Available online at www.elixirpublishers.com (Elixir International Journal)

Advanced Engineering Informatics

Elixir Adv. Engg. Info. 38 (2011) 4398-4400

ISSN: 2229-712X

An image encryption algorithm using chaos

R.Raja Kumar[1], A.Sampath[1] and P.Indumathi[2]

[1]Department of Mathematics, Sathyabama University, Chennai, TamilNadu, India.

[2]Department of Electronics Engineering, Anna University, Chennai, TamilNadu, India.

ARTICLE INFO

Article history:

Received: 22 August 2011;

Received in revised form:

26 August 2011;

Accepted: 31 August 2011;

Keywords

Image encryption,

Image decryption,

Chaos,

Hyper-chaos,

Shuffling.

ABSTRACT

This paper presents an image encryption algorithm using chaos. A more complex version of the chaos called Hyper-chaos is used to improve the security of the procedure. Hyper-chaotic system is used to shuffle the parts of the image. Then the shuffled image is encrypted with the chaos. At the receiving end, decryption is done and then the shuffled parts of the image are put back in their original positions.

Introduction

Current cryptographic techniques are based on number theories or algebraic concepts. Chaos is another way of encryption, which seems more promising. Chaos is an offshoot from the field of nonlinear dynamics. It is possible to encrypt a message (a text composed by some alphabets, an image file, or an audio file) using the Ergodic property of the simple low-dimensional and chaotic logistic equation. Chaos-based algorithms have suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption, and this has been proved in many aspects. This method appeals to be a good encryption scheme since it includes the following aspects. Firstly, the key has sensitivity to the cipher keys. Second, the key space is large enough to make brute-force attacks infeasible. The more complex version called the Hyper-chaos has more than one positive Lyapunov exponent, and exhibits dynamical characteristics which are more critical than chaos. The encryption algorithm of image using hyper-chaos too has the advantages of large key space and high security. Firstly, the Chen's hyper-chaotic system is used to shuffle the parts of the image. As this is a symmetric key method, the original key has to be used at the receiving end to decode the image from the cipher image. As proposed, this method owing to the large key space and resistivity to eavesdropping proves to be a very safe method for image encryption.

The Proposed Encryption Algorithm

Hyper-chaotic system has dynamical characteristics that are more complex than the Chaos. Also the key space is increased. Hyper-chaos was first reported by Rossler in 1979. In the past years, the generation of hyper-chaos has been studied with increasing interests. An example for the hyper-chaotic system is the Chen's hyper-chaotic system[1]. It can be modelled as

$$x_{n+1} = a(y_n - x_n) + w_n \quad (1)$$

$$y_{n+1} = d_n x_n - x_n z_n - c_n w_n \quad (2)$$

$$z_{n+1} = x_n y_n - b_n z_n \quad (3)$$

$$w_{n+1} = y_n z_n + r_n w_n \quad (4)$$

where x, y, z and w are the state variables, a, b, c, d and r are the parameters, when a =35,b =3,c =12,d =7 and $0.085 \leq r \leq 0.789$,the system is hyper-chaotic.

As the hyper-chaos has two positive Lyapunov exponents, so the prediction time width of a hyper-chaotic system is shorter than that of a chaotic system, as a result, it is safer than chaos in security algorithm [2].

Image value has strong correlations among adjacent pixels [1]. In order to disturb the high correlation among pixels, an image shuffling matrix is used to shuffle the position of the plain-image.

We assume that the dimension of the plain image is M x N ,the position matrix of pixel is Pi,j (I), i=1,2…..M , j=1,2……M , where Pi,j (I) stands for the grey value of the image. The procedure of shuffling image can be done as explained below.

Step 1: Assuming the initial state variables of the Hyper-chaotic system, iterate the system for n number of times till the output of the system is bounded.

Step 2: Generate m by using the formula, m=floor (mod (p, n)). The value of 'm' will range from 0 to n-1.

Shuffling Technique

The Value of m obtained as the result of iterating the Chen's hyper-chaotic system will decide the method of shuffling the parts of the image.

The image to be transmitted is shown in figure 1 and the different ways to shuffle the image are shown in figure 2.

Figure 1. Original Gray Image to be transmitted

Tele: +91-9444407487, +91-8015136537,+91-9444139382

E-mail addresses: rrkmird@yahoo.com, dr_asampath@yahoo.co.in

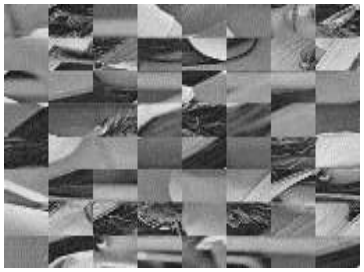

Figure 2(a)

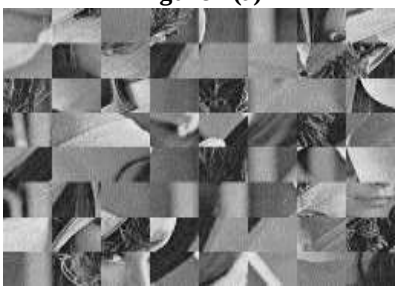

Figure 2(b)

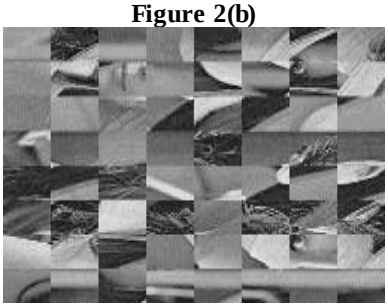

Figure2 (c)

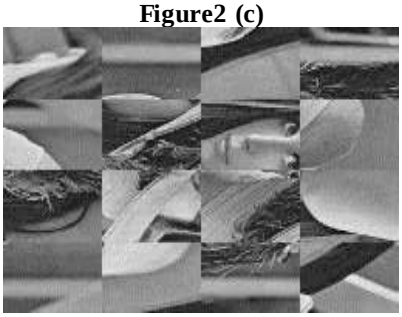

Figure 2(d)

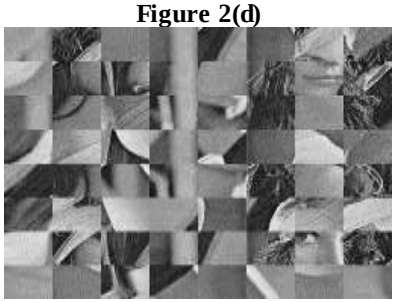

Figure2(e)

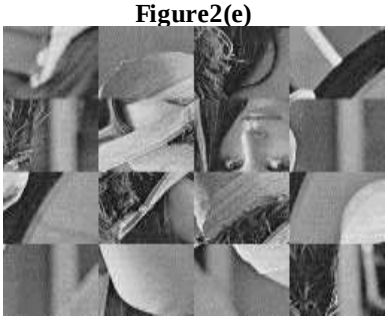

Figure 2(f)

Figure 2. Different ways to shuffle the image parts

4. ENCRYPTION WITH CHAOS

After shuffling the parts of the images, the shuffled image is encrypted using the chaos logistic equation, xn+1 = p*xn*(1-xn) by choosing the parameter 'p' for chaotic regime and with initial condition x0 ϵ (0,1). Due to ergodic property, the interval (0,1) is visited frequently by the iterates[3]. The density of such points is time invariant and this property is essential to cryptography [4].

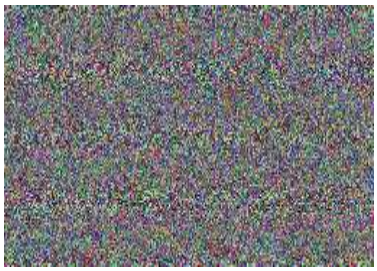

Figure 3. Shuffled image after encryption

The shuffled image after encrypting with chaos is shown in figure 3. Now the reverse operation, namely, decryption has to be considered. Key plays an important role here. The exact key which is used to encrypt the image should be used for decryption to get the actual image [5]. After the decryption is done, the parts of the images are put back in their original positions.

Analysis

The Histogram of the original image (Transmitted image before encryption) and the received image (after decryption) is taken as in figure 4 and figure 5.

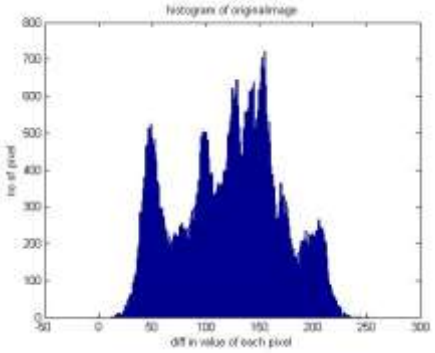

Figure 4. Histogram of the original Image

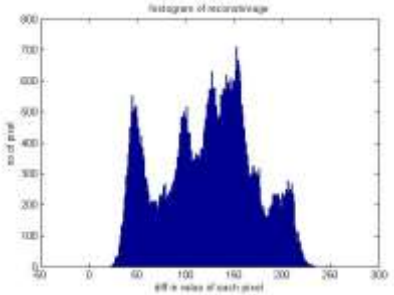

Figure 5. Histogram of the reconstructed Image

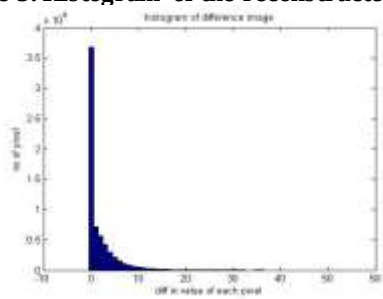

Figure 6. Histogram of the difference between the original image and the reconstructed image

We infer that the histograms of the original and the reconstructed images are nearly similar. Also the histogram of the difference image (difference of the original and the reconstructed image) shows that the majority of the values fall in the range of 0-10, which means that the corresponding pixel values of the original and the reconstructed image are exactly the same in most of the cases or they have a difference with the maximum limit of 20 pixel values.

We aim to collapse the correlation between the adjacent pixels (by means of shuffling the parts of the image) so that the original image cannot be inferred. The correlation plot of the original image and the image with shuffled parts can be shown as in Figure 7 and Figure 8.

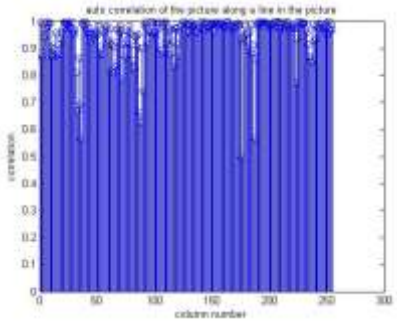

Figure 7.Correlation plot of the original image

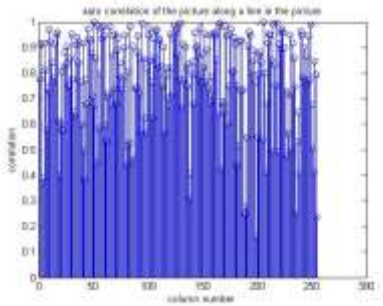

Figure 8. Correlation plot of the image after shuffling the parts

References

[1]. Chen zaiping, Li haifen, Dong enzeng, Du yang, A Hyper-chaos Based Image Encryption Algorithm, August 2010 Second International Conference on Intelligent Human-Machine Systems and Cybernetics2010.

[2]. Z. H. Guan, F.J. Huang, W. J. Guan. Chaos- based image encryption algorithm. Phys.Lett.A.2005, 346:153–157.

[3]. C. C. Chang, M. S. Hwang, T. S. Chen. A new encryption algorithm for image cryptosystems, J. Syst. Software 2001, 58:83–91.

[4]. T. G.. Gao, Z. Q. Chen. A new image encryption algorithm based hyper-chaos. Physics Letters A. Vol. 372, Issue 4, January 2008, Pages 394-400.

[5]. Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia, 1989,13: 29–42.