*I.J. Image, Graphics and Signal Processing*, **2012, 6, 52-60**
Published Online July 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2012.06.08

# An Image Hiding Scheme Using 3D Sawtooth Map and Discrete Wavelet Transform

Ruisong Ye and Wenping Yu
Department of Mathematics, Shantou University
Shantou, Guangdong, 515063, China
E-mail: rsye@stu.edu.cn

***Abstract***— An image encryption scheme based on the 3D sawtooth map is proposed in this paper. The 3D sawtooth map is utilized to generate chaotic orbits to permute the pixel positions and to generate pseudo-random gray value sequences to change the pixel gray values. The image encryption scheme is then applied to encrypt the secret image which will be imbedded in one host image. The encrypted secret image and the host image are transformed by the wavelet transform and then are merged in the frequency domain. Experimental results show that the stego-image looks visually identical to the original host one and the secret image can be effectively extracted upon image processing attacks, which demonstrates strong robustness against a variety of attacks.

***Index Terms***— Chaotic encryption, Sensitivity, Ergodicity, 3D sawtooth maps, Image hiding

## I. INTRODUCTION

Thanks to the rapid developments of multimedia and network technology, various data in digital form is transmitted over the Internet network. The transmitted data can be a digital representation of text, image, audio and video. They can be replicated, edited easily and spread openly through the Internet, which causes a serious problem that it is difficult even impossible to give proof of copyright once pirated. The security issue of digital images has attracted more attentions consequently. In order to ensure the security of the data transmission over the Internet, data encryption [1] and data hiding [2] are two widely used approaches. Data encryption is a technique to protect data from illicit access by transforming important data into meaningless code. Nevertheless, data hiding is different from data encryption as it conceals the existence of secret data by hiding the secret data into a meaningful host data to distract the attention of the observers.

A variety of image encryption algorithms (for example, see [3-14] and the references therein) have been studied and developed in the last two decades. Among them, chaos-based encryption algorithms have been considered to be a significant and potential technique in application thanks to chaotic systems' good properties in many concerned aspects such as security, complexity, speed and computational overhead, etc. As a matter of fact, due to some intrinsic features of digital images, such as bulk data capacity and high correlation among adjacent pixels, traditional encryption algorithms such as DES, IDEA and RSA [15] are not suitable for practical digital image encryption. The fundamental features of chaotic systems, such as ergodicity, pseudo-randomness and high sensitivity to initial conditions and control parameters, are close to confusion and diffusion in the cryptography.

Digital image hiding methods are ways of hiding secret images in host images such that an unintended observer will not be aware of the existence of the hidden images. Host images embedded the secret images are called stego-images. For digital image hiding methods, the image quality refers to the quality of the stego-images. The image hiding technology may be implemented in the frequency domain or in the spatial domain of a given digital image. One of the most common techniques in the spatial domain is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the host image with the secret message bits [16]. The LSB substitution scheme is irreversible, as a result, the host image can not be recovered exactly from the stego-image after extracting the hidden secret image. In the frequency domain, the host images and/or the secret images are transformed by DCT, DWT, etc. and then the proposed image hiding schemes are employed to the transformed images. For example, Ahmidi proposed a color image technique based on DCT, embedding the image into middle frequency coefficients of transformed blocks [17]. Hsieh proposed a watermarking method based on the qualified significant wavelet tree (QSWT) [18], where the embedding scheme took the relationships of DWT coefficients and spatial information into consideration. Many applications can benefit from image hiding schemes, including confidential video conferencing, pay-TV, confidential facsimile, medical applications.

In this paper, we apply the image encryption technique and the image hiding technique together to enhance the security, and improve the robustness against malicious attacks. An image hiding scheme with the preprocessing of secret image by the proposed encryption scheme is presented. Two 3D sawtooth maps with three control parameters are utilized to encrypt the secret image which will be imbedded in one host image. The encryption scheme consists of generating a chaotic orbit by one 3D sawtooth map to scramble the pixel positions and yielding a random gray value sequence by another sawtooth map to change the gray values. The encrypted secret image and the host image are transformed by DWT and then are merged in the frequency domain. The recovered secret images also show that the proposed image hiding scheme is robust against various attacks.

The rest of this paper is organized as follows. Section II introduces the 3D sawtooth map. One image encryption scheme is proposed in Section III. The image hiding scheme is presented and the robustness tests are performed in Section IV. Section V concludes the paper.

## II. 3D SAWTOOTH MAP

The sawtooth map $S_0 : [0,1] \to [0,1]$ is given by

$$S_0(x) = \begin{cases} x/a, & \text{if } x \in [0,a), \\ (x-a)/(1-a), & \text{if } x \in [a,1], \end{cases} \qquad (1)$$

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 $a = 0.5$ , map (1) becomes the well-known regular Bernoulli shift map $B_0 : [0,1] \to [0,1]$ given by

$$\begin{aligned} x_{n+1} &= B_0(x_n) := 2x_n \bmod 1 \\ &= \begin{cases} 2x_n, & \text{if } x_n \in [0,1/2) \\ 2x_n - 1, & \text{if } x_n \in [1/2,1] \end{cases} \end{aligned} \qquad (2)$$

The Bernoulli shift map (2) yields a simple example for an essentially nonlinear stretch-and-cut mechanism, as it typically generates deterministic chaos. Such basic mechanisms are also encountered in more realistic dynamical systems. The sawtooth map 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.

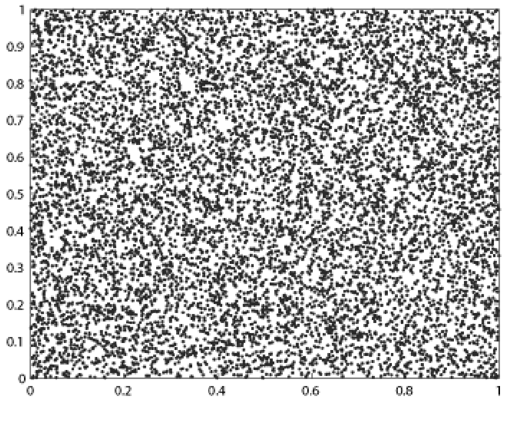
In this paper, we extend the sawtooth map to its 3D version $S : [0,1]^3 \to [0,1]^3$ by the following way.

$$S(x,y,z) = \begin{cases} (\frac{x}{a}, \frac{y}{b}, \frac{z}{c}), & (x,y,z) \in [0,a) \times [0,b) \times [0,c), \\ (\frac{x}{a}, \frac{y}{b}, \frac{z-c}{1-c}), & (x,y,z) \in [0,a) \times [0,b) \times [c,1], \\ (\frac{x}{a}, \frac{y-b}{1-b}, \frac{z}{c}), & (x,y,z) \in [0,a) \times [b,1] \times [0,c), \\ (\frac{x}{a}, \frac{y-b}{1-b}, \frac{z-c}{1-c}), & (x,y,z) \in [0,a) \times [b,1] \times [c,1], \\ (\frac{x-a}{1-a}, \frac{y}{b}, \frac{z}{c}), & (x,y,z) \in [a,1] \times [0,b) \times [0,c), \\ (\frac{x-a}{1-a}, \frac{y}{b}, \frac{z-c}{1-c}), & (x,y,z) \in [a,1] \times [0,b) \times [c,1], \\ (\frac{x-a}{1-a}, \frac{y-b}{1-b}, \frac{z}{c}), & (x,y,z) \in [a,1] \times [b,1] \times [0,c), \\ (\frac{x-a}{1-a}, \frac{y-b}{1-b}, \frac{z-c}{1-c}), & (x,y,z) \in [a,1] \times [b,1] \times [c,1]. \end{cases} \qquad (3)$$

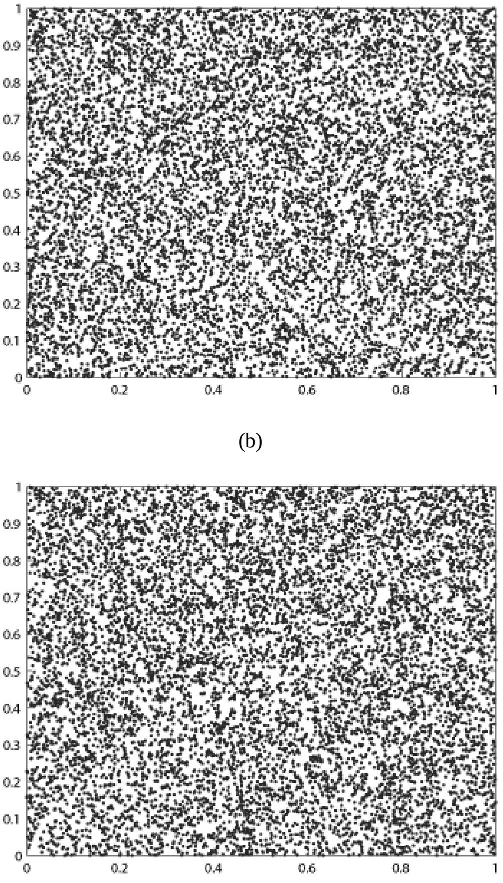
where $a,b,c \in (0,1)$ are the control parameters. It is easy to show that the three Lyapunov exponents are (see [19])

$$\begin{aligned} \lambda_x &= a\ln(\frac{1}{a}) + (1-a)\ln(\frac{1}{1-a}), \\ \lambda_y &= b\ln(\frac{1}{b}) + (1-b)\ln(\frac{1}{1-b}), \\ \lambda_z &= c\ln(\frac{1}{c}) + (1-c)\ln(\frac{1}{1-c})). \end{aligned}$$

It is obvious that $\lambda_x, \lambda_y, \lambda_z$ are all positive, implying that the 3D sawtooth 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 $x_0 = 0.21, y_0 = 0.83, z_0 = 0.46$ , $a = 0.5, b = 0.3, c = 0.7$ 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 $a,b,c$ 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.



(a)



(b)

(c)

Figure 1. Orbit derived from the considered 3D sawtooth map with $x_0 = 0.21, y_0 = 0.83, z_0 = 0.46, a = 0.5, b = 0.3, c = 0.7$. (a), (b), (c) are the $xy$, $xz$, $yz$-projections of the derived orbit respectively.

## III. The Proposed Image Ecryption Scheme

### *A. 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 permutation process, the 3D sawtooth map is utilized to realize the shuffling of pixel positions. In the diffusion process, another sawtooth map is utilized to generate a pseudo-random gray value sequence, 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. Let the plain-image to be $P$ with height $H$ and width $W$. The image encryption scheme is outlined as follows.

Step 1. Set the initial values and the control parameters

$$x_1 = 0.367, y_1 = 0.761, z_1 = 0.579,$$
$$a_1 = 0.413, b_1 = 0.684, c_1 = 0.725$$

Step 2. Iterate the 3D sawtooth map to get three sequences $\{x_i\}$, $\{y_i\}$, $\{z_i\}$,

$$(x_{i+1}, y_{i+1}, z_{i+1}) = S(x_i, y_i, z_i), i = 1, \cdots, HW - 1 \quad (4)$$

Step 3. Sort the sequence $\{x_i : i = 1, \cdots, HW\}$ to get index vector $I_{x_i}, i = 1, 2, ..., HW$. Rearrange the gray value matrix $P$ to be a vector with size $1 \times HW$. We still name the vector $P$.

Step 4. Permute the pixel positions by

$$P1(i) = P(I_{x_i}), i = 1, 2, ..., HW \quad (5)$$

to get the scrambled image $P1$.

Step 5. Set $i = 1$,

$$P2(1) = P1(1) \oplus [\, floor(L \times (y_1 + z_1) / 2) \bmod L] \quad ,$$

where $floor(x)$ denotes the largest integer number not larger than $x$, $L$ is the gray-scale level.

Step 6. Set

$$c(i) = floor(L \times y_i),\ d(i) = floor(L \times z_i).$$

Perform the diffusion by the bitxor operation by

$$\begin{aligned} P2(i+1) = P2(i) \oplus [(\, & floor((c(i) + d(i)) / 2) \\ & + P1(i+1)) \bmod L]. \end{aligned} \quad (6)$$

Step 7. Set $i = i + 1$ and repeat Step 6 till $i = HW - 1$.

We note that the above diffusion process implies that it can not influence the pixels before the tampered pixel with a gray value change. As a remedy, we here add a reverse diffusion process as a supplement to the above diffusion process.

Step 8. Set the initial values $x^* = 0.347, y^* = 0.532$, $z^* = 0.864$ and the control parameters $a_2 = 0.346$, $b_2 = 0.539$, $c_2 = 0.912$. Set $j = 1$ and calculate

$$u(M \times N) = floor(L \times x^*),$$
$$v(M \times N) = floor(L \times y^*),$$
$$w(M \times N) = floor(L \times z^*),$$
$$\begin{aligned} P3(M \times N) = P2(M \times N) \oplus [\, & floor((u(M \times N) \\ & + v(M \times N) + w(M \times N)) / 3) \bmod L]. \end{aligned}$$

Step 9. calculate

$$u(j) = floor(L \times x_j),$$
$$v(j) = floor(L \times y_j),$$
$$w(j) = floor(L \times z_j),$$

where $x_1 = x^*$, $y_1 = y^*$, $z_1 = z^*$.

Let

$s = 1 + [P3(M \times N - j + 1) \bmod 2]$,

and iterate the 3D sawtooth map $s$ times to get $(x_{j+1}, y_{j+1}, z_{j+1})$:

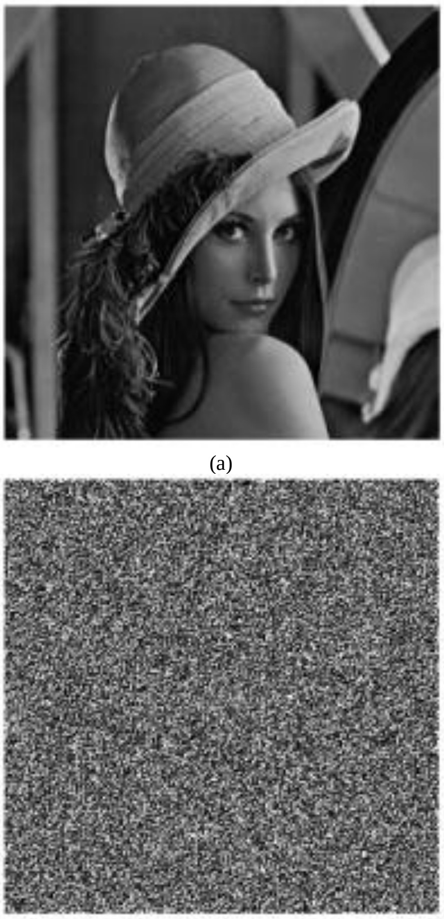
$$(x_{j+1}, y_{j+1}, z_{j+1}) = S^s(x_j, y_j, z_j). \tag{7}$$

The reverse diffusion is

$$\begin{aligned} P3(M \times N - j) = {} & P3(M \times N - j + 1) \oplus \\ & [(floor((u(j) + v(j) + w(j))/3) \\ & + P2(M \times N - j)) \bmod L]. \end{aligned} \tag{8}$$

Step 10. Set $j = j + 1$ and repeat Step 9 till $j = M \times N - 1$.

The obtained matrix $P3$ is reshaped to be a matrix $Q$ with height $H$ and width $W$, $Q$ is the cipher-image. The plain-image Lena is encrypted and the result is shown in Fig. 2(b).



(a)

(b)

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

## *B. Security analysis*

According to the basic principle of cryptology [15], a good encryption scheme requires sensitivity to cipher keys, i.e., the cipher-text should have close correlation with the keys. An ideal encryption scheme should have a large key space to make brute-force attack infeasible; it should also well resist various kinds of attacks like statistical attack, differential attack, etc. In this subsection, key sensitivity analysis and statistical analysis are performed. All the analysis shows that the proposed image encryption scheme is highly secure.

Shannon pointed out in his masterpiece [20] the possibility to solve many kinds of ciphers by statistical analysis. Therefore, passing the statistical analysis on cipher-image is of crucial importance for a cryptosystem. Indeed, an ideal cryptosystem should be highly 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. Fig. 3(b) shows that 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 effective statistical analysis attack on the encrypted image.

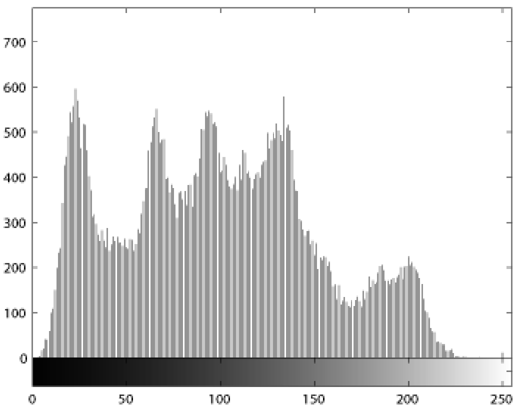
(ii) Correlation of adjacent pixels. To test the correlation between two adjacent pixels, the following performances are carried out. First, we select 1000 pairs of two adjacent pixels randomly from an image and then calculate the correlation coefficient of the selected pairs using the following formulae:

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

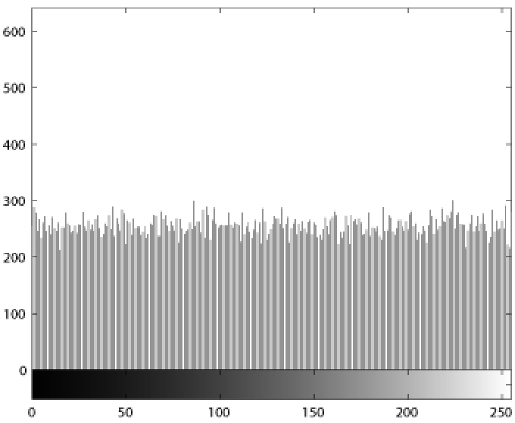
$$cov(x,y) = \tfrac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y)),$$

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

where $x, y$ are the gray-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 Ⅰ.



(a)



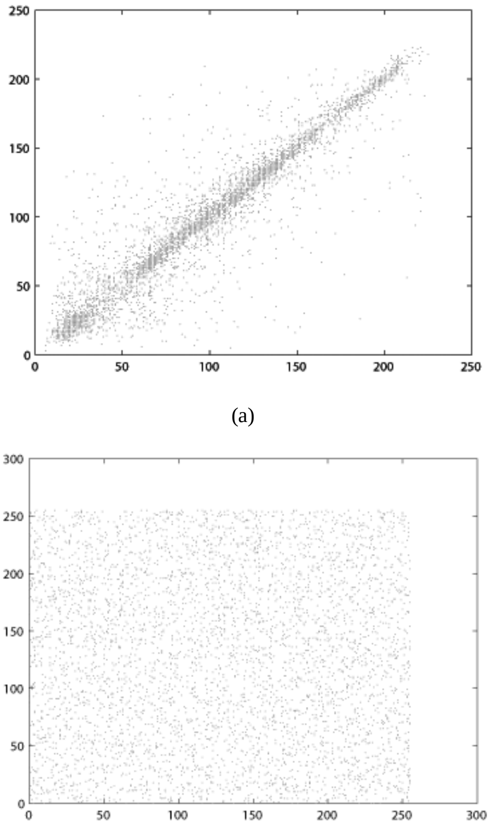
(b)

Figure 3. (a) Histogram of plain-image, (d) Histogram of cipher-image

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

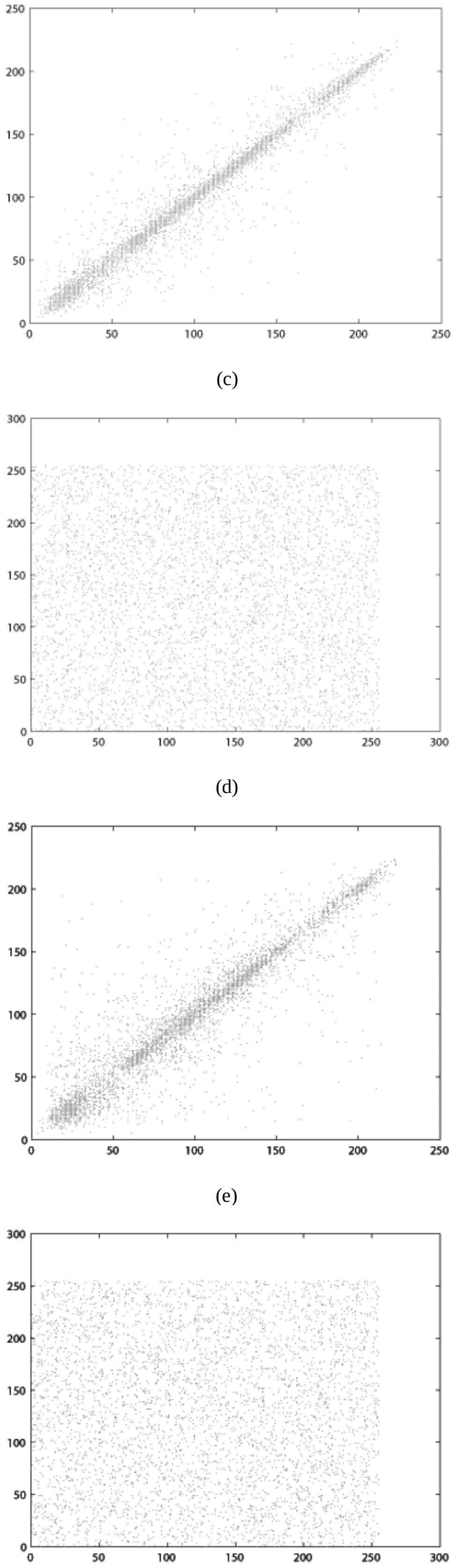
| | Plain-image | Cipher-image |
|---|---|---|
| Horizontal | 0.9387 | -0.0244 |
| Vertical | 0.9682 | -0.0128 |
| Diagonal | 0.9112 | -0.0231 |

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)



(c)

(d)

(e)

(f)

Figure 4. Correlations of two adjacent pixels in the plain-image and in the cipher-image: (a), (c), (e) are for the plain-image; (b), (d), (f) are for the cipher-image.

A good image encryption scheme also needs to contain sufficiently large key space for compensating the degradation dynamics in PC. It should be sensitive to cipher keys as well, and thus can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. The analysis results regarding the sensitivity and the key space are summarized as follows. Since the permutation process is irrelevant to the diffusion process, the key space consists of the cipher keys in both processes. Therefore, the control parameters $a_i, b_i, c_i (i = 1, 2)$ and the initial condition $x_0, y_0, z_0, x^*, y^*, z^*$ constitute the cipher keys. The sensitive tests with respect to all cipher keys have been carried out. To verify the sensitivity of key parameter $K$, the original plain-image $I = (I(i,j))_{H\times W}$ is encrypted with $K = p, K = p - \Delta\delta$ and $K = p + \Delta\delta$ respectively while keeping the other key parameters unchanged. The corresponding encrypted images are denoted by $I_1, I_2, I_3$ respectively. The sensitivity coefficient to the parameter $K$ is denoted by the following formula:

$$P_s(K) = \frac{1}{2\times H\times W}\sum_{i,j}[N_s(I_1(i,j), I_2(i,j)) + N_s(I_1(i,j), I_3(i,j))]\times 100\%$$

where

$$N_s(x,y) = \begin{cases} 1, & x \neq y, \\ 0, & x = y, \end{cases}$$

and $\Delta\delta$ is the perturbing value. $P_s(K)$ implies the sensitivity to the perturbation of parameter $K$. The greater of $P_s(K)$, the more sensitive for the parameter $K$. Table 1 shows the results of the sensitivity test where the initial key values are set to be the following

$$x_1 = 0.367, y_1 = 0.761, z_1 = 0.579,$$
$$a_1 = 0.4, b_1 = 0.6, c_1 = 0.7,$$
$$x^* = 0.347,\ y^* = 0.532,\ z^* = 0.864,$$
$$a_2 = 0.3,\ b_2 = 0.5,\ c_2 = 0.9$$

The variations $\Delta\delta$ of the considered parameters are all set to be $10^{-16}$.

We apply the proposed image encryption scheme one round with only perturbing one cipher key $K$ with the corresponding variation value while fixing other parameters.

Table II. Results regarding the sensitivity to cipher keys.

| $K$ | $x_1$ | $y_1$ | $z_1$ | $a_1$ | $b_1$ | $c_1$ |
|---|---|---|---|---|---|---|
| $P_s(K)$ | 0.9963 | 0.9961 | 0.9962 | 0.9961 | 0.9959 | 0.9962 |
| $K$ | $x*$ | $y*$ | $z*$ | $a_2$ | $b_2$ | $c_2$ |
| $P_s(K)$ | 0.9964 | 0.9957 | 0.9963 | 0.9961 | 0.9962 | 0.9960 |

## IV. IMAGE HIDING SCHEME

An image hiding scheme is proposed in this section. We first use the encryption scheme proposed in Section III to encrypt the secret image; the encrypted secret image and the host image are transformed by DWT and then are merged in the frequency domain. The secret image can be detected or extracted easily. The image hiding scheme is proposed as follows:

Step 1. Apply the encryption scheme to encrypt the secret image $P$ sized $H\times W$, we get a cipher secret image $P_1$.

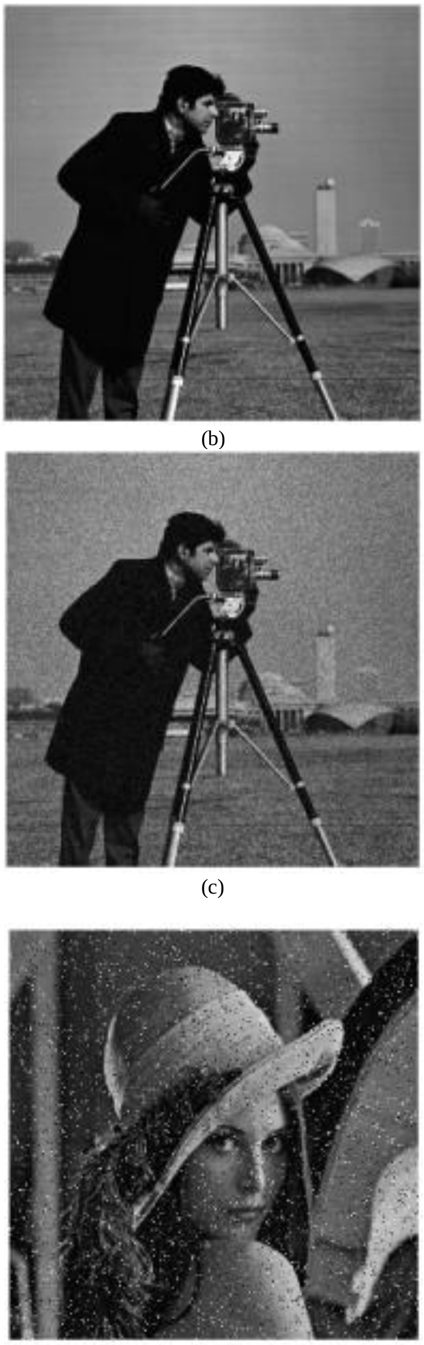
Step 2. Transform the host image $J$ with size $H\times W$ and the encrypted secret image $P_1$ by DWT with two-level SYM4 wavelet and get the corresponding coefficient matrices $J_1$ and $Q_1$, which are merged by the following formula:

$$R = \sigma Q_1 + (1-\sigma)J_1,\ t \in (0,1).$$

Step 3. Transform the merged matrix $R$ by the inverse wavelet transform to get the stego-image $H_s$.

We note that the merging factor $\sigma \in (0,1)$ should be chosen suitably in the imbedding scheme. If $\sigma$ is too large, the quality of the host image will be influenced. If $\sigma$ is too small, the information of the secret image becomes weak and it is difficult to extract the secret image. The extraction scheme is just the inverse of the imbedding scheme. Fig. 3 shows the hiding results where the 256X256 secret image Lena is imbedded in the host image Cameraman sized 256X256 with $\sigma$ =0.17. The experimental results are shown in Fig. 5.

(a)



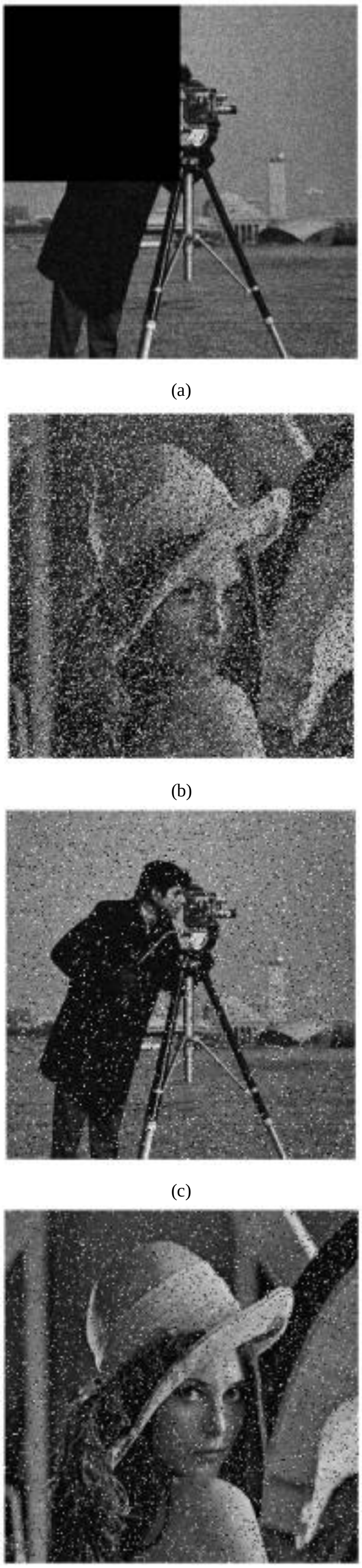
(b)

(c)

(d)

Figure 5. The hiding results: (a) secret image Lena, (b) host image cameraman, (c) stego-image, (d) extracted secret image.

Experiments are performed to test the robustness of the proposed image hiding scheme. Attacks in the experiments are cropping, salt and pepper noising, JPEG compression. Experimental results show the proposed scheme is robust against the considered attacks. All the attacking tests are applied to the stego-image with the same parameters as those in Fig. 5. The experimental results are shown in Fig. 6.

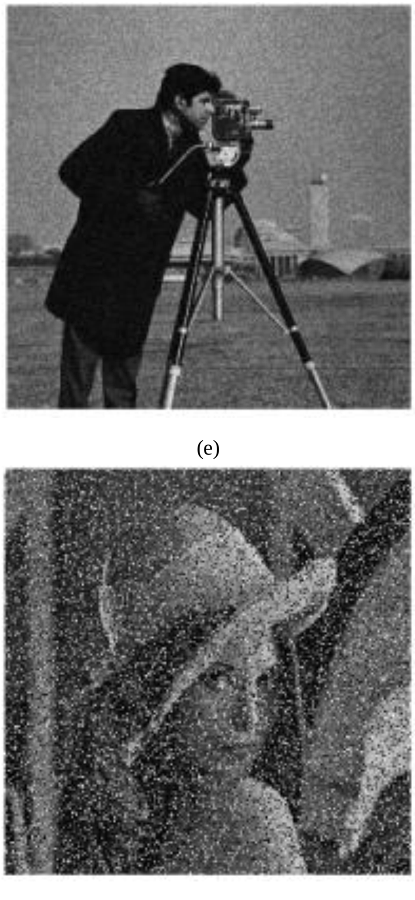


(a)

(b)

(c)

(d)



(e)

(f)

Figure 6. Results of attacking tests: (a) cropping attack with cut-off 128X128; (b) the extracted secret image from (a); (c) salt & pepper noising attack with density 0.02; (d) the extracted secret image from (c); (e) JPEG compression attack with quality 70; (f) the extracted secret image from (e).

## V. Conclusions

In this paper, the 3D sawtooth map is utilized to generate chaotic sequences for permuting the pixel positions and changing the pixel values to achieve the encryption of the secret images which are embedded in the host images. Simulation shows that the encryption scheme is secure and the image hiding scheme is robust against various kinds of attacks.

## Acknowledgment

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

## References

[1] M.S. Baptista, “Cryptography with chaos”, Physics Letter A, 240, 1998, pp. 50-54.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding”, IBM Syst. J. 35 (3-4) , 1996, pp. 313-336.

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

[4] 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.

[5] Guan Z.-H., Huang F., Guan W., Chaos-based image encryption algorithm, Physics Letters A, 2005, 346: 153-157.

[6] Lian S., Sun J., Wang Z., A block cipher based on a suitable use of the chaotic standard map, Chaos, Solitons and Fractals, 2005, 26: 117-129.

[7] V. Patidar, N. K. Pareek, K. K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer. Simulat., 14 (2009) 3056-3075.

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

[9] Zhu Z. L., Zhang W., Wong K. W., Yu H., A chaos-based symmetric image encryption scheme using a bit-level permutation, Information Sci., 2010, 181: 1171-1186.

[10] Liu, H., Wang, X., Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Opt. Commun. 2011, 284: 3895-3903.

[11] T. Gao, Z. Chen, A new image encryption algorithm based on hyper-chaos, Physics Letters A, 372(2008), 394–400.

[12] Ye R., Li H., A novel digital image scrambling and watermarking scheme based on cellular automata, in: Proceedings of the 2008 International Symposium on Electronic Commerce and Security, pp. 938-941.

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

[14] Ye, R., Zhou W., A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice, I. J. Computer Network and Information Security, 2012, 1: 38-44.

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

[16] Chan, C.K, Cheng, L.M., “Hiding data in images by simple LSB substitution”, Pattern Recognition, 2004, 37 (3): 469-474.

[17] Ahmidi, N., Safabakhsh, R., “A Novel DCT-based Approach for Secure Color Image Watermarking”, Proc. ITCC 2004 Int. Conf. Information Technology: Coding and Computing, 2004, 2: 709-713.

[18] Ming-Shing Hsieh, Din-Chang Tseng, and Yong-Huai Huang, “Hiding digital watermarks using multiresolution wavelet transform”, IEEE Trans. Industrial Electronics, 48, 2001, pp. 875-882.

[19] R. Clark Robinson, An Introduction to Dynamical Systems, Continuous and Discrete, Prentice Hall, 2004.Tan Zhiming. Research on Graph Theory Based Image Segmentation and Its Embedded Application Shanghai: Dissertation of Shanghai Jiao Tong University, 2007, 14-24.

[20] Shannon C. E., Communication theory of secrecy system. Bell Syst. Tech. J, 1949, 28: 656–715.

**Ruisong Ye** was 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.

**Wenping Yu** was born in 1986 and received her M.S. degree in Applied Mathematics in 2012 from Shantou University, Shantou, China. Her research interest is fractal geometry and its application in computer science.