Volume 1 No. 8, December 2011 ISSN-2223-4985
International Journal of Information and Communication Technology Research

http://www.esjournals.org

An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice

Ruisong Ye, Wei Zhou
Department of Mathematics, Shantou University
Shantou, Guangdong, 515063, P. R. China

ABSTRACT

This paper proposes a chaos-based image encryption scheme where one 2D tent map with two control parameters is utilized to generate chaotic orbits applied to scramble the pixel positions while one coupled map lattice is employed to yield random gray value sequences to change the gray values so as to enhance the security. Experimental results are carried out with detailed analysis to demonstrate that the proposed image encryption scheme possesses large key space to resist brute-force attack and possesses good statistical properties to frustrate statistical analysis attacks. Experiments are also performed to illustrate the robustness against malicious attacks like cropping, noising, JPEG compression.

Keywords: *2D tent map; coupled map lattice; chaotic system; image encryption*

1. INTRODUCTION

With the rapid developments in digital image processing and network communication, electronic publishing and wide-spread dissemination of digital multimedia data have been communicated over the Internet and wireless networks. Therefore it has become urgent to prevent them from leakages. Many applications, such as military image databases, confidential video conference, medical imaging system, online private photograph album, etc. require reliable, fast and robust secure system to store and transmit digital images. The requirements to fulfill the security needs of digital images have led to the development of effective image encryption algorithms. Digital images possess some intrinsic features, such as bulk data capacity, redundancy of data, strong correlation among adjacent pixels, being less sensitive as compared to the text data, etc. As a result, traditional encryption algorithms, such as DES, RSA [1], are thereby not suitable for practical digital image encryption due to the weakness of low-level efficiency while encrypting images. Fortunately, chaos-based image encryption algorithms have shown their superior performance. Chaos has been introduced to cryptography as its ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters are close to confusion and diffusion in cryptography. These properties make chaotic systems a potential choice for constructing cryptosystems [2,3,4].

Recently, some chaos-based image encryption algorithms are broken due to their small key spaces and weakly secure encryption mechanism [5,6]. To overcome the drawbacks such as small key space and weak security in chaos-based image encryption algorithms, many researchers turn to find some improved chaos-based cryptosystems with large key space and good diffusion mechanism [7,8,9]. In this paper, an efficient image encryption scheme based on the ergodicity of 2D tent map and coupled map lattice is proposed. Firstly, one 2D tent map with two control parameters is utilized to generate chaotic orbits applied to permute the pixel positions, then one coupled map lattice is employed to yield two random gray value sequences to change the gray values by bitxor operation so as to strengthen the security. Experimental results are carried out with detailed analysis to demonstrate that the proposed image encryption scheme possesses large key space to resist brute-force attack and possesses good statistical properties to frustrate statistical analysis attacks. The robustness against malicious attacks like cropping, noising, JPEG compression are also performed.

2. THE 2D TENT MAP

The 2D tent map $T_{a,b}:[0,1]^2 \to [0,1]^2$ is given by:

$$T_{a,b}(x)=\begin{cases}\begin{pmatrix}1/a & 0\\ 0 & 1/b\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}, & (x,y)\in[0,a]\times[0,b],\\ \begin{pmatrix}1/a & 0\\ 0 & 1/(1-b)\end{pmatrix}\begin{pmatrix}x\\ 1-y\end{pmatrix}, & (x,y)\in[0,a]\times[b,1],\\ \begin{pmatrix}1/(1-a) & 0\\ 0 & 1/b\end{pmatrix}\begin{pmatrix}1-x\\ y\end{pmatrix}, & (x,y)\in[a,1]\times[0,b],\\ \begin{pmatrix}1/(1-a) & 0\\ 0 & 1/(1-b)\end{pmatrix}\begin{pmatrix}1-x\\ 1-y\end{pmatrix}, & (x,y)\in[a,1]\times[b,1].\end{cases} \quad (1)$$

where $a,b\in(0,1)$. It is easy to show that the two Lyapunov exponents are (see [10])

$$\lambda_x = a\ln(\frac{1}{a})+(1-a)\ln(\frac{1}{1-a}),$$
$$\lambda_y = b\ln(\frac{1}{b})+(1-b)\ln(\frac{1}{1-b}), a,b\in(0,1).$$

It is obvious that λ_x, λ_y are all positive, implying that the 2D tent map is chaotic on $[0,1]^2$. A typical orbit of (x_0, y_0) derived from the dynamical system is $\{(x_k, y_k) = T_{a,b}^k(x_0, y_0), k = 0,1,\cdots\}$, which is shown in Fig.1 for $a = 0.2, b = 0.4, x_0 = 0.7, y_0 = 0.67$. The plotting orbit points fill $[0,1]^2$ as long as the orbit long enough, which indicates that the system is chaotic visually. The control parameters a, b and the initial condition x_0, y_0 can be regarded as cipher keys as the map is used to design image encryption schemes. There exist some good dynamical features in 2D tent maps, such as desirable auto-correlation and cross-correlation features demonstrated in Fig. 2.

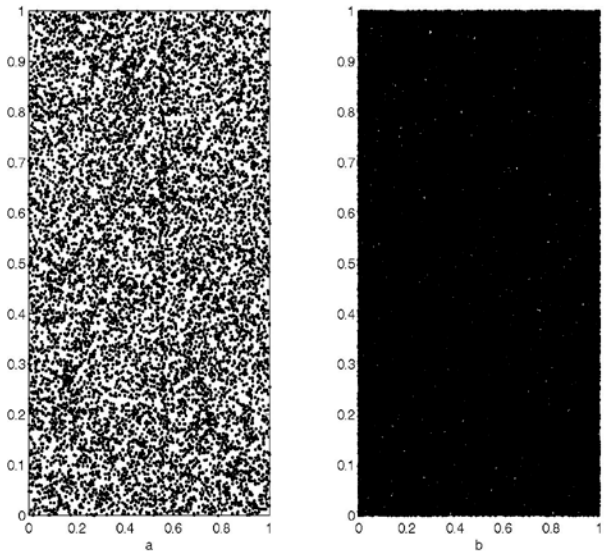

Fig. 1: The orbit ergodicity of 2D tent map. (a) plotting the beginning 10^4 orbit points, (b) plotting the beginning 10^5 orbit points

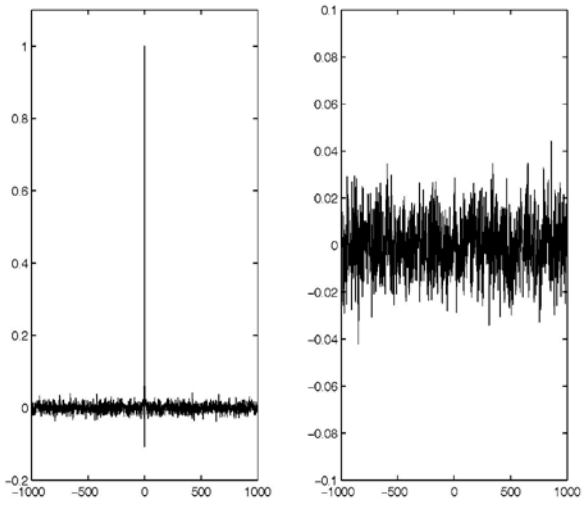

Fig. 2: The auto-correlation and corss-correlation of 2D tent map

3. THE IMAGE ENCRYPTION SCHEME BASED ON 2D TENT MAP AND COUPLED MAP LATTICE

3.1 Pixel positions permutation process

In this subsection, we propose a permutation process to confuse plain-image totally. Thanks to the chaotic nature of 2D tent map on the unit square $[0,1]^2$, one can easily get the chaotic orbit $\{(x_k, y_k), k = 0,1,\cdots\}$ of (x_0, y_0) with given control parameter a, b. Assume that the plain-image is expressed as a gray value matrix A, the height and the width of A are H and W respectively. Let $HW = H \times W$. The pixel positions permutation process is stated as follows.

Step 1: Set the values of the control parameter a, b and the initial condition x_0, y_0.

Step 2: Iterate the 2D tent map (1) to get the truncated orbit of (x_0, y_0), say $\{(x_k, y_k), k = 1,\cdots, N\}$ for a properly large integer N. Quantize $\{(x_k, y_k), k = 1,\cdots, N\}$ to get another two sequences X_n, Y_n:

$$(x_n, y_n) = T_{a,b}(x_{n-1}, y_{n-1}), n = 1,2,...,N,$$
$$X_n = \lceil x_n \times H \rceil, Y_n = \lceil y_n \times W \rceil, n = 1,2,...,N,$$

where $\lceil x \rceil$ rounds x to the nearest integer towards infinity.

Step 3: Let $(X_n, Y_n)(n = 1,..., N)$ to be the coordinates, and select those which do not repeat to form a matrix S with X_n, Y_n being its first and second column elements respectively.

Step 4: Let A to be a matrix sized $HW \times 2$, and set $A(n,1) = \left\lceil \frac{n}{W} \right\rceil$, $A(n,2) = \mathrm{mod}(n,W) + 1, n = 1,2,..., HW$,

where $\mathrm{mod}(n,W)$ is the mod function. Let the coordinates in A but not in S to form a matrix S^*.

Step 5: Apply coordinate matrix S and S^* to scramble the pixel positions by

$$P1(n) = P(S1(n,1), S1(n,2)), n = 1,2,..., N,$$

where $S1=(S,S^*)$. The obtained matrix $P1$ is rearranged to a matrix B sized $H\times W$ to get a permutated image.

3.2 Pixel Gray Values Changing Process

The bitxor operation is perform to change the pixel gray values to make the histogram of the cipher-image significantly different from that of the plain-image, therefore enhance the resistance to statistical attack and differential attack greatly. The opponent can not find any useful clues between the plain-image and the cipher-image and so can not break the cryptosystem even after they have spent a lot of time and effort. The following coupled map lattice is utilized to generate random gray value sequences [11].

$$\begin{aligned} y_1(n+1)&=(1-\varepsilon)f(y_1(n))+\varepsilon f(y_2(n)),\\ y_2(n+1)&=(1-\varepsilon)f(y_2(n))+\varepsilon f(y_1(n)),n=0,1,\cdots. \end{aligned} \quad (2)$$

where $\varepsilon\in(0,1)$ is the coupling intensity, $f(x)$ is the well-known Logistic map

$$f(x)=\alpha x(1-x),\ x\in(0,1),\ \alpha\in(3.5699456,4].$$

The coupled map lattice system (2) has two positive Lyaponuv exponents as $\varepsilon=0.99$ [11]. Therefore the coupled map lattice system is chaotic. The pixel gray values changing process is outlined as follows.

Step 1: Choose the parameters α, $y_1(0), y_2(0)$. α is the control parameter for the Logistic map, $y_1(0), y_2(0)$ belonging to (0,1) are the initial values for the coupled map lattice system.

Step 2: Iterate the coupled map lattice system with $H\times W$ times to get two sequences $\{y_1(k), y_2(k), k=1,...,HW$.

Let

$$\begin{aligned} Y_1(k)&=\lfloor y_1(k)\times 256\rfloor,\\ Y_2(k)&=\lfloor y_2(k)\times 256\rfloor, k=1,2,...,HW. \end{aligned}$$

Reshape $Y_1(k), Y_2(k)$ to be two matrices T_1, T_2 with size $H\times W$, here $\lfloor x\rfloor$ rounds x to the nearest integer towards minus infinity.

Step 3: T_1, T_2 are then employed to change the pixel gray values by the bitxor operation

$$Q=T_1\oplus T_2\oplus B,$$

where B is the shuffled image yielded by the pixel positions permutation process, Q is the resulted cipher-image. The inverse process is given by

$$B=T_1\oplus T_2\oplus Q.$$

4. SECURITY ANALYSIS

4.1 Key space analysis

Since the pixel positions permutation process is irrelevant to the pixel gray values changing process, the key space consists of the cipher keys in both processes. In the permutation process, the control parameter a,b, the initial condition x_0, y_0 form the cipher keys. The cipher keys in the pixel gray values changing process are $\alpha, y_1(0), y_2(0)$. According to the IEEE floating-point standard, the computational precision of the 64-bit double precision numbers is 2^{-52}. Therefore the total number of different values which can be used as a is 2^{52}, so are the numbers for $b, x_0, y_0, \alpha, y_1(0), y_2(0)$. The key space is up to $(2^{52})^7=2^{364}$. Such a large key space can efficiently prevent opponent's brute-force attack. The key sensitivity tests can be performed.

4.2 Statistical analysis

Passing the statistical analysis on cipher-image is of crucial importance for a cryptosystem. Indeed, an ideal cryptosystem should be robust against any statistical attack. In order to prove the security of the proposed encryption scheme, the following statistical tests are performed.

i. **Histogram:** Encrypt the image Lena one round, and then plot the histograms of the plain-image and cipher-image as shown in Fig. 3. The histogram of the cipher-image is fairly uniform and significantly different from the histogram of the original image and hence it does not provide any useful information for the opponents to perform any statistical analysis attack on the encrypted image.

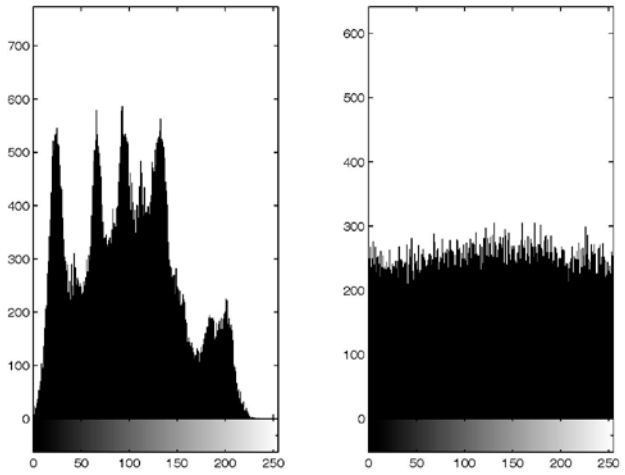

Fig. 3: Histograms of the plain-image and the cipher-image

ii. **Correlation of adjacent pixels:** To test the correlation between two adjacent pixels, the following performances are carried out. First, we select 6000 pairs of two horizontally adjacent pixels randomly from an image and then calculate the correlation coefficient of the selected pairs using the following formulae:

$$Cr = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

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

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i,\ \ D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2,$$

where x, y are the gray-scale values of two adjacent pixels in the image and $T = 6000$ is the total pairs of pixels randomly selected from the image. The correlations of two adjacent pixels in the plain-image and in the cipher-image are shown in the Table 1.

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

	Plain-image	Cipher-image
Horizontal	0.9435	-0.0092
Vertical	0.9680	0.0038
Diagonal	0.9157	0.0191

4.3 Robustness against attacks

The opponent can just damage the cipher-images if he does not need to know the secret. In such a case, the cryptosystem's robustness against such a kind of malicious attacks is very important. Attacks in the experiments are cropping, salt and pepper noising, and JPEG compression, etc. The results of tests to cipher-image attacks are shown in Figs. 4–6. Fig. 4 shows that the encryption scheme is robust against JPEG compression, Fig. 5 shows that the encryption scheme is robust against cropping and Fig. 6 shows that the encryption scheme is robust against salt and pepper noise pollution.

Fig. 4: Robust test for JPEG compression with quality=70, the upper left is the plain-image Lena, the upper right is the cipher-image, the lower left is the cipher-image attacked by JPEG compression, the lower right is the decrypted image for the attacked cipher-image.

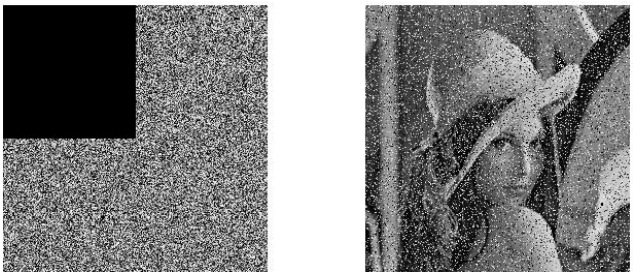

Fig. 5: Robust test for cropping attack with one quarter cut of the cipher-image

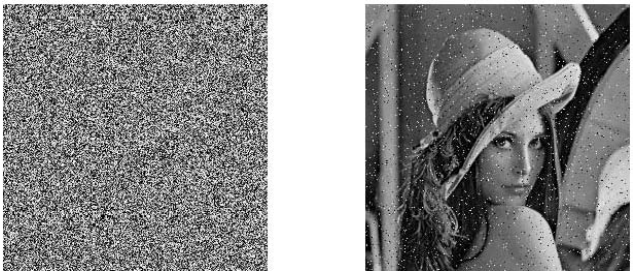

Fig. 6: Robust test for salt and pepper noise attack with intensity 0.05

5. CONCLUSIONS

An efficient image encryption scheme based on 2D tent map and coupled map lattice is proposed in the paper. The proposed scheme utilizes the 2D tent map to shuffle the plain-image efficiently in the pixel positions permutation process, while employs the coupled map lattice system to change the gray values of the whole image pixels greatly. The performance analysis including key space analysis, statistical analysis, robustness against malicious attacks, such as cropping, nosing, JPEG compression, are carried out numerically and visually.

ACKNOWLEDGMENTS

This research is supported by National Natural Science Foundation of China (No. 11071152) and Natural Science Foundation of Guangdong Province (No. 10151503101000023).

REFERENCES

[1] Schneier B.: Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995

[2] Fridrich, J.: Symmetric ciphers based on two dimensional chaotic maps. International Journal of Bifurcation and Chaos 8, 1259--1284 (1998)

[3] Chen, G. R., Mao, Y. B., Chui, C. K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 21, 749--761 (2004)

[4] Mao, Y. B., Chen, G., Lian, S. G.: A novel fast image encryption scheme based on the 3D chaotic Baker map. nternational Journal of Bifurcation and Chaos 14, 613--3624 (2004)

[5] Alvarez, G., Li, S.: Breaking an encryption scheme based on chaotic baker map. Physics Letters A 352, 78--82 (2006)

[6] Liu, J. M., Qu, Q.: Cryptanalysis of a substitution diffusion based on cipher using chaotic standard and logistic map. In: Third International Symposium on Information Processing, pp. 67--69 (2010)

[7] Liu, H., Wang, X.: Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284, pp. 3895--3903 (2011).

[8] Zhang, G. J., Liu, Q.: A novel image encryption method based on total shuffling scheme, Optics Communications, 284, pp. 2775--2780 (2011).

[9] Ye, R.: A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284, pp. 5290--5298 (2011).

[10] Robinson, C.: An Introduction to Dynamical Systems, Continuous and Discrete. Prentice Hall, 2004

[11] Keiji, K., Hideki K., Kentaro, H.: Stability of steady states in one way coupled map lattices. Physics Letters A 263, 307–314 (1999)