I. J. Computer Network and Information Security, **2012, 1, 38-44**
Published Online February 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.01.05

A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice

Ruisong Ye and Wei Zhou
Department of Mathematics, Shantou University
Shantou, Guangdong, 515063, P. R. China
Email: rsye@stu.edu.cn

Abstract—**This paper proposes a chaos-based image encryption scheme where one 3D skew tent map with three 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 have been 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.**

Index Terms—**Chaotic system, Coupled map lattice, Ergodicity, 3D skew tent map, Image encryption scheme**

I. 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 (Data Encryption Standard), 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 [2-4].

Recently, some chaos-based image encryption algorithms were 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 [7-10]. In this paper, an efficient image encryption scheme based on the ergodicity of 3D tent map and coupled map lattice is proposed. Firstly, one 3D tent map with three 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 have been 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 demonstrate the robustness against malicious attacks like cropping, noising, JPEG compression, etc.

The rest of the paper is organized as follows. The 3D skew tent map and its chaotic nature are introduced in Section II. An image encryption scheme consisting of a diffusion process and a permutation process is proposed then in Section III. The performance analysis is presented in Section IV, including the key space analysis, statistic analysis, differential attack, resistance to cipher-image attacks. Experimental results show that the proposed image encryption scheme is secure and robust. Section V concludes the paper.

II. 3D Skew Tent Mmaps and Its Chaotic Nature

The unimodal skew tent map $T_0:[0,1]\to[0,1]$ is given by

$$T_0(x)=\begin{cases} x/a, & \text{if } x\in[0,a], \\ (1-x)/(1-a), & \text{if } x\in(a,1], \end{cases} \tag{1}$$

where $x\in[0,1]$ is the state of the system, and $a\in(0,1)$ is the control parameter. It is a noninvertible transformation of the unit interval onto itself. As $a=0.5$, T_0 becomes the regular tent map. The transformation is continuous and piecewise linear, with the linear regions $[0,a]$ and $[a,1]$. Note that the slope of the left branch is $1/a>1$ and the slope of the right branch is $-1/(1-a)<-1$. For any $a\in(0,1)$, the piecewise linear map (1) has Lyapunov exponent $-a\ln a-(1-a)\ln(1-a)$, which is larger than 0, implying that the map is chaotic. There exist some good dynamical features in skew tent maps. It has been verified that the probability density function $\rho_0(x)$ of the skew tent map is the same as the regular tent map [11], that is,

$$\rho_0(x)=\begin{cases}1, & \text{if } x\in(0,1),\\ 0, & \text{otherwise.}\end{cases}$$

In this paper, we extend the unimodal skew tent map (1) to 3D skew tent map $T:[0,1]^3\to[0,1]^3$ by the following way.

$$T(x,y,z)=\begin{cases}(\frac{x}{\alpha},\frac{y}{\beta},\frac{z}{\gamma}), & (x,y,z)\in[0,\alpha)\times[0,\beta)\times[0,\gamma),\\ (\frac{x}{\alpha},\frac{y}{\beta},\frac{1-z}{1-\gamma}), & (x,y,z)\in[0,\alpha)\times[0,\beta)\times[\gamma,1],\\ (\frac{x}{\alpha},\frac{1-y}{1-\beta},\frac{z}{\gamma}), & (x,y,z)\in[0,\alpha)\times[\beta,1]\times[0,\gamma),\\ (\frac{x}{\alpha},\frac{1-y}{1-\beta},\frac{1-z}{1-\gamma}), & (x,y,z)\in[0,\alpha)\times[\beta,1]\times[\gamma,1],\\ (\frac{1-x}{1-\alpha},\frac{y}{\beta},\frac{z}{\gamma}), & (x,y,z)\in[\alpha,1]\times[0,\beta)\times[0,\gamma),\\ (\frac{1-x}{1-\alpha},\frac{y}{\beta},\frac{1-z}{1-\gamma}), & (x,y,z)\in[\alpha,1]\times[0,\beta)\times[\gamma,1],\\ (\frac{1-x}{1-\alpha},\frac{1-y}{1-\beta},\frac{z}{\gamma}), & (x,y,z)\in[\alpha,1]\times[\beta,1]\times[0,\gamma),\\ (\frac{1-x}{1-\alpha},\frac{1-y}{1-\beta},\frac{1-z}{1-\gamma}), & (x,y,z)\in[\alpha,1]\times[\beta,1]\times[\gamma,1].\end{cases}\quad(2)$$

where $,\alpha,\beta,\gamma\in(0,1)$ are the control parameters.

It is easy to show that the three Lyapunov exponents of (2) are (see [12])

$$\lambda_x=\alpha\ln(\frac{1}{\alpha})+(1-\alpha)\ln(\frac{1}{1-\alpha}),$$
$$\lambda_y=\beta\ln(\frac{1}{\beta})+(1-\beta)\ln(\frac{1}{1-\beta}),$$
$$\lambda_z=\gamma\ln(\frac{1}{\gamma})+(1-\gamma)\ln(\frac{1}{1-\gamma})).$$

It is obvious that $\lambda_x,\lambda_y,\lambda_z$ are all positive, implying that the 3D skew tent map is chaotic on $[0,1]^3$. A typical orbit of (x_0,y_0,z_0) derived from the dynamical system is $\{(x_k,y_k,z_k)=T^k(x_0,y_0,z_0),k=0,1,\cdots\}$, which is shown in Fig. 1 for $\alpha=0.13,\beta=0.3,\gamma=0.7$, $x_0=0.6,y_0=0.2,z_0=0.4$. The plotting orbit points fill $[0,1]^3$ as long as the orbit is long enough, which indicates that the system is chaotic visually. The control parameters α,β,γ and the initial condition x_0,y_0,z_0 can be regarded as cipher keys as the map is used to design image encryption schemes.

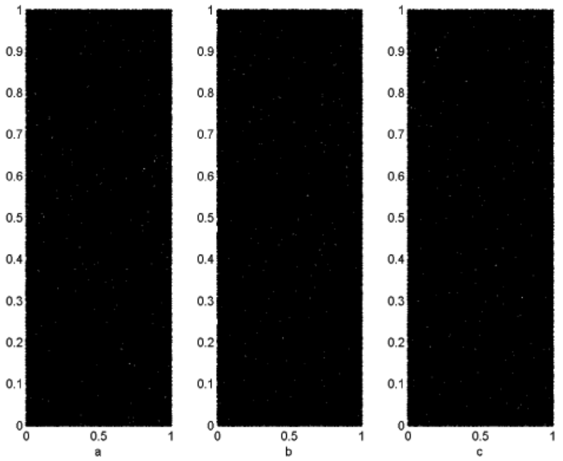


Figure 1. Orbit derived from the considered 3D skew tent map with $\alpha=0.13,\beta=0.3,\gamma=0.7,x_0=0.6,y_0=0.2,z_0=0.4$. (a), (b), (c) are the xy, xz, yz -projections of the derived orbit respectively.

III. The Proposed Image Encryption Scheme

We propose an image encryption scheme consisting of two processes: diffusion of pixel gray values and permutation of pixel positions. In the diffusion process, the coupled map lattice system is utilized to generate pseudo-random gray value sequences, then bitxor operation and mod operation are performed to change the pixel gray values so that the histogram of the cipher-image is significantly different from that of the plain-image, therefore enhancing 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. In the permutation process, the 3D skew tent map is utilized to realize the shuffling of pixel positions.

A. Diffusion of pixel gray values

Let the processed image is of height H and width W and let $HW=H\times W$. The following coupled map lattice is utilized to generate pseudo-random gray value sequences [13].

$$\begin{aligned}y_1(n+1)&=(1-\varepsilon)f(y_1(n))+\varepsilon f(y_2(n)),\\ y_2(n+1)&=(1-\varepsilon)f(y_2(n))+\varepsilon f(y_1(n)),n=0,1,\cdots\end{aligned}\quad(3)$$

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

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

The coupled map lattice system (3) has two positive Lyaponuv exponents as $\varepsilon=0.99$ [13]. Therefore the coupled map lattice system is chaotic. The diffusion process of pixel gray values is outlined as follows.

Step 1. Set the values of the control parameter λ for the logistic map and the initial conditions $y_1(0),y_2(0)$ for the coupled map lattice system.

Step 2. Iterate the coupled map lattice system HW times to get two sequences $\{y_1(k), y_2(k), k=1,\cdots, HW\}$. Let

$$Y_1(k) = floor(y_1(k)\times 256),$$
$$Y_2(k) = floor(y_2(k)\times 256), k=1,2,\cdots,HW,$$

where $floor(x)$ rounds x to the nearest integer towards minus infinity. The two sequences Y_1, Y_2 are then applied to obtain another pseudo-random gray value sequence $\varphi(k), k=1,2,\cdots,HW$ by the bitxor operation $\oplus$: $\varphi = Y_1 \oplus Y_2$.

Step 3. The following diffusion function is utilized to achieve the pixel gray value diffusion.

$$C(k) = \varphi(k)\oplus\{(P(k)+\varphi(k))\text{mod } 256\}$$
$$\oplus C(k-1),\ k=1,2,\cdots,HW,$$

where $P(k)$ is the gray value of the current operated pixel in the original image which has been rearranged according to the order of row or column to a vector with length HW, $C(k-1)$ is the previous output cipher-pixel gray value. The diffusion process is well defined as the initial condition $C(0)$ is provided. $C(0)$ can be set to be part of the keys in the diffusion process or can just take the value of $C(0)=Y_1(1)$ for simplicity. Note that the inverse diffusion function is

$$P(k) = \{\varphi(k)\oplus C(k)\oplus C(k-1)-\varphi(k)\}\text{mod } 256,$$
$$k=1,2,\cdots,HW.$$

Step 4. Reshape $P(k), k=1,2,\cdots,HW$ to be a matrix Q with height H and width W. Q is the resulted image.

B. Permutation of pixel positions

We pile up the gray value matrix Q yielded in the diffusion process to one 3D matrix R with size $l_1\times l_2\times l_3$ such that $HW = l_1\times l_2\times l_3 + l_4$ where $l_i(i=1,\cdots,4)$ are non-negative integer numbers. If l_4 is not zero, then put the remainder l_4 pixel gray values into a vector $R1$ for the use later.

Step 1. Set the values of $\alpha, \beta, \gamma, x_0, y_0, z_0$. Iterate the 3D skew tent map for HW times to yield three sequences $\{x_n, y_n, z_n, n=1,2,\cdots,HW\}$, then quantize them by

$$X(n) = ceil(x_n\times l_1), Y(n) = ceil(y_n\times l_2),$$
$$Z(n) = ceil(z_n\times l_3),\ \ n=1,2,\cdots,HW$$

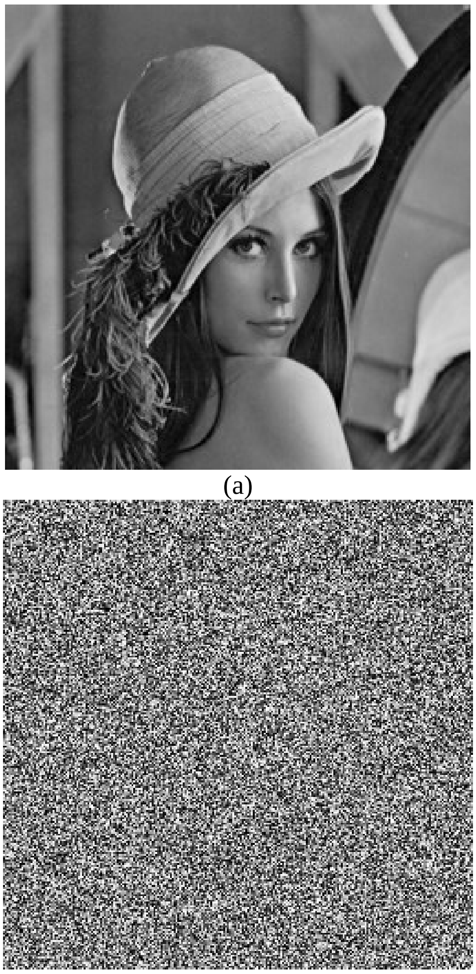
where $ceil(x)$ rounds x to the nearest integer towards infinity.

Step 2. Due to the restriction of iteration times, the coordinates $(X(n)$, $Y(n)$, $Z(n)), n=1,2,\cdots,HW$ may not fill the cube sized $l_1\times l_2\times l_3$. Find the coordinates which are not ergodic and rearrange them after $(X(n), Y(n), Z(n))$, we finally obtain one 2D coordinate matrix C with size $l_1l_2l_3\times 3$.

Step 3. The yielded matrix C is then employed to shuffle the 3D matrix R

$$R2(i) = R(C(i,1), C(i,2), C(i,3)),\ i=1,2,\cdots,l_1l_2l_3.$$

Set the remainder vector $R1$ after $R2$ to form a vector with length HW, which is reshaped to be the final cipher-image S with height H and width W. The permutation process is completed.


(a)

(b)

Figure 2. The encryption results. (a) plain-image, (b) cipher-image

We choose the plain image Lena sized 256×256. Fig. 2 shows the encryption results. The cipher keys are

$$\lambda = 4.0,\ y_1(1) = 0.6,\ y_2(1) = 0.3,\ \alpha = 0.2,\ x_0 = 0.4,$$
$$\beta = 0.7,\ y_0 = 0.44,\ \gamma = 0.56,\ z_0 = 0.23,$$
$$n = 43,\ m = 34,\ l = 33.$$

IV. Performance Analysis

A. Key space analysis

Since the permutation process is irrelevant to the diffusion process, the key space consists of the cipher keys in both processes. In the permutation process, the control parameters α,β,γ , the initial conditions x_0, y_0, z_0 and l_1, l_2, l_3 form the cipher keys. The cipher keys in the diffusion process are $\lambda, y1(1), y2(1)$. According to the IEEE floating-point standard, the computational precision of the 64-bit double precision number is 2^{-52}. Therefore the total number of different values which can be used as α is 2^{52} , so are the numbers for $\beta,\gamma,x_0,y_0,z_0,\lambda,y1(1),y2(1)$. The key space is $(2^{52})^9 = 2^{468}$ even without considering l_1, l_2, l_3. Such a large key space can efficiently prevent opponent's brute-force attack.

B. 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 with one round, and then plot the histograms of plain-image and cipher-image as shown in Fig. 3, respectively. Fig. 3(b) shows that the histogram of the cipher-image is fairly uniform and significantly different from the histogram of the plain-image and hence it does not provide any useful information for the opponents to perform any statistical analysis attack on the encrypted image.

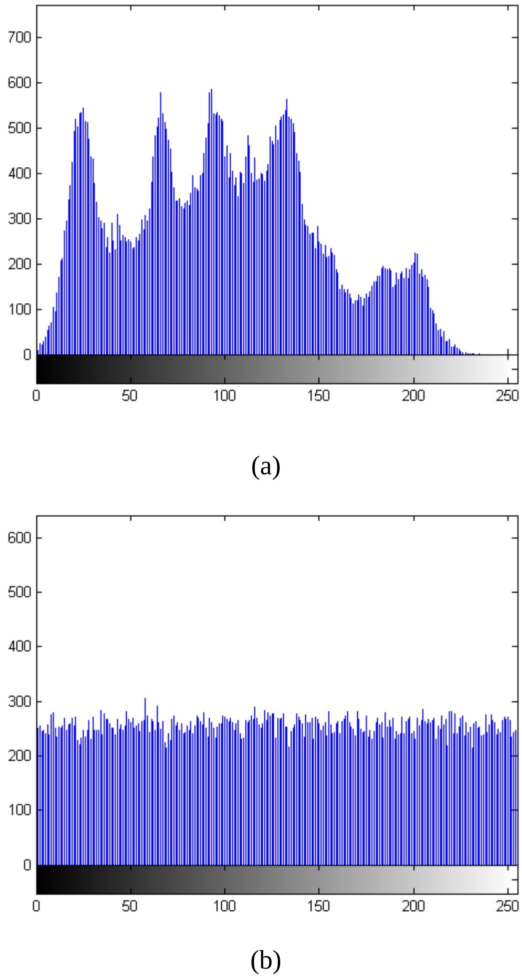
(ii)The correlations of adjacent pixels. To test the correlations between two adjacent pixels, the following performances are carried out. First, we select 6000 pairs of two horizontally (vertically, diagonally) adjacent pixels randomly from an image and then calculate the correlation coefficients of the selected pairs using the following formulae:

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

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

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

where x, y are the grey-scale values of two adjacent pixels in the image and T 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. The correlation distribution of two horizontally adjacent pixels in the plain-image and that in the cipher-image are shown in Fig. 4.



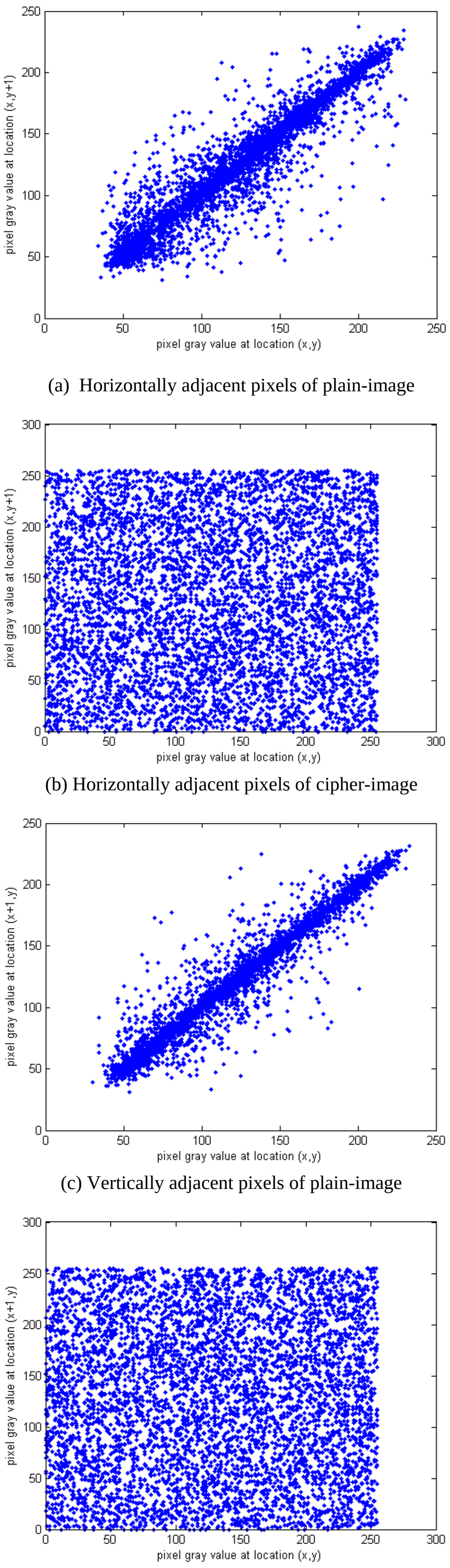
(a)

(b)

Figure 3. The histograms of the plain-image and the cipher-image. (a) the plain-image, (b) the cipher-image.

Table 1. Correlation coefficients of two adjacent pixels in two images

	Plain-image	Cipher-image
Horizontal	0.9725	0.0116
Vertical	0.94073	0.0038
Diagonal	0.9235	0.0239



(a) Horizontally adjacent pixels of plain-image

(b) Horizontally adjacent pixels of cipher-image

(c) Vertically adjacent pixels of plain-image

(d) Vertically adjacent pixels of cipher-image

Figure 4. The correlation distributions of adjacent pixels.

(iii) Information entropy analysis. The entropy is the most outstanding feature of randomness. The entropy $H(m)$ of a message source m can be measured by

$$H(m) = -\sum_{i=0}^{L-1} p(m_i)\log(p(m_i))$$

where L is the total number of symbols m , $p(m_i)$ represents the probability of occurrence of symbol m_i and log denotes the base 2 logarithm so that the entropy is expressed in bits. For a random source emitting 256 symbols, its entropy is $H(m) = 8$ bits. For the encrypted image of Lena, the corresponding entropy is 7.9970bits. This means that the cipher-image is close to a random source and the proposed algorithm is secure against the entropy attack.

C. Differential attack

In general, attacker may make a slight change (e.g., modify only one pixel) of the plain-image to find out some meaningful relationships between the plain-image and the cipher-image. If one minor change in the plain-image will cause a significant change in the cipher-image, then the encryption scheme will resist the differential attack efficiently. To test the influence of only one-pixel change in the plain-image over the whole cipher-image, two common measures are used: number of pixels change rate (NPCR) and unified average changing intensity (UACI). They are defined as

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

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%$$

where C_1, C_2 are the two cipher-images corresponding to two plain-images with only one pixel difference, W and H are the width and height of the processed image, D is a bipolar array with the same size as image C_1 . $D(i,j)$ is determined as: if $C_1(i,j) = C_2(i,j)$, then $D(i,j) = 0$, otherwise $D(i,j) = 1$. NPCR measures the percentage of different pixels numbers between the two cipher-images whose plain-images only have one-pixel difference. UACI measures the average intensity of differences between the two cipher-images. To resist difference attacks, the values of NPCR and UACI should be large enough. The plain-image Lena is tested to show the two measures. Experimental results are depicted in Fig. 5. We can see from the figure that the NPCR is near 100% and the UACI is about 33% since the second round of encryption.

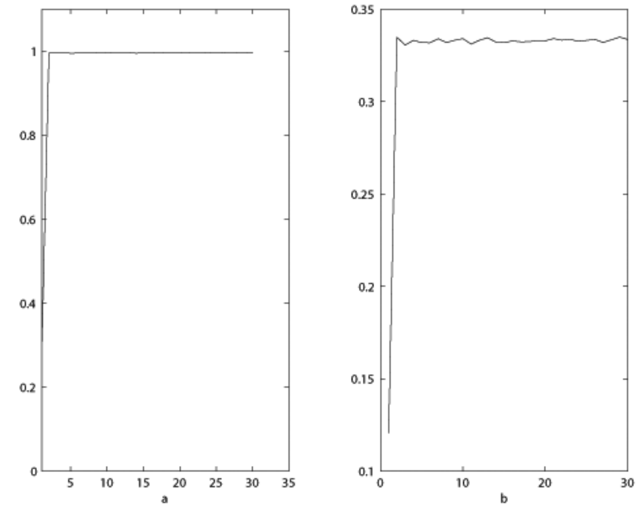
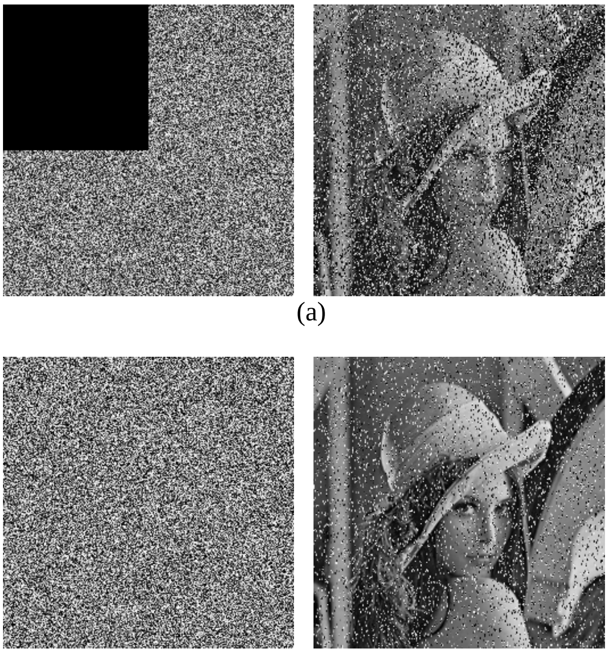


Figure 5. The NPCR and UACI tests. (a) NPCR test, (b) UACI test.

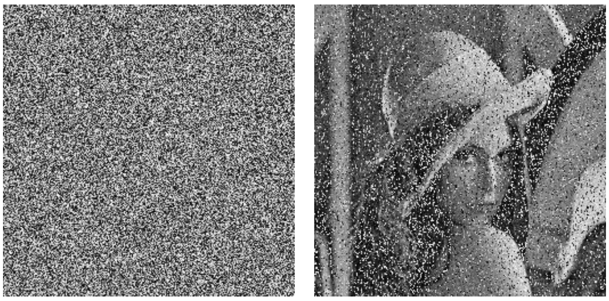
D. Resistance to cipher-image attacks

Cipher-image attack means that the opponent performs image processing like cropping, noising, compression, etc. on the cipher-images. 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. A secure encryption scheme should consider the robustness against cipher-image attacks. The results of tests to cipher-image attacks are shown in Fig. 6, demonstrating that the encryption scheme is also robust against cropping, salt & pepper nosing, JPEG compression.



(a)

(b)



(c)

Figure 6. The robustness against attacks. (a) cropping one-quarter of cipher-image, (b) salt & pepper noising with intensity 0.1, (c) JPEG compression with quality factor 70.

IV. Conclusions

An efficient image encryption scheme based on 3D skew tent map and coupled map lattice is proposed in the paper. The proposed scheme utilizes the 3D skew 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.

Acknowledgment

We thank anonymous referees for their constructive comments. This research was 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, 1998, 8: 1259-1284.

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

[4] Mao, Y. B., Chen, G., Lian, S. G., A novel fast image encryption scheme based on the 3D chaotic Baker map. International Journal of Bifurcation and Chaos, 2004, 14: 3613-3624.

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

[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, Opt. Commun. 2011, 284: 3895-3903.

[8] Zhang, G. J., Liu, Q., A novel image encryption method based on total shuffling scheme. Opt. Commun. 2011, 284: 2775-2780.

[9] Ye, R., Huang, H., Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking, I. J. Image, Graphics and Signal Processing, 2010, 1: 19-29

[10] Ye, R., A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Opt. Commun. 2011, 284: 5290-5298.

[11] Hasler M., Maistrenko, Y. L., An introduction to the synchronization of chaotic systems: Coupled skew tent map, IEEE Transactions on Circuits and Systems, 1997, 44: 856-866.

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

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

Ruisong Ye, born in 1968 and received the B.S. degree in Computational Mathematics in 1990 from Shanghai University of Science and Technology, Shanghai, China and the Ph. D. degree in Computational Mathematics in 1995 from Shanghai University, Shanghai, China. He is a professor at Department of Mathematics in Shantou University, Shantou, Guangdong, China since 2003. His research interest includes bifurcation theory and its numerical computation, fractal geometry and its application in computer science, chaotic dynamical system and its application in computer science, specifically the applications of fractal chaotic dynamical systems in information security, such as, digital image encryption, digital image hiding, digital image watermarking, digital image sharing.

Wei Zhou was born in 1985 and received his M.S. degree in Applied Mathematics in 2011 from Shantou University, Shantou, China. His research interest is chaotic dynamical system and its application in computer science.