Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):2073-2082

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

A novel biological image encryption algorithm based on two-dimensional Feigenbaum chaotic map

Li Tu[1], Yingzheng Zhang[2], Xuehua Huang and Liyuan Jia[1]

[1]*School of Information Science and Engineering, Hunan City University, Yiyang, Hunan, China*
[2]*Department of Information and Engineering, Hunan Engineering Polytechnic, Changsha, Hunan, China*

ABSTRACT

This paper proposes a nonlinear coupled two-dimensional generalized Feigenbaum chaotic mapping, by using bifurcation graphics, we studied the complex nonlinear dynamic activities of two-dimensional formula. By using the coupled two-dimensional generalized Feigenbaum chaotic mapping a chaotic sequence is generated, then the chaotic sequence is optimized into secret key stream, and scrambling method is introduced in this encryption algorithm, this changes values of pixels. The results of experiment simulation show that the extremely sensitive to the key , the choice of chaotic sequence depends on the plaintext sensitively that enhances the ability of resisting the chosen plaintext attack, the information entropy of the cipher image is 7.99694974187328, it is very close to the ideal value 8,the encrypted image has random-like distribution behavior of grey values, the correlation between the encrypted image and the plain image is very small, the adjacent pixels have zero co-correlat ion properties, the algorithm has the advantages of large key space and high speed of encryption.

Keywords: Transcendental equation; Chaotic sequence; Image encryption; Bifurcation

---

INTRODUCTION

With the rapid development of modern communication technology and the wide application of computer internet technology, information sharing and transmission becomes more and more important[1-3]. It has brought us great convenience and a great number of information security problems as well. Such as information theft, copyright protection of multimedia data and image authentication.

The major goal of image information encryption is to enhance communication security by inserting secret message into the digital image[4-6]. The image after the embedding of the secret message is then sent to the receiver through a public channel. In the transmission process, the public channel may be intentionally monitored by some opponent who tries to prevent the message from being successfully sent and received. The opponent may randomly attack the stegoimage if he/she doubts the stego-image carries any secret message.

Image processing of biological information is a branch of the bio-engineering disciplines[8], including biological information processing technology, biotechnology， image processing and analysis, Biological image processing and analysis, which is one of the fastest growing disciplines in the field of bio-engineering direction. Image analysis of biological information is committed to the digital information extracted from biological images or biological image sequences, there is a wide range of applications in the field of life sciences.

Because the biological characteristic is unique and steady during a period, and it is not easy to be faked and forged, the biology image encryption technology is used to recognize identity, and it is safe, reliable, and accurate.Moreover, the biological image encryption product aided by the computer technology is easy to implement the functions including safety certification, monitoring and management. The breakthrough of biological image encryption

technology will not only bring the great development of the theory of safety certification, monitoring, management and pattern recognition, but also bring great social and economy effect.

Chaos is characterized by ergodicity, sensitive dependence on initial conditions and random-like behaviors, which is an aperiodic dynamics process, seeming disorderly and unsystematic; actually it contains order[15]. Introducing chaos theory into the field of image encryption and information security is an important frontier subject of e nonlinear science and information science.The chaos theory was used in applications to cryptology from the 1980s.And a number of chaos based image encryption scheme have been developed in recent years which we discuss in brief in this paragraph.In 1992,Bourbakis and Alexopoulos [9] have proposed an image encryption scheme which utilizes the SCAN language to encrypt and compress an image simultaneously. Wu Yue [10] demonstrated the construction of a symmetric block encryption technique based on two-dimensional standard baker map.Since 2010, Liu Huibin et al. have proposed a number of different encryption schemes based on one or more chaotic maps[9-13].Recent cryptanalytic results[14-16] have shown that these schemes proposed in contain security defects.

EXPERIMENTAL SECTION

2.1. Feigenbaum chaotic mapping

Formula 1 is a transcendental equation, Feigenbaum has studied its bifurcation and chaotic characteristics, and made its corresponding figure.

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

Here parameter a is a non-negative real number,from any initial value, $x_k \in [0,1]$,selected the initial values of x1=0.1234 and a=3, Figure1 is the scatter plot of a transcendental equation. Figure 1 shows that:

(1) When parameter a∈(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∈(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∈(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.

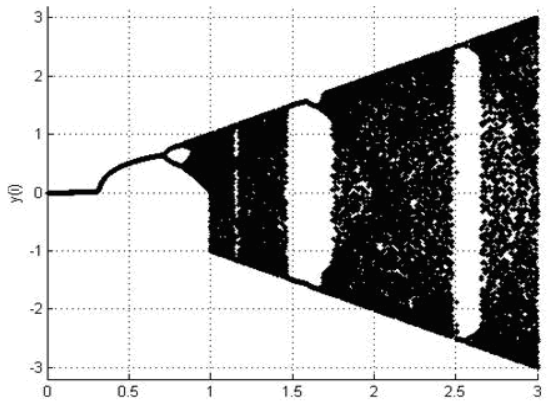


Figure 1. Bifurcation and Blank window for Feigenbaum chaotic mapping

2.2.Two-dimensional Feigenbaum chaotic mapping

We built a two-dimensional Feigenbaum chaotic mapping,and the mapping has a coupling term,it is shown in formula (2):

$$\begin{cases} x_{n+1} = 3\lambda_1 \sin(\pi x_n) + \gamma_1 y_n \\ y_{n+1} = 3\lambda_2 \sin(\pi y_n) + \gamma_2 x_n \end{cases} \quad (2)$$

Where $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ are control parameters,and experimental results show that,when the control parametersare in the range of (0，1)，the system will appear Bifurcation and Chaotic characteristics.

Select the parameters λ_1, λ_2 as fixed values,and the parameters γ_1, γ_2 are in the range of(0,1), select two groups of data to have experiments:

(1) The first group of data: $\lambda_1 = \lambda_2$

① $\lambda_1 = \lambda_2 = 0.1, \gamma_1 = \gamma_2 \in [0,1]$,x1=0.22，y1=0.43,the bifurcation diagram is shown in Figure 2(a1),when the parameters γ_1, γ_2 are in the range of(0.7,0.9),the system is in chaos;

② $\lambda_1 = \lambda_2 = 0.2, \gamma_1 = \gamma_2 \in [0,1]$,x1=0.22，y1=0.43, the bifurcation diagram is shown in Figure 2(b1),when the parameters γ_1, γ_2 are in the range of(0.36,1),the system is in chaos;

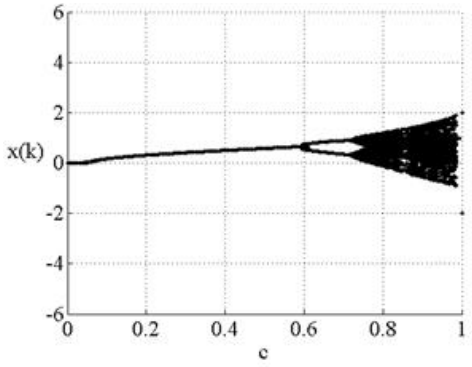
③ $\lambda_1 = \lambda_2 = 0.3, \gamma_1 = \gamma_2 \in [0,1]$,x1=0.22，y1=0.43, the bifurcation is shown in Figure 2(c1), the bifurcation diagram of the system is very irregular.

(2) The first group of data: $\lambda_1 \neq \lambda_2$

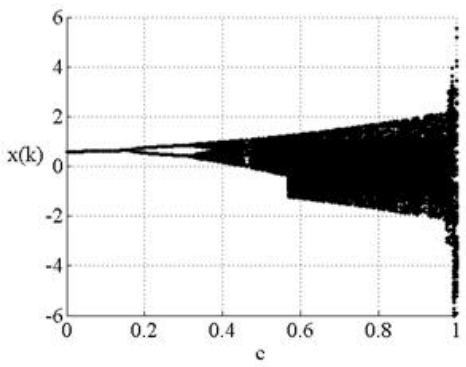
① $\lambda_1 = 0.1, \lambda_2 = 0.2, \gamma_1 = \gamma_2 \in [0,1]$,x1=0.22，y1=0.43, the bifurcation diagram is shown in Figure 2(a2)；

② $\lambda_1 = 0.2, \lambda_2 = 0.3, \gamma_1 = \gamma_2 \in [0,1]$,x1=0.22，y1=0.43, the bifurcation diagram is shown in Figure 2(b2)；

③ $\lambda_1 = 0.3, \lambda_2 = 0.4, \gamma_1 = \gamma_2 \in [0,1]$,x1=0.22，y1=0.43, the bifurcation diagram is shown in Figure 2(c2), when the parameters γ_1, γ_2 are in the range of (0.76,1),there are some blank window in the bifurcation diagram of the system.



(a1).a=b=0.1



(b1).a=b=0.2

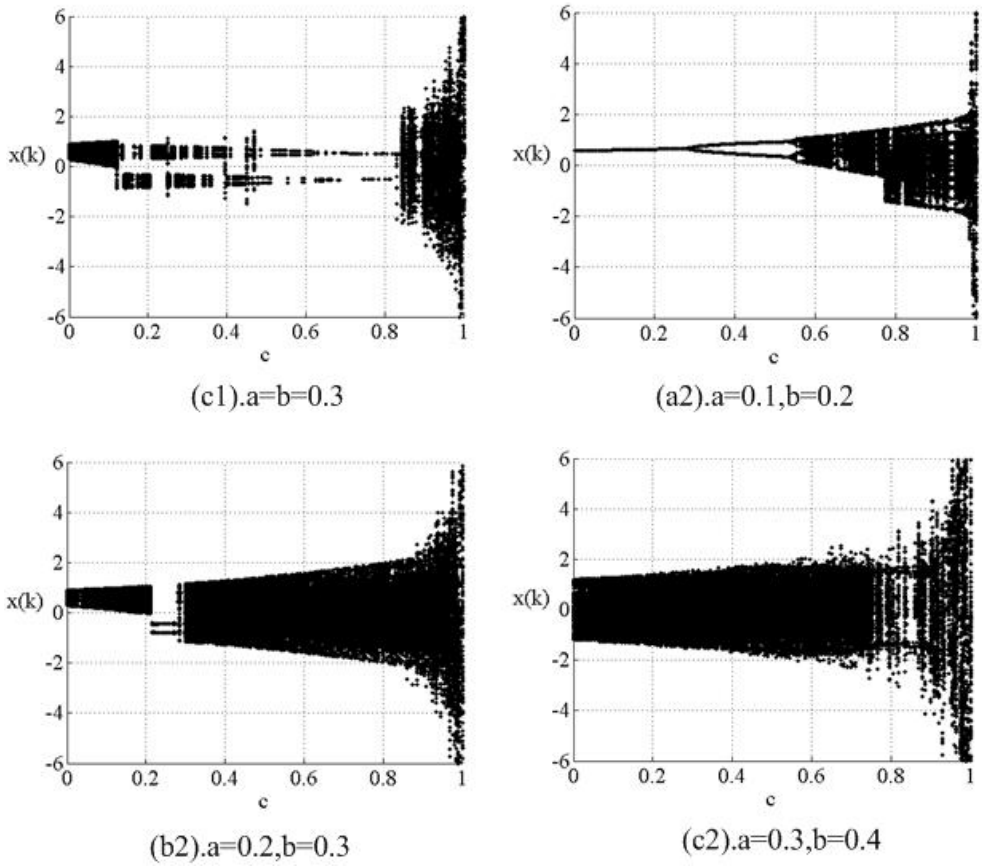


Figure 2. Bifurcation and Blank window for the 2-dimensional Feigenbaum chaotic mapping

RESULTS AND DISCUSSION

3.1 *Encryption Algorithm and Decryption Scheme*

Selected the initial value of the the parameters as: $\lambda_1 = 0.9, \lambda_2 = 1.01, \gamma_1 = 0.1, \gamma_2 = 0.2$, $x_1 = 0.22, y_1 = 0.43$,had iterative calculation using the 2-dimensional Feigenbaum chaotic mapping, generated two chaotic sequences, they were sequence X and sequence Y.

3.1.1 Encryption algorithm

The image were encrypted in three steps:

Step 1: Positional encryption

① Read a size of 256*256 pixel image, put its pixel value into a one-dimensional matrix A;

② Constructed a matrix two-dimensional M(3, 256*256),the first row of matrix M is an arithmetic progression whose initial value and tolerances are 1,the values of sequence X was put in the second row of matrix M,and the values of matrix A was put in the third row of matrix M;

③ Sorted the values of the second row of matrix M,and the other two rows changed too;

④ Removed the data of the third row in matrix M, put them in a one-dimensional matrix B,then converted matrix B into a two-dimensional matrix C(256,256), matrix C is the positional encrypted image.

Step 2: Scrambling encryption

The gray value of each pixel (decimal) can be converted into an 8-bit binary number,that is:

bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1

① Converted matrix C into a one-dimensional matrix D;

② Got the binary digital on odd bit and even bit of each pixel in matrix D;

③ Put these binary digital scrambling in the following way:

bit8	Bit6	Bit4	Bit2	Bit7	Bit5	Bit3	bit1

④ Converted these scrambling digital into decimal digital, a one-dimensional matrix E was obtained, then converted matrix E into a two-dimensional matrix F(256,256), matrix F is the scrambling encrypted image.

Step 3: Gray value encryption

① In order to increase the difficulty of the ciphertext,took the first,the fifth and the eighth digit of the elements in sequence Y after the decimal point to form a three-digit number, had it on 256 remainder operation,got sequence G;

②XORed sequence E and sequence G, got sequence H, then converted matrix H into a 2-dimensional matrix K(256,256), matrix K is the last encrypted image.

3.1.2 Decryption Scheme

Step 1: Gray value decryption

XORed sequence E and sequence G again, got sequence E1.this is the decryption process on gray value;

Step 2: Scrambling decryption

Took out each binary digital of squence E,and proceed them as follows:

8→8 7→6 6→4 5→2 4→7 3→5 2→3 1→1

(Put the eighth binary bit in the eighth bit,put the seventh binary bit in the sixth bit...),then converted it to a decimal number,and we can get matrix B, converted this sequence B to a two-dimensional matrix,we can get a secondary decryped image.

Step3: Positional decryption

① Built a two-dimensional matrix N(2, 256*256), the first row of matrix N is an arithmetic progression whose initial value and tolerances are 1,the values of sequence X was put in the second row of matrix N;

② Sorted the values of the second row of matrix N,and the first row changed too, put the values of the first row of matrix N in sequence Xn;

③ Constructed a two-dimensional matrix L(2, 256*256),put the values of sequence Xn in the first row of matrix L,and put the values of matrix B in the second row of matrix L;

④ Sorted the values of the first row of matrix L,and the second row changed too, put the values of the second row of matrix L in sequence P, converted sequence P into a two-dimensional matrix Q(256,256), matrix Q is the last decrypted image.

3.2. *Experimental results*

We had an encryped experiment using MATLAB 7.0， the key was selected as: $\lambda_1 = 0.9$, $\lambda_2 = 1.01$, $\gamma_1 = 0.1, \gamma_2 = 0.2, x_1 = 0.22$, $y_1 = 0.43$.

Figure 3 is an original image and histogram of the original image.

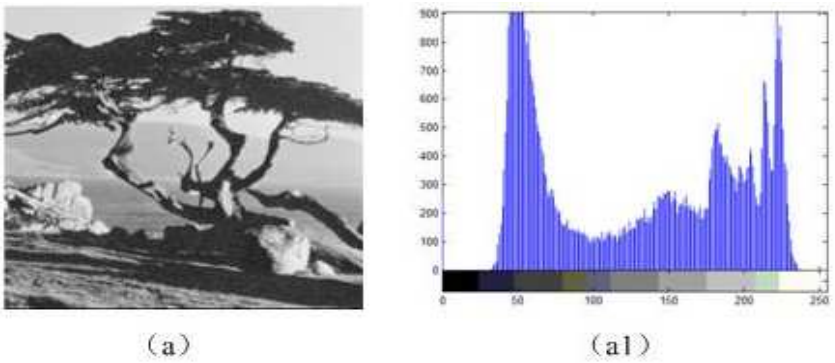


Figure 3. Original image (a) and histogram of original image (a1)

Figure 4 is the encrypted image (b) and its histogram (b1) after the first step of encryption (positional transformation).

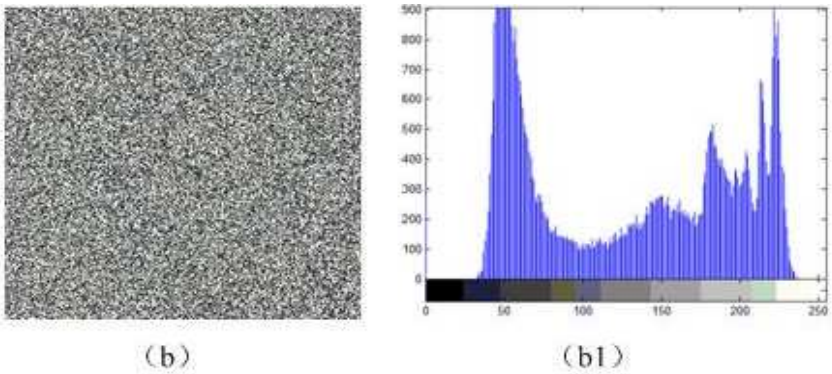


Figure 4. Encrypted image (b) and its histogram (b1) after positional transformation

Figure 5 is the encrypted image (c) and its histogram (c1) after the second step of encryption (gray value encryption).

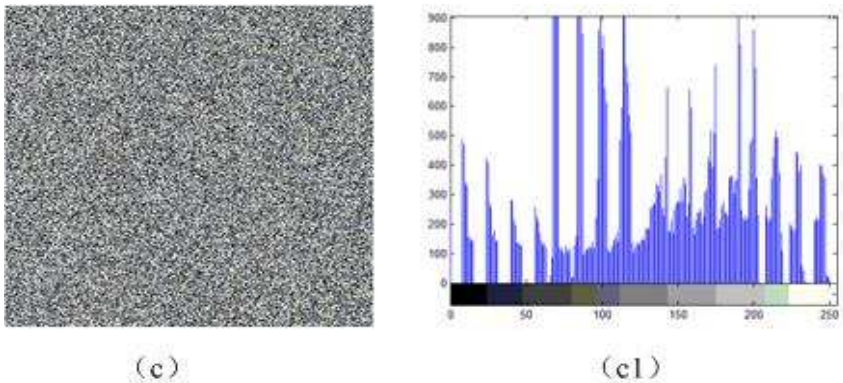


Figure 5. Encrypted image (c) and its histogram (c1) after the gray value encryption

Figure 6 is the encrypted image (d) and its histogram (d1) after the third step of encryption (XOR encryption).

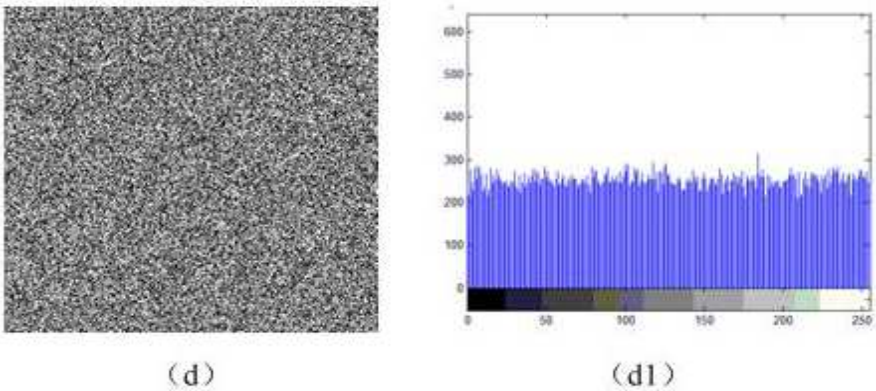


Figure 6. Encrypted image (d) and its histogram (d1)after XOR encryption

3.3. Performance and security analysis

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

3.3.1. Histogram analysis

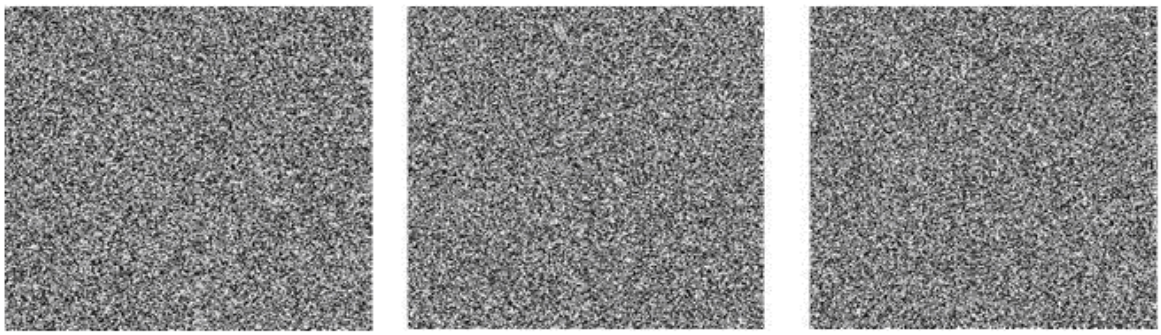
The histogram is the number of each gray level of pixels in the image, It means the frequency of each gray level .The figures show that the histogram in figure 4 (a1) is the same as that in figure 5 (b1),this is because the positional encryption only changes the position of each pixel,while the value of each pixel has NOT been changed. But in figure 6 (c1) and figure 7 (d1) the scrambling encryption(Double encryption) and the gray value encryption(Triple encryption) has changed the value of each pixel, the characteristics of the original image histogram is completely destroyed.

There are many ways to decrypt the image encryption，one is statistical analysis. The grayscale values of the encrypted image are uniformly distributed in the range of [0,255], this algorithm has a good ability to resist histogram analysising.

3.3.2. Key sensitivity analysis

(1) The key sensitivity is the degree of changing in the ciphertext when a little changing in the initial key.Key sensitivity is an essential property for any good cryptosystem, which ensures the security of the cryptosystem against brute-force attacks. The encrypted image produced by the cryptosystem should be sensitive to secret keys.

Here we made an experiment on the original image,we changed the key a little,and the encryped image is not identifiable.And we used the right key to decrypt the encryped image, we can get the right image.Figure 8 shows that, if we change the initial value of key λ_1, γ_1, x_1,we can't get the right encryped images, even if the initial value is changed only 0.00000001,we can't get any useful information from the encryped images,this means that the encryption algorithm has high sensitivity to initial value of key λ_1, γ_1, x_1.



（a）λ_1=0.9+0.00000001　　（b）γ_1=0.1+0.00000001　　（c）x_1=0.1+0.00000001

Figure 7. Decryped image(Using wrong decryption key)

Figure 7(a) is the decryped image obtained from the decryption key($\lambda_1 = 0.9 + 0.00000001$, $\gamma_1 = 0.1, x_1 = 0.22$, λ_2 =1.01, γ_2 =0.2, y_1 =0.43), Figure 8(b) is the decryped image obtained from the decryption key （λ_1 =0.9， γ_1 =0.1+0.00000001， x_1 =0.22； λ_2 =1.01， γ_2 =0.2， y_1 =0.43), Figure 8(c) is the decryped image obtained from the decryption key (λ_1 =0.9， γ_1 =0.1， x_1 =0.22+0.00000001； λ_2 =1.01, γ_2 =0.2, y_1 =0.43),and these images are beyond recognition.

(2) Mean square error (MSE)

The mean square error (MSE) is defined as formula (3):

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} [D(i, j) - P(i, j)]^2 \tag{3}$$

Where M=N=256,D is the gray value matrix of the encrypted image, P is the gray value matrix of the original image, L is a range of gray value of these images, For 8-bit gray images, L=255.Using equation (4.1) calculated the MSE of the encryption image,the decryped image and the decryped image using error key,we can get table 1.In table 1,the MSE of the right decryped image is 0,ithis means that, if the correct key is

used to decrypt the decryped image, we can get the correct image,and we can get the information of the original image; if any wrong key is used to decrypt the decryped image,the MSE of the decryped image is not equal to 0, even if the initial key and the correct key only issue a difference of 10^{-10},we can't get the correct decryped image. Compared the MSE of images processed with different initial values,we got table 1,and table 1 shows the key sensitivity of the two-dimensional Feigenbaum chaotic mapping.

Table 1. Analysis of MSE

Initial value of key	MSE
a=0.9,b=1.01,c=0.1,d=0.2, x=0.22, y=0.43 (Encryption)	20413.23
a=0.9,b=1.01,c=0.1,d=0.2, x=0.22,y=0.43 (Decryption)	0
a=0.9+10^{-10} ,b=1.01,c=0.1,d=0.2, x=0.22,y=0.43 (Decryption)	21325.73
x=0.22+10^{-10} ,b=1.01,c=0.1,d=0.2, x=0.22, y=0.43 (Decryption)	21396.39
a=0.9+10^{-10},x=0.22+10^{-10},b=1.01,c=0.1,d=0.2,x=0.22,y=0.43 Decryption)	21381.27

3.3.3. Correlation analysis of adjacent pixels

Correlation of adjacent pixels means the scrambling effect of an image[17]. Figure 8 shows that in the original image, the gray values of several adjacent pixels are very close, the correlation of level adjacent pixels , horizontal adjacent pixels and diagonal adjacent pixels of the original image distribut in a straight line of y=x,while figure 9 shows in an encryped image, each pixel neighboring points are scattered, the correlation of adjacent pixels of the encryped image are dispersed more, the scrambling degree of the encryped image is more obvious, and the encryption effect is more significant.

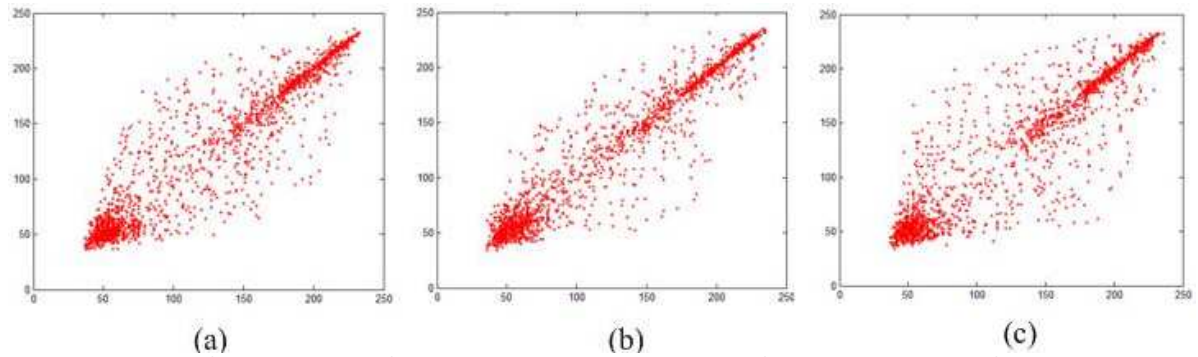


Figure 8. Correlation of adjacent pixels of the original image: (a) Correlation of level adjacent pixels of the original image, (b) Correlation of horizontal adjacent pixels of the original image, (c) Correlation of diagonal adjacent pixels of the original image

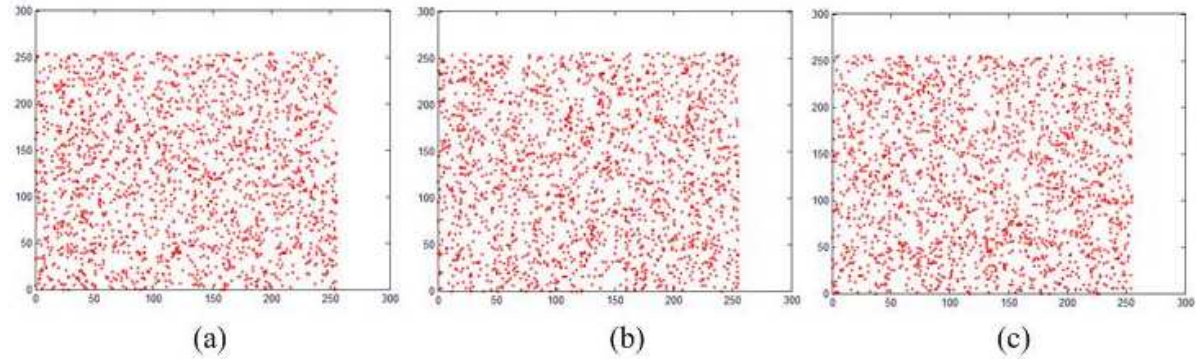


Figure 9. Correlation of adjacent pixels of the encryped image:(a) Correlation of level adjacent pixels of the encryped image , (b) Correlation of horizontal adjacent pixels of the encryped image, (c) Correlation of diagonal adjacent pixels of the encryped image

3.3.4. Information entropy analysis

Information entropy is one of the criteria to measure the strength of a cryptosystem, its formula is descripted as formula (4):

$$H(\mathrm{s}) = -\sum_{i=0}^{2^n-1} P(\mathrm{s}_i)\log_2[P(\mathrm{s}_i)] \qquad (4)$$

Where P(si) means the probability of symbol S_i, 2^n is the total state number of information source s. A random source that can send 2n symbols,its information entropy is n.For example, take a 256 gray

level image as the information source , it has 2^8 possible values,so its ideal information entropy is 8.And if the information entropy of a 256 gray level image is close to 8,it means the cipher image closes to random distribution.In a 256 gray level image, the information entropy can be descripted as formula (5):

$$H(\mathrm{s}) = -\sum_{i=0}^{i=255} P(i)\log_2 P(i) \tag{5}$$

Where P(i) means the proportion of pixels whose gray value is i.

We encrypted figure 4(a) using this algorithm,we can get table 2.Table 2 shows that the information entropy of the last edcryped image is 7.99694974187328,it is very close to the ideal value 8,this means the encryped image closes to random distribution,and the effect of our encryption algorithm is very good.

Table 2. Information entropy

Image	Original image	Encryped image
Information entropy	7.31027244830323	7.99694974187328

CONCLUSION

(1)In this paper we studied Feigenbaum mapping first,then we improved it as a two-dimensional Feigenbaum chaotic mapping,this chaotic mapping has 6 control parameters, the chaotic interval, the bifurcation and the blank window of the chaotic mapping are controled by these 6 parameters,the chaotic interval changes with any one of the 6 parameters, and then it affects the effect of the encryption.

(2) The generated chaotic sequences are optimized，and the randomness and the distribution of new chaotic sequences are better than that of ordinary Feigenbaum mapping.

(3) In this paper we put forward an image encryption algorithm based on the two-dimensional chaos mapping, the characteristics of the algorithm are:its key space is large enough to resist differential attack and exhaustive analysis, the information entropy of the encryped image is very close to the ideal value 8, the key sensitivity of the two-dimensional Feigenbaum chaotic mapping is high.

(4) This encryption algorithm can be extended to encrypt colour images(RGB format). The encryption algorithm can be further improved to a kind of diffusion encryption，and this can improve the efficiency and 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] Chengqing Li, Shunjun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez, Guangrong Chen. *Image Vision Comput.* **2009**,27(9):1371-1381
[2] álvarez G, Montoya F, Romera M, Pastor G. *Phys Lett A.* **2003**,319(3-4):334-339.
[3] N. K. Ratha, J. H. Connell, R. M. Bolle, Secure data hiding in wavelet compressed fingerprint images[C], in: International Multimedia Conference, Proceedings of the 2000ACM Workshop on Multimedia. **2000**:127-130.
[4] ZHOU Qing，HU Yue，LIAO Xiao- feng. *Computer Engineer ing and Applications*,**2007**,43(22):47-49.
[5] SUN Kehui, BAO Shanqin. *Journal of Central South University (Science and Technology*) , **2011**,42(2):404-408.
[6]DENG Shaojiang, ZHANG Daigu, PU Zhongliang. *Application Research of Computers*, **2008**,25(10): 3097-3099.
[7] YANG Gelan, Yue WU, Huixia JIN. *Journal of Computational Information Systems*, **2012**, 8(10): 4315-4322.
[8]Gelan Yang, Huixia Jin, and Na Bai. *Mathematical Problems in Engineering*, **2014**, vol. 2014, Article ID 632060, 13 pages, doi:10.1155/2014/632060.
[9]Wu Yue, Yang Gelan, Jin Huixia, Noonan Joseph P. *Journal of Electronic Imaging*, **2012**,21(1): 013014-1.
[10] LU Huibin, LIU Haiying. *Journal of Computer Applications*,**2010**,30(7):1812-1817.
[11] Zhang Huaguang, Ma Tiedong, Huang Guang-bin, Wang Cun-xu. *IEEE Trans Syst Man Cybern B Cybern*, **2010**,40(3):831-844.

[12] YANG Fan, XUE Mogen. *Journal of Heifei University of Technology*, **2009**,32(8):1128-1131.
[13] Liu Hongjun, Wang Xingyuan. *Opt Communications*, **2011**, 284 (16-17): 3895-3903.
[14]Gelan Yang, Huixia Jin, and Na Bai. *Mathematical Problems in Engineering*, **2013**, vol. 2013, Article ID 272567, doi:10.1155/2013/272567.
[15] Wang Xingyuan,Liu Lintao. *Nonlinear Dynamics*,**2013**,73(1-2):795-800
[16] XIE Jian-quan, XIE Qing, YANG Chunhua1, HUANG Dazu. *Journal of Chinese Computer Systems*, **2010**,31(6): 1073-1076.
[17] YANG Gelan, Yue WU, Huixia JIN. *Journal of Computational Information Systems*, **2012**, 8(10): 4315-4322.