A New Multi-chaos Based Image Encryption Algorithm

Nan Lin, Xiaofeng Guo, Ping Xu, and Yuqin Wang

Zhengzhou Institute of Information Science and Technology Zhengzhou, China
linnan_2011@126.com

Abstract. A new multi-chaos based image encryption algorithm is proposed in this paper. Four chaotic mappings are involved in the encryption algorithm. The renew function of CML mapping is determined by the status of Chebyshev mapping. The encryption of pixel value and the permutation of pixel position are obtained with CML and Chebyshev iteration. It is from analysis and experimental results that the encryption algorithm possesses higher security.

Keywords: Multi-Chaos, Chebyshev Mapping, Cml, Image Encryption.

1 Introduction

With the rapid development of Internet and multimedia data processing, protection of multimedia data against illegal copying and distribution has become extremely important. To meet this requirement, many new encryption algorithms have been proposed. The chaos-based cryptographic algorithm have suggested some new ways to develop efficient multimedia encryption schemes[1-10], which have been motivated by the chaotic properties(pseudorandom property, non-periodicity and topological transitivity and extreme sensitivity to initial conditions and parameters).

In [3] and [4], the positions of image pixels are permutated by an image total shuffling matrix, and the pixel values of the permuted image are encrypted by a hyper-chaotic system. The security weakness of the algorithm in [3] is analyzed in [5,6], and the algorithm is broken by two attacks proposed in [5,6].

In this paper, a new image encryption algorithm is proposed to solve the problem of the algorithm in [3]. In the new image encryption algorithm, four chaotic systems are applied. The partial renew function of CML is chosen according to the state of Chebyshev mapping. Then the encryption of the positions and values of the plain image are performed based on CML and Chebyshev iterations. Analysis and experimental results show the security of the new image encryption algorithm.

2 Chaotic Systems

In the new encryption algorithm, four chaotic systems are applied, which are Chebyshev mapping, Sin mapping, Cubic mapping and 2D coupled map lattice (CML). The functions of them are as follows:

Chebyshev mapping:

$$x_{n+1} = \cos(a \cos^{-1} x_n), \tag{1}$$

Z. Du (Ed.): Intelligence Computation and Evolutionary Computation, AISC 180, pp. 215–221.
springerlink.com

Sin mapping:

$$x_{n+1} = b\sin(\pi x_n), \tag{2}$$

Cubic mapping:

$$x_{n+1} = \lambda x_n(1-x_n^2), \tag{3}$$

CML:

$$y_{n+1}^{i,j} = (1-\varepsilon)f(y_n^{i,j}) + \frac{1}{2}\varepsilon[f(y_n^{i+1,j}) + f(y_n^{i,j+1})] \tag{4}$$

where 2≤a, -1≤xn≤1, b=0.99, 0<xn<1, λ=2.59, 0<xn<1. $0<\varepsilon<1$, $0<y_n^{i,j}<1$, $0\le x\le 1$, $f(x)$ is the partial renew function of CML. The periodic boundary conditions of CML are $y_n^{i+H,j} = y_n^{i,j}$, $y_n^{i,j+W} = y_n^{i,j+1}$.

In this algorithm, the partial renew function $f(x)$ of CML is determined by Chebyshev mapping, Sin mapping and Cubic mapping. Sin mapping or Cubic mapping is chosen according to the state of Chebyshev mapping as the partial renew function $f(x)$, the detailed chosen method is shown in the following formula:

$$f(x_n) = \begin{cases} b\sin(\pi x_n) & if\ x_{chebyshev} < 0.5 \\ \lambda x_n(1-x_n^2) & if\ x_{chebyshev} \ge 0.5 \end{cases}, \tag{5}$$

Where $x_{chebyshev}$ is the state of Chebyshev mapping.

3 Multi-chaos Based Image Encryption Algorithm

Assume that a plian image is $\boldsymbol{P} = (p_{i,j})_{N\times N}$, where $p_{i,j} \in \mathcal{P}$, $\mathcal{P} = \{0,1,2,\cdots,255\}$, $\mathcal{N} = \{1,2,\cdots,N\}$. Let $\boldsymbol{A} = (a_{i,j})_{N\times N}$ denote the DCT coefficient matrix of plaintext after pre-coding (for example block partitioning), DCT transformation and quantization. Two positive integer M_1, M_2 ($M_1, M_2 \le 1024$) are chosen as the generation parameters of the keystream, which are also part of the secret key.

Before encryption, the DCT coefficient matrix is divided into $k-1$ blocks of size $T\times T$, then $\boldsymbol{A} = \{A^t\}_{t=1}^{k-1}$, where $A^t = (a_{i,j}^t)_{T\times T}$, $t = 0,1,2\cdots,k-1$, $i, j = 0,1,2\cdots,T-1$. For the t th block $A^t = (a_{i,j}^t)_{T\times T}$, $t = 0,1,2\cdots,k-1$, the encryption procedure are detailed as follows:

1. Pre-iterate Chebyshev mapping by initial value x_0 for n_0 times, and denote the new state of Chebyshev mapping by x_0;
2. Interate Chebyshev mapping by x_0, and denote the state by x_t; then determine the partial renew function $f(x)$ of CML with x_t and Eq.错误！未找到引用源。;
3. Iterate CML with the row initial vector $IV = (x_{0,1}, x_{0,2}, \cdots, x_{0,T})$ and $f(x)$, and denote the obtained $T\times T$ state matrix by $R = (r_{i,j})_{T\times T}$;

4. Generate the matrix $S=(s_{i,j})_{T\times T}$ which is the keystream of this algorithm by quantization $R=(r_{i,j})_{T\times T}$ with the following equation:

$$s_{i,j}=\begin{cases}\left\lfloor r_{i,j}\times 2^{M_1}\right\rfloor \bmod M_1 & i=j=0\\ \left\lfloor r_{i,j}\times 2^{M_2}\right\rfloor \bmod M_2 & else\end{cases}. \tag{6}$$

5. Encrypt $A^t=(a^t_{i,j})_{T\times T}$ by the matrix $S=(s_{i,j})_{T\times T}$ with

$$c^t_{i,j}=\begin{cases}a^t_{i,j}\oplus s_{i,j} & i=j=0\\ sign(a^t_{i,j})[|a^t_{i,j}|\oplus s_{i,j}] & else\end{cases}, \tag{7}$$

and the cipher block $C^t=(c^t_{i,j})_{T\times T}$ of $A^t=(a^t_{i,j})_{T\times T}$ is obtained, where $sign(a^t_{i,j})=\begin{cases}1 & a^t_{i,j}>0\\ -1 & a^t_{i,j}\le 0\end{cases}$.

6. If $t<k-1$, then let $x_0=x_t$, go to 1, carry out 2 to 5; otherwise, continue;
7. Let $X=\{x_t\}_{t=0}^{k-1}$, rearrange sequence $\{x_0,x_1,\cdots x_{k-1}\}$ from small to large, and sequence $\{x_{r_0},x_{r_1},\cdots x_{r_{k-1}}\}$ is obtained. Obviously, there is a permutation function σ: $\sigma(i)=r_i$, which is shown as follows:

$$\begin{pmatrix}0 & 1 & 2 & \cdots & k-1\\ \sigma(0)=r_0 & \sigma(1) & \sigma(2) & \cdots & \sigma(k-1)\end{pmatrix} \tag{8}$$

8. Permute $\boldsymbol{C}=\{C^t\}_{t=1}^{k-1}$ by block with permutation function σ, and obtain the cipher image $\boldsymbol{D}=\{D^t\}_{t=1}^{k-1}$, $D^t=C^{\sigma(t)}$, that is

$$\begin{pmatrix}C^0 & C^1 & C^2 & \cdots & C^{k-1}\\ C^{\sigma(0)}=C^{r_0} & C^{\sigma(1)} & C^{\sigma(2)} & \cdots & C^{\sigma(k-1)}\end{pmatrix} \tag{9}$$

4 Decryption Algorithm

The decryption procedure is the inverse procedure of the encryption algorithm. In the decryption procedure, the sequence $X=\{x_t\}_{t=0}^{k-1}$ is first generated with Chebyshev mapping, and the inverse permutation function σ^{-1} is obtained, then the ciphertext is first inversely permuted by the inverse permutation function σ^{-1}; thirdly, the data after inverse permutation is divided into $k-1$ blocks of size $T\times T$, and finally the plaintext is obtained by decrypting the data block by block with matrix $S=(s_{i,j})_{T\times T}$ which is generated from CML.

5 Key Space Analysis

In this algorithm, the secret key is $Key=\{x_0,M_1,M_2,IV\}$, where x_0 is the initial value of Chebyshev mapping, $IV=(x_{0,1},x_{0,2},\cdots,x_{0,T})$ is the row initial value of CML. The key space of the algorithm is $K=K(x_0)\times K(IV)\times K(M_1)\times K(M_2)$. If double-precision

floating-point number of 64bit of IEEE is applied in the encryption algorithm, since x_0 and $IV = (x_{0,1}, x_{0,2}, \cdots, x_{0,T})$ can not equal to 0 and 1, then $K(x_0) = 2^{52} - 2$, $K(IV) = (2^{52} - 2)^T$. If the block size $T \times T = 8 \times 8$, and let $K(M_1) = K(M_2) = 1$ (that is M_1, M_2 are two secret constant) then the key space of this algorithm is $K = K(x_0) \times K(IV) \times K(M_1) \times K(M_2) = (2^{52} - 2) \times (2^{52} - 2)^8 \approx 2^{468}$. So the keyspace of this algorithm is considered to be large enough for practical applications.

6 Experiments

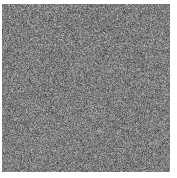
In this section the encryption and decryption experiments of a 256×256 pixel image "Lena.bmp" are performed under Matlab6.5 on a PC with 2GB RAM. In the experiments, the block size is $T \times T = 8 \times 8$, the initial value of Chebyshev mapping $x_0 = 0.123456$, the row initial value of CML is $IV = (0.152, 0.1735, 0.1653, 0.343, 0.2536, 0.635, 0.472, 0.2397)$, and the parameter $M_1 = M_2 = 1024$.

(a) Plain image (b) Cipher image

Fig. 1. Plain image and cipher image

6.1 Key Sensitivity Test

In this subsection, the key sensitivity of the algorithm is test. Plain image "Lena.bmp" is encrypted by using the test key $x_0 = 0.123456$, $M_1 = M_2 = 1024$, $IV = (0.152, 0.1735, 0.1653, 0.343, 0.2536, 0.635, 0.472, 0.2397)$, and decrypted with all the parameters unchanged except for the initial value of Chebyshev mapping $x_0 = 0.123457$. The experimental results are shown in Figure 2, where Figure 2(a) is the decrypted image with the tiny changed key, and Figure 2(b) is the decrypted image with the correct key. We can find that a slight change of the key will generate a completely different decryption result and can't get the correct plain image, that is, the encryption scheme is sensitive to the secret key.

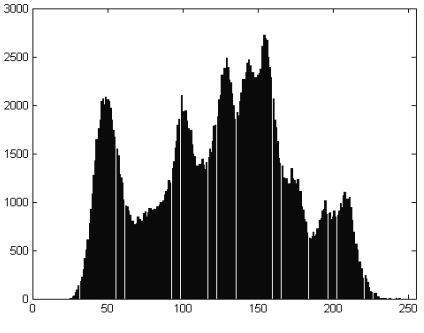


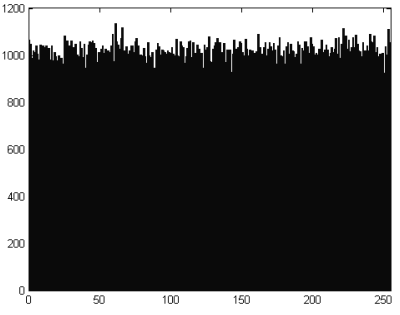

(a) decryption results with wrong key (b) decryption with correct key

Fig. 2. Key sensitivity text results

6.2 Image Statistic Characteristic

The histograms of the plain image and the cipher image are evaluated in this subsection. The histogram of image "Lena.bmp" is shown in Figure 3(a), and that of the cipher image is shown in Figure 3(b). According to the experimental results, the histogram of the cipher image is significantly different from that of the plain image and is fairly uniform.





(a) Histogram of plain image (b) Histogram of cipher image

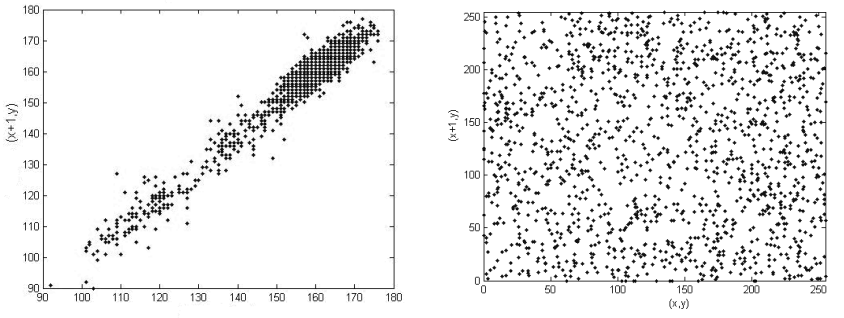
Fig. 3. Histogram of images before and after encryption

6.3 Analysis of Correlation of Two Adjacent Pixels

In this section, some simulations are carried out to test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels respectively. Firstly, 4096 pairs of two adjacent pixels are chosen randomly from the plain image and the cipher image, and the correlation distribution of two vertically adjacent pixels in the plain image and that in the cipher image is tested. The results are shown in Figure 4. Then the correlation coefficient of each pair is calculated by Eq (10). And the calculation results of correlation coefficients are shown in Table 1. We can find that the correlation of two adjacent pixels has decreased obviously, that is, the close correlation property between pixels in plain image has been removed.

$$r_{xy} = \mathrm{cov}(x, y)/(\sqrt{D(x)}\sqrt{D(y)}), \tag{9}$$

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



(a) Correlation in the plain image (b) Correlation in the cipher image

Fig. 4. Correlations of two vertically adjacent pixels in the image before and after encryption

Table 1. Correlation coefficients of two adjacent pixels in images before and after encryption

	Horizontal	Vertical	Diagonal
Plain image	0.988378	0.988778	0.983117
Cipher image	0.035188	0.046506	0.060353

7 Conclusions

A new multi-chaos based image encryption algorithm is proposed in this paper. Four chaotic mappings are involved in the encryption algorithm. The renew function of CML mapping is determined by the status of Chebyshev mapping. The encryption of pixel value and the permutation of pixel position are obtained with CML and Chebyshev iteration. It is from analysis and experimental results that the encryption algorithm possesses higher security.

References

[1] Mao, Y.B., Chen, G.: Chaos-based image encryption. In: Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics. Springer, New York (2003) (in press)

[2] Li, S., Chen, G., Zheng, X.: Chaos-based encryption for digital images and videos. In: Furht, B., Kirovski, D. (eds.) Multimedia Security Handbook, ch. 4, pp. 133–167. CRC Press (2004)

[3] Gao, T., Chen, Z.: A new image encryption algorithm based on hyper-chaos. Phys. Lett. A 372, 394–400 (2008)

[4] Gao, T., Chen, Z.: Image encryption based on a new total shuffling algorithm. Chaos, Solitons and Fractals 38, 213–220 (2008)

[5] Rhouma, R., Belghith, S.: Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Phys. Lett. A (2008) (in press), doi:10.1016/j.physleta.2008.07.057

[6] Ge, X., Liu, F., Lu, B., Yang, C.: Improvement of Rhouma's Attacks on Gao Algorithm. Physics Letters A 374, 1362–1367 (2010)
[7] Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image and Vision Computing 24(9), 926–934 (2006)
[8] Behnia, S., Akhshani, A., Mahmodi, H.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons and Fractals 35(2), 408–419 (2008)
[9] Kwok, H.S., Tang, W.K.S.: A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons and Fractals 32, 1518–1529 (2007)
[10] Arroyo, D., Li, C.Q., Li, S.J., Alvarez, G., Halang, W.A.: Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos, Solitons and Fractals (available online November 5, 2008) (corrected proof, in press)