JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

A Novel Image Encryption Approach based on Chaotic Piecewise Map

Linhua Wang, Xuebing Liao

Department of Computer Science, Minjiang University, Fuzhou, CHINA

Accepted: 5th November, 2012

ABSTRACT

In recent years, a variety of effective chaotic image encryption schemes have been proposed. The chaotic cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. However, many of the proposed algorithms are not suitable in the fields of application, because they are cryptographically weak. In the present work, we propose a new approach for image encryption based on chaotic Piecewise map in order to meet the requirements of the secure image transfer. The algorithm has increased the strength of security of the image encryption against cipher-text-only, chosen-plaintext and chosen-cipher-text attacks. Further more, the results of several experimental, statistical analysis and key sensitivity tests show that the proposed image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

Keywords

Chaotic piecewise map, Image encryption, statistical analysis, key sensitivity test.

1. INTRODUCTION

The encryption is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. To achieve the above purpose researchers look for more secure cryptography incessantly [1]. This paper aims to discuss digital cryptosystems. Many different chaotic systems like Logistic map and piecewise linear chaotic maps have been used to construct chaotic cryptosystems. These are in fact the simplest chaotic systems. In recent years, many algorithms based on Logistic map [2-4], piecewise linear maps [5-7] and piecewise nonlinear maps [8] have been proposed. Piecewise linear chaotic maps have perfect dynamical properties and can be realized simply in both hardware and software, so. They are widely used in digital chaotic ciphers [9, 10]. Although one-dimensional chaotic system has the advantages of high-level efficiency and simplicity [11], there are fundamental drawbacks in this chaotic cryptosystem, such as small key space, slow performance speed and weak security function [12-15]. This paper is arranged as follows. In section 2, the chaotic confusion step is discussed. In section 3, we propose a chaotic image encryption scheme based on the chaotic Piecewise map. In section 4, the analysis of security of the proposed encryption scheme is discussed and finally, in Section 5, we conclude the paper.

2. THE CHAOTIC CONFUSION STEP

The chaotic systems used for information security can be classified into two categories: one-dimensional Logistic map and three-dimensional Lorenz system. These are all excellent models that bear all the classical chaotic characteristics, yet, they have their own disadvantages. Low-dimensional chaotic system is easy to be cracked [4]; therefore, it will require two or more low-dimensional maps to work simultaneously [5, 9], or to merge with other chaotic systems to form a composite one [7, 9]. Three-dimensional Lorenz system is a continuous dynamic system [13], and therefore, a fixed step numerical integration method is needed to solve differential equations; however, this process will lead to the dynamic behaviors of the chaotic system degradation. In this section, we proposed a lattice of the chaotic picecwise map as the chaotic confusion step. This method increases the space of the confusion key, that be caused the development of robustness and security. We first review chaotic piecewise map. The general form of one-dimensional chaotic map is

$$x_n = f(x_{n-1}).$$

With these maps we can produce series $\{x_n \mid n = 1,2,3,\ldots\}$ that are full chaotic and $f : I \to I\ (I = [0,1])$. The chaotic piecewise map is defined as follows:

$$x_{n+1} = \begin{cases} \dfrac{x_n}{m} & 0 \le x_n < m \\ \dfrac{x_n - m}{1-m} & m \le x_n \le 1 \end{cases} \qquad (1)$$

where x_n *and* m are the iterative value and the system parameter, respectively. To obtain random and nonperiodic numbers, it is better to restrict m in the $[0,1]$ range. Since, in this range, the system demonstrate chaotic behavior, therefore, the generated numbers are nonperiodic.

For this purpose, to consider a two-dimensional chaotic system which is defined as follows:

$$\begin{cases} x_{n+1} = f_1(x_n) & n = 1,2,\ldots \\ y_{n+1} = f_2(y_n) & n = 1,2,\ldots \end{cases} \qquad (2)$$

that f_1 and f_2 are the chaotic piecewise maps(Eq. 1). Therefore, the m_1, m_2, x_0, y_0 are our secret keys. These keys must be shared between sender and receiver as secret keys. x_{n+1} *and* y_{n+1} generate random numbers in the [0,1] interval.

3. THE PROPOSED CHAOTIC IMAGE ENCRYPTION SCHEME

In the pixel diffusion step,proposed an encrypted scheme based on the coupled map lattices. In the proposed scheme, the composite of the chaotic coupled map lattices are employed to achieve the goal of image encryption. To consider a gray scale image with the size of $m \times n$ ($I_{m \times n}$). The gray scale image $I_{m \times n}$ is transformed into the matrix $I_{(m \times n) \times 1}$. Now, using the chaotic coupled map lattices (Eq. 2), the encryption shceme is defined as

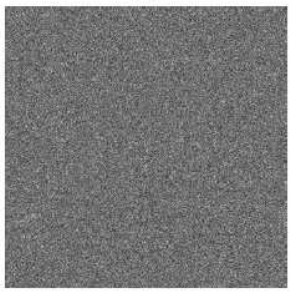
$$\begin{cases} E_i = \left[(X_i \times 10^{14}) \bmod (m \times n) \right] \oplus I_{i \times 1} \\ F_i = \left[(Y_i \times 10^{14}) \bmod (m \times n) \right] \oplus I_{i \times 1} \end{cases}$$

Therefore,

$$C_i = E_i \oplus F_i \qquad (3)$$

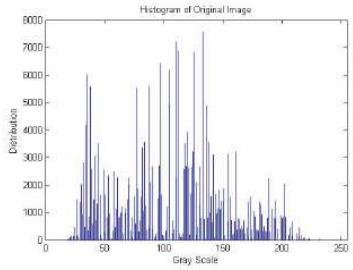
where C and $\oplus$ are the matrix of the encrypted image and the bitwise XOR operator, respectively. Note that x_i , y_i are, in fact, the results of the iteration of the chaotic coupled map lattices. The decryption process is almost the same as the encryption but with reverse steps. An indexed image of an 'Lena' sized (see Fig. 1(a)) is used as a plain image and the encrypted image is shown in Fig. 1(b). The grey scale histograms are given in Fig. 2. The Fig. 2(b) shows uniformity in distribution of grey scale of the encrypted image. In addition, the average pixel intensity for plain image is 97.42, and for encrypted image is 127.80, respectively.

(a)

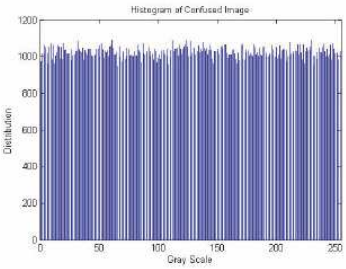


(b)

Figure 1. (a) Plain image; (b) Encrypted image.



(a)



(b)

Figure 2. Histograms of images.

4. ANALYSIS OF SECURITY OF THE PROPOSED ENCRYPTION SCHEME

The Security is a major intransitive of a cryptosystem. Here, a complete analysis is made on the security of the cryptosystem. We have tried to explain that this cipher image is sufficiently secure against various cryptographical attacks, as shown below:

4.1. Key space analysis

In the proposed scheme, the confusion stage and diffusion stage are applied respectively. Thus, the key space of the

encryption is the multiplication between the confusion key and the diffusion key, i.e. $S = S_1 + S_2$

where S_1, S_2 and S are the confusion key, the diffusion key and the key space, respectively. On the other hand, the key space size is the total number of different keys that can be used in the encryption [10,14]. Security issue is the size of the key space. If it is not large enough, the attackers may guess the image with brute-force attack. If the precision is 10^{-14}, the size of key space for initial conditions and control parameters of the proposed scheme is more than 2^{256}. This size is large enough to defeat brute-force by any super computer today.

4.2. Correlation Coefficient analysis

The statistical analysis has been performed on the encrypted image. This is shown by a test of the correlation between two adjacent pixels in plain image and encrypted image. We randomly select 2000 pairs of two-adjacent pixels (in vertical, horizontal, and diagonal direction) from plain images and ciphered images, and calculate the correlation coefficients, respectively by using the following two equations (see Table 1 and Fig. 3) [10,11]:

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),$$

$$r_{xy} = \frac{Cov(x,y)}{(D(x))^{\frac{1}{2}}(D(y))^{\frac{1}{2}}}$$

where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i), \quad D(y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 .$$

where, E(x) is the estimation of mathematical expectations of x, D(x) is the estimation of variance of x, and Cov(x,y) is the estimation of covariance between x and y, where x and y are grey scale values of two adjacent pixels in the image.

Table 1: Correlation coefficients of two adjacent pixels in the plain image and the encrypted image

Direction	*Plain Image*	*Encrypted Image*
Horizontal	***0.982208***	***0.002637***
Vertical	***0.946102***	***0.004612***
Diagonal	***0.925623***	***0.003869***

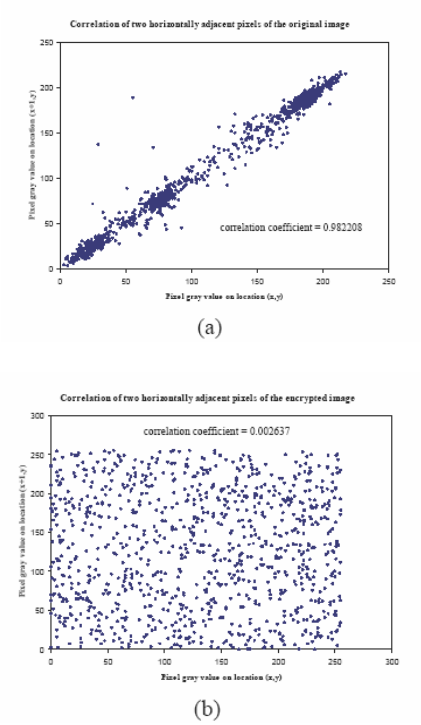


Figure 3. Correlation distributions of two horizontally adjacent pixels in the plain image and the encrypted image.

4.3. Differential attack

Attackers try to find out a relationship between the plain image and the encrypted image, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key [12,15]. Trying to make a slight change such as modifying one pixel of the plain image, attacker observes the change of the encrypted image [12]. Because of the existence of the diffusion in the proposed cryptosystem, the encrypted image is so sensitive to the plain image that even a one-pixel change in the plain image leads to a completely different encrypted image. Diffusion refers, in fact, to rearrange or spread out the bits in the message. So, any redundancy in the plain image is spread out over the encrypted image [13,10]. In order to demonstrate influence of one pixel change on the whole encrypted image by the proposed scheme, two common measures are used:

Number of Pixels Change Rate (NPCR) stands for the number of pixels change rate while, one pixel of plain image is changed. Unified Average Changing Intensity (UACI) measures the average intensity of differences between the plain image and ciphered image. The NPCR and The UACI, are used to test the influence of one pixel change on the whole image encrypted by the proposed scheme and can be defined as following:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%$$

where W and H are the width and height of C_1 or C_2. C_1 and C_2 are two ciphered images, whose corresponding original images have only one pixel difference and also have the same size. The $C_1(i,j)$ and $C_2(i,j)$ are grey-scale values of the pixels at grid (i,j). The D(i,j) determined by $C_1(i,j)$ and $C_2(i,j)$. If $C_1(i,j)=C_2(i,j)$, then, D(i, j) = 1; otherwise, D(i, j) = 0. We have done some tests on the proposed scheme (256 grey scale image of size 256×256) to find out the extent of change produced by one pixel change in the plain image. We have obtained NPCR=0.28% and UACI=0.17%. The results demonstrate that the proposed scheme can survive differential attack.

5. CONCLUSION

We have proposed a chaotic encryption scheme based on chaotic piecewise map.The security of the encrypted image of this scheme is evaluated by the key space analysis, the correlation of two adjacent pixels and differential attack. The distribution of the encrypted image is very close to the uniform distribution, which can well protect the information of the image to withstand the statistical attack. We suggest that this encryption scheme is suitable for applications like internet image encryption and secure transmission of confidential information in the internet.

6. REFERENCES

[1] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., VoA S., 2010. NIST special publication, 5-125.

[2] R. Brown, L.O. Chua, Int. J. Bifur. Chaos, 1996, 219.

[3] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, A. Shang, Int. J. Bifur. Chaos, 1992, 973.

[4] O. Morgul, M. Feki, Phys. Lett. 1999, 169.

[5] M.S. Baptista, Phys. Lett. A 240, 1998, 50.

[6] K.W. Wong, Phys. Lett. A 298 (4) ,2002, 238.

[7] F. Huang, Z.-H. Guan, Chaos Solitons Fractals 23, 2005, 851.

[8] Weng J., Yao G., Deng R. H., Chen M., Li X., "Cryptanalysis of a certificateless signcryption scheme in the standard model," Information Sciences, 2012, 1, 661–667.

[9] R.A.J. Matthews, Cryptologia 1989, 13-29.

[10] L. Kocarev, G. Jakimoski, Phys. Lett. A 289, 2001, 199.

[11] N. Masuda, K. Aihara, IEEE Trans. Circuits Syst.-I 49 ,2002, 28.

[12] H. Zhou, X. Ling, Int. J. Bifur. Chaos 7, 1997, 205.

[13] F. Huang, Z.-H. Guan, Chaos Solitons Fractals 23, 2005, 1893.

[14] T. Sang, R. Wang, Y. Yan, Acta Eletronica Sinica 1999, 27, 43-47.

[15] Chen G., Mao Y., Chui C.K., "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons Fractals, 2004, 749-761.