Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices*

Wang Xing-Yuan(王兴元)† and Liu Lin-Tao(刘林涛)

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, *China*

(Received 30 October 2012; revised manuscript received 23 November 2012)

A digital image encryption scheme using chaotic map lattices has been proposed recently. In this paper, two fatal flaws of the cryptosystem are pointed out. According to these two drawbacks, cryptanalysts could recover the plaintext by applying the chosen plaintext attack. Therefore, the proposed cryptosystem is not secure enough to be used in the image transmission system. Experimental results show the feasibility of the attack. As a result, we make some improvements to the encryption scheme, which can completely resist our chosen plaintext attack.

Keywords: cryptanalysis, chosen plaintext attack, image encryption, chaotic map lattice

PACS: 05.45.Gg, 05.45.Ra, 42.30.Va, 05.45.Vx **DOI:** 10.1088/1674-1056/22/5/050503

1. Introduction

Chaos is a definitive and similar random process which appears in a nonlinear system. A chaotic dynamics system has some good features, such as sensitive dependence on initial conditions, ergodicity, non-periodicity, and non-convergence. Under the control of certain parameters, we can obtain very good pseudo-random numbers. Therefore, chaotic cryptography has aroused extensive concern, and many researchers have proposed their chaotic cryptosystems over the years. Some cryptosystems are based on a low-dimensional chaotic map[1–5] with obvious drawbacks, such as small key space, while others based on a high-dimensional chaotic map[6–9] are more secure.

Though many cryptosystems based on chaotic maps are proposed, some of them are proved to be not secure enough to be used to encrypt images. Cokai, Wang, Alvarez, and coworkers[10–12] showed that a cryptosystem using a cat map or a baker map should not be adopted when encrypting an image. Wang, Arroyo, Peng, Rhouma, and coworkers[13–16] proved that some cryptosystems based on high-dimensional chaotic maps and spatiotemporal chaotic maps are still not secure.

In this paper, we analyze the digital image encryption scheme with chaotic map lattices proposed in Ref. [17]. We change the pixel value of the cryptosystems using one of the eight operations which is decided by the key stream generated by chaotic map lattices. Though it seems secure enough, we find that the method is vulnerable to the chosen plaintext attack, and has two fatal drawbacks: the unchanged key stream and two classes of operations used by the key stream.

This paper is organized as follows. Section 2 briefly introduces the cryptosystem under study. Section 3 demonstrates a chosen plaintext attack that reveals the equivalent keys. Section 4 illustrates the success of our attack with simulation examples. Section 5 improves the original encryption scheme. Finally, Section 6 presents the conclusions.

2. Description of the encryption algorithm

The cryptosystem proposed by Sun and Lü uses chaotic map lattices (CMLs), which can be described as

$$x_{n+1}^{j} = (1-\varepsilon)f(x_n^j) + \varepsilon f(x_n^{j-1}), \tag{1}$$

where x_n^j represents the state variable for the j-th site ($j = 1,2,\ldots,L$, L is the lattice number in the CML) lattice, n is the discrete time index, and ε is the coupling constant. In general, the periodic boundary condition $x_n^0 = x_n^L$ is assumed, and the mapping function $f(x_n)$ is chosen to be the logistic map

$$x_{n+1} = f(x_n) = ax_n(1-x_n), \quad (x_n \in (0,1), \ a \in (0,4]). \tag{2}$$

The encryption scheme proposed is for an RGB image. RGB images use the RGB color model, which is an additive model where the three primary colors including red, green, and blue are combined to produce other colors. The integer numbers between [0, 255] are used to describe these gray levels. The final displayed color is determined by these three components. In digital computer communication, each color level for red, green, and blue, is usually represented by an 8-bit value.

To change the parameter of the logistic map during the encryption process, the expression of the CML is adopted as

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61173183, 60973152, and 60573172), the Doctoral Program Foundation of Institution of Higher Education of China (Grant No. 20070141014), the Program for Excellent Talents in Universities of Liaoning Province, China (Grant No. LR2012003), the Natural Science Foundation of Liaoning Province, China (Grant No. 20082165), and the Fundamental Research Funds for the Central Universities of China (Grant No. DUT12JB06).

†Corresponding author. E-mail: wangxy@dlut.edu.cn

© 2013 Chinese Physical Society and IOP Publishing Ltd

follows:

$$x_{n+1}^j = (1-\varepsilon)f(x_n^j, a_j) + \varepsilon f(x_n^{j-1}, a_{j-1}), \quad (3)$$

$$f(x_n^j, a_j) = (3.9 + 0.1a_j)x_n^j(1-x_n^j), \quad (4)$$

where $j = 1,2,\ldots,8$, $x_n^0 = x_n^8$, and ε is set to be 0.99. The system parameter $a_j \in (0,1)$. The initial condition of f, $x_0^j \in (0,1)$ serves as the secret key, denoted as $a = \{a_1, a_2, \ldots, a_8\}$ and $x_0^j = \{x_0^1, x_0^2, \ldots, x_0^8\}$, respectively.

The encryption process can be summarized as follows.

(i) Read four pixels from the image file. $D_{\rm r}(i)$, $D_{\rm g}(i)$, and $D_{\rm b}(i)$ denote the components of red, green, and blue of the i-th pixel, respectively.

(ii) Iterate Eq. (3) using the key, then the system can have eight output variables: $x_n^1, x_n^2, \ldots, x_n^8$, simultaneously. Compute K_n^j using

$$K_n^j = int(x_n^j \times 2^u) \bmod (2^v), \quad (5)$$

where u is set to be 52, and v is set to be 32.

(iii) Calculate N using the following formula:

$$N = \bmod(x_n^j \times 10^{13}, 8). \quad (6)$$

Since $N \in [0,7]$, we select the corresponding group to perform the encryption operation if N equals the group number of the sequence of the group.

Operation 0 Invert the bits of all three RGB bytes.

Operation 1 $D_{\rm r}(i) \oplus K_n^1$, $D_{\rm g}(i) \oplus K_n^2$, and $D_{\rm b}(i) \oplus K_n^3$.

Operation 2 Encryption operation:

$$S_{\rm r}(i) = (D_{\rm r}(i) + K_n^1) \bmod (2^v),$$

$$S_{\rm g}(i) = (D_{\rm g}(i) + K_n^2) \bmod (2^v),$$

$$S_{\rm b}(i) = (D_{\rm b}(i) + K_n^3) \bmod (2^v).$$

Decryption operation:

$$D_{\rm r}(i) = (S_{\rm r}(i) - K_n^1) \bmod (2^v),$$

$$D_{\rm g}(i) = (S_{\rm g}(i) - K_n^2) \bmod (2^v),$$

$$D_{\rm b}(i) = (S_{\rm b}(i) - K_n^3) \bmod (2^v).$$

Here, $S_{\rm r}(i)$, $S_{\rm g}(i)$, and $S_{\rm b}(i)$ are ciphered image, $\oplus$ means bitwise XOR, and "mod" denotes the modulus operation.

Operation 3 Encryption operation:

$$\mathrm{NOT}(D_{\rm r}(i) \oplus K_n^1),$$

$$\mathrm{NOT}(D_{\rm g}(i) \oplus K_n^2),$$

$$\mathrm{NOT}(D_{\rm b}(i) \oplus K_n^3).$$

Decryption operation:

$$[\mathrm{NOT}(S_{\rm r}(i))] \oplus K_n^1,$$

$$[\mathrm{NOT}(S_{\rm g}(i))] \oplus K_n^2,$$

$$[\mathrm{NOT}(S_{\rm b}(i))] \oplus K_n^3.$$

Operation 4 Similar to operation 1 except that K_n^4, K_n^5, and K_n^6 are used instead of K_n^1, K_n^2, and K_n^3.

Operation 5 Similar to operation 2 except that K_n^4, K_n^5, and K_n^6 are used instead of K_n^1, K_n^2, and K_n^3.

Operation 6 Similar to operation 3 except that K_n^4, K_n^5, and K_n^6 are used instead of K_n^1, K_n^2, and K_n^3.

Operation 7 No operation is made.

(iv) Repeat processes (i)–(iii) for the next 12 pixels of the image file.

(v) After encryption of a block of 16 pixels of the image file, modify the session keys a_n^j as follows:

$$a_n^j = 1 - \bmod(x_n^j + x_n^{j+2}, 1), \quad (j = 1,2,\ldots,8). \quad (7)$$

After modifying the secret key in the above manner, repeat steps (i)–(iv) until the entire image file is exhausted.

3. Chosen plaintext attack

When analyzing a cryptosystem, the general assumption is that the cryptanalyst knows everything about the cryptosystem, such as the design and working mechanism, except the secret key. An attack of a cryptosystem means that cryptanalyst can obtain the plaintext without the key. Traditionally, there are four classical types of attack. (i) Cipher text only: the cryptanalyst only possesses a collection of cipher texts. (ii) Known cipher text: the attacker has some plaintext/cipher-text pairs. (iii) Chosen plaintext: the attacker can choose arbitrary plaintexts and have the corresponding cipher texts. (iv) Chosen cipher text: the cryptanalyst can choose an arbitrary cipher text and have the corresponding plaintexts.

Any cryptosystem which cannot resist any of the above four attacks is insecure. Though the encryption scheme under study has fast encryption speed, it has two fatal drawbacks. (i) The key-stream generated by the CML remains unchanged when encrypting an image. (ii) The encryption operations selected from the eight kinds of operation when changing the pixel values remain the same. Based on these two points, we can conduct the chosen plaintext attack. First, we must say that the value of v should be 8 in the encryption scheme under study since each component is represented by an 8-bit value. Checking the eight kinds of operations carefully, we find that the encryption function at operation 0 can be replaced by

$$S_{\rm r}(i) = D_{\rm r}(i) \oplus k_1,$$

$$S_{\rm g}(i) = D_{\rm g}(i) \oplus k_2,$$

$$S_{\rm b}(i) = D_{\rm b}(i) \oplus k_3, \quad (8)$$

where $k_1 = k_2 = k_3 = 255$. Similarly, the encryption function at operation 3 can be replaced by

$$S_{\rm r}(i) = D_{\rm r}(i) \oplus k_1,$$

$$S_{\rm g}(i) = D_{\rm g}(i) \oplus k_2,$$
$$S_{\rm b}(i) = D_{\rm b}(i) \oplus k_3, \tag{9}$$

where $k_1 = K_n^1 \oplus 255$, $k_2 = K_n^2 \oplus 255$, and $k_3 = K_n^3 \oplus 255$.

The encryption functions at operations 1, 4, 6, and 7 can also be replaced by Eq. (8), but the values of k_1, k_2, and k_3 are different. The encryption function at operations 2 and 5 can be replaced by

$$S_{\rm r}(i) = (D_{\rm r}(i) + k_1) \bmod (2^8),$$
$$S_{\rm g}(i) = (D_{\rm g}(i) + k_2) \bmod (2^8),$$
$$S_{\rm b}(i) = (D_{\rm b}(i) + k_3) \bmod (2^8). \tag{10}$$

The values of k_1, k_2, and k_3 are decided by the operation group number. Thus, the eight kinds of operations can be divided into two classes. The equivalent key stream is k_1, k_2, and k_3 used to encrypt all the pixels. To recover the plaintext from cipher text, we just need to obtain the k_1, k_2, and k_3 sequence and the operation class for any pixel, since the two operation classes are both reversible.

3.1. Extracting the equivalent key stream

Choose a plaintext image P_0 whose pixel components are all 0. The corresponding cipher image is C_0. According to Eqs. (8) and (10), we can see that the three component values of any pixel in C_0 are just the values of k_1, k_2, and k_3 used to encrypt this pixel. In short, we obtain the equivalent key stream.

3.2. Deciding the operation class

We choose plaintext/cipher-text pairs P_j and C_j ($j = 1, 2, \ldots, 7$). The three components of any pixel in P_j are all 2^{j-1}. Then, we can assert that the j-th pixel can be thought to be encrypted by Eq. (8) if equation (11) holds. Otherwise, it can be thought to be encrypted by Eq. (10).

$$P_j^{\rm r}(s,t) = C_j^{\rm r}(s,t) \oplus C_0^{\rm r}(s,t), (j = 1, 2, \ldots, 7). \tag{11}$$

Here, $C_j^{\rm r}(s,t)$ represents the R component of the pixel at s-th row and r-th column in C_j, and $P_j^{\rm r}(s,t)$ represents the R component of the pixel at s-th row and r-th column in P_j. The assertion can be proved as follows.

If equation (11) does not hold, it can be easily seen that the pixel must be encrypted by Eq. (10). Now suppose that equation (11) holds, but the pixel is encrypted by Eq. (10), then we can obtain the following results. Since the pixel is encrypted by Eq. (10), equation (11) can be changed into

$$P_j^{\rm r}(s,t) = ((P_j^{\rm r}(s,t) + k_1) \bmod (2^8)) \oplus k_1,$$
$$(j = 1, 2, \ldots, 7). \tag{12}$$

Express k_1 in binary mode

$$k_1 = k_1^8 k_1^7 k_1^6 k_1^5 k_1^4 k_1^3 k_1^2 k_1^1. \tag{13}$$

Let j= 1 in Eq. (12), we have

$$1 = ((1 + k_1) \bmod (2^8)) \oplus k_1. \tag{14}$$

If $k_1^1 = 1$ and $k_1^2 = 0$, $k_1 + 1$ can be given by

$$k_1 + 1 = k_1^8 k_1^7 k_1^6 k_1^5 k_1^4 k_1^3 10, \tag{15}$$

then $((1 + k_1) \bmod (2^8)) \oplus k_1 = 3 \neq 1$. When $k_1^2 = 1$, $k_1 + 1$ can be represented by

$$(k_1 + 1) \bmod (2^8) = k_{11}^8 k_{11}^7 k_{11}^6 k_{11}^5 k_{11}^4 k_{11}^3 00. \tag{16}$$

Then, $((1 + k_1) \bmod (2^8)) \oplus k_1 = k_{111}^8 k_{111}^7 k_{111}^6 k_{111}^5 k_{111}^4 k_{111}^3 11 \neq 1$. Hence, we let $k_1^1 = 0$. Let $j = 2, 3, \ldots, 7$ in Eq. (12), we have

$$k_1^2 = k_1^3 = k_1^4 = k_1^5 = k_1^6 = k_1^7 = 0. \tag{17}$$

Then, $k_1 = 0$ or $k_1 = 128$. However, in these two cases, equation (10) can be replaced by Eq. (8). The assertion holds.

At last, for any cipher image, we can obtain the plaintext image using the following method. If equation (11) holds, then

$$P^{\rm r}(s,t) = C^{\rm r}(s,t) \oplus C_0^{\rm r}(s,t),$$
$$P^{\rm g}(s,t) = C^{\rm g}(s,t) \oplus C_0^{\rm g}(s,t),$$
$$P^{\rm b}(s,t) = C^{\rm b}(s,t) \oplus C_0^{\rm b}(s,t). \tag{18}$$

Otherwise,

$$P^{\rm r}(s,t) = (C^{\rm r}(s,t) + 256 - C_0^{\rm r}(s,t)) \bmod (256), \tag{19}$$
$$P^{\rm g}(s,t) = (C^{\rm g}(s,t) + 256 - C_0^{\rm g}(s,t)) \bmod (256), \tag{20}$$
$$P^{\rm b}(s,t) = (C^{\rm b}(s,t) + 256 - C_0^{\rm b}(s,t)) \bmod (256). \tag{21}$$

4. Experimental results

We encrypt the images of Lena.bmp and Baboon.bmp with size of 512×512 using the method proposed in Ref. [17], and then break them using our chosen plaintext attack described above. We run this process by Microsoft Visual C++6.0 on computer with 3-GHz CPU, 512-MB memory, and Microsoft Windows XP operation system. The keys we choose are:

$$a_1 = 0.234567,\ a_2 = 0.334567,\ a_3 = 0.814567,$$
$$a_4 = 0.512345,\ a_5 = 0.123456,\ a_6 = 0.234567,$$
$$a_7 = 0.4534589,\ a_8 = 0.654321,$$
$$x_0^1 = x_0^2 = x_0^3 = x_0^4 = x_0^5 = x_0^6 = x_0^7 = x_0^8 = 0.3456789.$$

At the beginning, we iterate CML 200 times to avoid transient effect. The experimental results are shown in Fig. 1. We can see that the recovered images are identical with the original ones, which implies that the original algorithm is not suitable to be used in image encryption system with high security level.

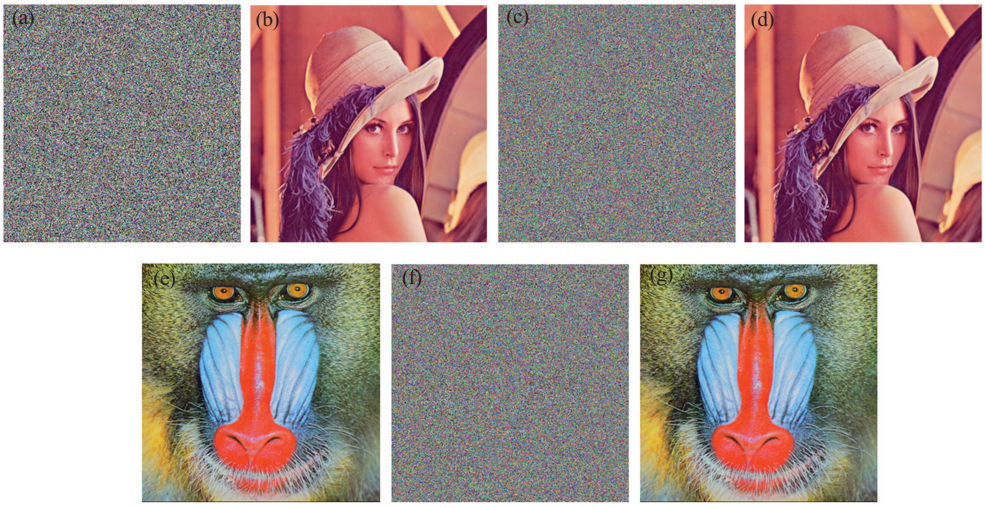


Fig. 1. (color online) Experimental attack results. (a) Equivalent key-stream image; (b) original image; (c) cipher image; (d) recovered image; (e) original image; (f) cipher image; (g) recovered image.

5. Remedy

Since the color image encryption method proposed in Ref. [17] is not secure enough, now we give a remedy to enhance it.

From the encryption process, we can see that the equivalent keys are the encryption operation selected from the eight operation groups as well as the values of k_1, k_2, and k_3. Unfortunately, both the two parts of the equivalent keys remain the same, which is the fatal drawback, and can be seen from Eqs. (5)–(10). The fact that the key stream depends on neither the plain-text image nor the cipher image is the original reason for the fatal drawback. To make the proposed image encryption scheme able to resist chosen plain-text attacks, we must associate the encryption system with the plaintext image or cipher image. To achieve the goal, in step (v) of the encryption process, we modify the session keys a_n^j using the following formula:

$$a_n^j = 1 - \mathrm{mod}\left(x_n^j + x_n^{j+2} + \frac{R+G+B}{256\times 3}, 1\right), \quad (j = 1,2,\ldots,8), \tag{22}$$

instead of Eq. (7). The other encryption steps remain unchanged. Here, R, G, and B are the three color components of the previous cipher image pixel.

In this way, we do not change the frame of the scheme proposed in Ref. [17], but different state variables will be generated when encrypting different images, leading to different sequences of k_1, k_2, and k_3 and different operations chosen to be used. Thus, the chosen plaintext attack proposed in this paper will be ineffective. We show the experimental results of our chosen plaintext attack on the improved encryption scheme in Fig. 2. Figures 2(a) and 2(d) are the

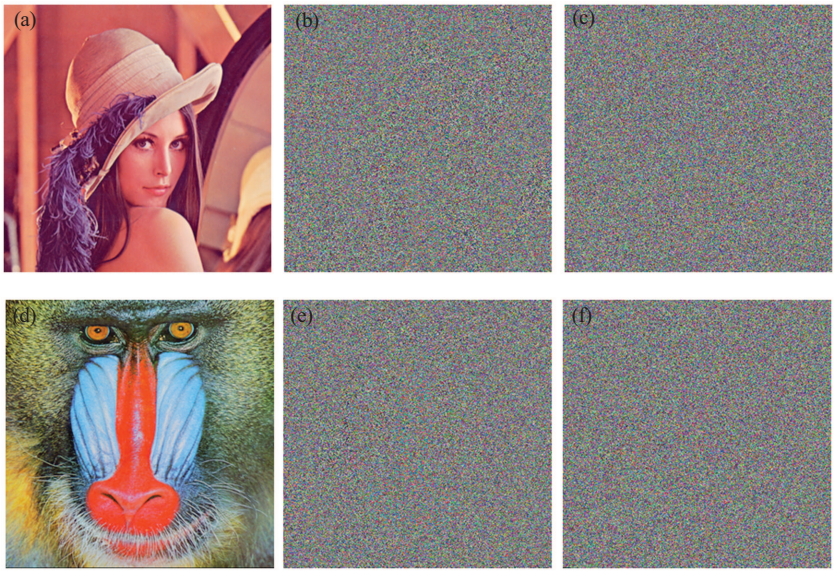


Fig. 2. (color online) Improved experimental results. (a) original image; (b) cipher image; (c) recovered image; (d) original image; (e) cipher image; (f) recovered image.

original images of lena.bmp and Baboon.bmp with size (512×512), respectively. We can see that the chosen plaintext attack is completely ineffective.

6. Conclusions

In this paper, we give a complete break of the spatiotemporal chaotic encryption system proposed for RGB images. The main weakness is that the key stream generated depends on neither the plaintext image nor the ciphered image. The operations chosen to encrypt the pixels remain unchanged too. Based on these fatal drawbacks, we choose eight pairs of plaintext/cipher-text to recover the plaintext of any cipher image. Experimental results show that our method can successfully decrypt the cipher image. Therefore, the encryption algorithm under study is not supposed to be used for image transmission. Finally, we improve the encryption scheme, and the experimental results show that the improved encryption scheme can completely resist the chosen plaintext attack we proposed in this paper.

References

[1] Pareek N K, Patidar V and Sud K K 2006 *Image Vis. Comput.* **24** 926
[2] Gao H J, Zhang Y S, Liang S Y and Li D Q 2006 *Chaos Soliton. Fract.* **29** 393
[3] Zhang G J and Liu Q 2011 *Opt. Commun.* **284** 2775
[4] Fu C, Chen J J, Zou H, Meng W H, Zhan Y F and Yu Y W 2012 *Opt. Express* **20** 2363
[5] Chen G R, Mao Y B and Chui C K 2004 *Chaos Soliton. Fract.* **21** 749
[6] Huang C K and Nien H H 2009 *Opt. Commun.* **282** 2123
[7] Guan Z H, Huang F J and Guan W J 2005 *Phys. Lett. A* **346** 153
[8] Gao T G and Chen Z Q 2008 *Phys. Lett. A* **372** 394
[9] Xu S J, Chen X B, Zhang R, Yang Y X and Guo Y C 2012 *Phys. Lett. A* **376** 1003
[10] Cokal C and Solak E 2009 *Phys. Lett. A* **373** 1357
[11] Wang K, Pei W J, Liu H Z and He Z Y 2005 *Phys. Lett. A* **343** 432
[12] Alvarez G and Li S J 2006 *Phys. Lett. A* **352** 78
[13] Wang X Y and He G X 2012 *Chin. Phys. B* **21** 060502
[14] Arroyo D, Li C Q, Li S J, Alvarez G and Halang W A 2009 *Chaos Soliton. Fract.* **41** 2613
[15] Peng J, Zhang D and Liao X F 2009 *Fundamen. Inform.* **90** 269
[16] Rhouma R and Safya B 2008 *Phys. Lett. A* **372** 5973
[17] Sun F Y and Lü Z W 2011 *Chin Phys. B* **20** 040506