A Novel Scheme for Image Encryption Based on Piecewise Linear Chaotic Map

Jun Peng[1, 2], Shangzhu Jin[1], Yongguo Liu[3, 4], Zhiming Yang[1], Mingying You[1] and Yangjun Pei[1]
[1] College of Electronic Information Engineering
Chongqing University of Science and Technology, Chongqing 400050, P. R. China
pengjun70@126.com
[2] Department of Computer Science, California State University, CA 95819, U.S.A
[3] School of Computer Science and Engineering
University of Electronic Science and Technology of China, Chengdu 610054, P. R. China
[4] National Laboratory on Machine Perception, Peking University, Beijing 100871, P. R. China

Abstract—**Recently, the chaos based cryptographic algorithms have suggested some meaningful techniques to develop efficient image encryption schemes. In this paper, we propose a new digital image encryption scheme based on the piecewise linear chaotic map (PWLCM) in order to meet the requirements of the secure encryption. The proposed scheme is described in detail, along with the security analyses including key space analysis, sensitivity analysis, information entropy analysis and differential attack analysis. The results show that the suggested image encryption scheme has some properties desirable in a good security cryptosystem.**

Keywords—**image encryption, piecewise linear chaotic map, chaotic cryptography, information security**

I. INTRODUCTION

Recently, image encryption schemes have been increasingly studied to meet the requirements for secure transmission over the Internet. Traditional encryption algorithms, such as 56-bit DES, are not suitable for the image encryption due to the shorter key length which is weak for assisting the brute-force attack. RSA can provide a key with 1024 bits length, however its encryption speed is too slow to meet the fast encryption speed requirement for those data such as images, up to now it is mainly used in digital signature.

Therefore, it is necessary for people to find some new schemes suitable for the image encryption. Since chaotic systems have several significant properties favorable to the information security, such as random-like behavior, ergodicity, extreme sensitivity to the initial condition and control parameters, they have attracted people's great attention especially on the application to the secure communications and cryptography. In early 90's, Pecora and Carroll were the first to propose a method to synchronize two identical chaotic systems to implement a secure communication [1, 2], and Matthews presented an earliest chaotic stream cipher [3]. Furthermore, the close relationship between chaotic maps and cryptographic algorithms has been observed in [4-6]. High sensitivity of chaotic systems with respect to the initial condition and parameters implies a strong cryptographic property of chaotic cryptosystem which makes them robust against any statistical attacks. Therefore, we believe that chaotic systems can be employed to design good image encryption algorithm.

In this paper we mainly focus on the image encryption using chaos. A number of chaos based image encryption schemes have been reported in recent years, and we will offer a brief overview here. Fridrich [4] represented a method to adapt an invertible two-dimensional standard baker map on a torus or on a square to create symmetric block encryption scheme. The standard baker map, according to [4], is firstly generalized by introducing parameters and then discretized to a finite rectangular lattice of points. After that the map is extended to three dimensions to obtain a more complicated substitution cipher that can be used for the purpose of image encryption. Yen and Guo [7] proposed a chaotic key-based algorithm (CKBA) in which a binary sequence as a key is generated using a chaotic system, and the image pixels are arranged according to the generated binary sequence, and then the scale-gray values of pixels are XORed or XNORed bit-by-bit to one of the two predetermined keys. However, the analysis conducted in [8] showed that the algorithm in [7] has some drawbacks: it is vulnerable to the chosen or known-plain-text attack using only one plain-image, and its security to brute-force attack is also questionable. Recently, Chen et al. [9] proposed a symmetric image encryption in which a 3D cat map was exploited to shuffle the positions of image pixels and another chaotic map was also used to confuse the relationship between the original image and its encrypted image. In [10], Pareek et al. employed an external secret key of 80-bit and two chaotic logistic maps to construct an encryption scheme, in which the initial conditions of the both logistic maps were derived from the external key and eight different types of operators were used to encrypt the pixels of the original image. Furthermore, Pisarchik et al. [11] suggested a new practical algorithm based on a chaotic map lattice (CML). The main idea is to convert, pixel by pixel, the image color to lattices of chaotic maps one-way coupled by initial conditions. After small numbers of iteration and cycles, the source image will become an indistinguishable one due to the intrinsic properties of the chaotic system. Very recently, similar to [9], Gao et al. [12] exploited an image total shuffling matrix to shuffle the position of image pixels and then used a hyper-chaotic Chen system to confuse the relationship between the original image and encrypted image. Obviously, the research achievements that are mentioned above are very useful to the latter studies on the chaos-based image encryption algorithm.

978-1-4244-1674-5/08 /$25.00 ©2008 IEEE

In this paper, we will investigate a new image encryption scheme based on the chaotic system. As we know, the chaotic map should not be too complex for the complementation, but at same time should have sufficient complex dynamics features. Hence, we introduce a piecewise linear chaotic map into the design of the encryption algorithm. The aim of the design is to obtain an easily realizable and secure one.

The rest of the paper is organized as follows. In Section 2, we introduce a piecewise linear chaotic map, and then describe the procedure of image encryption in details. To demonstrate its performance withstand the most common attacks, in Section 3, we analyze the proposed image encryption scheme in terms of key space analysis, sensitivity analysis, information entropy analysis and differential attack analysis. Finally, we conclude the paper in Section 4 with remarks on future work.

II. THE PROPOSED ENCRYPTION SCHEME

A. Choosing the Chaotic System

There are lots of chaotic systems that can be used in the application on the information security, such as Logistic map, Tent map, Baker map and chaotic neural networks. Here, we will employ a piecewise linear chaotic map (PWLCM) to generate the desirable binary chaotic sequences for the image encryption. The research of Li and Chen, et al. [13] has shown that the PWLCM has many excellent dynamical properties including ergodicity, random-like behavior, a larger positive Lyapunov exponent, a uniform invariant density function and an exponential attenuation auto-correlation function. These properties are very useful for the purpose of cryptographic application with the PWLCM.

The PWLCM is defined as follows:

$$x_{n+1} = f(x_n, \mu) = \begin{cases} x_n \cdot \frac{1}{\mu}, & \text{if } x_n \in [0, \mu); \\ (x_n - \mu) \cdot \frac{1}{0.5-\mu}, & \text{if } x_n \in [\mu, 0.5]; \\ f(1 - x_n, \mu), & \text{if } x_n \in (0.5, 1]; \end{cases} \tag{1}$$

Where $x_n \in [0,1]$, μ is a control parameter and when $\mu \in (0, 0.5)$ this map is in chaotic state.

Fig.1 shows the chaotic sequences obtained from the PWLCM with different initial condition and control parameter, and the correlation functions are also displayed. Fig.1 (a) is the sequence S^1 with $x_0 = 0.2$ and $\mu = 0.3041$ while Fig.1 (b) is the sequence S^2 with $x_0 = 0.393$ and $\mu = 0.4775$. Besides, Fig.1 (c) and (d) are auto-correlation function of S^1 and cross-correlation function of S^1 and S^2, respectively.

The results of Fig. 1 indicate that PWLCM has a desirable statistical property of correlation function, which is of great benefit to the generation of the binary sequences that will be used for the image encryption. However, we must keep in mind that when using this map in practice we should avoid $x_n = 0$, $x_n = 0.5$ or $x_n = 1$, as they will all at last result in a same fixed point x_n=0 due to $f(0,\mu) = 0$, $f^3(0.5,\mu) = 0$ and $f^2(1,\mu) = 0$ for any $\mu \in (0, 0.5)$.

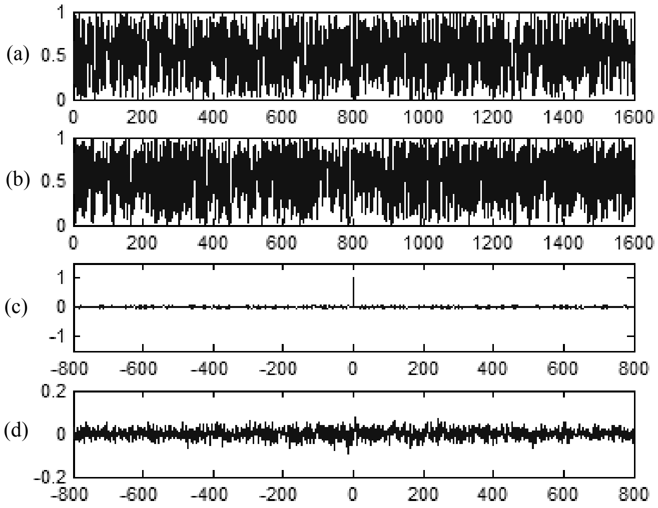

Figure 1. The chaotic sequences and correltion functions.

B. Description of the Encryption Scheme

In this section, we will discuss the procedures of the proposed image encryption as well as decryption process in details. The scheme proposed here operates on a 192-bit key, which is mapped to the system parameters and as to compute the initial condition and control parameters of the PWLCM to further generate the chaotic keystream for the encryption process. Besides, we take advantage of the inherent features of the chaotic map when designing the encryption process. The scheme diagram is given in Fig.2.

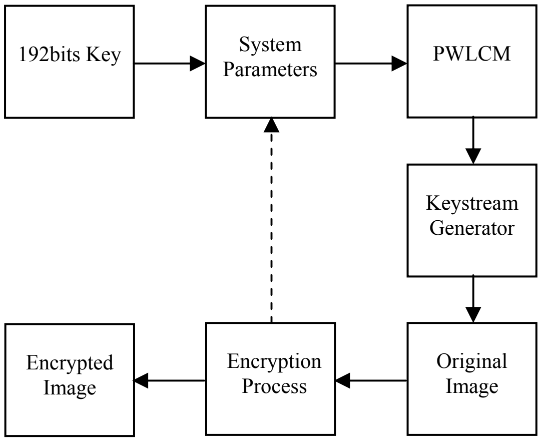

Figure 2. The diagram of encryption scheme.

For the sake of making the description of the encryption scheme more comprehensible, some mathematical symbols are firstly displayed as follows:

$Z^{<<\alpha}$: cyclic left-shift by α bits of Z ;

$Z^{>>\alpha}$: cyclic right-shift by α bits of Z ;

$Z^1 \oplus Z^2$: bitwise exclusive-OR of Z^1 and Z^2 ;

iw, ih : the width and height of the image;

m_i : the source image, $i = 1, 2, \cdots, iw \times ih$;

e_i : the encrypted image, $i = 1, 2, \cdots, iw \times ih$;

$K_1 K_2 \cdots K_{24}$: 192-bit secure key.

The steps of the encryption process are given as follows.

Step 1: compute the following system parameters that will be used in latter encryption.

$$S = \sum_{i=1}^{24} K_i \bmod 256 ;$$

$$P = K_1 \oplus K_2 \oplus \cdots \oplus K_{24} ;$$

$$Q_1 = K_1 \oplus K_5 \oplus K_9 \oplus K_{13} ;$$

$$Q_2 = K_2 \oplus K_6 \oplus K_{10} \oplus K_{14} ;$$

$$Q_3 = K_3 \oplus K_7 \oplus K_{11} \oplus K_{15} ;$$

$$Q_4 = K_4 \oplus K_8 \oplus K_{12} \oplus K_{16} ;$$

$$Q_5 = K_{17} \oplus K_{19} \oplus K_{21} \oplus K_{23} ;$$

$$Q_6 = K_{18} \oplus K_{20} \oplus K_{22} \oplus K_{24} .$$

Repeat step 2 to step 5 until all the pixels of the source image are encrypted. Let the loop variable $h = 1$.

Step 2: Determine the initial condition, control parameter and iteration number of the PWLCM:

$$x_0 = (Q_1^{<<2} + Q_2^{>>2} + Q_3^{<<3} + Q_4^{>>3} + S) / (5 \times 256) ;$$

$$\mu = 0.5 \times (Q_5^{<<3} + Q_6^{>>4} + P) / (3 \times 256) ;$$

$$N = 200 + (S \times P) \bmod 1024 .$$

Step 3: Let x^N denotes N-th iteration of the PWLCM and it can be expressed as $x^N = 0.b_1(x)b_2(x)\cdots b_i(x)\cdots$, and the i-th bit $b_i(x)$ can be represented as:

$$b_i(x) = \sum_{r=1}^{2^i-1} (-1)^{r-1} \Theta_{(r/2^i)}(x),$$

Where $\Theta_t(x)$ is a threshold function which is defined as:

$$\Theta_t(x) = \begin{cases} 0, & x < t \\ 1, & x \geq t \end{cases}$$

As a result, a binary sequence $\{b_i(x)\}_{i=1}^{d}$ can be obtained. Here suppose $d = 32$, then a binary sequence $b_1(x)b_2(x)\cdots b_{32}(x)$ is obtained. We assemble these 32 bits into four unsigned numbers w_1 , w_2 , w_3 and w_4 . Finally, we got h-th keystream $c_h = w_1 \oplus w_2 \oplus w_3 \oplus w_4$.

Step 4: Encrypt the h-th pixel m_i of the source image with the following formula:

$$e_h = (c_h + m_h) \bmod 256 .$$

Step 5:

$$h = h + 1 ;$$

$$S = (w_1^{<<1} + w_2^{<<2} + w_3^{<<3} + w_4^{<<4} + e_h^{<<5} + S) \bmod 256 ;$$

$$P = (w_1^{>>1} \oplus w_2^{>>2} + w_3^{>>3} \oplus w_4^{>>4} + e_h^{>>5} \oplus P) \bmod 256 .$$

If $h \leq iw \times ih$ then goto Step 2 else output the encrypted image $\{e_i\}_{i=1}^{iw \times ih}$ and encryption process end.

As the proposed encryption algorithm is a symmetrical one, thus the decryption process is similar to the encryption process except using the same secure key to reconstruct the keystream c_h and recover the source image according to the following formula:

$$m_h = (e_h - c_h) \bmod 256 .$$

III. Security Analysis

From the cryptography point of view, an effective encryption algorithm should have desirable features for withstanding all kinds of known attacks. In this section, we will address some security analysis on the proposed algorithm in terms of key space analysis, sensitivity analysis, information entropy analysis and different attack analysis.

A. Key Space

It's well known that a large key space is very important for an encryption algorithm to against the brute-force attack. As the algorithm has a 192-bit key, the key space size is 2^{192} which is large enough to resist all kinds of brute-force attacks with the current computer technology. The advantage of our algorithm is that the users only need to remember the 192-bit secret key due to that the algorithm auto-mapped the 192-bit key to the system parameters. However many other chaos-based algorithms viewed the initial condition and control parameters of the chaotic system as the part of the secret key, resulting in the difficulties for users to keep these complex secure key.

B. Sensitivity Analysis

The experiments of sensitivity with respect to the key and the plaintext of the encryption algorithm are performed. The image "girl.bmp" with size 512×512 is used as the source image, and two keys key^1 and key^2 are randomly selected as follows except only last one character difference between them.

key^1 = "H6Ja*1NMw104cRS72Nu4m6F5";

key^2 = "H6Ja*1NMw104cRS72Nu4m6F6".

The results are shown in Fig.3. From the results we can see that the obtained encrypted images (b) and (c) are very different when using a slightly different key. Furthermore, to investigate the sensitivity of the encryption algorithm to the source image, we make a tiny change on the gray-scale value of one pixel at grid (1, 1) of the source image (a). The obtained encrypted image is in (d), and obviously (d) and (b) are violently different with each other even they both are produced by the identical key. For the sake of understanding the difference between the encrypted images, the following correlation coefficients are computed and listed in Table I.

$$C_r = \frac{M\sum_{i=1}^{M}(x_i \times y_i) - \sum_{i=1}^{M} x_i \times \sum_{i=1}^{M} y_i}{\sqrt{\left(M\sum_{i=1}^{M} x_i^2 - \left(\sum_{i=1}^{M} x_i\right)^2\right) \times \left(M\sum_{i=1}^{M} y_i^2 - \left(\sum_{i=1}^{M} y_i\right)^2\right)}} \tag{2}$$

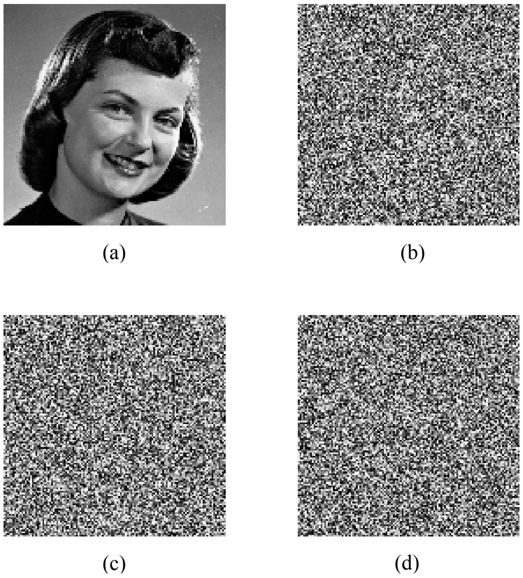
(a)
(b)
(c)
(d)

Figure 3. Sensitivity test results of the encryption scheme. (a) is the source image, (b) and (c) are obtained encrypted images using key^1 and key^2, respectively. (d) is corresponding encrypted image of a slightly changed source image using identical key^1.

Where M denotes the total number of the pixels of the image, x and y denote the gray-scale value of the pixels at the corresponding grid. From the results of Table I. we can see the correlation coefficients are very small, which means the encryption algorithm is very sensitive to the source image, showing that the encryption algorithm can against the known-plaintext attack.

TABLE I. CORRELATION COEFFICIENTS OF TWO ENCRYPTED IMAGES

Computation objects	Correlation coefficients
Fig.3 (b) and (c)	-0.0029
Fig.3 (c) and (d)	-0.0026
Fig.3 (b) and (d)	-0.0025

C. *Information Entropy*

It is well know that the information entropy $H(m)$ of a plaintext message m can be calculated as

$$H(m) = -\sum_{i=1}^{n} p(m_i)\log_2 p(m_i) \tag{3}$$

where $p(m_i)$ represents the probability mass function of message m_i and $n = 256$ for image. For a 256-gray-scale image, if every gray value has an equal probability, then information entropy equal to 8, indicating that the image is a purely random one. When the information entropy of an image is less than 8, there exists a certain degree of predictability, which will threaten its security. Therefore, we hope the entropy of the encrypted image is near to ideal value to against the entropy attack effectively.

The information entropy of the four source images and their corresponding encrypted images are computed and displayed in Table II. From the computation results we found that all the entropies of the source images are smaller than the ideal one because of the fact that practical information sources seldom generate random messages. While the entropy of every encrypted image is very close to the theoretical value of 8, showing the suggested encryption scheme is sufficient secure upon the entropy attack.

TABLE II. INFORMATION ENTROPY OF THE SOURCE IMAGES AND THE ENCRYPTED IMAGES

Images (512×512)	**Information Entropy**	
	Source Image	***Encrypted Image***
Girl	7.0818	7.9993
Boats	7.1238	7.9994
Peppers	7.5936	7.9994
Lena	7.4455	7.9993

D. *Differential Attack*

As we know, in order to avoid the known-plaintext attack and the chosen-plaintext attack, a good encryption algorithm should have the desirable property which spreads the influence of a single plaintext bits over as much of the ciphertext as possible so as to hide the statistical structure of the plaintext [14]. This means the small difference of the plaintext should be diffused to the whole ciphertext. To evaluate the influence of one-pixel change on the whole encrypted image, two common measures [9] are used, i.e., number of pixels change rate (NPCR) and unified average changing intensity (UACI). These two measures are defined as:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{4}$$

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{\left|E^1(i,j) - E^2(i,j)\right|}{255}\right] \times 100\% \tag{5}$$

where E^1 and E^2 denote two encrypted images, respectively, W and H are the width and height of image, and the gray-scale values of the pixels at grid (i, j) of E^1 and E^2 are labeled as $E^1(i, j)$ or $E^2(i, j)$, respectively. $D(i, j)$ is related to $E^1(i, j)$ and $E^2(i, j)$. If $E^1(i, j) = E^2(i, j)$ then $D(i, j)$=1 else $D(i, j)$=0.

The NPCR measures the different pixel numbers between two images, and the UACI measures the average intensity of differences between two images.

We randomly choose a pixel of the source image and make a slightly change on the gray-scale value of this pixel. The encryption algorithm is performed on the modified source image and then the two measures NPCR and UACI are computed. This kind of experiment is carried out 256 times, and the average value of NPCR and UACI are calculated. We obtained NPCR $\approx$ 99.62%, and UACI $\approx$ 32.15%. The results show that a slightly change in the source image will result in a great change in the encrypted image, this imply that the proposed algorithm has an excellent capability to resist the differential attack, in which way, the opponent may be able to find out a meaningful relationship between the source image and the encrypted image.

IV. Conclusions

In this paper, a novel image encryption scheme based on a piecewise linear chaotic map is proposed. One of the main motivations for using this kind of map is that we want to achieve a more sophisticated chaotic sequence to be used for encrypting the plaintext and this map can be easily complemented in software. The scheme used a 192-bit key and through a special procedure that maps the key to the system parameters. Security analyses indicate that the proposed image encryption scheme has desirable properties from cryptographic point of view. It should be mentioned that, although the proposed scheme mainly focused on image encryption, it can also be modified to apply in the other fields such as secure information communication over the Internet.

The future research directions will be directed to a more detailed study of security analysis of the proposed scheme. Also, we intend to design a modified version for color image encryption.

Acknowledgment

The work described in this paper was supported by the National Science Foundation of China under Grant No. 60573047, the Science and Technology Research Project of Chongqing Municipal Education Commission of China under Grant No. KJ051402, No. KJ081406 and the Natural Science Foundation Project of CQ CSTC under Grant No. 2005BB2050. Jun Peng acknowledges support from the Innovative Team Construction Project of Chongqing University of Science and Technology, China.

References

[1] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.,* vol. 64, no. 8, pp. 821-824, 1990.

[2] L. M. Pecora and T. L. Carroll, “Driving systems with chaotic signals,” *Phys. Rev. A*, vol. 44, no. 4, pp. 2374-2383, 1991.

[3] R. Matthews, “On the derivation of a chaotic encryption algorithm,” *Cryptologia*, vol. XIII, no. 1, pp. 29-42, 1989.

[4] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284, 1998.

[5] J. Fridrich, “Image encryption based on chaotic maps,” *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics*, pp. 1105-1110, 1997.

[6] L. Kocarev, “Chaos-based cryptography: A brief overview,” *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001.

[7] J. C. Yen and J. I. Guo, “A new chaotic key-based design for image encryption and decryption,” *Proc. IEEE Int. Conf. Circuits and Systems*, vol. 4, pp. 49-52, 2000.

[8] S. J. Li and X. Zheng, “Cryptanalysis of a chaotic image encryption method,” *Proc. IEEE Int. Symposium Circuits and Systems*, vol. 2, pp. 26-29, 2002.

[9] G. R. Chen, Y. Mao and C. K. Chui, “A symmetric image encryption based on 3D chaotic maps,” *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749-761, 2004.

[10] N. K. Pareek, V. Patidar and K. K. Sud, “Image encryption using chaotic logistic map,” *Image and Vision Computing*, vol. 24, no. 9, pp. 926-934, 2006.

[11] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, “Encryption and decryption of images with chaotic map lattices,” *Chaos*, vol. 6, no. 3, pp. 033118.1-033118.6, 2006.

[12] T. G. Gao and Z. Q. Chen, “A new image encryption algorithm based on hyper-chaos,” *Phys. Lett. A*, vol. 372, no. 4, pp. 394-400, 2008.

[13] S. J. Li, G. R. Chen and X. Q. Mou, “On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps,” *Int. J. Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119-3151, 2005.

[14] B. Schneier, *Applied Cryptography (2nd Edition)*, John Wiley & Sons, 1996..