Available online at www.sciencedirect.com

SciVerse ScienceDirect

AASRI Procedia 3 (2012) 141 – 147

AASRI Procedia

www.elsevier.com/locate/procedia

2012 AASRI Conference on Modelling, Identification and Control

Study and Realization of Encrypting and Hiding Images Algorithm Based on Dual Chaos Projections

YongSong Zhu*

School of Science, Hubei University of Technology, Wuhan, Hubei,China, 430068

Abstract

The paper realizes dual encrytions of images by using Logistic and Lorenz chaotic systems to change the the locations and the sizes of Pixel values. The dual encrytions hide the encripted information in the carriers and prevent it from being noticed, improving the safety of the information transferred. The process of decryption is the reverse process of encription, which withdraws the information and undergoes anti-scrambling with secret keys to restore the images identical to original ones. The peak signaltonoise ratio between the restored pictures and the original ones is 21.78. The experiments prove that this method preserves the good ramdon of chaotic order. In addtion, it makes decipher really difficult and therefore improves the safety of the encrypted pictures.

Keywords:Chaotic system,Logistic projection,Lorenz projection,DCT transform;

1. Introduction

In the 21st century, computer caculations speed up and the technology of internet communication and multi-media develops rapidly, therefore digital images and the safety of transfering and storing information become vitally important. People have been looking for ways to encrypt pictures difficult to decipher. The

* Corresponding author. Tel.: +86-017307129143.
E-mail address: zoyoso@yahoo.com.cn.

doi:10.1016/j.aasri.2012.11.024

encryption of pictures differs from encryptions of words mainly because of the large number of data, high redundance and Pixel values relations. Chaos is a movement controlled by nonlinear dynamic system. Its regularity, ergodicity and intrinsic stochastic properties of chaotic motion and unpredictablity makes its popular in encrypting pictures. Encryption transfers and hides the information before transferring in order to improve safety during the process. The receivers can use encryption key to restore encrypted information. Information hiding technology uses the insensitivity of human beings and redundancy in multi-media digital signals to hide secret information so that it can be safely transferred.

2. DualChaotic systems

2.1 Logistic Chaotic system

Logistic projection is a very simple yet widely researched chaotic model with the definition as follows

$$x_{k+1} = \mu x_k (1 - x_k) \tag{1}$$

Among which $0 < \mu < 4$ is the branch parameter, $x_0 \in (0,1)$, when $3.5699456... < \mu < 4$, under the influence of Logistic projection with initial condition x_0 ,the chaotic sequence it produces is non-periodic, non-constringency and sensitivity to the initial value of the model of Logistic.

Among chaotic systems, Logistic projection chaotic system is widely noticed because of its ergodicity and sensitivity to initial values. In formula (1), μ is the coefficient, n is the number of iteration. When μ probability function distribution is $\rho(x)$,

$$\rho(x) = 1/\pi\sqrt{x(1-x)}(0 < x < 1) \tag{2}$$

which proves the ergodicity of formula (1) and the probability density function has nothing to do with the initial values. Thus it provides theory for projection function to scramble pictures.

2.2 Lorenz system

Lorenz system is a classic three-dimentional chaotic system. Its dynamic formular is :

$$\begin{cases} dx/dt = a(y - x) \\ dy/dt = bx - zx - y \\ dz/dt = xy - cz \end{cases} \tag{3}$$

In which a,b,c are system parameters,the typical value are a=10,b=28,c=8/3,while a,c remain unchanged,when b>24.74 ,Lorenz system enters chaotic state. Numerical Integration can be used to solve the differential equations. The four-step Runge-Kutta is used to get the solution and the step size is 0.01. As a result, a numerical sequence is achieved at good ramdon. Lorenz system is a three-dimentional chaotic system, so the numerical sequence achieved is a three-dimentional real value array. The different ways of three chaotic encryption process undergoing single variable and multivariable make the designs of encryption sequences multiple.

3. Dual Encryption of pictures based on Logistic projection and Lorenz system

While encrypting pictures twice with Logistic projection and Lorenz system, we assume that the length and width of the encrypted picture A is M and N respectively.

The process of encrytion is as follows:

1) To ensure the safety, set the two initial values as X_0, Y_0 (X_0, Y_0 are the keys for decrypting Keyl，Key2)，use the formula(1)to generate chaotic sequences $L_1 = \{X_1, X_2, X_3, ..., X_{M\times N}\}$ and $L_2 = \{Y_1, Y_2, Y_3, ..., Y_{M\times N}\}$.

2) Take the odd numbers from chaotic sequence L_1 and the even numbers from chaotic sequence L_2 and combine them into a new chaotic sequence $L_1 = \{X_1, X_3, X_5, ..., Y_2, Y_4, Y_6, ...\}$， its length being M×N.

3）Put line i of A after i-1 (i=2，3，4，… M) and form sequence C with the length of M ×N and generate a arithmetic progression S with the length of M ×N.

4)Put the values of M ×N in chaotic L in size order and form ordered sequence; locate all the elements from L in ordered sequence L'and form the replaced location set $T\{t_1, t_2, t_3, ..., t_{M\times N}\}$.

5)Find out the numbers which do not appear in arithmetic progression S from replaced sequence T and put them in set ret. Then find out the numbers that appears reaptedly in replaced sequence and their locations. Locate the pixel values of the numbers in sequence ret in the places where the repeated numbers appear. Place other pixel values to the locations accordingly in the replaced sequence and get relaced sequecne C'.

6)Set the initial values as x_1, y_1, z_1， a=10，b=28，c=8 / 3，and generate three Lorenz chaotic sequeces R_1, R_2, R_3 with the length of M ×N according to formula (3). First delete integer in the chaotic sequeces and take their absolute values, and then binaryzate them with threshold value 0.2 and get sequences R_1', R_2', R_3'.

(7) Exclusive or R_1', R_2', R_3' and get a sequence R.

(8) Exclusive or the Pixel values of R and C'and the encryptions of pictures are realized.

Apply the above mentioned arithmetic to encrypt the original picture(Fig. 1) and get the encrypted picture(Fig. 2).

Fig. 1 original picture

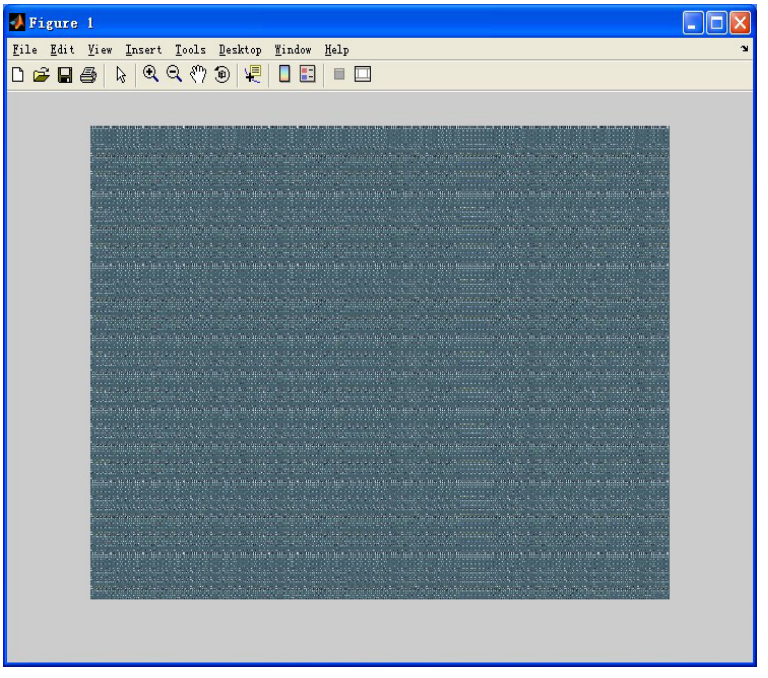

Fig. 2 encripted picture

4. Encription picture hidden arithmetic based on DCT

DCT is a picture orthogonal transformation in real number field. DCT can move the information in image to frequency domain, which takes advantage of the characteristics of human visual system and compacts the image while maitaining its quality. The DCT formula is as follows:

$$F(p,q) = a(p)a(q) \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)\cos\left[\frac{(2m+1)p\pi}{2M}\right]\cos\left[\frac{(2q+1)q\pi}{2N}\right] \quad (4)$$

$p = 0,1,\cdots,M-1; q = 0,1,\cdots,N-1$, the reverse change DCT formula is as follows

$$f(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} a(p)a(q)F(p,q)\cos\left[\frac{(2m+1)p\pi}{2M}\right]\cos\left[\frac{(2n+1)q\pi}{2N}\right] \quad (5)$$

$m = 0,1,\cdots,M-1; n = 0,1,\cdots,N-1$, in those two formulae, $a(p), a(q)$ is defined by

$$a(p) = \begin{cases} \sqrt{1/M}, & p = 0 \\ \sqrt{2/M}, & p = 1,2,\cdots,M-1. \end{cases} \quad a(q) = \begin{cases} \sqrt{1/N}, & q = 0 \\ \sqrt{2/N}, & q = 1,2,\cdots,N-1. \end{cases} \quad (6)$$

First, divide the carrier picture into several segments with different pixels. Then transform each segment via DCT. Take frequence coefficient matrix sized 8*8 for example. The value of the matirx reaches the maximum with coordinate (0,0).

Which is called DC. The other 63 frequency coefficients mostly approaches the positive or negative floating-point numbers，which are called AC. DC represents the brightness of the segment. The larger the data are, the brighter the picture will be. The high frequency parts of AC shows the complex degree of the picture texture. The small high frequency value reflects the smooth zone in the picture while the big value shows the complex texture picture. In other words, most of the picture's energy is focused on DC and some high frequencyAC while other absolute values of AC are relatively small，the absolute values of most low and middle frequency coefficients approches 0[4,5]. So DC and some high frequency AC can be characteristic data of the segment. Divide the encripiton picture into pixel segment of the same size, 4*4 for example. Replace the 16 smallest coefficient in AC of in the carrier picture segments with the information in encription picture. Then use DCT to get the reverse change and get the new picture embedded with encripted information. Fig. 3 give the carrier pictures before and after embedding the information.

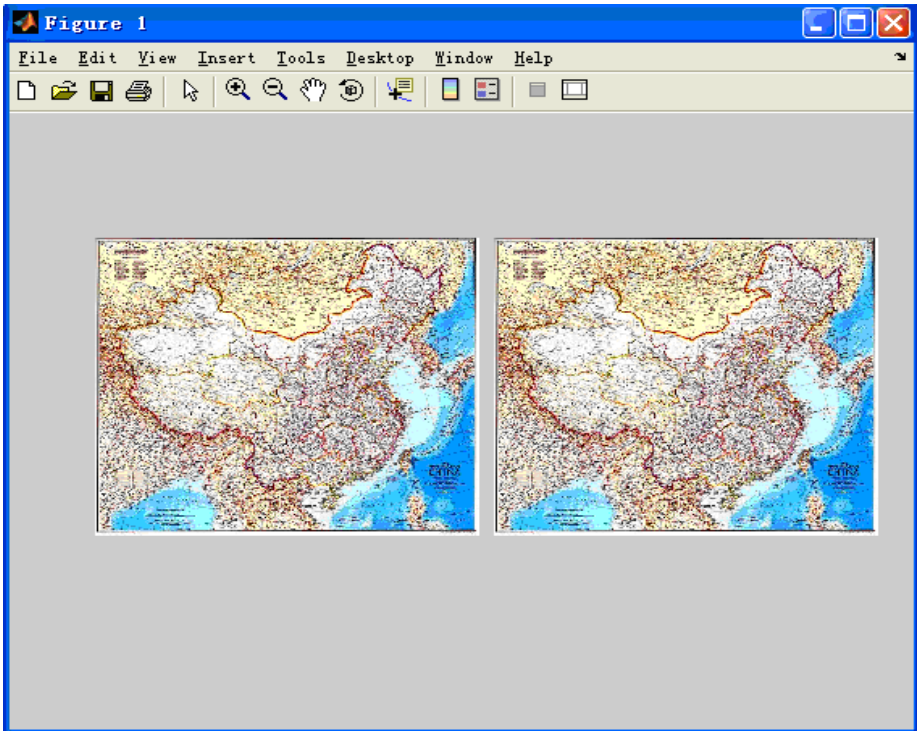

Fig. 3 carrier picture before/after information hidden

Fig. 4 carrier picture after segmented information hidden

The greater the differences between the size of the encripted picture segments and the carrier picture segmens are, the less information is changed and the embedded effect is better.But the method usually enlarges the picture, causes mosaic effects to some degree and wastes much room to embed information. To solve the problems, another way of embedding information is offered. First, change the size of the carrier picture and make it the same size as the encripted picture. Second, segment boththe carrierpicture and the encription picture by 8*8 at the same time. Third, tranform each segment of the carrier picture via DCT and keep only two decimal fractions of the coefficient. Then ensure that each part is a realdecimal no bigger than 0.01, add it to the related part in DCT coefficient matrix and finish the embedment of the data in encription picture. Last, transform the embedded data via DCT and get the carrier picture with encripted information. Fig. 4 gives the carrier picture with embedded information.

Though there are slight differences in color, no mosaic effects appear and the visual effect is much better. Because the size of the segments are the same in encription picture and carrier picture, the arithmetic is much simplier than the privious one in the realization process. In addition, the time is shorter in the simulation process with the former arithmetic 15.307s and the latter only 4.1099 s.

5.The extract and decoding of the hidden information in encription picture

The process of extacting hidden information in encription picture is the reverse operation of encripting information.Through the encription key, conversion code encripting data can be easily gotten and encription picture can be restored through anti-scrambling data. Fig. 5 shows the restored picture.

Fig. 5 picture restored

6. Arithmetic effect measurement based on pixel

Arithmetic effect measurement based on pixel is a quantitativen measurement which allows fair comparism among different arithmetics. Many distortion measures or quality measures dealing with visual information belong to difference distortion measures. Now the measure index in picture visual coding compression are Signal to Noise Ratio (SNR) or Peak Signal to Noise Ratio (PSNR) with dB as their unit. The SNR of the picture reflects the changes before and after the picture data are processed. It shows the statistical average of the change of the picture data. The higher the SNR is , the better the effect will be.The definition of PSNR is as follows

$$PSNR = -10 \times \log_{10}(PMSE) \tag{7}$$

PMSE means the variance

$$PMSE = \frac{\frac{1}{MN}\sum_{K=1}^{3}\sum_{n=1}^{N}\sum_{m=1}^{M}[f_k(m,n)-g_k(m,n)]^2}{3\times A^2} \quad (8)$$

In the formula, $f_k(m,n)$ means the k color byte in pixel elements order in the original picture, $g_k(m,n)$ means the k color byte in pixel elements order in the restored picture and A is the biggest value of $g_k(m,n)$ ($k=1,2,3$， $m=1,\cdots,M$， $n=1,\cdots,N$).

For the carrier picture, the SNR is 56.36 before and after hidding the picture information and the effect is good. The SNR of the original and the restored picture is 21.78 and the differeces mainly appear in the places where there are obvious color changes and thick complex textures.

References

[1] HUANG Wu-hui,LIU Hai-ying,QI Ying-hong.A DCT-based Watermarking Algorithm and Its Realization[J]: Computer Knowledge and Technology.2009-10
[2] WANG Linjuan.Multiple image encryption technology based on Logistic Mapping [J]: Science and Technology.2011(8)
[3] DUAN Wen-wen, LI Bi.New digital image scrambling algorithm based on chaos and its parameters optimization[J]: Application Research of Computers.2011-01
[4] Song Xiaotao, Li Jun. A Blind Spread Spectrum Watermarking Algorithm Based on the DCT Transform [J]: Computer & Digital Engineering. 2009-07-043
[5] YU Li,CHEN Ying-qi. Noise estimation based on DCT transform [J]:Information Technology. 2010-07-009
[6] ZOU Zhang-hua,TAN Shi-heng,LIN Tu-sheng.Digital Watermarking Algorithm in DCT Based on Chaotic Scrambling and Chaotic Encryption[J]: Microelectronics & Computer. 2011-05
[7] TIAN Xiao-ping,WU Cheng-mao. Evaluation of image scrambling quality based on DCT transform [J]: Computer Engineering and Applications. 2008-35-054
[8] BI Weiguang,WU Aiguo.A Chaos Generating Circuit for Chaotic Information Security[J]:China Information Security.2007-05
[9] MA Xiao-lei,LI Hong-chang. Multiple image watermarking based on Logistic chaotic sequence and Turbo code [J]: Computer Engineering and Applications.2009-31-052
[10] Liu Chong-Xin.Analysis of Chua's dual chaotic circuit[J]:Acta Physica Sinica.2002-06
[11] WANG Guang-yi1, QIU Shui-sheng2, CHEN Hui1, CUI Jia-dong1.A new chaotic system and its circuitry design and implementation[J]: Journal of Circuits and Systems.2008-05
[12] YUAN Di. Analysis of Chaotic Dynamics of a Lorenz-like System[J]: Journal of Anyang Normal University.2009-02
[13] LIU Xing-sha,LI Min,FEI Yao-ping.A Digital Image Encryption Algorithm of High Security[J]: Microelectronics & Computer.2007-02
[14] YUAN Di.Chaos and Its Forming Mechanism of a New Lorenz-Like System[J]: Journal of Anyang Normal University.2008-05
[15] FENG Zhan-shen,HE Qin,ZANG Zhen-rong. A DCT Digital Watermarking Algorithm and Its Matlab Reality based on Pretreatment of Image[J]: Journal of Xuchang University, 2009-02
[16] TAN Li ,LONG Min. Real-Time Video Stream Encryption Algorithm Based on Complicated Chaotic Sequence[J]: Computer Engineering and Applications.2011-3