological images become an issue of the universal concern.

EXPERIMENTAL SECTION

2.1.Logistic Mapping

One-dimensional Logistic map is a simple chaotic map[2], its mathematical expression is:

$$x_{k+1} = ux_k(1-x_k), k = 0,1,2,... \tag{1}$$

here $x_k \in (0,1), k = 0,1,2,..., \mu \in (0,4]$,and parameter μ is a bifurcation parameter[9].Fig. 1 shows the different characteristics with different values of μ.The horizontal axis is the values of the parameter μ and the vertical axis is the possible long-term values of x_k .

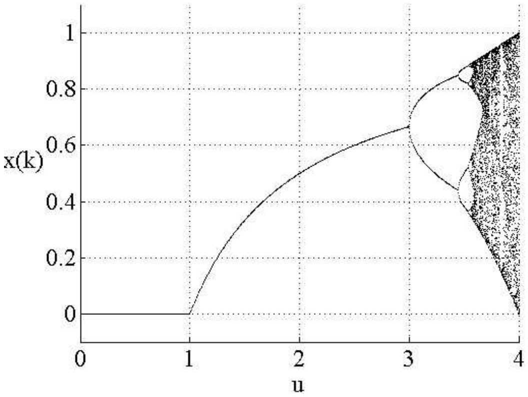


Figure 1. Iterative results diagram for the logistic map (Insect population model)

When μ=3,in figure 1 a single line begin to get into two directions,when $\mu = 1 + \sqrt{6}$,the system begins to appear four cycles.After this,a lot of period-doubling branch appear in the increasingly narrow μ interval,after n-th branch,the cycle length is 2n.This periodic doubling process is not limited, however, the corresponding a parameter μ has a limit: μ=3.56994567…,when 3.56994567<μ≤4, the system gets into a chaotic state, when μ=4, the mapping is a full map[9-10],the chaotic sequence generated by the system has ergodicity on the interval (0,1).

The Logistic map has some common problems such as stable windows,blank windows, uneven distribution of sequences and weak key[3-8].

We will use these two Logistic maps which have different chaotic region and range, in the following encryption process, making the encryption effect better.

2.2. Transcendental Equation

Function 2 is a transcendental equation, Feigenbaum has studied its bifurcation and chaotic characteristics, and made its corresponding figure.

$$x_{k+1} = \lambda \sin(\pi x_k), k = 0,1,2,... \tag{3}$$

In function 1,parameter γ is a non-negative real number, from any initial value $x_0 \in [0,1]$, after iterative computation, we can obtain a certain sequence x_1, x_2, ... X_n. When the parameters in the range [0,6],so the x coordinate is [0,6]; the value of y have negatives, so the y coordinate is [-6,6],the bifurcation and blank window for transcendental equation is shown in Figure 1(b).

For different values of parameter λ, the equation(1) will present different characteristics, with the increase of the parameter λ, the system experiences period-doubling bifurcation continuously, and reaches the chaos eventually, the specific process is as follows:

When parameter λ is in the range of [0,0.3],the value of y keeps at 0, then it begins to increase; when parameter λ is in the vicinity of 0.75, the function curve gets into two branches. With the increasing of parameter λ, the iterative sequences is more complex, the iterative results may fall in any sub-interval of the interval (-6,6) randomly, and it may be repeated. This is the ergodicity of chaos. With the increasing of parameter λ, the function curve shows a periodicity.

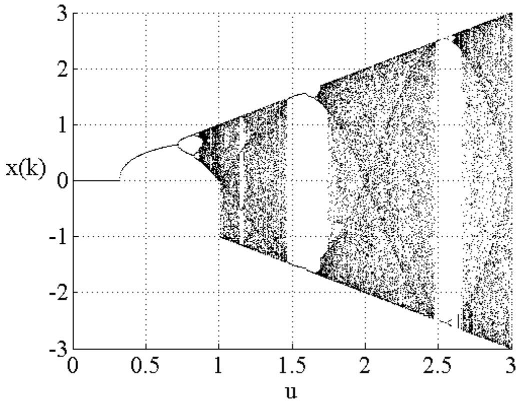


Figure 2. Iterative results diagram for the transcendental equation.

2.3Improved transcendental equation

In this study we proposed an improved transcendental formula, its mathematical expression is:

$$x_{k+1} = u\sin(\pi x_k)(1-\frac{\mu}{2\gamma}\sin(\pi x_k)), k = 0,1,2,... \tag{4}$$

In fact, we have introduced a Logistic chaotic mapping, and had it as a parameter of the transcendental equation. In order to ensure that the parameter of the sine function is a chaotic sequence, we selected the following range of parameters $\mu \in [0,6]$ and $\gamma = 3.8$, then we made the following function diagram, the bifurcation and blank window for the improved transcendental equation is shown in Figure 3.

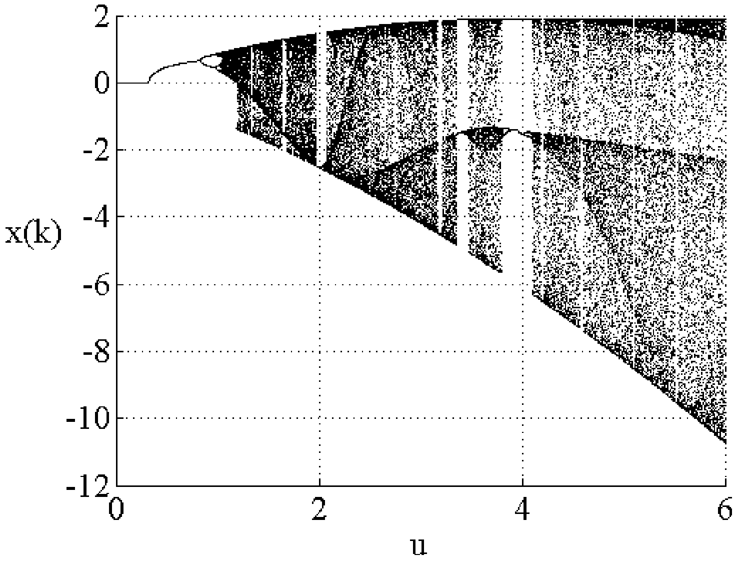


Figure 3.Bifurcation and blank window for the improved transcendental equation

In order to analyze the modified transcendental equation further, we selected the following range of parameters $\gamma \in [1,6]$ and $\mu = 3.8$, took an initial value x1=0.123456,then we made the following function diagram, the bifurcation and blank window for the improved transcendental equation is shown in Figure 4.

Figure 4 shows that, the function has chaotic characteristics only,there are some stable windows and blank windows in Figure 4.When parameter γ is greater than 5.3, the bifurcation and blank window for the improved transcendental equation get into a single line.

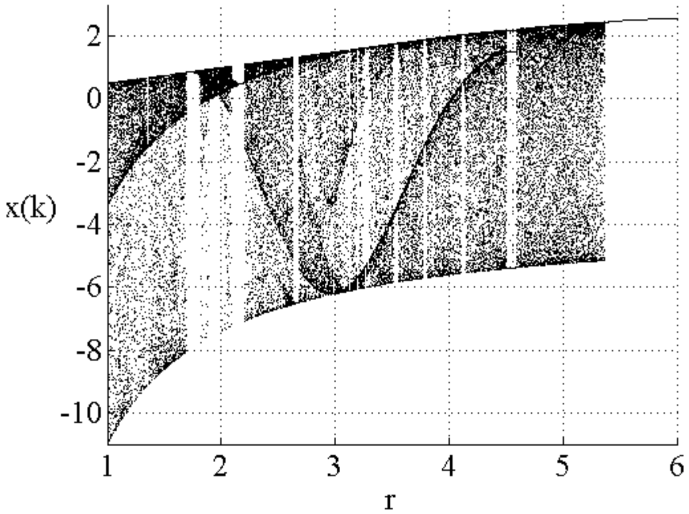


Figure 4.Bifurcation and blank window for the improved transcendental equation

RESULTS AND DISCUSSION

3.1. *Position transformation and encryption*

3.1.1 Encryption algorithm

(1)Grayscale encryption

Step 1) Read a size of 256*256 pixels colour image M, converted it to grayscale orginal image A, converted A to a length of 256*256 one-dimensional sequence A1.

Step 2) Selected the parameter μ=5.6,the initial value $x_1 = 0.654321$, and γ=3.81, we discarded the results before 200 times iterative operation, it generated a length of 256*256 one-dimensional sequence L1 using the modified transcendental equation of formula (3). In order to increase the difficulty of the ciphertext, took the second, the sixth and the fifth digit of the elements in sequence L1 after the decimal point to form a three-digit number, had it on 256 remainder operation, and we got sequence L2.

Step 3) XORed each binary bit of the elements in one-dimensional matrix A1 and matrix L2, then we got matrix A2,and it was the grayscale encrypted ciphertext.

(2)Position encryption

Step 1) Selected the initial value $x_1 = 0.618$, $\mu = 5.3$,γ=3.8, we discarded the results before 300 times iterative operation,and it generated chaotic sequence k1 from the modified transcendental equation, this is a length of 256*256 one-dimensional sequence too. We changed all numbers in matrix k1 into absolute values, found the maximum value($y_{\max}$) and the minimum value($y_{\min}$) of the array matrix k1,and then divided sequence A1 by the value of ($y_{\max} - y_{\min}$), and sequence k1 has been converted into a chaotic sequence in range of [0,1].

Step 2) Corresponded the various elements in sequence A2 and sequence k1, built a two- dimensional matrix p, its column length is 2, and its line length is 65536(256* 256). We put the elements of sequence k1 on the first row of the matrix P, elements of A2 on the second row, the elements of third row of A2 is 1,2,3,…,65536,the two-dimensional matrix p is also the decryption matrix.

Step 3) Sorted the first row of matrix P, we got a two-dimensional matrix P1, took the second line of the sorted matrix P1, we got a one-dimensional sequence A3. this means the position of elements in sequence A2 has changed following the elements in chaotic sequence k1, it has generated the ciphertext sequence A3. Matrix A3 is the grayscale encrypted ciphertext.

(3) Information hiding

Information hiding is to hide a kind of information in another kind of information,it is to hide information using the insensitivity of sense organ of human beings. The hidden information is not easy to be detected,and it doesn't it affect the feeling effect and the use value of the carrier information.Information hiding has robustness,imperceptibility, transparency,security,self recovery and other characteristics.

In this paper, we used the LSB(least significant bit) algorithm to hide the encryped image. An image can be represented by a two-dimensional matrix, each numerical of the matrix represents the color information of a pixel.We treated the image as a surface,and we treated the 8 bit binary number corresponds to the pixels of an image as the height, it formed a stereoscopic histogram,the same pixels formed a plane,it is called “bit plane”.

The zeroth bit plane to the seventh bit plane of an image are regarded as the unimportant bit plane to the most important bit plane, the zeroth bit plane is called the least significant bit,and the seventh bit plane is called the most significant bit(MSB).In a byte, the importance of each bit is different.In information hiding, there is different effect on image by modifying different binary bits. We can conclude from the results that, the MSB(most significant bit) have the greatest influence on the effect of an image, after modified the MSB, the color data of images has been destroyed completely,but the LSB(least significant bit) have the lowest influence on the effect of an image. For example: 11110110 and 11110111 represent two different levels of red,but we couldn't tell the difference of them by eyes, so after modified the LSB,the change of an image almost cannot be identified with the naked eye,so we can hide the information of images through modifying the values on low bit plane.

Step 1) Performed an and operation between each binary bit of each pixel value from the carrier image and the number 252,the zeroth binary bit and the first binary bit have been 0.

Step 2）Performed an and operation between each binary bit of each pixel value from the encryped image and the number 3, converted it into a one-dimensional array,we got a matrix M1,the zeroth binary bit and the first binary bit were retained in the array M1; Performed an and operation between each binary bit of each pixel value from the encryped image and the number 12, converted it into a one-dimensional array, moved each value of the matrix 2 binary bits to the right, we got a matrix M2,the third binary bit and the fourth binary bit were retained in the array M2;by the same way, Performed an and operation between the encryped image and the number 48(192), moved each value of the matrix 4(6) binary bits to the right, we got a matrix M3(M4).The four arrays saved all binary bits of pixel values of the encryped image.

Step 3) Connect the 4 arrays into a long array M5,the length of array M5 is 4*256*256, converted M5 into a two-dimensional matrix M6,added the values in matrix M6 and the values in the carrier image,wo can get the carrier image embedded an encrypted image.

3.1.2. Decryption Scheme

(1) Extraction of hidden information

Extraction of hidden information is the inverse process of information hiding.The extraction of hidden information is shown as follow:

Step 1) Extracted the lower 2 binary bits of each pixel value from the carrier image embedded an encrypted image, performed an and operation between each binary bit of each pixel value from the carrier image and the number 3, built 4 one-dimesional matrix k1,k2,k3,and k4, the length of each matrix is 65536. Took out the elements from first row to the 256th row of the matrix, put them into matrix K1,and the other values were put into 3 one-dimesional matrix K2,k3 and k4.

Step 2) Moved each value of matrix k2 2 binary bits to the left, moved each value of matrix k3 4 binary bits to the left, and matrix k3 for 6 binary bits, added k1,k2,k3 and k4 all together,we got a one-dimesional matrix K5.

Step 3) Converted matrix K5 to a two-dimensional matrix k6,this is the extracted hidden image.

(2)Position decryption

The decryption method is very easy, we sort the second row of ciphertext matrix P1 respectively (shown in the 3.1.1(2)), the first row of matrix P2 is the decryption.

(3)Grayscale encryption

Established a one-dimensional matrix L2 using the method described in 3.1.1(1).XORed each binary bit of the elements in one-dimensional matrix A1 and matrix L2, then we got matrix A2,and it was the grayscale decrypted ciphertext. Converted matrix A2 to a two-dimensional matrix Y, matrix Y is the last decrypted image.

3.2. *Experimental results*

Figure 4 (a) is an colour orginal image, it is a fetus,but the encryption algorithm is carried out on a gray image,so figure 4 (a) must be converted into a gray image, figure 4 (b) is the gray image converted from the colour original image. Figure 4 (c) is the image after gray value encryption,and figure 4 (d) is the image after position transformation.

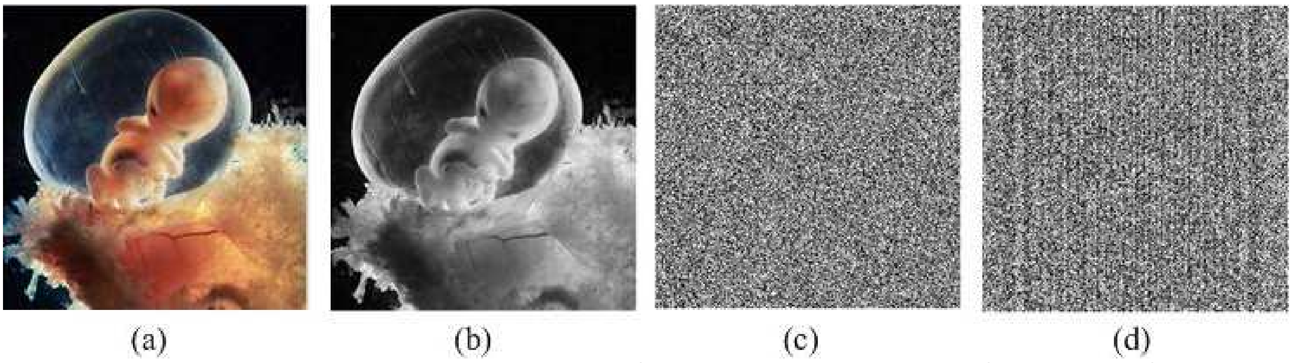


Figure 4. Original colour image (a), original gray image (b), image after gray value encryption (c), image after position transformation (d)

Figure 5(e) is a carrier image,its size is 512*512 pixels. There is any logical connection between the carrier image and the encrypted image.Figure 5(f) is the carrier image embedded an encrypted image. In fact, we can't see the difference between figure 5(e) and figure 5(f).

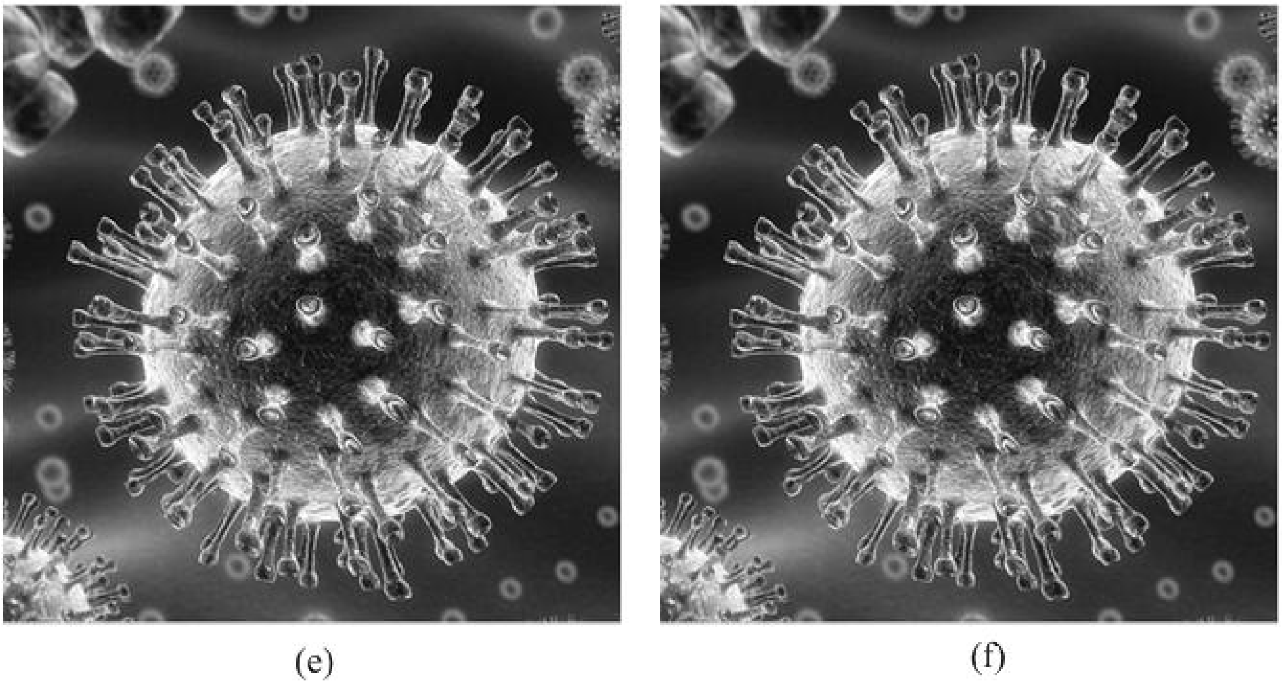


Figure 5. Carrier image(e), Carrier image embedded an encrypted image(f)

Figure 6 is the decrypted image. Figure 6(g) is the image extracted from the carrier image, figure 6(h) is the image after position transformation , figure 6(i) is the image after gray value decryption.

3.3. *Security analysis*

3.3.1. Histogram analysis:

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level[9-11]. We have calculated and analyzed the histograms of the several encrypted as well as its original colored images that have widely different content. Figure 7 (a) shows the histogram of the original gray image,and Fig.7 (b) is the histogram of the image after gray value encryption, Fig.7 (c) is the histogram of the image after position transformation.

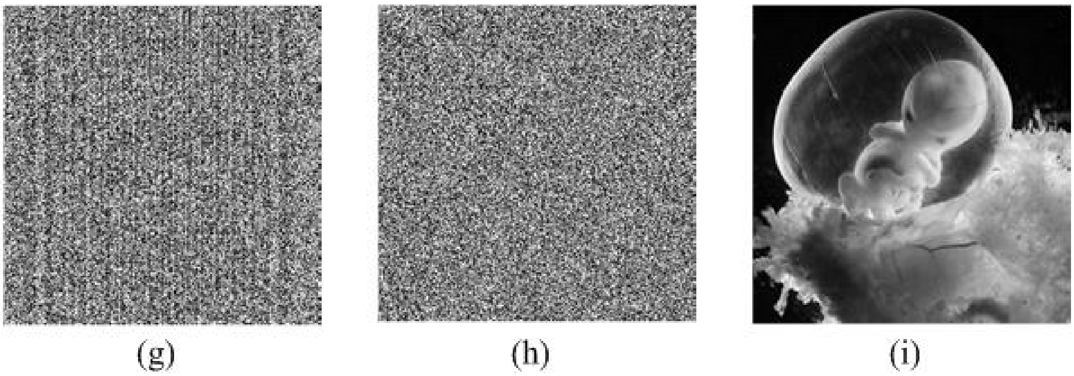
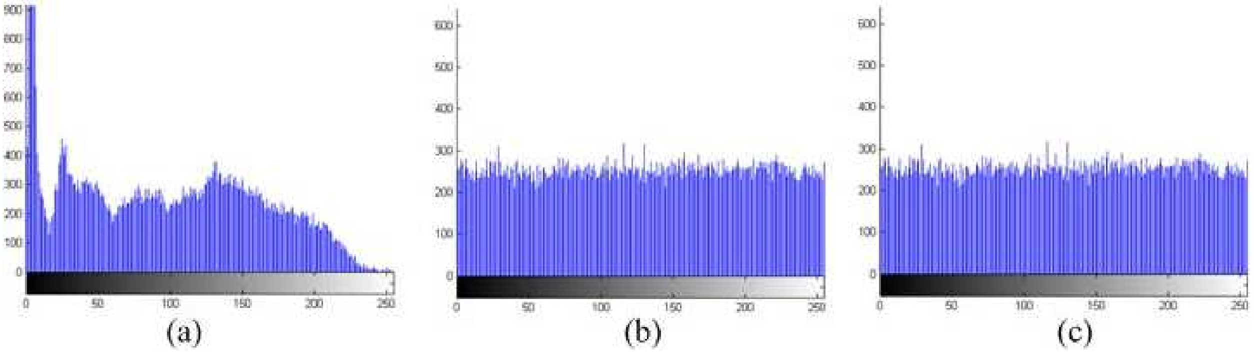

(g) (h) (i)

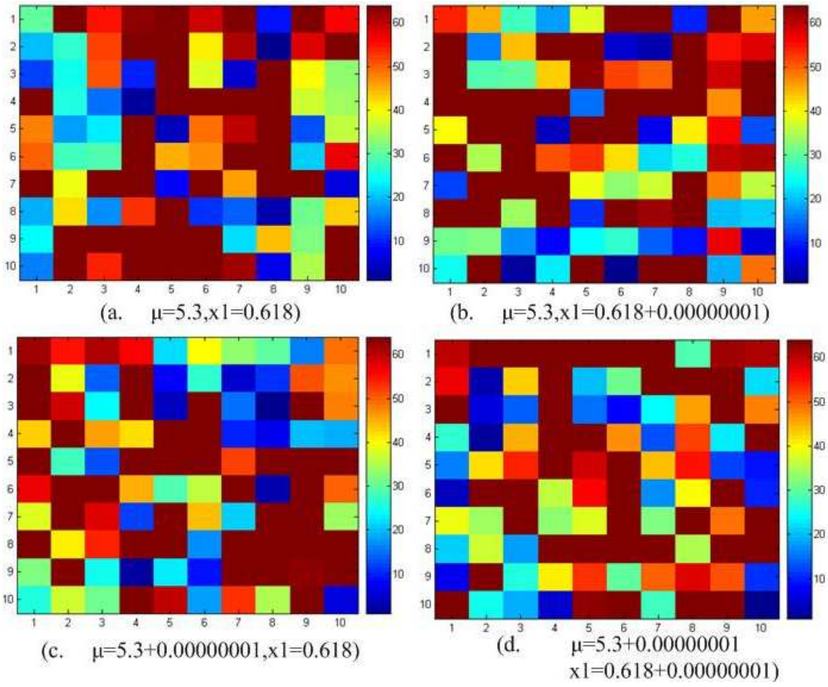
Figure 6. Image extracted from the carrier image(g), image after position transformation (h),image after gray value decryption(i)



(a) (b) (c)

Figure 7. Histogram of the original gray image(a), histogram of the image after gray value encryption (b)histogram of the image after position transformation (c)

It is clear from Fig. 7 that the histograms of the encrypted image are fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.



(a. μ=5.3,x1=0.618)

(b. μ=5.3,x1=0.618+0.00000001)

(c. μ=5.3+0.00000001,x1=0.618)

(d. μ=5.3+0.00000001
x1=0.618+0.00000001)

Figure 8. Diagrams of key sensitivity of the improved transcendental equation

3.3.2.Information entropy analysis:

3.3.4.Sensitivity analysis

The key sensitivity is the degree of changing in the ciphertext when a little changing in the initial key. An ideal image encryption procedure should be sensitive with respect to the secret key.Key sensitivity is an essential property for any good cryptosystem,which ensures the security of the cryptosystem against brute-force attacks[12].

In this paper we detected the sensitivity of the key using renderings of matrix transformations.We analyzed the sensitivity of the modified transcendental equation, it can be seen from figure 8 that, the parameter μ and the initial value of x1 have greatly impact on the encryption method,when slightly transformed values of x1 and parameter μ,we got 4 quite different encrypted images.

3.3.4.Correlation of adjacent pixels

In a natural image, the correlation among adjacent pixels is strong,this makes the content of the image to be identified easily[13].A good encryption algorithm must disrupt this correlation effectively,and make the correlation coefficient close to 0.

If p_i and c_i denote the pair of horizontally/vertically adjacent pixels in an image[14],then the correlation between them is calculated using the following formula 3:

$$c = \frac{\frac{1}{N}\sum_{i=1}^{N}(\mathrm{p_i} - \overline{\mathrm{p}})(\mathrm{c_i} - \overline{\mathrm{c}})}{\sqrt{(\frac{1}{N}\sum_{\mathrm{i=1}}^{\mathrm{N}}(\mathrm{p_i} - \overline{\mathrm{p}})^2)(\frac{1}{N}\sum_{\mathrm{i=1}}^{\mathrm{N}}(\mathrm{c_i} - \overline{\mathrm{c}})^2)}} \tag{5}$$

Here p_i and c_i are the averages of pi and ci respectively.

We selected 3000 adjacent pixels in the original image and the encrypted image,the distribution is shown in Figure 9 and figure 10.The correlation among the original image pixels shows a linear distribution,the correlation among the encrypted image pixels is a random distribution.

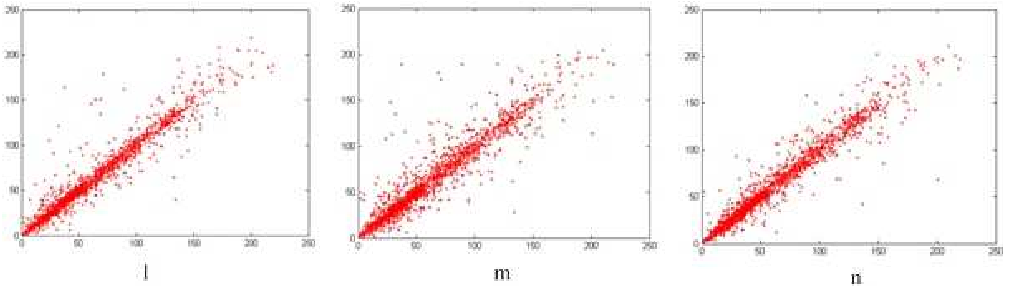


Figure 9. Correlation of level adjacent pixels (l),correlation of Horizontal adjacent pixels(m),correlation of diagonal adjacent pixels (n) for original image

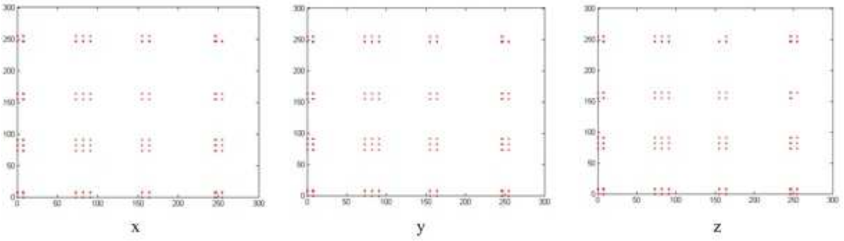


Figure 10. Correlation of level adjacent pixels(x),correlation of horizontal adjacent pixels(y), correlation of diagonal adjacent pixels(z) for encrypted image after the position transforming and the gray value changing

It can be seen from figure 9 and figure 10,the degree of image scrambling is very significant.

3.3.5. Robustness test

The robustness of the proposed method against noise and occlusion attacks are considered. MSE(Mean Square Error) is used to measure the performance of encryption[15,16]. the larger the value of mean square error is, the better the effect of encryption is.The formula of MSE is shown in formula (6):

$$MSE = \frac{\sum_{n=1}^{Framesize} (I_n - P_n)^2}{Framesize} \tag{6}$$

where parameter I_n is the gray value of the n-th pixel in the orginal image, parameter P_n is the the gray value of the n-th pixel in the encrypted image ,and parameter framesize is the number of the pixels.

Table 1. Mean square error

I_n	P_n	MSE
Orginal image	Encrypted image	12113.53
Orginal image	Decrypted image using the right key	0
Orginal image	Decrypted image using the key of μ=5.3+0.000001,x1=0.618,λ=3.8	14423.42
Orginal image	Decrypted image using the key of μ=5.3,x1=0.618+0.000001,λ=3.8	12167.63
Orginal image	Decrypted image using the key of μ=5.3,x1=0.618,λ=3.8+0.000001	17068.53
Orginal image	Decrypted image using the key of μ=5.3+0.000001,x1=0.618+0.000001,λ=3.8	16536.87
Orginal image	Decrypted image using the key of μ=5.3,x1=0.618+0.000001,λ=3.8+0.000001	15231.93

PSNR (Peak Signal to Noise Ratio) is a kind of objective standard of image, in order to measure an encryped image, PSNR is used to identify the satisfaction of a program. It is shown in formula (7):

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) \tag{7}$$

Where MSE is the Mean Square Error, PSNR is measured in dB, the larger the the value of PSNR is, the less the image distortion is.

In this paper, we compared the original image Fig.4(b) and the encrypted image Fig. 4(d),and we can get $MSE = 12113.53$, $PSNR = 16.805$ using formula (6) and formula (7).So the encryption effect is very good.

3.3.6. Key Space Analysis

For a secure image encryption scheme, the key space should be large enough to make the brute-force attack infeasible. Key space is the total number of different keys that can be used in the encryption[13].In this study the key of the improved transcendental equation is $K = (\lambda, x_1, \mu\ )$, parameter x_1 can be taken any value in the range of (0,1), parameter μ can be taken any value in the range of (3.569945672, ∞),and the value scope of the parameter λ can reach the range of (3,∞), so the key space of the improved transcendental equation is infinite, the uncertainty of parameter λ, x_0, μ increases the key space greatly.So exhaustive attacking on key K is not feasible.

In this encryption algorithm the size of the image is m×n. The main operations of this encryption algorithm is to sort the sequence and to replace the pixel position and the pixel value.The time complexity of sequence sorting algorithm is $O(n^2)$,these operation of replacement is to take the digital image array according to the corresponding relations of a sorted sequence, so its time complexity of sequence sorting algorithm is $O(n^2)$ too,and the total time complexity of the encryption algorithm is $O(n^2)$.

CONCLUSION

(1) In this work a kind of modified transcendental equation is proposed, the control parameters increase from 1 to 3,so the key space increases 3 times, the bifurcation and the chaotic interval of the modified transcendental equation are controlled by the control parameters,the key space is large enough,it can resist differential attack, and it is enough to prevent all kinds of exhaustive analysis, 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.

(2) 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.

(3) The encryption algorithm proposed in this paper introduced the information hiding mechanism, its features are as follow:the correlation of adjacent pixels of encrypted images is close to 0, the encrypted image produced by the cryptosystem is sensitive to the initial values of parameter x1, parameter λ and parameter μ.

(4) This encryption algorithm can be extended, and it can be used to encrypt color images (RGB format).In this study,two lowest binary bits of an encryped image can be given up,this reduces the accuracy of an encrypted image,but it improves the encryption efficiency, and reduces the complexity of the algorithm.

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

REFERENCES

[1] Wu, Yue, Gelan Yang, Huixia Jin, and Joseph P. Noonan. *Journal of Electronic Imaging*. ,**2012,**21(1): 013014-1.
[2] Wang Yong,Li Changbing,He Bo.Chaotic encryption algorithm and Hash function construction research. Publishing House of Electronic Industry, Beijing China,**2011**; 94-120.
[3] Hu Da-hui, Du Zhi-guo. *International Journal of Digital Content Technology and its Applications.* **2012**, 6(8): 169-176.
[4] Dongming Chen, Yongming Liu, Xiaodong Chen, Yunpeng Chang, Jing Wang. *International Journal of Advancements in Computing Technology*. **2011**, 3(7):198-205.
[5] Guangrong Chen, Yaobin Mao, Charles K Chui. *Chaos, Solitons Fractals*. **2004**,21(3):749-761.
[6] Hun-Chen Chen, Jui-Cheng Yen. *J Syst Archit*, **2003**,49(7-9): 355-67.
[7] Dongming Chen, Yunpeng Chang. *Advances in Information Sciences and Service Sciences*. **2011**,3(7): 364-372.
[8] Zhenjun Tang ,Xianquan Zhang. *Journal of Multimedia*.**2011**,6(2):202-206.
[9] Qing Guo, Zhengjun Liu, Shutian Liu. *Optics and Lasers in Engineering* .**2010**, 48:1174–1181.
[10] Zhengjun Liu, Lie Xu, Ting Liu , Hang Chen , Pengfei Li , Chuang Lin , Shutian Liu. *Optics Communications.* **2011**, (284):123−128.
[11] W. Chen, C. Quan, C.J. Tay. *Optics Communications*. **2009** ,(282): 3680−3685.
[12] Kwok-Wo Wong,Ching-Hung Yuen. *IEEE Trans Circuits Syst Express Brief*. **2008**,55(11):1193-1197.
[13] Pareek N, Patidar V,Sud K. *Phys Lett* A. **2003**, 309(1-2): 75-82.
[14] Pareek N,Patidar V, Sud K. *Image Vision Comput*. **2006,**24 (9): 926-934,.
[15] Wu Yue, Gelan Yang, Huixia Jin, and Joseph P. Noonan. *Journal of Electronic Imaging*. ,**2012,**21(1): 013014-1.
[16] álvarez G, Montoya F, Romera M, Pastor G. *Phys Lett* A. **2003**,319(3-4):334-339.