Vol 17 No 11, November 2008
1674-1056/2008/17(11)/4027-06

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

An improved image encryption algorithm based on chaotic maps*

Xu Shu-Jiang(徐淑奖)[a)†], Wang Ji-Zhi(王继志)[a)], and Yang Su-Xiang(杨素香)[b)]

[a)] *Shandong Computer Science Center, Jinan* 250014, *China*

[b)] *School of Statistics and Mathematics, Shandong Economic University, Jinan* 250014, *China*

(Received 10 March 2008; revised manuscript received 20 March 2008)

Recently, two chaotic image encryption schemes have been proposed, in which shuffling the positions and changing the grey values of image pixels are combined. This paper provides the chosen plaintext attack to recover the corresponding plaintext of a given ciphertext. Furthermore, it points out that the two schemes are not sufficiently sensitive to small changes of the plaintext. Based on the given analysis, it proposes an improved algorithm which includes two rounds of substitution and one round of permutation to strengthen the overall performance.

Keywords: chaos, chaotic cryptosystem, image encryption, chosen plaintext attack
PACC: 0545

1. Introduction

Image data has strong correlations among adjacent pixels. Statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical, and also diagonal directions for both natural and computer-graphical images.[1] Therefore, most image encryption algorithms combine shuffling the pixels positions and changing the grey values of image pixels together to achieve expected cryptographic properties. In recent years, many chaotic cryptosystems have been designed to realize secure communications through public channels,[1−4] but most of them are fundamentally flawed by lack of robustness and security.[5,6] For example, a type of chaotic encryption scheme which was based on circular bit shift and XOR operations was proposed in Refs.[3, 4]. However, it was shown that there are some defects with this type of algorithm in Refs.[6, 7].

In Ref.[8], a chaotic image encryption scheme has been proposed, in which shuffling the positions and changing the grey values of image pixels are combined. In this scheme, the pixel values of a plain image are modified randomly by using the binary stream as a key stream firstly. Secondly, the modified image is encrypted again by a permutation matrix. In Ref.[9], another image encryption scheme has been proposed based on Lorenz system, in which the positions of the plain image were first shuffled and then the grey values of the shuffled image pixels were modified. Though the orders of substitution (changing the grey values of image pixels) and permutation (shuffling the positions) in the two schemes are different, they both have one round of substitution and one round of permutation and the grey values are only XOR-ed with the obtained random numbers in the substitution process. That is to say the key ideas of them are the same, so we can regard these two algorithms as one type of image encryption scheme.

In Section 4 of Ref.[9], the authors have claimed that the image scheme is secure enough even against statistical analysis. However, only with a plain-image whose grey values of image pixels are all zero, the shuffled image can be obtained by the known/chosen plaintext attack. According to Ref.[10], only shuffling the positions of the plain-image, an image encryption scheme is vulnerable to the statistical analysis. Therefore, algorithm in Ref.[9] is not as secure as the authors have declared. In fact, the two algorithms are all insecure against chosen plaintext attack. In this paper, we provide a chosen-plaintext attack to recover the corresponding plain-image of a given cipher-image. Furthermore, we pointed out that this type of scheme has low sensitivity of encryption to plaintext and show the deep reasons for the loophole. Finally, an improved scheme is proposed to strengthen the overall performance of the focused type of chaotic image encryption

*Project supported by the Natural Science Foundation of Shandong Province, China (Grant No Y2007G43).
†Corresponding author. E-mail: xushj@keylab.net

scheme.

The rest of the paper is organized as follows: Section 2 gives a brief introduction to the two original image encryption algorithms. Section 3 gives the main cryptanalytic results about chosen plaintext attack and other defects of this type of image encryption scheme. Section 4 proposes the improved scheme. Section 5 shows the experimental result by the improved encryption scheme. Finally, Section 6 concludes the work.

2. The two original chaotic image encryption algorithms

2.1. The image encryption scheme based on logistic map

This encryption scheme combined the spatial-domain encryption of digital images and the traditional stream ciphers technology. Instead of encrypting an image in a chaotic signal directly, the encryption scheme is composed of two chaotic systems. One creates a binary stream and the other creates a permutation matrix $\boldsymbol{P}$. First, the pixel values of the plain image are modified randomly using the binary stream by the traditional stream ciphers technology, namely bit-wise XOR operation. Then the modified image is encrypted again by the permutation matrix $\boldsymbol{P}$.

The basic Logistic-map which is adopted in this scheme is formulated as:

$$f(x) = \mu x(1-x), \tag{1}$$

where $x \in (0, 1)$. The parameter μ and the initial value x_0 can be adopted as the system key (μ, x_0).

Suppose there exist an image plaintext $f(i, j)$, and the key $k(k_1; k_2) = k(\mu^1, x_0^1; \mu^2, x_0^2)$, where the sub-keys $k_1 = (\mu^1, x_0^1)$, $k_2 = (\mu^2, x_0^2)$ are the initial conditions of two chaotic systems, respectively. This scheme of encrypting image consists of five steps:

(1) Generate a chaotic sequence using the sub-key k_1 as the initial condition of the first chaotic system.

(2) Transform the chaotic sequence into a binary stream by a threshold function.

(3) Modify pixel values of the plain image $f(i, j)$ using the binary stream a_{ij} as a key stream and get the image $f'(i, j)$. The performing operation is bit-wise XOR, i.e. $f'(i, j) = f(i, j) \oplus a_{ij}$, where $\oplus$ is the XOR operator.

(4) Construct a permutation matrix $\boldsymbol{P}$ using the sub-key k_2 as the initial condition of the second chaotic system.

(5) Encrypt the image $f'(i, j)$ by permutation matrix $\boldsymbol{P}$ and get the encrypted image $f''(i, j)$. Suppose that the permuted pixel position of the pixel (i, j) is (i', j'), hence $f''(i', j') = f'(i, j) = f(i, j) \oplus a_{ij}$.

2.2. The image encryption scheme based on Lorenz system

This image encryption scheme is based on a 3-D Lorenz system:

$$\begin{cases} \dot{x} = \sigma(y - z), \\ \dot{y} = rx - xz - y, \\ \dot{z} = xy - bz. \end{cases} \tag{2}$$

The control parameters are σ=10, r=28, b=8/3. The initial parameters x_0, y_0, z_0 can be chosen as the secret key.

The key idea of this scheme is getting x, y, z analogue sequences from Lorenz equations, and then the three sequences are preprocessed and quantified. The x and y sequences are used for position permutation and z sequence is used for greyscale substitution.

Assume that image size is $M \times N$, the algorithm is described as follows.

(1) Select a random $\{x_0, y_0, z_0\}$ as initial parameter of Lorenz equations, calculate enough step k and use $\{x_k, y_k, z_k\}$ as the key.

(2) Use $\{x_k, y_k, z_k\}$ as initial parameter of Lorenz system to get x, y, z analogue sequence, and preprocess these sequences, thus get three chaotic analogue sequences with good stochastic properties.

(3) Quantify the pre-process x, y analogue sequence to integer range $x_i \in [0, M-1]$, $y_i \in [0, N-1]$ and z analogue sequence to integer range $z_i \in [0, 255]$, generating an encryption matrix:

$$\begin{bmatrix} x_0, y_0, z_0 & x_0, y_1, z_1 & \cdots & x_0, y_{n-1}, z_{n-1} \\ x_1, y_0, z_n & x_1, y_1, z_{n+1} & \cdots & x_1, y_{n-1}, z_{2n-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m-1}, y_0, z_{n(m-1)} & x_{m-1}, y_1, z_{n(m-1)+1} & \cdots & x_{m-1}, y_{n-1}, z_{mn-1} \end{bmatrix}.$$

(4) Encrypt the image as following rules: for each pixel $(p_i,\ p_j)$ in plain image, move it to the place where the corresponding element (x_i, y_i) in encryption matrix appoints, and then do XOR operation on its greyscale with corresponding z_i, accomplish greyscale substitution.

3. Cryptanalysis

In this section, we present a chosen plaintext attack to recover the corresponding plaintext of a given ciphertext, and point out that this type of image encryption has low sensitivity of encryption to the small change of the plaintext.

3.1. Low sensitivity of encryption to the small change of the plaintext

As it can be seen from the above section, this type of encryption scheme has no relation to the input plaintext symbols or the output ciphertext symbols. Each of the two schemes has two processes: substitution and permutation. In fact, only the substitution operation changes the grey values $f(i, j)$ of image pixel $(i,\ j)$; the permutation operation merely permutes a pixel from one position $(i,\ j)$ to another position $(i',\ j')$. Therefore, one bit change of the plaintext $f(i,\ j)$ will cause only one pixel's grey value $f''(i, j)$ change of the corresponding ciphertext. As a result, the two encryption algorithms are not sufficiently sensitive to small changes of the plaintext.

3.2. Chosen plaintext attack

The weakness described in the above section is useful for a chosen plaintext attack. By this weakness, the chosen plaintext attack will be given for this type of encryption scheme in this subsection.

We show the cryptanalysis of a given permutation scheme first. If enough couples of plaintext and its corresponding ciphertext are known, we can easily determine the relationship between the position of the plain image pixels and the permuted position of them. That is to say the permutation process is easily analysed.

To facilitate the cryptanalysis, we make the following assumptions:

(1) The plain image and cipher image are all 256 grey-scale BMP image of size $M \times N$.

(2) The grey value of pixel $(i,\ j)$ before permutation and after permutation are $f(i,\ j)$ and $f'(i,\ j)$ respectively.

(3) The pixel $(i,\ j)$ is permuted to the pixel position $(i',\ j')$ after shuffling the pixels position, i.e., $f(i, j) = f'(i, j)$.

The detailed cryptanalysis for the given permutation scheme is as follows:

(1) Choose a 256 grey-scale plain image P' of size $M \times N$ whose grey values are all zero, and encrypt P' by the given permutation scheme, then obtain the permuted image M'.

(2) Choose a 256 grey-scale plain image P^{kl} of size $M \times N$ whose grey values are shown as follows: $f(k,\ l)$=1, $f(i,\ j)$=0 $(i = 0,\ 1,\ \ldots, M-1;\ j$=0, 1, $\ldots, N-1$; and $(i,\ j) \neq (k,\ l))$. Encrypt P^{kl} by the given permutation scheme, and then obtain the corresponding permuted image M^{kl}. Compare M^{kl} with M', there will be only one pixel different between them. Mark the different pixel position as $(k',\ l')$. That is to say the grey value $f(k,\ l)$ is permuted from pixel position $(k,\ l)$ to $(k',\ l')$ in the shuffled image M^{kl}, i.e. $f(k,\ l) = f'(k',\ l')$.

(3) Let $(k,\ l)$ as (0, 0), (0, 1), ..., (0, N-1), (1, 0), ..., $(M-2,\ N-1)$, $(M-1,\ 0)$, ..., $(M-1,\ N-3)$, $(M-1,\ N-2)$ respectively, and mark all the $(k,\ l)$ and $(k',\ l')$ into a table $\boldsymbol{T}$, then the permutation matrix can be obtained. Note that the permuted position of the rest pixel $(M-1,\ N-1)$ can be automatically confirmed.

According to Section 3.1, one bit change of the plaintext will cause only one pixel's grey value of the corresponding ciphertext change. Therefore, by the above cryptanalysis method, we can determine the corresponding position in the cipher image of every plain image pixel; mark them into a permutation matrix $\boldsymbol{T}$. Using the same secrete key, we can easily obtain the corresponding position in the cipher/plain image of each pixel in plain/cipher image from the matrix $\boldsymbol{T}$.

The whole cryptanalysis is as follows:

(1) Choose a 256 grey-scale plain image P' of size $M \times N$ whose grey values are all zero, and encrypt P' by the type of encryption scheme, then obtain the cipher image C'. For algorithm in Ref.[8], the ciphertext C' is a permuted binary stream, the original form of it is used to XOR with the plaintext. For algorithm in Ref.[9], the ciphertext C' just is the binary stream which is used to XOR with the permuted plaintext.

(2) Using the above method, we generate the per-

mutation matrix $\boldsymbol{T}$.

(3) Give a cipher image C which is encrypted by the same secret key as above. Using the given ciphertext C to do XOR operation with the obtained binary stream C', and do inverse permutation operation for it by the permutation matrix $\boldsymbol{T}$, we can recover the plaintext P corresponding to the given cipher image C.

4. Improved image encryption scheme

In above section, two defects about this type of image encryption scheme are pointed out: 1) low sensitivity of encryption to the small change of plaintexts; 2) inability of resisting the chosen plaintext attack. To avoid the above defects, an improved scheme is proposed in this section.

Similarly to the scheme in Ref.[8], two different chaotic maps are used in the improved scheme, one creates a binary stream for the substitution, and another creates a permutation matrix. To anti-attack and to let this scheme more sensitive to the small change of the plaintext, three measures are adopted in the improved scheme. 1) The plaintext is first encrypted by two rounds of substitution operation, and then is encrypted by a round of permutation operation. 2) The ciphertext feedback method is adopted. The previous ciphertext is adopted as the feedback to the current plaintext in the substitution process, so as to dissipate the effect of one single plaintext bit to more ciphertext bites. Especially, the last encrypted plaintext in the first round substitution is chosen as the initial feedback to the second rounds of substitution. 3) In the substitution process, we will give a small perturbation to a control parameter of the chaotic system which is used in the substitution process. Moreover, the control parameter of the chaotic system which is used in the second round of substitution is also obtained from the first round of substitution.

In the substitution process, the Chen's chaotic system (CCS)

$$\begin{cases} \dot{x} = \alpha(y - x), \\ \dot{y} = (\gamma - \alpha)x - xz + \gamma y, \\ \dot{z} = xy - \beta z, \end{cases} \tag{3}$$

is used to generate the binary stream for the substitution, where α, β and γ are control parameters. When α=35, β=3, γ ∈[20,28.4], the system enters chaotic domain which is shown in Fig.1.

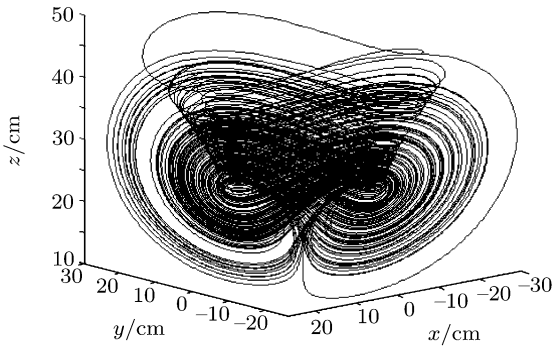


Fig.1. 3-D Chen's chaotic system.

The dynamical property of the CCS is more complicated than the Lorenz chaotic system (2). Therefore this feature is very useful in secure communications. The fourth order Runge–Kutta algorithm is used to iterate CCS. The step of the Runge–Kutta algorithm h and the initial value x_0, y_0 and z_0 all can be considered as secret key. Suppose that x is a double-point value, we can quantify it into an integer number

$$a(x) = \mathrm{mod}(10^{14} \cdot (\mathrm{abs}(x) - \lfloor \mathrm{abs}(x) \rfloor),\ 256), \tag{4}$$

where mod(x,y) returns the remainder after division, abs(x) returns an absolute value of x. $\lfloor x \rfloor$ presents getting the largest integer that is less than or equal to x. Iterate CCS consecutively, we can obtain three analogue sequences of x_i, y_i and z_i. We quantify the analogue sequences of x_i, y_i, z_i into binary stream by the above method and use them in substitution process.

In the permutation process, a chaotic sequence is generated by the logistic map Eq.(1) and then we use the chaotic sequence to generate an asc-ergodic matrix which was first proposed in Ref.[11] as a permutation matrix. Suppose the plain image is a 256 grey-scale BMP image of size $M \times N$, the detailed improved scheme is as follows:

(1) To avoid the transient effect, iterate CCS N_0 times and get the starting-point (x_0, y_0, z_0) from the last time iteration.

(2) Arrange the plain image by the order from left to right and then top to bottom, we can obtain a set $P = p_0,\ p_1,\ \ldots,\ p_{MN-1}$. Divide it into subsequences P_j of length 32 bytes: $P_j = p_{32j},\ p_{32j+1},\ \cdots, p_{32(j+1)-1}$.

(3) According to the substitution scheme which is shown in Fig.2, iterate CCS 11 times, we can ob-

tain the random number sequences a_0, a_1, ..., a_{32} by Eq.(4), and then encrypt the plaintext block P_j as follows:

$$c^1_{32j+i} = p_{32j+i} \oplus a_i \oplus c^1_{32j+i-1}, \tag{5}$$

where i=0, 1, ..., 31. Then the encrypted block $C^1_j = c^1_{32j}$, c^1_{32j+1}, ..., $c^1_{32(j+1)-1}$ is obtained. (c^1_{-1} is the initial feedback.) Note that $d_j = a_{32} \oplus c^1_{32(j+1)-1}$.

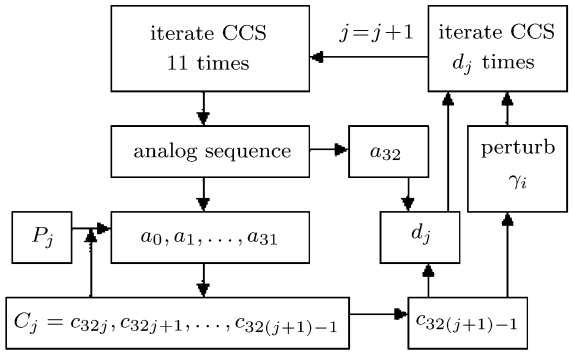


Fig.2. Substitution scheme.

(4) If all the plaintext has already been encrypted, then the encrypted text $C^1 = C^1_0, C^1_1, \ldots, C^1_{MN-1}$ is obtained, and turn to step 5. Otherwise, perturb the control parameter γ_j of CCS according to the perturbing scheme which is shown in Fig.3, iterate CCS d_j times and then go to step 2.

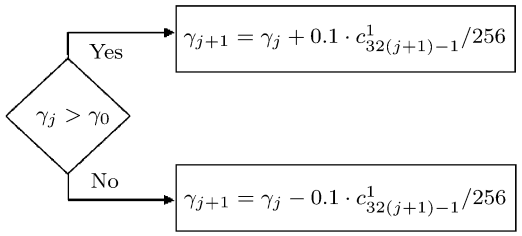


Fig.3. Perturbing scheme for parameter of CCS.

(5) In Fig.3, let j=MN-1, we generate the parameter γ'_0 of CCS and choose the initial feedback as $c^2_{-1} = c^1_{MN-1}$. With another group of key, do the substitution which is shown in Fig.2 again for the encrypted text C^1. Then the encrypted text C^2 can be gained.

(6) Iterate the logistic map N_1 times so as to avoid the transient effect, and then construct a permutation matrix $\boldsymbol{A}$.

(7) Encrypt the text C^2 by permutation matrix $\boldsymbol{A}$, and then the cipher image C can be obtained.

In the improved scheme, the control parameter γ'_0 and the initial feedback c^2_{-1} in the second round of substitution are also considered as two elements of the ciphertext, that is to say the ciphertext is (C, γ'_0, c^2_{-1}). The decryption scheme is just the inverse process of the encryption scheme.

5. Experimental result

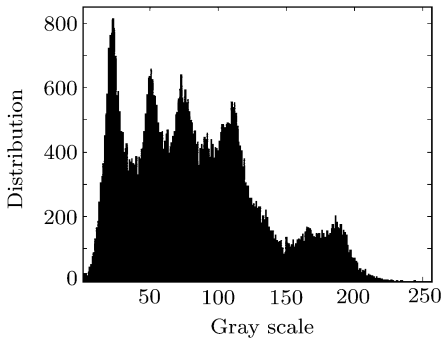
This section gives an example of the improved scheme. Figure 4 shows the experimental results with Lena BMP image by the proposed scheme. Figure 4(a) is the 256 grey-scale Lena plain-image of size 256×256. Figure 4(b) is the corresponding encrypted image with the encryption key (γ_0, x_0, y_0, z_0, N_0, c^1_{-1})=(28, −10.058, 0.368, 37.368, 200, 126) in the first round of substitution but (x_0, y_0, z_0, N_0)=(28, –10.058, 0.368, 37.3680000001, 200) in the second round of substitution. As we can see from Fig.4(b), the encrypted image is rough-and-tumble and unknowable, so the diffusion and confusion properties are confirmed.



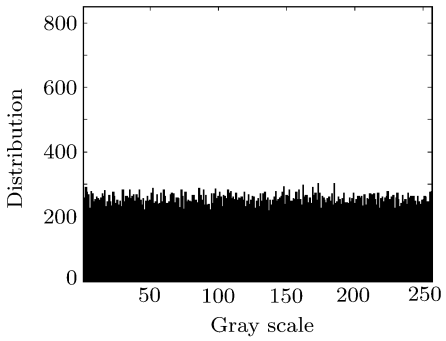
(a) plain-image (b) cipher-image

Fig.4. Experimental result.

Considering the statistical analysis of Lena image and its encrypted image, we show the grey-scale histograms of them in Fig.5. From Fig.5(b), we can see that the greyscale distribution of encrypted image has good balance property, which is strong against known plaintext attack.



(a) histogram of plain-image



(b) histogram of cipher-image

Fig.5. Greyscale histogram.

To test the influence of one-pixel change on the whole image encrypted, two common measures, namely, number of pixels change rate (NPCR) and unified average changing intensity (UACI) were used in Ref.[12]. In the improved scheme, a higher performance such as NPCR $> 99.5\%$ and UACI > 0.331 can be achieved by the three measures which are presented in the above section. Moreover, the improved scheme only has two rounds of substitution and one round of permutation.

It is well known that the information entropy is defined to express the degree of uncertainties in the system. The information entropy can be expressed as:

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\log_2[P(m_i)], \qquad (5)$$

where $P(m_i)$ is the emergence probability of m_i. If every symbol has an equal probability, i.e., $m = \{m_0,\ m_1,\ \ldots,\ m_{2^8-1}\}$ and $P(m_i) = 1/2^8$ (i=0, 1, ..., 255), then the entropy is $H(m)$=8, which corresponds to a random source. Actually, a practical information source seldom generates random messages. Usually, its information entropy is less diverse to the ideal case. To design a good cryptosystem, however, the entropy which is close to the ideal case is expected. Here, the information entropy is $H(m)$=7.99732 which is very close to the ideal one.

6. Conclusion

This paper deeply studies a type of chaotic image encryption scheme based on permutation and one round of XOR operations. Its two defects are pointed out. As is shown in the cryptanalysis, this type of chaotic image encryption scheme is not secure enough against the chosen plaintext attack and not sensitive enough to small changes in plaintext. Based on the analysis, we propose an improved scheme to overcome the weaknesses and to strengthen the overall performance of this type of chaotic image encryption scheme.

References

[1] Guan Z H, Huang F and Guan W 2005 *Phys. Lett.* A **346** 153
[2] Baptista M S 1998 *Phys. Lett.* A **240** 50
[3] Xiang T, Liao X F, Tang G P, Chen Y K and Wong W 2006 *Phys. Lett.* A **349** 109
[4] Yu W W and Cao J D 2006 *Phys. Lett.* A **356** 333
[5] Alvarez G, Montoya F, Romera M and Pastor G 2003 *Phys. Lett.* A **311** 172
[6] Li C Q, Li S J, Alvarez G, Chen G R and Lo K T 2007 *Phys. Lett.* A **369** 23
[7] Xu S J and Wang J Z 2008 *Acta Phys. Sin.* **57** 37 (in Chinese)
[8] Xiao H P and Zhang G J 2006 *Proc. Fifth Int. Conf. on Machine Learning and Cybernetics* **5** 2707
[9] Fu C, Zhang Z C and Cao Y Y 2007 *Third Int. Conf. on Natural Comput.* **3** 189
[10] Qiao L and Nahrstedt K 1998 *Int. J. Computers and Graphics* **22** 437
[11] Li C M and Hong L X 2007 *IEEE Int. Workshop on Anti-counterfeiting, Security, Identification* p237
[12] Chen G R, Mao Y B and Chui C K 2004 *Chaos, Solitons and Fractals* **21** 749