*Available online www.jocpr.com*

**Journal of Chemical and Pharmaceutical Research, 2014, 6(3):1312-1319**

**Research Article**

**ISSN : 0975-7384**
**CODEN(USA) : JCPRC5**

# Medical image encryption based on multiple chaos mapping

**Li Tu[1], Chi Zhang[1*], Chuan Xie[2] and Liyuan Jia[1]**

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

---

**ABSTRACT**

*In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. In this paper, we propose a novel method to encrypt a gray image based on Arnold transform and Kent mapping. It is a digital medical image encryption algorithm, dual scrambling that based on chaos of pixel position and pixel values. The results of experimental and the statistical analysis show that the histogram of the encryped image is fairly uniform and significantly different from the histogram of the original image. The algorithm improves the traditional image encryption algorithm of image scrambling based on chaos, and it is valid and has good performance.*

**Keywords:** Chaos, Arnold mapping, Image encryption, Salt and pepper noise

---

## INTRODUCTION

With the rapid development of the networked multimedia, communication and propagation techniques, the trend of sending or receiving the digital data, especially images has greatly increased. To protect the privacy of the authorized users and to guarantee the legal data access, security is an important issue in communication and storage of images. Encryption is one way to ensure the security[1].Many applications like medical image databases, confidential video, cable TV, etc. require a reliable, fast and robust security system to store and transmit images.

There are the following characteristics in medical image encryption:

(1).The information of the image is large, so the algorithm should be as simple as possible, this can save time and ensure the practicality. In telemedicine the real-time image encryption is used, this requires encryption algorithm is simple and efficient.

(2). Medical image encryption requires high degree of secrecy, medical image comes to personal privacy, the encryption algorithm must be well conceal the image information.

(3).Medical image encryption requires for high tamper resistant ability. A tampered image with maybe result in misdiagnosis and other serious problems.

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. The image is a kind of two-dimensional information[2-5],and it is lucid and well informed, many of the traditional encryption methods cannot well cover the information of images, so chaotic system is introduced into image encryption. To meet the requirements of modern applications with high levels of security, a kind of image encrypting algorithm based on Arnold mapping and Kent mapping is proposed in this paper.

## EXPERIMENTAL SECTION

Dynamic chaos is a very interesting non-linear effect, which has been intensively studied since Lorenz found the first canonical chaotic attractor in 1963[6]. The effect is very common, it has been detected in a large number of dynamic systems of various physical natures.

### 2.1 *Arnold mapping*

Arnold mapping is proposed by Vladimir I. Arnold, a Russian mathematician, it is also called cat mapping transform[7-10].Arnold mapping is only suitable for encrypting N×N images. It is defined as function (1):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ 1) \tag{1}$$

where ($x_n$, $y_n$) and ($x_{n+1}$, $y_{n+1}$) are the pixel coordinates of the original image and the encrypted image, respectively, and A is a two-dimensional matrix, $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$,mod 1 means taking the decimal fraction part of a real number. It is $x \bmod 1 = x - \lfloor x \rfloor, \lfloor x \rfloor$ means a greatest integer that not greater than x, so the phase space of ($x_n$, $y_n$) is a reality in the unit square of $[0,1] \times [0,1]$.

In fact, we can extend the pixels of a digital image to another image. For an image, its size is N*N. Then we got formula(2):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ N) \tag{2}$$

In particular, to make sure that the map is one-to-one, the determinant of A must equal 1,it is |A|=1,so $A = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$.

The cat mapping can be described by formula(3).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ N), A = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \tag{3}$$

where $x_{n+1}, y_{n+1}, x_n, y_n \in \{0,1,2,\cdots,N-1\}$,a and b are two positive integers, the parameters a, b and the number of iterations all can be used as the secret keys. After be encrypted using cat mapping each time, the image needs to be decrypted by an inverse operation.

The digital image can be regarded as a two-dimensional matrix, each matrix element has only one row and column coordinate. Arnold mapping is actually a pixel position transformation, the transformation is a kind of one-to-one correspondence, and it can be repeated.

Arnold mapping can be seen as to rearrange the points in the matrix of pixel values, as the number of pixel values in a digital image is limited, after N times transformation the image will be restored to the original image[10]. Arnold transformation has periodicity. Dyson and Falk analyzed the periodic of discrete Arnold mapping, and they got the period of any Arnold transform, this is the best result yet. Overall, the Arnold mapping can be regarded as a kind of image scrambling transformation algorithm based on geometric operation. So this kind of encryption method is unsafe, if someone knows the encryption algorithm, starting from a random state of the cipher text space, after some rounds of iterations, an image will turn back to its original in a limited number of times, and the time is very short. Two Lyapnuov indices of cat mapping are $\lambda_1 = \ln\left(\frac{3+\sqrt{5}}{2}\right) > 0$ and $\lambda_2 = \ln\left(\frac{3-\sqrt{5}}{2}\right) < 0$, so the cat mapping is a

kind of chaos mapping.

Besides the general property of chaos system, Arnold mapping has some important characteristics:

(1). The determinant of cat map |A|=1 is an area preserving maps;

(2). The cat mapping is a one-to-one mapping, each point inside a matrix is transformed into another point within the matrix. Figure 1 is the schematic diagram of the cat mapping, The two factors have on chaotic motion can be seen from figure 1: stretching (by multiplying matrix A, x and y become large) and folding (through modular arithmetic, x and y return to the unit matrix)

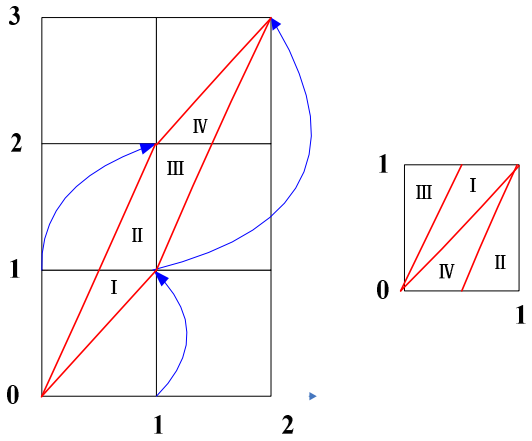


**Figure 1. Arnold mapping**

An encrypted image after cat transform needs an inverse scrambling to be decrypted. The inverse formula of Arnold mapping is described as formula(4):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A^{-1} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N} \tag{4}$$

where $A^{-1}$ is a two-dimensional matrix too ,and $A^{-1} = \begin{bmatrix} 1 & -a \\ -b & ab+1 \end{bmatrix}$ .

**2.2. *Kent mapping***

Kent mapping is a kind of piecewise function, is described as formula(5):

$$x_{n+1} = \begin{cases} \dfrac{x_n}{a} & 0 < x_n \le a \\ \dfrac{1-x_n}{1-a} & a < x_n \le 1 \end{cases} \tag{5}$$

When $a \in (0,1), x \in [0,1]$ ,the mapping is in chaos. Figure 2 is the bifurcation and blank window for the Kent mapping.

For a general chaos mapping of $x_{n+1} = f(x_n)$ , the probability density $\rho(x)$ can be obtained by Perron-Frobenious equation, it is described as formula(6):

$$\rho(x) = \sum_{x_i = f^{-1}(y)} \frac{\rho(x_i)}{f'(x_i)} \tag{6}$$

So the probability density of Kent mapping obeys the law of [0,1] distribution, that is formula(7):

$$\rho(x)=\begin{cases}1 & x\in[0,1]\\ 0 & other\end{cases} \tag{7}$$

the probability of Kent mapping is on 0.5 symmetrical distribution.

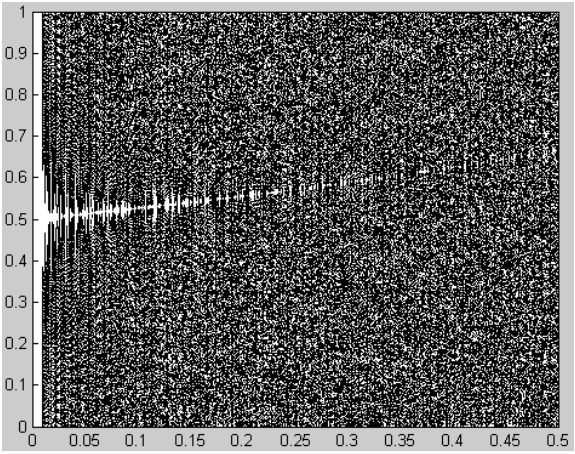


**Figure 2. Bifurcation and blank window for the Kent mapping**

## RESULTS AND DISCUSSION

The images need to be transmitted are regard as plain text, then they are safely transmitted under the control of the secret key through encryption algorithm such as DES,AES and so on[11-15].The encryption algorithm based on this kind of encryption mechanism can be disclosed, the system security depends on the key. The framework of image encryption is shown in figure 3.

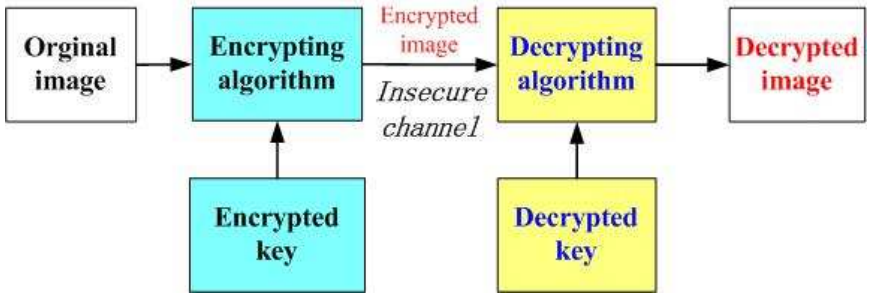


**Figure 3. The framework of image encryption**

### 3.1. *Position transformation and Kent mapping encryption*

*3.1.1 Encryption algorithm*

(1)Arnold position transform encryption:

① Read a size of 256*256 pixels image, converted it to a gray image M1, and converted M1 to a 256*256 one-dimensional matrix A;

② Found the coordinates of all the elements in matrix A, stored the horizontal coordinates and the vertical coordinates in matrix M, multiplied matrix M and matrix B, where B=[1,1;1,2]. This disrupted the order of the elements in matrix M, and we got matrix A1.

③ Had the values of matrix A1on 256 remainder operation, we got matrix A2;

④Because we will get 0 after we had remainder operation, and the coordinates of the elements of a matrix in matlab system starting with 1.So we added 1 on all elements in matrix A2,and we got matix A3. Then we assigned the elements in matrix A to matrix A3.

(2) Kent mapping grayscale encryption

①Selected the initial value $x_0$ =0.800001, a=0.4,discarded the results before 1000 times iterative operation which generated chaotic sequence L1 from Kent mapping, it is a length of 256*256 one-dimensional sequence;

②In order to increase the difficulty of the ciphertext, we took the fifth, the seventh and the third digit of the elements in sequence X after the decimal point to form a three-digit number, had it on 256 remainder operation, and we got sequence B1;

③XORed each binary bit of the elements in one-dimensional matrix A4 and matrix B1, we got sequence A7, matrix A7 was the grayscale encrypted ciphertext.

(3) Kent mapping Sequence encryption

① Selected the initial value $x_0$ =0.9800001, a=0.618,discarded the results before 1000 times iterative operation which generated chaotic sequence B2 from Kent mapping, it is a length of 256*256 one-dimensional sequence;

② Built a two-dimensional matrix S, its column length is 3, and its line length is 65536(256* 256). We put the elements of sequence B2 on the first row of the matrix S, elements of A7 on the second line, and put 1,2,…65535 on the third row of the matrix S, the two-dimensional matrix S is also the decryption matrix. Then sorted the elements in the second line, that sorted the first line of matrix S, took the second line of sorted matrix P1, we got a one-dimensional sequence A3. The position of elements in sequence A7 has changed following the elements in chaotic sequence B2, it has generated the ciphertext sequence B4;

③ Took the second line of matrix B4, and transformed it to a two-dimensional matrix A8, matrix A8 is the last encrypted ciphertext.

*3.1.2. Decryption Scheme*

Decryption is simply the reverse of encryption.

(1) Kent mapping sequence decryption

① Built a two-dimensional matrix K, its column length is 2, put the elements of the third line of matrix P1 on the first row of the matrix K ,and put the elements of the second line of matrix B4 on the second row of the matrix K;

②Sorted the elements in the first line, that sorted the second line of matrixK, took the second line of sorted matrix K, we got a one-dimensional sequence K1;

③ Transformed K1 to a two-dimensional matrix A9, matrix A9 is the Kent mapping sequence decryption ciphertext.

(2)Kent mapping grayscale decryption

Transformed A9 to a one-dimensional matrix K2, XORed each binary bit of the elements in one-dimensional matrix K2 and matrix B1,we got a one-dimensional matrix K2,and then we transformed A9 to a two-dimensional matrix K3.

(3)Arnold position transform encryption

① Because matrix $B=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$,so $B^{-1}=\begin{bmatrix}1 & -a\\ -b & ab+1\end{bmatrix}=\begin{bmatrix}1 & -1\\ -1 & 2\end{bmatrix}$, multiplied matrix $B^{-1}$ and matrix K3,we got K4;

② Had the values of matrix K4,on 256 remainder operation, we got matrix K5;

③ Then assigned the elements in matrix K3 to matrix K5, matrix K5 is the last decryped image.

**3.2.** ***Experimental results***

Figure 4(a) is the original image, figure 4(b) is the image after Arnold position transformation, figure 4(b) is the image of the gray value encryption, figure 4(b) is the image after sequence position transformation.

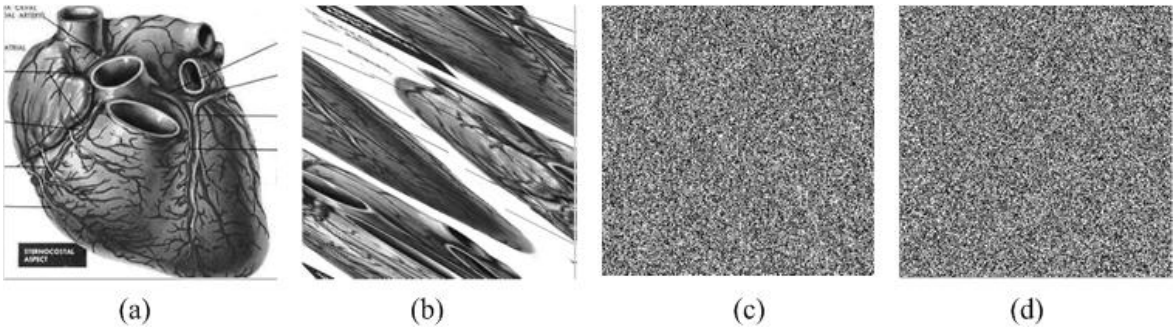


**Figure 4. Original image (a), image after Arnold position transformation(b), image of the gray value encryption(c), image after sequence transformation**

Figure 5 is the image after Kent mapping decryption and the image after decryption of Arnold mapping.

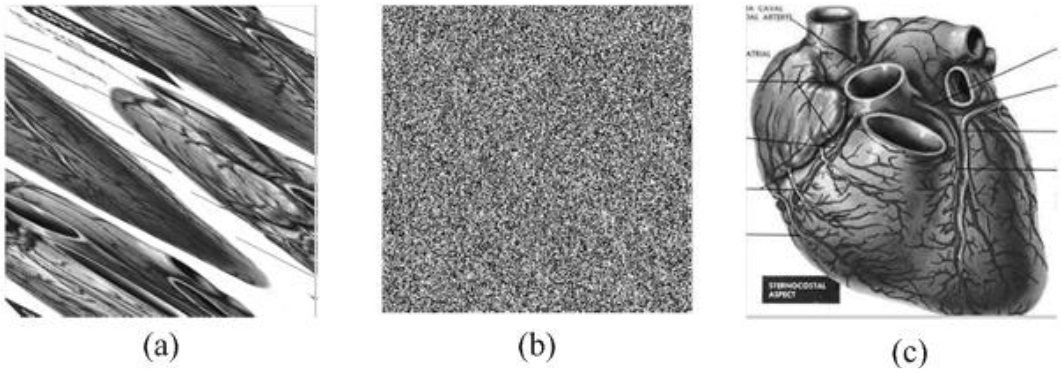


**Figure 5. Image after decryption of sequence transformation (a), image after decryption of Arnold position transformation (b), the last decrypted image(c)**

### 3.3. *Security analysis*

*3.3.1. Histogram analysis*

To analyze the image histogram is one way to attack the image encryption[16]. An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level[17]. Figure 6(a), Figure 6(b), Figure 6(c) and Figure 6(d) are the histogram of the image before and after encryption. Arnold position transformation and sequence position transformation can not change the histogram, so figure 6(a) and figure 6(b) are the same, so are figure 6(c) and figure 6(d).From figure 6,it is clear that the histogram of the cipher image (figure 6(a))is fairly uniform and significantly different from the histogram of plain image(Figure 6(c) and Figure 6(d)), and the histogram shows, before encryption the rise and fall of the histogram is very large, the distribution is not uniform, and after encryption the histogram is 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 original image.

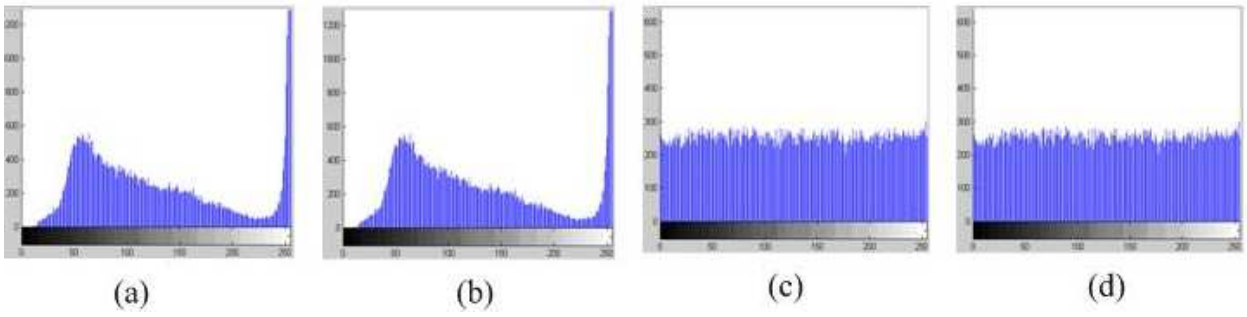


**Figure 6. Histogram of the original image (a), Histogram of the image after Arnold position transformation(b), Histogram of the image after gray value encryption(c), Histogram of the image after sequence position transformation**

It can be seen from Figure 6 that, in the image after Arnold position transformation, the position of pixels have been disrupted, but we still can see the general image, and we had gray encryption based on Arnold mapping on the position transformed image, We can not see the original image at all, it improves the performance of image

encryption greatly; the position of pixels of the image after sequence position transformation have been disrupted again, and it increased the difficulty of decryption once again

*3.3.2.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[18].Information entropy of image describes the distribution of grey value [10] ,its formula is:

$$H(X) = -\sum \frac{N(i)}{256^2} \log_2 \frac{N(i)}{256^2} \tag{7}$$

Where N(i) is the number of pixels, $\frac{N(i)}{256^2}$ is the probability gray value.

Information entropy analysis is to analyze the performance of the encryption algorithm, when the image pixels are uniform distributed,the probability of each gray value is equal nearly, the information entropy reachs the maximum. The more dispersive the gray value is, the better the encryption performance is.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 of the images is shown on table 1.

Table 1 shows that, the information entropy of the image after gray value encryption is 7.9966, is close to 8, the information entropy had changed a lot,their performance of encryption method is very good,it is hard to be decryped.

**Table 1.Information entropy**

| Information entropy of the orginal image | Information entropy of the after Arnold position transformation | Information entropy of the image after gray value encryption |
|---|---|---|
| 6.7056 | 6.7056 | 7.9966 |

*3.3.3. Anti-noise test*

If an image was attacked in the transmission process, the encryped image was harmed, the noise can't be ignored[19], medical image encryption algorithm requires to resist the attack of noise, an attacked image can be decrypted.

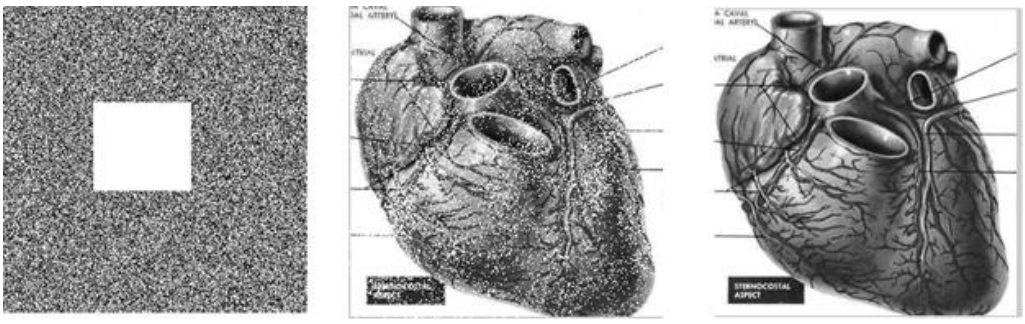


**Figure 7. Attacked image 1(a), decrypted image (b), image after noise reduction(c)**


**Figure 8. Attacked image 2(a), decrypted image 2(b), image after noise reduction 2(c)**

In this paper , we chosed two attacked images to test, the attacked images are shown in fig.7(a) and fig.8(a). The decrypted image are shown in fig.7(b) and fig.8(b), in these figures the damaged parts become dispersed noise point, they are evenly distributed in these figures, and they are similar with the salt and pepper noise. Usually we can suppress the salt and pepper noise effectively using the median filtering method. The de-noised attacked images are shown in fig.7(c) and fig.8(c). These figures show that this algorithm has good ability of anti cropping attack.

## CONCLUSION

(1)In this paper, we used an encryption algorithm based on Arnold mapping and gray value encryption based on Kent mapping, this makes up the shortcomings of the two encryption methods, it can cover all the original information, and it can protect the privacy of patients.

(2) The information entropy of the encrypted image is 7.9966,it is close to 8, the encrypted image closes to the random distribution, and it is hard to decryped.

(3)This algorithm has good ability of anti cropping attack, it ensures the security of medical images. The security characteristics are discussed in detail to demonstrate that the proposed cryptosystem is robust and secure.

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

## REFERENCES

[1] Wang Yong,Li Changbing,He Bo.Chaotic encryption algorithm and Hash function construction research. Publishing House of Electronic Industry, Beijing China,**2011**; 94-120.
[2] Hu Da-hui, Du Zhi-guo. *International Journal of Digital Content Technology and its Applications*. **2012**, 6( 8): 169-176.
[3] Dongming Chen, Yongming Liu, Xiaodong Chen, Yunpeng Chang, Jing Wang. *International Journal of Advancements in Computing Technology*. **2011**, 3(7):198-205.
[4] Guangrong Chen, Yaobin Mao, Charles K Chui. *Chaos, Solitons Fractals*. **2004**,21(3):749-761.
[5] Hun-Chen Chen, Jui-Cheng Yen. *J Syst Archit*, **2003**,49(7-9): 355-67.
[6] Dongming Chen, Yunpeng Chang. *Advances in Information Sciences and Service Sciences*. **2011**,3(7): 364-372.
[7] Zhenjun Tang ,Xianquan Zhang. *Journal of Multimedia*.**2011**,6(2):202-206.
[8] Qing Guo, Zhengjun Liu, Shutian Liu. *Optics and Lasers in Engineering* .**2010**, 48:1174–1181.
[9] Zhengjun Liu, Lie Xu, Ting Liu, Hang Chen, Pengfei Li, Chuang Lin, Shutian Liu. *Optics Communications.* **2011**, (284):123−128.
[10] W. Chen, C. Quan, C.J. Tay. *Optics Communications*. **2009** ,(282): 3680−3685.
[11] Kwok-Wo Wong,Ching-Hung Yuen. IEEE *Trans Circuits Syst Express Brief*. **2008**,55(11):1193-1197.
[12] Pareek N, Patidar V,Sud K..*Phys Lett A*. **2003**, 309(1-2): 75-82.
[13] Pareek N,Patidar V, Sud K. *Image Vision Comput*. **2006,**24 (9): 926-934,.
[14] Wu Yue, Gelan Yang, Huixia Jin, and Joseph P. Noonan. *Journal of Electronic Imaging*. ,**2012,**21(1): 013014-1.
[15] álvarez G, Montoya F, Romera M, Pastor G. *Phys Lett A*. **2003**,319(3-4):334-339.
[16] Chengqing Li, Shunjun Li, Gonzalo álvarez, Guangrong Chen, Kwok-Tung Lo. *Chaos, Solitons Fractals*. **2008**, 37(1):299-307.
[17] Chengqing Li, Shunjun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez, Guangrong Chen. *Image Vision Comput.* **2009**,27(9):1371-1381
[18] Yuling Luo, Minghui Du. *chaos Journal of Convergence Information Technology*,**2012**, 7(3):199-207.
[19] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li. *International Journal of Advancements in Computing Technology*.**2011**,3(5):223-233.