I.J. Modern Education and Computer Science, **2014, 3, 19-30**
Published Online March 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.03.03

A Secure and Efficient Image Encryption Scheme Based on Tent Map and Permutation-substitution Architecture

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

Shaojun Zeng
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
Email: 10sjzeng@stu.edu.cn

Junming Ma
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
Email: 10jmma@stu.edu.cn

Chuting Lai
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China
Email: 10ctlai@stu.edu.cn

***Abstract*—**A secure image encryption scheme based on 2D skew tent map is proposed for the encryption of color images. The proposed encryption scheme is composed of one permutation process and one substitution process. The 3D color plain-image matrix is converted to 2D image matrix first, then 2D skew tent map is utilized to generate chaotic sequences, which are used for both permutation process and substitution process. The chaotic sequence for permutation process is dependent on plain-image and cipher keys, resulting in good key sensitivity and plaintext sensitivity. The substitution process is first initiated with the initial vectors generated by the cipher keys and 2D skew tent map, then the gray values of row and column pixels of 2D image matrix are mixed with the pseudorandom number sequences via bitxoring operation. Both permutation process and substitution process are executed row-by-row and column-by-column instead of pixel-by-pixel to improve the speed of encryption. The security and performance of the proposed image encryption have been analyzed, including histograms, correlation coefficients, information entropy, key sensitivity analysis, key space analysis, differential analysis, encryption/decryption rate analysis etc. All the experimental results suggest that the proposed image encryption scheme is robust and secure and can be used for secure image and video communication applications.

***Index Terms*—**Chaotic system, skew tent map, image encryption, permutation-substitution architecture

I. Introduction

Chaos theory is one nonlinear science theory and has a great reputation. It is called the third resolution after the relativity and the quantum mechanics in the 20th century. It covers most aspects of science, such as mathematics, physics, biology, computer, finance and even arts. Especially chaos theory has been successfully introduced to modern cryptography thanks to its fantastic features, such as ergodicity, pseudo-randomness, orbit inscrutability, sensitivity to initial conditions and control parameters, etc. which are in line with the fundamental requirements like confusion and diffusion in cryptography. These properties make chaotic systems a potential candidate for constructing cryptosystems [1-6]. With the rapid developments of innovative technologies in information and computer science in the last decades, a bulk of digital multimedia data like images, videos, audios is being stored on different media, increasingly shared and communicated over the Internet and wireless networks. Therefore protection of digital image information against illegal copying and distribution has become extremely urgent. Encryption is a direct and efficient way to protect the information from unauthorized eavesdropping. Digital images possess some intrinsic features, such as bulk data capacity, high correlation among adjacent pixels, and human visual properties. As a consequence, traditional encryption algorithms, such as DES, RSA [7], 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. In 1998, Fridrich

firstly proposed the fundamental architecture of chaos-based image encryption [1]. The proposed architecture is usually composed of two processes: chaotic confusion of pixel positions by permutation process and diffusion of pixel gray values by diffusion process, where the former permutes the plain-image pixel positions governed by a 2D chaotic map, while the latter changes the pixel gray values sequentially controlled by a 1D chaotic map, so that a tiny change for one pixel can spread out to almost all pixels in the whole image. The Fridrich architecture has become the most popular structure adopted in a great number of chaos-based image encryption algorithms subsequently proposed [2-6, 8-14]. A good permutation process should show good shuffling effect and a good diffusion process should cause great modification over the cipher-image even if only a minor change for one pixel in the plain-image. However it has been pointed out that the proposed permutation-diffusion architecture with fixed parameters has one fatal flaw in [15], that is, the two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value. Therefore, such a kind of encryption algorithms can be attacked by the following steps: (i) a homogeneous image with identical pixel gray values is adopted to eliminate the confusion effect; (ii) the key-stream of the diffusion process is obtained via known-plaintext or chosen plaintext attacks; (iii) the remaining cipher-image can be regarded as the output of a kind of permutation-only cipher, which has been shown insecure and can be cryptanalyzed by known-plaintext or chosen plaintext attacks [16,17].

In this paper, we propose an image encryption scheme with the so-called permutation-substitution mechanism. We refer the readers to [18] for a brief description of chaos-based permutation-substitution technique. Patidar et al. subsequently contributed several papers also owning such a kind of permutation-substitution mechanism [19-21]. Especially, the recent contribution [21] proposes a novel image encryption scheme consisting three processes: preliminary permutation, substitution and main permutation. The proposed image encryption scheme demonstrates strong robustness and great security. It is a loss-less symmetric block cipher and specifically designed for the color images but may also be used for the gray scale images. A cipher key of 161-bit, comprising of the initial conditions and system parameters of the considered chaotic standard map, number of iterations and number of rounds, is used in the algorithm. All the three processes are done row-by row and column-by-column instead of pixel-by-pixel to improve the speed of encryption. To yield excellent key sensitivity and plaintext sensitivity, both preliminary permutation and main permutation are designed to be dependent on the plain-image and controlled through the pseudo random number sequences (PRNS) generated from the chaotic standard map. The substitution process is initialized with the initial vectors generated via the cipher keys and chaotic standard map, and then the pixel gray values of row and column pixels of input 2D matrix are bitxored with the PRNS generated from the standard map. Although the proposed substitution process is operated row-by row and column-by-column, which is different from conventional diffusion functions acting on the input image pixels subsequently one by one, the diffusion effect is also obtained, showing good resistance against differential analysis.

Benefited from the idea of permutation-substitution structure, we design a novel cryptosystem to avoid the drawback of the conventional Fridrich architecture. We make two improvements over the algorithm proposed in [21]. One is the use of 2D chaotic skew tent map instead of the use of standard map. The other is our image encryption scheme is composed of two stages: one permutation stage and one substitution stage. The 2D skew tent map shows excellent chaotic features, such as ergodicity, pseudo-randomness, and sensitivity to initial conditions and control parameters [22]. It has already been well-tested and proved to be a good pseudo-random number generator [23]. The application of 2D skew tent map will own higher computational efficiency than 2D standard map because sine function exists in the latter map. In more details, there are three multiplication operations and two division operations for one pseudo-random gray value between 0 and 255 in case of standard map, while there are two multiplication operations and two division operations in case of 2D skew tent map. Furthermore, there exists one sine function operation in standard map. As a result, it is more efficient to generate one pseudo-random gray value via 2D skew tent map, especially for large images. In our encryption scheme, only one permutation stage and one substitution stage are applied, however, two permutation stages and one substitution stage are applied in [21]. Therefore it is obvious to see that our proposed image encryption scheme demonstrates more efficient regarding the speed of encryption. Experiments also verify such a conclusion. The security and performance analysis of the proposed image encryption are carried out using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis etc. All the experimental results show that the proposed image encryption scheme is highly secure and excellent performance, which makes it suitable for practical application.

The rest of the paper is organized as follows: In Section II, we briefly introduce the 2D skew tent map and discuss its chaotic natures. Section III devotes to designing the image encryption scheme. One permutation stage and one substitution stage are presented to encrypt color images. In Section IV, we present the results of security and performance analysis of the proposed image encryption scheme using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis etc. Section V concludes the paper.

II. The 2D Skew Tent Map

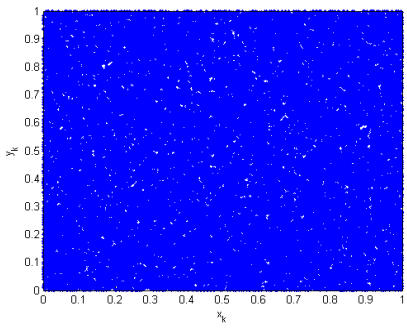
The 2D skew tent map $T_{a,b}:[0,1]^2 \to [0,1]^2$ is given by

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

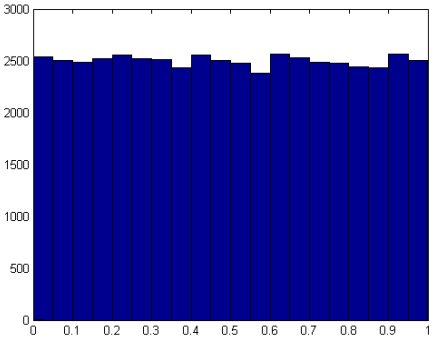
where $a,b\in(0,1)$. It is easy to show that the two Lyapunov exponents of 2D skew tent map are (see [23])

$$\begin{aligned}\lambda_x &= a\ln(\frac{1}{a})+(1-a)\ln(\frac{1}{1-a}),\\ \lambda_y &= b\ln(\frac{1}{b})+(1-b)\ln(\frac{1}{1-b}),\ a,b\in(0,1).\end{aligned} \quad (2)$$

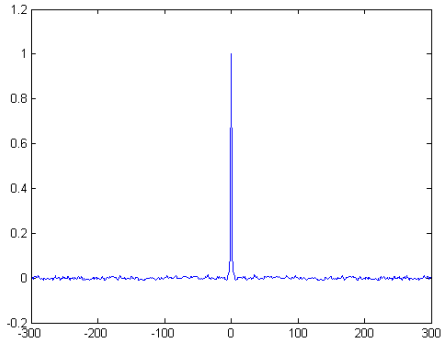
It is obvious that λ_x,λ_y are all positive, implying that (1) is chaotic on $[0,1]^2$. The 2D tent map therefore owns good chaotic natures, its orbits are ergodic over $[0,1]^2$ and its distribution density function is uniform which shows good pseudo-randomness. A typical orbit of (x_0,y_0) derived 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(a) for $a=0.21,b=0.43,x_0=0.37,y_0=0.67$. The plotting orbit points will theoretically fill the unit square $[0,1]^2$. As long as the orbit is long enough, the orbit points will fill $[0,1]^2$ 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. Fig.1(b) depicts the histogram of $\{y_k,k=1,2,\cdots,50000\}$, demonstrating the uniformity of the orbit points distribution. There exist some other good dynamical features in 2D tent maps, such as desirable auto-correlation and cross-correlation features demonstrated in Figs. 1(c)-(d).



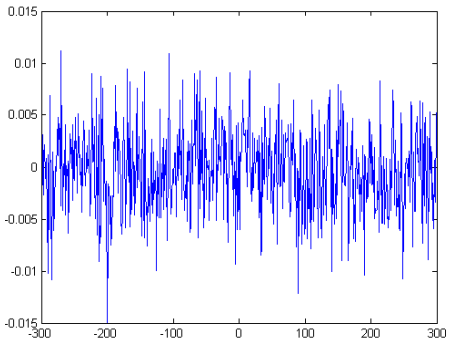
(a) the orbit $\{(x_k,y_k),k=1,2,\cdots,50000\}$



(b) the histogram diagram of $\{y_k,k=1,2,\cdots,50000\}$



(c) Auto-correlation of sequence $\{y_k\}$



(d) Cross-correlation of sequence $\{x_k\}$ and $\{y_k\}$

Fig 1. The chaotic nature of 2D tent map.

III. The Proposed Image Encryption Scheme

We discuss the detailed image encryption procedure step-by-step in this section. The encryption procedure comprises of one permutation and one substitution.

A. Preparation for Encryption

This part just makes some preliminary preparations for the encryption. It only depends on the cipher keys and size of the plain-image. If the size of the image and cipher keys are fixed, then this part may be executed in advance and the results may be stored for further use to speed up the encryption. In this part, we read the plain-

image and get the corresponding height H and width W of the color plain-image, then calculate the height NH and width NW of the 2D matrix, which is used to place all the red, green, blue intensity values of the color plain-image. We also generate the initialization vectors for the row and column substitutions and the substitution vectors to be used in the substitution process. The detailed preparation process is outlined as follows.

1. Reading the plain-image.

The color plain-image with height H and width W is the image to be encrypted. The image can be modeled as one 3D matrix $P(i, j, k)$ of integers between 0 and 255, where $1 \le i \le H$, $1 \le j \le W$ and $1 \le k \le 3$. The read input image matrix is then one 3D matrix sized $H \times W \times 3$ with integer elements.

2. Calculating the height NH and width NW of new 2D matrix.

The height NH and width NW of new 2D matrix is calculated by

$$\begin{cases} \min\ (NW - NH), \\ s.\ t. \\ NH \times NW = H \times W \times 3, \\ NW \ge NH. \end{cases} \tag{3}$$

NH and NW calculated by (3) can form a 2D matrix with height and width as approximately equal as possible. The best case is $NH = NW$; if it is not possible, then we form a rectangular matrix with the lowest possible difference in the number of rows and columns. The motive of such a calculation is to reduce the workload of the encryption.

3. Generating the initial vectors for the row and column substitutions in the substitution process.

With the initial conditions x_0, y_0, system parameters a, b and N given in the cipher keys, we iterate the 2D skew tent map (1) for N times to get rid of transient effect. The values of (x_N, y_N) are stored for further use. Now use the following algorithm to generate the initial vectors for row and column substitutions:

$x = x_N$
$y = y_N$
for $k = 1$ to NW *step* 1
  $[x, y] = tent(x, y, a, b, 1)$;
  $IVR(k) = \lfloor x \cdot 256 \rfloor$
  $IVC(k) = \lfloor y \cdot 256 \rfloor$
end

where $[x, y] = tent(x, y, a, b, 1)$ denotes the module function of skew tent map (1). The input parameters $x, y, a, b, 1$ in $tent(x, y, a, b, 1)$ refer to the state variables, system parameters and the iteration time. The output parameters are also set to be x, y. $\lfloor \cdot \rfloor$ represents the floor function. Now consider only the first NH elements of IVC and throw away the rest, and then set IVC=transpose(IVC). In this way we finally generate a row vector IVR having NW elements and a column vector IVC having NH elements.

4. Generating the substitution vectors.

Use the following algorithm to generate the substitution vectors for the substitution of rows and columns of 2D matrix.

for $j = 1$ to NW *step* 1
  [x,y]=tent(x,y,a,b,1);
  $SVR(j) = \lfloor x \cdot 256 \rfloor$
  $SVC(j) = \lfloor y \cdot 256 \rfloor$
end

B. Permutation Process

In this part, 3D color plain-image matrix is first changed to a 2D matrix. Permutations of row-by-row and column-by-column are performed to shuffle the elements of the yielded 2D matrix. The permutation process mixes the pixels of red, green and blue channels of the input color plain-image. The permutation process is designed to be dependent on the content of input plain-image; it is also governed by the pseudo-random sequences generated by the chaotic 2D skew tent map with the cipher keys. As a result, the permutation process is dependent on both cipher keys and plain-image. The encryption scheme is thereby owns one-time key effect. Even with the cipher keys fixed, the pseudo-random sequences generated by the chaotic 2D skew tent map is completely different as it is plain-image dependent. We use the following Steps 5 & 6 for executing this part.

5. Converting 3D color plain-image matrix into 2D matrix.

We first generate an initialized 2D matrix sized $NH \times NW$, and then read the data of 3D matrix with size $H \times W \times 3$ column-by-column and place them in the 2D matrix column-by-column. The newly formed 2D matrix is then represented by $P(i, j)$ where $1 \le i \le NH$ and $1 \le j \le NW$, NH and NW respectively are height and width of the 2D matrix.

6. Permuting the 2D matrix row-by-row and column-by-column.

We calculate the number of iterations to skip before starting the permutation. It is calculated by

$$N1 = P(1,1) + P(1,2) + \ldots + P(1,NW) + P(2,1) + \ldots + P(NH,NW) \quad mod\ 256. \tag{4}$$

Therefore the number of iterations $N1$ is related to the 2D matrix elements and equivalently related to the color plain-image. Starting with the initial conditions (x_N, y_N) generated in Step 3 and the parameter a,b given in the cipher keys, we iterate the 2D skew tent map for $N1$ times and then save the new values as (x, y). Now use the following algorithm for the permutation of the 2D matrix:

for $j = 1$ to NW *step* 1
  [x,y]=tent(x,y,a,b,1);
  $PPR1(j) = 1 + \lfloor x \cdot NH \rfloor$
  $PPC1(j) = 1 + \lfloor y \cdot NW \rfloor$
  [x,y]=tent(x,y,a,b,1);
  $PPR2(j) = 1 + \lfloor x \cdot NH \rfloor$
  $PPC2(j) = 1 + \lfloor y \cdot NW \rfloor$
end

for $j = 1$ *to* NH *step* 1
  interchange $P(PPR1(j),:)$ *and* $P(PPR2(j),:)$
end

for $j = 1$ *to* NW *step* 1
  interchange $P(:,PPC1(j))$ *and* $P(:,PPC2(j))$
end

In the above algorithm $P(i,:)$ and $P(:,j)$ respectively, represent all the elements of ith row and all the elements of jth column.

C. Substitution Process

We perform the substitution operations on the 2D matrix obtained after the execution of permutation. The substitution is also implemented row-by-row and column-by-column sequentially. The detailed algorithm is outlined as Steps 7 & 8.

7. Substituting the 2D matrix row-by row and column-by-column.

The substitution of elements of first row is done by bitxoring them with the elements of row initialization vector IVR and the first element of row substitution vector, SVR(1), generated in the first part Preparation for encryption. The substitution of remaining rows is done sequentially by bitxoring them with the previous row and the corresponding element of row substitution vector. After performing the row substitution of all rows, the column substitution is similarly processed. The substitution of elements of first column is done by bitxoring them with the elements of column initialization vector IVC and the first element of column substitution vector SVC(1). The substitution of remaining columns is done sequentially by bitxoring them with the previous column and the corresponding element of column substitution vector. The execution algorithm for the substitution is outlined as follows:

for $i = 1$ to NR *step* 1
  % *substitution*
  $P(1,:) = (P(1,:) \oplus IVR) \oplus SVR(1)$
  for $j = 2$ *to* NH *step* 1
    $P(j,:) = (P(j,:) \oplus P(j-1,:)) \oplus SVR(j)$
  end

  $P(:,1) = (P(:,1) \oplus IVC) \oplus SVC(1)$
  for $j = 2$ *to* NW *step* 1
    $P(:,j) = (P(:,j) \oplus P(:,j-1)) \oplus SVC(j)$
  end
end

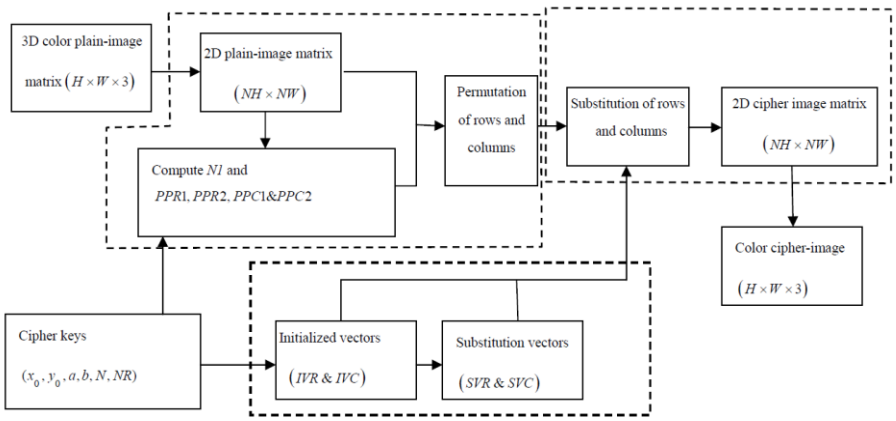


Fig 2. Flow chart of the proposed image encryption scheme.

8. Converting the resulted 2D matrix back into 3D color cipher image matrix.

Create one initialized 3D zero matrix with size $H \times W \times 3$ and then read the data of resultant 2D matrix P (obtained after the above mentioned encryption) column-by-column and place them in the 3D matrix CI column-by-column. The 3D matrix $CI(i, j, k)$ ($1 \le i \le H$, $1 \le j \le W$, $1 \le k \le 3$) is thus formed and finally converted to a color image, which is the final encrypted image.

The flow chart of the complete encryption scheme is depicted in Fig. 2, where the three parts (Parts A, B and C as described above) are separately marked by dotted boxes.

IV. Performance and Security Analysis

According to the basic principle of cryptology [7], a good encryption scheme requires desired sensitivity to cipher keys, i.e., the cipher-text should have close correlation with cipher keys. Furthermore, 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 analysis attack, differential attack, chosen plaintext and known plaintext, etc. In this section, some security and performance analyses have been carried out for the proposed image encryption scheme, including the most important ones, such as histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis etc. Experimental results suggest that the proposed image encryption technique is robust and secure and can be used for the secure image and video communication applications.

A. Key Space Analysis

The key space of an encryption scheme is composed of the total number of different cipher keys that can be used in the encryption procedure. 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. If the key space of an encryption scheme is large enough (for example, more than 128-bit, which is considered to be secure for most common cryptographic applications in view of the speed of the up-to-date computing machines), then the brute-force attack on such scheme becomes infeasible. The cipher keys of the proposed image encryption scheme consists of four floating point numbers and one integer (x_0, y_0, a, b, N) where $x_0, y_0, a, b \in (0,1)$, N is any integer value, ideally should be greater than 100. If we use the precision of 10^{-14} as we have used in the key sensitivity tests, then the total number of possible values of x_0, y_0, a, b are $10^{14\times 4} = 10^{56}$. The total number of possible values of N is 10^3. Thus the complete key space for the proposed encryption scheme is 10^{59}, which is equivalently equal to $\log_2 10^{59} \approx 196$ bits, that is, we can get the effective key length 196 bits. The key space is large enough to resist the brute-force attack.

B. Statistical Analysis

Shannon pointed out in his masterpiece [24] 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. Histogram analysis is a visual test which shows the pixel distribution over the available intensity levels. An image histogram is a graph showing the number of pixels at each different intensity value existing in the considered image. For an 8-bit gray image, there are 256 different possible intensities; hence the histogram will graphically display the distribution of pixels among these 256 intensity values. For a 24-bit color image, three histograms can be drawn for each 8-bit red, green and blue channel. Encrypt the color image Lena one round with cipher key (0.27, 0.34, 0.22, 0.66, 108), and then plot the histograms of plain-image and cipher-image as shown in Fig. 3. One can conclude from the histograms of the cipher-image that they are fairly uniform and significantly different from the corresponding histograms of the plain-image. Hence the proposed image encryption scheme does not provide any useful information for the opponents to perform any effective statistical analysis attack on the cipher-image.

(ii) Correlation of adjacent pixels. It is common sense that for an ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. An ideal encryption technique should produce cipher-images with less correlation in the adjacent pixels. To quantify and compare the horizontal, vertical and diagonal correlations of adjacent pixels in the plain and cipher images, we calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels respectively. First, we select 6000 pairs of two adjacent pixels randomly from an image and then calculate the correlation coefficient of the selected pairs using the following formulae:

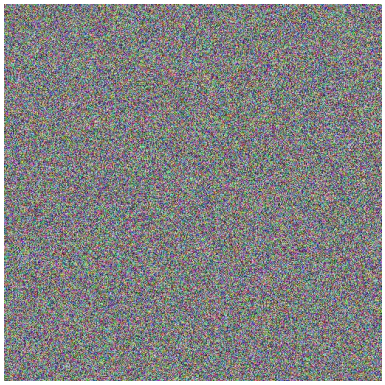
$$Cr = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

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

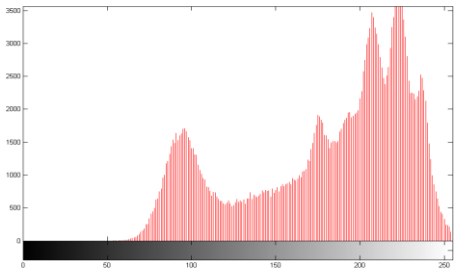
$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i,\ D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2, \quad (5)$$

where x_i, y_i form the ith pair of horizontally, vertically or diagonally adjacent pixels and T is the total number of pairs of adjacent pixels randomly selected. The correlation coefficients of horizontally, vertically, diagonally adjacent pixels for plain-image Lena and the cipher-image are given in Table I. It is clear from Table I that the proposed image encryption technique significantly reduces the correlation between the adjacent pixels of the plain image.

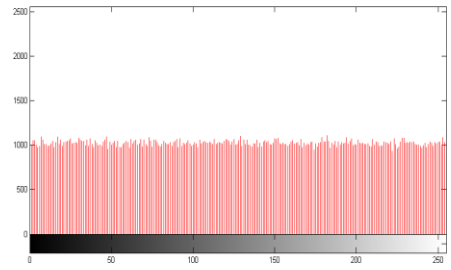
(a) Plain-image Lena



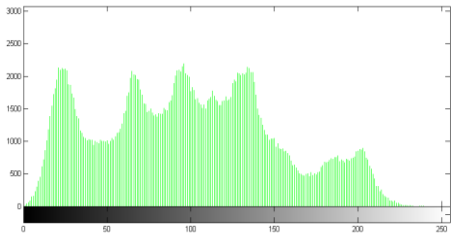
(b) cipher-image of Lena



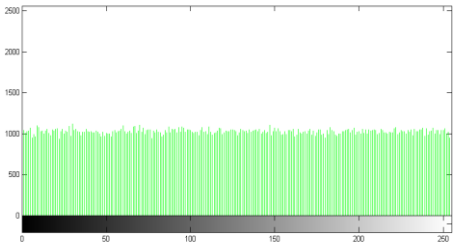
(c) Histogram of the red channel of plain-image



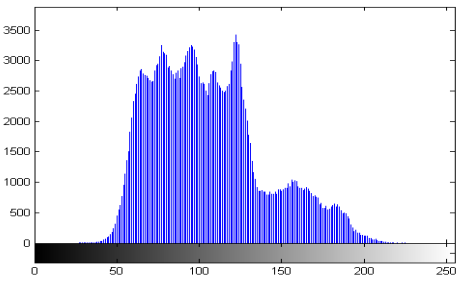
(d) Histogram of the red channel of cipher-image



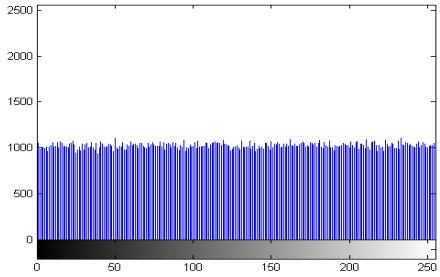
(e) Histogram of the green channel of plain-image



(f) Histogram of the green channel of cipher-image



(g) Histogram of the blue channel of plain-image



(h) Histogram of the blue channel of cipher-image

Fig 3. Histograms of the plain-image Lena and its cipher-image.

(iii) Information entropy analysis. Information entropy is a measure of the uncertainty associated with a random variable and can be also a measure of disorder and randomness. It quantifies the amount of information contained in data, usually in bits/symbol. Two extremely cases are: a long sequence of repeating characters and a truly random sequence. The former has entropy of 0 since every character is predictable, and the latter has maximum entropy since there is no way to predict the next character in the sequence. Regarding image, it can be used to measure the uniformity of image histograms. The entropy $H(m)$ of a message source m can be measured by

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

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 a 24-bit color image, the information entropy for each color channel (Red, Green and Blue) is given as

$$H^{R/G/B}(m) = \sum_{i=0}^{2^8-1} P^{R/G/B}(RI_i)\log_2 \frac{1}{P^{R/G/B}(RI_i)} \text{ (bits)}.$$

We have calculated the information entropy for plain-image Lena and its corresponding cipher image. The results are shown in Table II. Comparing the results with those presented in [21], one can see that the results obtained here are better than those produced in [21]. The value of information entropy for the cipher-image produced by the proposed image encryption scheme is very-very close to the expected value of truly random image, i.e., 8bits. Hence the proposed encryption scheme is extremely robust against entropy attacks.

Table I. CORRELATION BETWEEN ADJACENT PIXELS OF PLAIN-IMAGE AND CIPHER-IMAGE.

		Correlation between adjacent pixels		
		Red	Green	Blue
Horizontal	Plain-image	0.9756	0.9753	0.9540
	Cipher-image	0.0152	-0.0026	-0.0086
Vertical	Plain-image	0.9868	0.9873	0.9737
	Cipher-image	0.0106	-0.0019	-0.0277
Diagonal	Plain-image	0.9624	0.9627	0.9333
	Cipher-image	0.0246	0.0044	0.0071

C. Correlation between Plain and Cipher Images

We have also analyzed the correlation between plain-image and cipher-image by computing the two-dimensional correlation coefficients between various color channels of plain-image and cipher-image. The 2D-correlation coefficients are calculated by

$$C_{AB} = \frac{\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(A_{i,j}-\bar{A})(B_{i,j}-\bar{B})}{\sqrt{\left(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(A_{i,j}-\bar{A})^2\right)\left(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(B_{i,j}-\bar{B})^2\right)}},$$

$$\bar{A} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}A_{i,j}, \quad \bar{B} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}B_{i,j}.$$

where A represents one of the red, green and blue channel of the plain image, B represents one of the red, green and blue channel of the cipher image, $\bar{A}$ and $\bar{B}$ are the mean values of the elements of 2D matrices A and B respectively; H and W are respectively the height and width of the plain/cipher image. In this way, we have total nine different correlation coefficients (C_{RR}, C_{RG}, C_{RB}, C_{GR}, C_{GG}, C_{GB}, C_{BR}, C_{BG} and C_{BB}) for a pair of plain and cipher images. We have computed the correlation coefficients for the pair of plain-image Lena and its corresponding cipher-image. The results are shown in Table III. One can see from the results that the correlation coefficients between various channels of the plain image and cipher image are very small (or practically zero), hence the cipher-image owns the characteristics of a random image.

Table II. INFORMATION ENTROPY ANALYSIS.

	Red	Green	Blue
Plain-image Lena	7.2634	7.5899	6.9854
Cipher-image	7.9993	7.9993	7.9994
Cipher-image [21]	7.9957	7.9963	7.9951

D. Key Sensitivity Analysis

A good image encryption scheme should be extremely sensitive to cipher keys, which is an essential feature for any good cryptosystem in the sense that it can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. The key sensitivity of a cryptosystem can be observed in two ways: (i) the cipher-image derived from the cryptosystem should be extraordinarily sensitive to cipher keys, i.e., if we use two slightly different keys to encrypt the same plain-image, then two cipher-images should possess negligible correlation; (ii) the cipher-image cannot be decrypted correctly although there is a slight difference between the encryption and decryption keys. The plain-image is respectively encrypted with one master cipher and five other cipher keys which have only a minor difference in any one of five parts of master cipher key. The following cipher keys are used to perform the simulation.

Master cipher key: Mkey (0.27,0.34,0.22,0.66,108);

Five slightly different keys:

SKEY1 $\left(0.27\text{-}10^{-14}, 0.34, 0.22, 0.66, 108\right)$,

SKEY2 $\left(0.27, 0.34\text{-}10^{-14}, 0.22, 0.66, 108\right)$,

SKEY3 $\left(0.27, 0.34, 0.22\text{-}10^{-14}, 0.66, 108\right)$,

SKEY4 $\left(0.27, 0.34, 0.22, 0.66\text{-}10^{-14}, 108\right)$,

SKEY5 $\left(0.27, 0.34, 0.22, 0.66, 108+1\right)$.

(i) For the first kind of key sensitivity analysis, the plain-image Lena is encrypted using MKEY and also using all five slightly different keys SKEY1--SKEY5. Then we have computed the 2D correlation coefficients between the various color channels of the cipher-image yielded using MKEY and five other cipher-images produced using slightly different keys from SKEY1 to SKEY5. The results have been given in Table IV. All the correlation coefficients are very small or practically zero indicating that all the cipher-images are highly different and hence the cipher-images produced by the proposed image cipher possess extreme sensitivity to cipher keys.

(ii) For the second kind of key sensitivity analysis, plain-image Lena is encrypted using MKEY, and the encrypted image is decrypted with five slightly different keys from SKEY1 to SKEY5. Now the 2D correlation coefficients between the various color channels of plain-image and five decrypted images with slightly different keys from SKEY1 to SKEY5 are calculated. The results are given in Table V. It is clear that all the correlation coefficients are very small or practically zero, i.e., the images decrypted using slightly different keys are highly different.

Table III. CORRELATION BETWEEN PLAIN-IMAGE LENA AND ITS CIPHER-IMAGE.

	Cipher-image Red	Green	Blue
Plain-image Lena			
Red	0.0031	-0.0022	-0.0031
Green	0.0024	-0.0027	-0.0055
Blue	0.0014	-0.0019	-0.0061

Table IV. KEY SENSITIVITY ANALYSIS I.

	Correlation coefficients between the encrypted images obtained using MKEY and				
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5
Crr	0.0001	−0.0024	−0.0001	0.0012	−0.0014
Crg	−0.0013	−0.0023	0.0005	−0.0046	0.0044
Crb	0.0018	−0.0006	−0.0020	−0.0001	−0.0024
Cgr	−0.0007	−0.0024	0.0007	−0.0003	0.0012
Cgg	−0.0012	0.0014	0.0017	0.0006	0.0014
Cgb	−0.0001	0.0012	−0.0020	0.0020	0.0013
Cbr	−0.0029	−0.0003	0.0024	−0.0016	0.0004
Cbg	−0.0009	0.0008	−0.0051	0.0016	0.0023
Cbb	0.0005	0.0004	−0.0017	0.0010	−0.0013

Table V. KEY SENSITIVITY ANALYSIS II.

	Correlation coefficients between the decrypted images obtained using MKEY and				
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5
Crr	−0.0002	0.0048	0.0021	0.0004	0.0017
Crg	−0.0026	0.0012	0.0004	−0.0032	−0.0003
Crb	−0.0035	0.0022	−0.0024	0.0007	−0.0012
Cgr	0.0027	0.0000	0.0003	−0.0001	0.0030
Cgg	0.0001	0.0057	0.0012	−0.0024	−0.0013
Cgb	0.0003	0.0026	−0.0010	0.0010	−0.0013
Cbr	−0.0001	−0.0006	0.0023	−0.0005	0.0007
Cbg	−0.0011	−0.0032	0.0005	−0.0026	−0.0021
Cbb	−0.0010	−0.0005	−0.0011	−0.0005	−0.0008

E. Differential Analysis

The differential cryptanalysis of a block cipher is the study of how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. It is usually done by implementing the chosen plaintext attack but now there are extensions which use known plaintext as well as ciphertext attacks also. As for image cryptosystems, attackers may generally make a slight change (e.g., modify only one pixel) of the plain-

image, and compare the two cipher-images (obtained by applying the same cipher key on two plain-images having one pixel difference only) to find out some meaningful relationships between the plain-image and the cipher-image. If a meaningful relationship between plain-image and cipher-image can be found in such analysis, which may further facilitate the opponents to determine the cipher key. If one minor change in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the encryption scheme will resist differential attack efficiently. To test the robustness of image cryptosystems against the differential cryptanalysis, two most common measures NPCR (number of pixel change rate) and UACI (unified average changing intensity) are used.

NPCR is used to measure the percentage number of pixels in difference of a particular color channel in two cipher-images obtained by applying the same cipher key on two plain-images having one pixel difference only. If $C^{R/G/B}$ and $\bar{C}^{R/G/B}$ represent the R, G, B channels for two cipher-images, then NPCR for each color channel is defined as:

$$\mathrm{NPCR}^{R/G/B} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}^{R/G/B}}{W \times H} \times 100\%,$$

$$D_{i,j}^{R/G/B} = \begin{cases} 0\ , \ if\ \ \mathrm{C}_{i,j}^{R/G/B} = \bar{C}_{i,j}^{R/G/B}, \\ 1, \ \ if\ \ \mathrm{C}_{i,j}^{R/G/B} \neq \bar{C}_{i,j}^{R/G/B}. \end{cases}$$

The NPCR for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$\mathrm{NPCR}_{Expected}^{R/G/B} = (1 - 2^{-L^{R/G/B}}) \times 100\%,$$

where $L^{R/G/B}$ is the number of bits used to represent the red, green or blue channels of the considered image. For a 24-bit true color image (8 bit for each color channel) $L^{R/G/B}$=8, hence $\mathrm{NPCR}_{Expected}^{R/G/B} = 99.6094\%$.

UACI, the average intensity difference of a particular channel between two cipher-images $C^{R/G/B}$ and $\bar{C}^{R/G/B}$, is calculated by

$$\mathrm{UACI}^{R/G/B} = \frac{1}{W \times H} \sum_{i=1}^{H}\sum_{j=1}^{W} \frac{C_{i,j}^{R/G/B} - \bar{C}_{i,j}^{R/G/B}}{2^{L^{R/G/B}} - 1} \times 100\%.$$

The UACI for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$\mathrm{UACI}_{Expected}^{R/G/B} = \frac{1}{2^{2L^{R/G/B}}} \cdot \frac{\sum_{i=1}^{2^{L^{R/G/B}}-1} i(i+1)}{2^{L^{R/G/B}} - 1} \times 100\%.$$

For a 24-bit true color image, $\mathrm{UACI}_{Expected}^{R/G/B} = 33.4635\%$.

We have performed the differential analysis by calculating NPCR and UACI on plain-image Lena. The analysis has been done by randomly choosing 500 pixels (one at a time, including the very first and very last pixels) in each plain-image and changing their all three color values by one unit. The average values of NPCR and UACI thus obtained for all three images are given in Table VI. It is clear that the NPCR and UACI values are very close to the expected values, thus the proposed image encryption technique shows extreme sensitivity on the plaintext and hence not vulnerable to the differential attacks. The results by the proposed scheme [21] are also shown in Table VI for the comparison.

Table VI. DIFFERENTIAL ANALYSIS.

	Average NPCR (%)			Average UACI (%)		
	Red	Green	Blue	Red	Green	Blue
The proposed scheme here	99. 6163	99. 6031	99. 5972	33. 4371	33. 4556	33. 4782
The proposed scheme [21]	99. 6072	99. 5971	99. 5997	33. 3916	33. 5013	33. 4664

F. Encryption Speed Analysis

We have also estimated the encryption rate of the proposed image encryption scheme. The operation system, hardware and software are Windows 7 Ultimate system, Intel Core i3 CPU with 2 GB RAM, and MATLAB 7.11 respectively. In Table VII, we present the average value of encryption rate of the proposed encryption technique for "all-zeros" images of five different sizes (1.5, 9, 24, 44 and 72 Mb (Mega-bits)). Randomly generating 100 cipher keys for each image, we encrypt the image and get the average encryption time. The results show that the proposed image encryption scheme has an average encryption rate of 18.82Mbps or so in case of encrypting one round. We have also estimated the encryption rate of the proposed scheme in [21] for a comparison using the same computing environment. The average encryption rate of 16.15Mbps is obtained for the proposed scheme in [21]. All the results indicate that our proposed scheme is more efficient than the proposed one in [21] except the case of image size 1.5Mb. It is really interesting to get such a surprise. We guess the reason may be due to the programming strategy. We believe that further proper programming optimization will improve the rate of encryption. Anyway, at the case of large image data, our image encryption scheme shows great potential. To see

that, we also encrypt images with different image sizes for two rounds and analyze the encryption rate of the two comparing encryption schemes. The results are shown in Table VIII. At this time, all the results are better than the proposed scheme in [21]. From the point of view of key space capacity, we note that the proposed scheme here owns actually competitive advantage than that one in [21] as well.

Table VII. COMPARISON BETWEEN THE ENCRYPTION RATES OF THE PROPOSED SCHEME HERE AND ONE RECENT CHAOS-BASED PERMUTATION-SUBSTITUTION IMAGE ENCRYPTION SCHEME [21]. THE TIME MEASURED IS IN SECONDS AND THE ENCRYPTION ROUND IS ONE.

Image size	Time by the proposed scheme here	Rate by the proposed scheme here	Time by the scheme [21]	Rate by the scheme [21]
1.5Mb	0.069425	21.72881	0.066567	22.62074
9Mb	0.465213	19.37031	0.560659	16.06661
24Mb	1.263075	19.01921	1.587176	15.1316
44Mb	2.413065	18.29366	3.041134	14.49423
72Mb	4.587131	15.70034	5.787705	12.4417

Table VIII. COMPARISON BETWEEN THE ENCRYPTION RATES OF THE PROPOSED SCHEME HERE AND ONE RECENT CHAOS-BASED PERMUTATION-SUBSTITUTION IMAGE ENCRYPTION SCHEME [21]. THE TIME MEASURED IS IN SECONDS AND THE ENCRYPTION ROUND IS TWO.

Image size	Time by the proposed scheme here	Rate by the proposed scheme here	Time by the scheme [21]	Rate by the scheme [21]
1.5Mb	0.114727	13.12117	0.117694	12.77492
9Mb	0.764261	11.77992	0.981884	9.167196
24Mb	2.040941	11.76194	2.692466	8.914763
44Mb	4.228149	10.45221	5.563949	7.933595
72Mb	7.880533	9.138145	10.34188	6.963046

V. Conclusions

A novel chaos-based pseudorandom permutation–substitution technique for image encryption has been proposed. The pseudorandom number sequences produced through 2D chaotic skew tent map have been used in an effective way to achieve the desired level of confusion and diffusion in the encryption process. All the permutation processes have been made dependent on the plaintext as well as cipher keys, which produce an excellent combination of plaintext sensitivity and key sensitivity in the encryption technique. Moreover the substitution process used in the proposed image encryption also contributes to both the key and plaintext sensitivity, as it is initiated by the initial vectors generated from the cipher key and tent map and then followed by a mixing of the properties of image pixels and pseudorandom sequences. The robustness and security of the proposed image encryption technique have been tested thoroughly using rigorous security analysis tools commonly used in the image processing as well as chaos-based cryptosystems. The results are perfect as required for any secure image and video communication application.

Acknowledgment

This research is partly supported by National Natural Science Foundation of China (No. 11071152 & No. 11271238), and partly supported by Innovation and Entrepreneurship Training Program of Guangdong Colleges.

References

[1] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998), 1259–1284.
[2] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, 1(2001), 6–21.
[3] F. Huang, Z.-H. Guan, A modified method of a class of recently presented cryptosystems, Chaos, Solitons and Fractals, 23(2005), 1893–1899.
[4] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(2006), 926-934.
[5] G. J. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Communications, 284(2011), 2775–2780.
[6] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284(2011), 5290–5298.
[7] B. Schiener, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley and sons, New York, 1996.
[8] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(2006), 926-934.
[9] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Syst. I, 49(2002), 28–40.
[10] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(2011), 3895–3903.

[11] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Phys. Lett. A, 366(2007), 391–396.
[12] R. Ye, H. Huang, Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking, I. J. Image, Graphics and Signal Processing, 1(2010), 19–29.
[13] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map, Chaos, Solitons and Fractals, 26 (2005), 117–129.
[14] 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.
[15] Y. Wang, K.W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals, 41(2009), 1773–1783.
[16] S. J. Li, C. Q. Li, G. R. Chen, N. G. Bourbakis, K. T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. Signal Process. Image Commun., 23(2009), 212–223.
[17] C. Q. Li, S. J. Li, G. R. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP J. Appl. Signal Process., 8(2005), 1277–1288.
[18] Patidar Vinod, N.K. Pareek, K.K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulations, 14 (2009), 3056-3075.
[19] Patidar Vinod, N.K. Pareek, G. Purohit, K.K. Sud, Modified substitution–diffusion image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulations, 15 (2010), 2755-2765.
[20] Patidar Vinod, N.K. Pareek, G. Purohit, K.K. Sud, A new chaos based permutation-substitution approach for image incryption, in: L.M. Patnaik, K.R. Venugopal (Eds.), Proceedings of the 4th International Conference on Information Processing, I. K. International Publishing House, New Delhi, 2010.
[21] Vinod Patidar, N.K. Pareek, G. Purohit, K.K. Sud. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption, Optics Communications, 284(2011), 4331-4339.
[22] Ruisong Ye, Wei Zhou. An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice, International Journal of Information and Communication Technology Research, 1:8(2011), 344-348.
[23] C. Robinson, An Introduction to Dynamical Systems, Continuous and Discrete. Prentice Hall, 2004
[24] C.E. Shannon, Communication theory of secrecy system. Bell Syst. Tech. J, 28(1949), 656–715.

Prof. 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.

Shaojun Zeng: Undergraduate student at department of mathematics in Shantou University.

Junming Ma: Undergraduate student at department of mathematics in Shantou University.

Chuting Lai: Undergraduate student at department of mathematics in Shantou University.

