ISSN 2277-3061

An Image Encryption Scheme Using 2D Generalized Sawtooth Maps

Ruisong Ye, Wenping Yu
Department of Mathematics, Shantou University
Shantou, Guangdong, 515063, P. R. China
rsye@stu.edu.cn

ABSTRACT

In this paper, a new image encryption scheme based on 2D generalized sawtooth map is proposed. Utilizing the chaotic nature of 2D generalized sawtooth maps, image pixel positions are scrambled and image pixels gray values are changed to encrypt the plain-images. 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.

Keywords

Chaotic System; Ergodicity; Sawtooth Map; Image Encryption

ISSN 2277-3061

INTRODUCTION

Thanks to the rapid developments in multimedia and network communication, electronic publishing and wide-spread dissemination of digital multimedia data have been communicated over the Internet and wireless networks. 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 [2-8].

Recently, some chaos-based image encryption algorithms were broken due to their small key spaces and weakly secure encryption mechanism [9-15]. As we know, a good encryption scheme should be sensitive to cipher keys; the key space should be large enough to resist brute-force attack; the permutation and diffusion processes should possess good statistical properties to frustrate differential attack, entropy attack, known-plaintext attack and chosen-plaintex attack, etc. 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 [16-20]. In this paper, an efficient image encryption scheme based on the ergodicity of 2D generalized sawtooth maps is proposed. Firstly, one 2D generalized sawtooth map with multi control parameters is utilized to generate chaotic orbits applied to permute the pixel positions, then another 2D generalized sawtooth map is employed to yield 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.

The rest of the paper is organized as follows. The 2D generalized sawtooth map and its chaotic nature are introduced in Section 2. An image encryption scheme consisting of a diffusion process and a permutation process is proposed then in Section 3. The performance analysis is presented in Section 4, including the key space analysis, statistic analysis, differential attack analysis. Experimental results show that the proposed image encryption scheme is highly secure. Section 5 concludes the paper.

2D GENERALIZED SAWTOOTH MAP

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

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

where $(x,y)\in[0,1]^2$ are the states of the system, and $a,b\in(0,1)$ are the control parameters. It is a noninvertible transformation of the unit square onto itself. The transformation is continuous and piecewise linear. For any $a,b\in(0,1)$, the piecewise linear map (1) has two Lyapunov exponents

$$\lambda_x=-a\ln a-(1-a)\ln(1-a),\quad \lambda_y=-b\ln b-(1-b)\ln(1-b),$$

which are both larger than 0, implying that the map is chaotic.

In this paper, we extend the 2D sawtooth map (1) to 2D generalized map $S_{a,b}:[0,1]^2 \to [0,1]^2$ with vectors a,b by the following way

$$S_{a,b}(x,y)=\begin{pmatrix}\frac{1}{a(i)-a(i-1)} & 0\\ 0 & \frac{1}{b(i)-b(i-1)}\end{pmatrix}\begin{pmatrix}x-a(i-1)\\ y-b(i-1)\end{pmatrix}, \quad (2)$$

where

$(x,y)\in[a(i-1),a(i))\times[b(i-1),b(i)),i=1,...,N$,

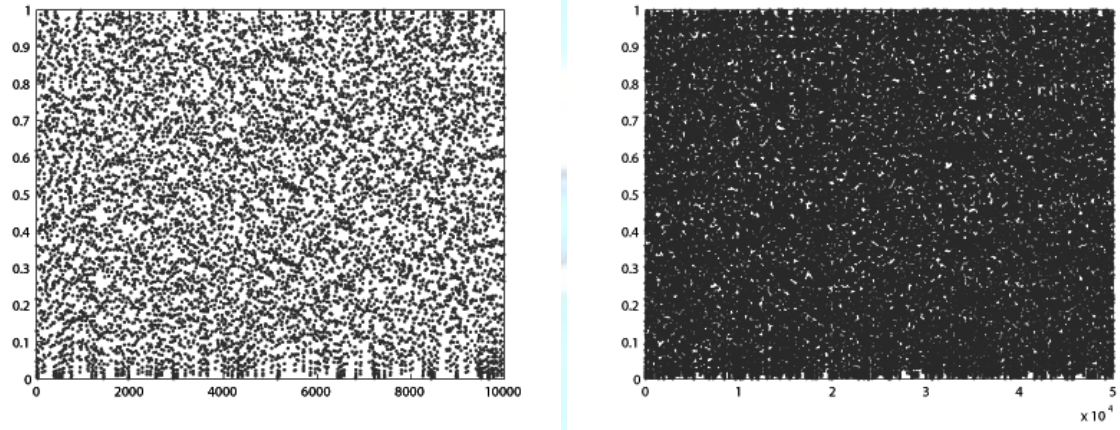
$a(i),b(i)\in(0,1),i=1,...,N-1$, $a(0)=0$, $a(N)=1$, $b(0)=0$, $b(N)=1$

are the control parameters.

It is easy to show that the two Lyapunov exponents of (2) are (see [21])

$$\lambda_x=\sum_{i=1}^{N}(a(i)-a(i-1))\ln(\frac{1}{a(i)-a(i-1)}),\ \ \lambda_y=\sum_{i=1}^{N}(b(i)-b(i-1))\ln(\frac{1}{b(i)-b(i-1)}).$$

It is obvious that λ_x,λ_y are all positive, implying that the 2D generalized sawtooth map is chaotic on $[0,1]^2$. A typical orbit of (x_0,y_0) derived from the dynamical system is $\{(x_k,y_k)=T^k(x_0,y_0),k=0,1,\cdots\}$, which is shown in Fig. 1. The plotting orbit points fill $[0,1]^2$ as long as the orbit is long enough, which indicates that the system is chaotic visually.



(a) orbit points 10000 (b) orbit points 50000

Fig. 1. Orbit derived from the considered 2D generalized sawtooth map

THE PROPOSED IMAGE ENCRYPTION SCHEME

We propose an image encryption scheme consisting of two processes: permutation of pixel positions and diffusion of pixel gray values. In the permutation stage, one 2D generalized sawtooth map is utilized to realize the shuffling of pixel positions. In the diffusion stage, another 2D generalized sawtooth map is used 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.

Permutation of Pixel Positions

Let the processed plain-image is of height H and width W and let $HW=H\times W$. The gray image is expressed as a matrix $P_{H\times W}$ with its entry $P(i,j)$ denoting the gray value of the pixel at (i,j). The permutation of pixel positions is outlined as follows.

Step 1. Set the initial values and the control parameters.

$x(0)=0.367, y(0)=0.761$, $a_1=(0,0.13,0.24,0.45,0.68,0.74,1)$, $b_1=(0,0.16,0.32,0.47,0.58,0.86,1)$.

Step 2. Iterate the 2D generalized sawtooth map for $\max\{H,W\}$ times to yield two sequences $\{x(n),y(n),n=1,2,\cdots,\max\{H,W\}\}$:

ISSN 2277-3061

$$(x(i), y(i)) = S_{a_1,b_1}(x(i-1), y(i-1)), i = 1,2,\cdots,\max\{H,W\}.$$

Step 3. Sort $\{x(i): i = 1,\cdots,H\}$, $\{y(j): j = 1,\cdots,W\}$ to get two index vectors

$$\{I_x(i), i = 1,2,...,H\}, \quad \{I_y(j), j = 1,2,...,W\}.$$

Step 4. The yielded index vectors are utilized to permute the pixel positions by

$$P1(i, j) = P(I_x(i), I_y(j),), i = 1,2,...,H, j = 1,2,...,W$$

and the scrambled image $P1$ is the obtained.

Diffusion of Pixel Gray Values

For a secure encryption algorithm, a mechanism of diffusion is necessary. There are two reasons for introducing diffusion process. On one hand, the diffusion processing can render the discretized chaotic Baker map non-invertible. On the other hand, it can significantly change the statistical properties of the plain-image by spreading the influence of each bit of the plain-image all over the cipher-image. Though the shuffling process has changed the pixel positions of the plain-image, it can not change the statistical properties of the plain-image. The diffusion process will enhance the resistance to the statistical attack and differential attack greatly, in which the histogram of the cipher-image is fairly uniform and is significantly different from that of the original image. We proposed a bilateral diffusion here and the diffusion stage is outlined as follows.

Step 1. Set the initial values and the control parameters. $x1(0) = 0.46, y1(0) = 0.27$,

$a_2 = (0, 0.17, 0.24, 0.35, 0.58, 0.84, 1)$, $b_2 = (0, 0.26, 0.33, 0.48, 0.68, 0.79, 1)$.

Step 2. Reshape the permuted image $P1$ to be a vector sized $1 \times HW$. Set $i = 1$,

$$P2(1) = P1(1) \oplus floor(L \times (x1(0) + y1(0))/2),$$

where $floor(x)$ indicates the largest integer number not greater than x, L is the gray scale of the considered image.

Step 3. Set

$$c(i) = floor(L \times x1(i)), \quad d(i) = floor(L \times y1(i)), \quad s = 1 + [P2(i) \bmod 2].$$

The 2D generalized sawtooth map is then iterated s time to get $(x1(i+1), y1(i+1))$:

$$(x1(i+1), y1(i+1)) = S^s_{a_2,b_2}(x1(i), y1(i)).$$

The bitxor operation $\oplus$ and the mod operation are then applied to change the pixel gray value.

$$P2(i+1) = P2(i) \oplus [(floor((c(i) + d(i))/2) + P1(i+1)) \bmod L].$$

Step 4. Set $i = i + 1$ and repeat Step 3 till $i = HW - 1$ and one diffused image $P2$ is yielded.

We note that the above diffusion process implies that it cannot 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. The chaotic map used here is also the 2D generalized sawtooth map.

Step 5. The initial values are set to be $x2(0) = 0.34$, $y2(0) = 0.86$ and the same control parameters a_2, b_2. The 2D generalized sawtooth map is then applied.

$$(x2(j), y2(j)) = S_{a_2,b_2}(x2(j-1), y2(j-1)),$$
$$u(j) = floor(L \times x2(j)), v(j) = floor(L \times y2(j)), j = 1,2,...,HW.$$

Step 6. Set

$$P3(M \times N) = P2(M \times N) \oplus floor((u(M \times N) + v(M \times N))/2).$$

Step 7.

$$P3(M \times N - j) = P3(M \times N - j + 1) \oplus [(floor((u(j) + v(j))/2) + P2(M \times N - j)) \bmod L], \ j = 1,2,...,M \times N - 1.$$

Convert $\{P3(k), k = 1,2,\cdots,HW\}$ to a 2D matrix Q with height H and width W. Q is the resulted cipher-image. The diffusion process is completed. The plain-image and the cipher-image are shown in Fig. 2.

We note that the above encryption scheme is invertible. The reverse diffusion stage can be stated as

$$P2(M\times N)=P3(M\times N)\oplus floor((u(M\times N)+v(M\times N))/2),$$

$$P2(HW-j)=[(P3(HW-j)\oplus P3(HW-j+1))-floor((u(j)+v(j))/2)]\bmod L,\ j=1,2,...,HW-1.$$

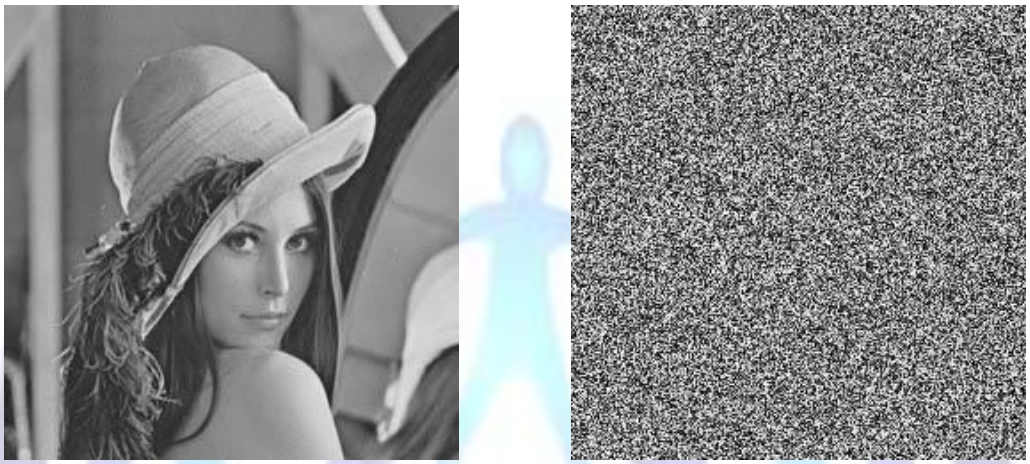
$$P1(1)=P2(1)\oplus floor(L\times(x1(0)+y1(0))/2),$$

$$P1(i+1)=[(P2(i)\oplus P2(i+1))-floor((c(i)+d(i))/2)]\bmod L,\ \ i=1,2,...,HW-1.$$

Rearrange $P1$ to be a matrix with size $H\times W$, and let

$$P(I_x(i),I_y(j))=P1(i,j),i=1,2,...,H,\ j=1,2,...,W.$$

P is then the decrypted original image.



(a) (b)

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

PERFORMANCE ANALYSIS

According to the basic principle of cryptology [1], 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 section, some security analysis has been performed on the proposed image encryption scheme, including the most important ones like key space analysis, statistical analysis, and differential analysis. All the analysis shows that the proposed image encryption scheme is highly secure.

Key Space Analysis

A good image encryption scheme 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 vectors

$$a_1(i),b_1(i),i=1,\cdots,N_1-1,a_2(j),b_2(j),\ j=1,\cdots,N_2-1$$

and the initial conditions $x(0),y(0),x1(0),y1(0),x2(0),y2(0)$ consist of 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

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

ISSN 2277-3061

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 ($N_1 = N_2 = 6$):

Keys of permutation process are

$x(0) = 0.367, y(0) = 0.761$, $a_1 = (0, 0.13, 0.24, 0.45, 0.68, 0.74, 1)$, $b_1 = (0, 0.16, 0.32, 0.47, 0.58, 0.86, 1)$.

Keys of Diffusion process

$x1(0) = 0.46, y1(0) = 0.27$, $x2(0) = 0.34, y2(0) = 0.86$,

$a_2 = (0, 0.17, 0.24, 0.35, 0.58, 0.84, 1)$, $b_2 = (0, 0.26, 0.33, 0.48, 0.68, 0.79, 1)$.

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. The results are shown in Table 1. The results imply that the control parameters and the initial conditions are all strongly sensitive. It also implies from the results that the key space is more than 10^{416}, which is large enough to make brute-force attack infeasible.

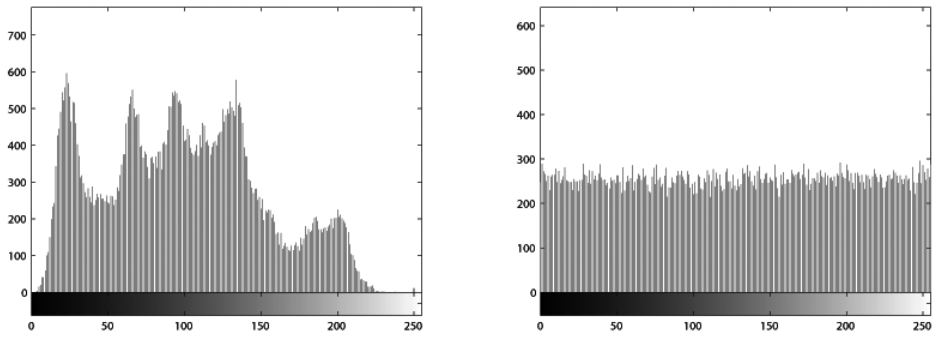
Table 1. The sensitivity to cipher keys

K	$x(0)$	$y(0)$	$x1(0)$	$y1(0)$	$x2(0)$	$y2(0)$
$P_s(K)$	99.60	99.61	99.61	99.62	99.58	99.63
K	$a_1(1)$	$a_1(2)$	$a_1(3)$	$a_1(4)$	$a_1(5)$	
$P_s(K)$	99.62	99.59	99.64	99.62	99.58	
K	$b_1(1)$	$b_1(2)$	$b_1(3)$	$b_1(4)$	$b_1(5)$	
$P_s(K)$	99.61	99.57	99.63	99.60	99.61	
K	$a_2(1)$	$a_2(2)$	$a_2(3)$	$a_2(4)$	$a_2(5)$	
$P_s(K)$	99.62	99.60	99.61	99.58	99.63	
K	$b_2(1)$	$b_2(2)$	$b_2(3)$	$b_2(4)$	$b_2(5)$	
$P_s(K)$	99.61	99.61	99.62	99.59	99.64	

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.



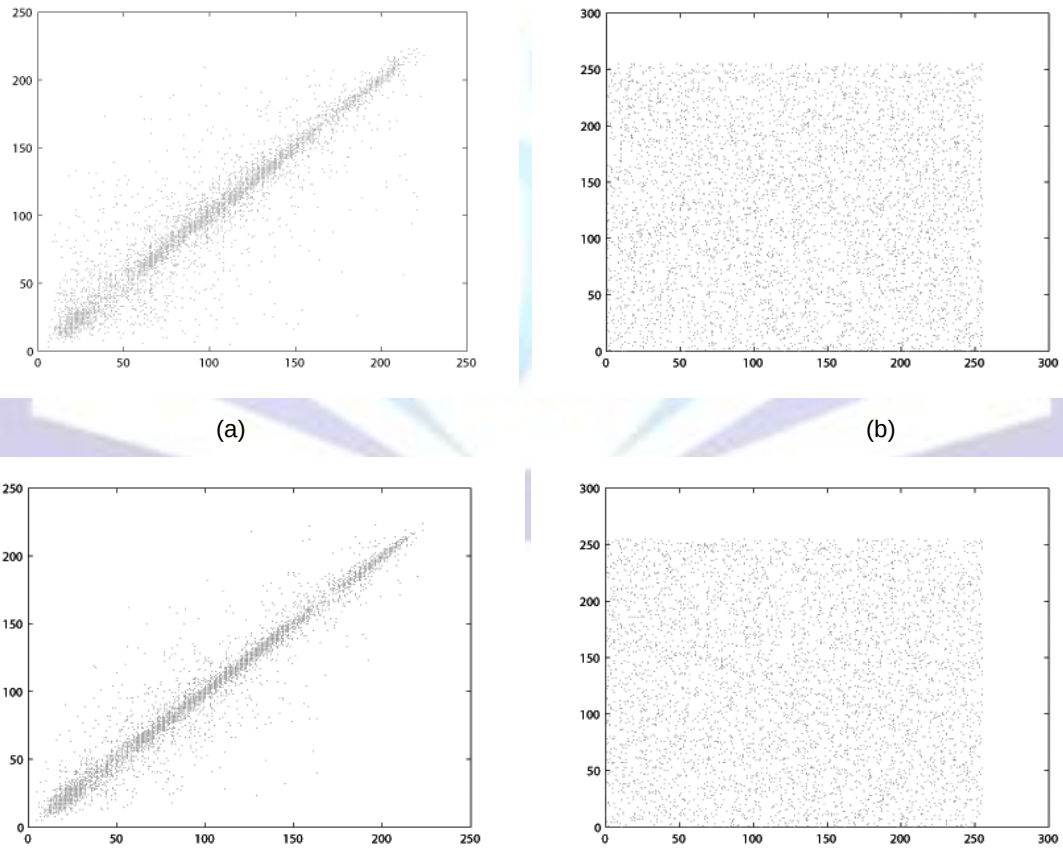
(a) (b)

Fig. 3. (a) histogram of plain-image, (b) histogram of cipher-image

(ii)The correlations of adjacent pixels. To test the correlations between two adjacent pixels, the following performances are carried out. First, we select 1000 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:

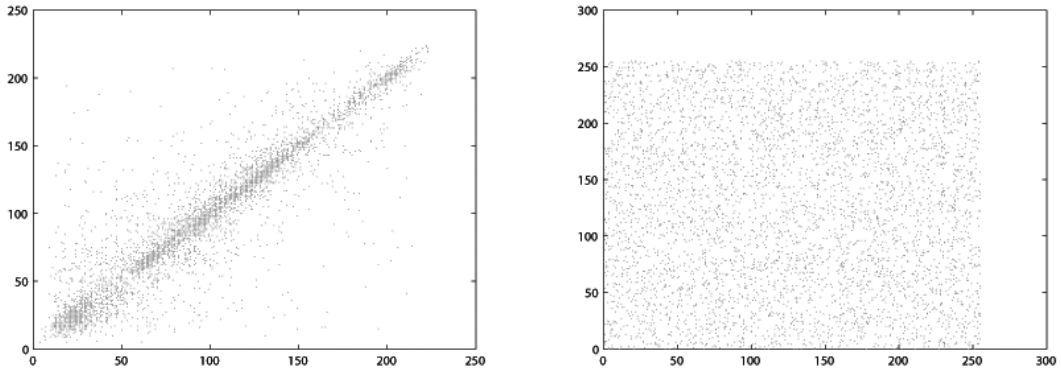
$$Cr = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},\ cov(x,y) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y)),\ E(x) = \frac{1}{T}\sum_{i=1}^{T}x_i,\ D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2,$$

where x, y are the 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 Table 2. 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)

Fig. 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

Table 2. Correlation coefficients of two adjacent pixels

	Plain-image	Cipher-image
Horizontal	0.9488	0.0076
Vertical	0.9658	-0.0089
Diagonal	0.9219	-0.0039

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

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

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 test of the plain-image is Lena image. We randomly select 5 pixels and change the gray values with a difference of 1, for example, we replace the gray value of the pixel at position (32,167) by 1, and get NPCR=99.63%, UACI=34.70%. The numerical results are shown in Table 3. We observe from Table 3 that the two measure values are exceptionally good undergoing only one round of encryption.

Table 3. Results of NPCR and UACI tests of Lena

Position	(32,167)	(78,96)	(125,46)	(210,4)	(225,129)
NPCR(%)	99.63	99.76	99.69	99.82	99.60
UACI(%)	34.70	33.31	38.73	32.27	30.80

CONCLUSIONS

An efficient image encryption scheme based on 2D generalized sawtooth map s is proposed in the paper. The proposed scheme can shuffle the plain-image efficiently in the permutation process. An effective diffusion process is also presented to change the gray values of the whole image pixels. Security analysis including key space analysis, statistical attack analysis and differential attack analysis are performed numerically and visually. All the experimental results show that the proposed encryption scheme is secure thanks to its large key space, its highly sensitivity to the cipher keys and plain-

images. The proposed encryption scheme is easy to manipulate and can be applied to any images with unequal width and height as well. All these satisfactory properties make the proposed scheme a potential candidate for encryption of multimedia data such as images, audios and even videos.

ACKNOWLEDGMENTS

This research is supported by National Natural Science Foundation of China (No. 11071152 & No. 11271238).

REFERENCES

[1] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.

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

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

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

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

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

[7] K. W. Wong, B. Kwok and W.S. Law, "A fast image encryption scheme based on chaotic standard map," Physics Letters A , 372, pp. 2645-2652, 2008.

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

[9] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," In Proc. IEEE Int. Symposium on Circuits and Systems, vol. II, pp. 708-711, 2002.

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

[11] C. Li, S. Li, G. Chen and W.A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence", Image and Vision Computing, 27, pp. 1035-1039, 2009.

[12] D. Xiao, X. Liao and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm", Chaos, Solitons and Fractals, 40, pp. 2191-2199, 2009.

[13] R. Rhouma, E. Solak and S. Belghith, "Cryptanalysis of a new substitution-diffusion based image cipher", Commun. Nonlinear Sci. Numer. Simulat., 15, pp. 1887-1892, 2005.

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

[15] J. M. Liu and Q. Qu, "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.

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

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

[18] R. Ye and H. Huang, "Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking", I. J. Image, Graphics and Signal Processing, 2(1), pp. 19-29, 2010.

[19] R.Ye and W. Zhou, "A chaos-based image encryption scheme using 3D skew tent map and coupled map Lattice", I. J. Computer Network and Information Security, 4(1), pp. 38-44, 2012.

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

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

Author biography

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.

Wenping Yu, a master degree candidate at department of mathematics in Shantou University.