A Chaos-based Image Encryption Scheme Using Multimodal Skew Tent Maps

1 Ruisong Ye, 2 Weichuang Guo
1, 2 Department of Mathematics, Shantou University Shantou, Guangdong, 515063, P. R. China
rsye@stu.edu.cn

ABSTRACT

Chaotic multimodal skew tent maps are constructed to design an efficient chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, in which permuting the positions of image pixels incorporates with changing the grey values of image pixels to confuse the relationship between cipher-image and plain-image. In the permutation process, a multimodal skew tent map is utilized to generate one chaotic orbit used to permute the image pixel positions, while in the diffusion process, another two multimodal skew tent maps are employed to yield two pseudo-random grey value sequences for designing a two-way diffusion process. The yielded grey value sequences are not only sensitive to the control parameters and initial conditions of the considered chaotic maps, but also strongly depend on the plain-image processed, therefore the proposed scheme can resist statistical attack, differential attack, known-plaintext as well as chosen-plaintext attack. Experimental results are carried out with detailed analysis to demonstrate that the proposed image encryption scheme is highly secure thanks to its large key space and robust permutation-diffusion mechanism.

Keywords: multimodal skew tent map, chaotic system, image encryption, permutation, diffusion

1. INTRODUCTION

Chaos theory is a blanketing theory that covers most aspects of science, therefore it shows up everywhere in the world nowadays: mathematics, physics, biology, computer, finance and even arts. Especially it consistently plays an active role in modern cryptography. Chaos has been introduced to cryptography thanks to its ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters, which are close to confusion and diffusion in cryptography. These properties make chaotic systems a potential choice for constructing cryptosystems [1-7]. With the rapid developments in digital image processing and network communication in the last decades, electronic publishing and wide-spread dissemination of digital multimedia data have been communicated over the Internet and wireless networks. Therefore protection of digital image information against illegal copying and distribution has become extremely urgent. Digital images possess some intrinsic features, such as bulk data capacity and high correlation among adjacent pixels. As a result, traditional encryption algorithms, such as DES, RSA [8], 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 [1,2]. Chaos-based image encryption schemes are usually composed of two processes generally: chaotic confusion of pixel positions by permutation process and diffusion of pixel grey values by diffusion process, where the former permutes a plain-image with chaotic systems, while the latter changes the pixel values sequentially so that a tiny change for one pixel can spread out to almost all pixels in the whole image. 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.

The chaos-based encryption was first proposed by Matthews [9], since then, many chaos-based digital image encryption schemes have been proposed and analyzed in the literature. Among these encryption schemes, one-dimensional and two-dimensional chaotic systems, such as Logistic map, unimodal skew tent map, Arnold map, baker map and standard map, were applied widely owing to the advantage of simplicity [4-7,10-12]. However, some chaos-based image encryption algorithms are broken recently due to their small key spaces and weakly secure encryption mechanisms [13-19]. 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 statistical attack, differential attack, known-plaintext attack and chosen-plaintext attack, etc. To overcome the drawbacks such as small key space and weakly secure permutation-diffusion architecture in chaotic systems, many researchers turn to find some improved chaos-based cryptosystems with large key spaces and good permutation-diffusion mechanisms. For instance, [1,3] introduced 3D chaotic baker maps with modifications to the conventional baker map to strengthen the security; Piecewise nonlinear chaotic algorithm was proposed in [20]; Zhang et al. [21] recently proposed an image encryption method based on a unimodal skew tent map and a good permutation-diffusion architecture. This method generates a P-box with the same size of plain-image and shuffle the positions of image pixels totally; it uses different key streams depending on plain-image in the diffusion process, so the method is strongly secure in the sense of preventing known-plaintext attack and chosen-plaintext attack. Ye [22] recently proposed a novel image encryption scheme with an efficient permutation-diffusion mechanism, which show good performance, including huge key space, efficient resistance against statistical attack, differential attack, known-plaintext as well as chosen-plaintext attack. Other improvements like applying hyper-chaotic differential systems, cellular
automa and multi chaotic systems have been investigated and utilized to devise image encryption schemes to promote the security as well [23-26].

In this paper, a novel chaos-based image encryption scheme with an efficient permutation-diffusion structure is proposed. In both the permutation process and the diffusion process, chaotic maps are utilized. First, the permutation process employs one chaotic multimodal skew tent map to generate a chaotic orbit \{x_i, k = 0,1,\ldots\} of \(x_0\) with given control parameter \(a_i (i = 1,\cdots,2N-1)\) where \(N\) is the number of tents; \(\{x_i, k = 1,\cdots,H \times W\}\) (\(H\) and \(W\) are the width and the height of the processed image respectively) is then sorted to yield one index order sequence applied to permute the image pixel positions totally. To improve the diffusion effect, a two-way diffusion process is presented, where another two multimodal skew tent maps are utilized to generate two pseudo-random grey value sequences. The two sequences are then used to modify the pixel grey values sequentially. The yielded grey value sequences are not only sensitive to the control parameters and initial conditions of the considered chaotic maps, but also strongly depend on the plain-image processed, therefore the proposed scheme can resist statistical attack, differential attack, known-plaintext attack as well as chosen-plaintext attack. The proposed image encryption scheme also possesses large key space, therefore efficiently frustrating brute-force attack. If \(N\), the number of tents, is set to be 3 for all the three multimodal skew tent maps used in the experiments, the key space will be \(10^{38}\). As a matter of fact, the key space will become \(10^{32}\) times larger if \(N\) increased by 1 for one multimodal skew tent map. The proposed image encryption scheme promotes the key space significantly. The proposed scheme is easy to manipulate and it can be applied to any images with unequal width and height. All these satisfactory properties make the proposed scheme a potential candidate for image encryption.

The rest of the paper is organized as follows. In Section 2, multimodal skew tent map with \(N\) tents is constructed and its chaotic properties are analyzed. Section 3 proposes a novel image encryption scheme composed of one permutation process and one diffusion process based on multimodal skew tent maps. The security of the proposed scheme is evaluated via detailed analysis and experiments in Section 4. Section 5 includes some conclusions.

2. THE MULTIMODAL SKEW TENT MAP

The unimodal skew tent map \(T_a : [0,1] \rightarrow [0,1]\) given by

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

(1)

where \(x \in [0,1]\) is the state of the system, and \(a \in (0,1)\) is the control parameter. It is a noninvertible transformation of the unit interval onto itself. As \(a = 0.5\), \(T_a\) becomes the regular tent map. The transformation is continuous and piecewise linear, with the linear regions \([0,a]\) and \([a,1]\). Note that the slope of the left branch is \(1/a > 1\) and the slope of the right branch is \(-1/(1-a) < -1\). For any \(a \in (0,1)\), the piecewise linear map (1) has Lyapunov exponent \(-a \ln a - (1-a) \ln (1-a)\), which is larger than 0, implying that the map is chaotic. There exist some good dynamical features in the skew tent map. It has been verified that the probability density function \(\rho_0(x)\) of the skew tent map is the same as the regular tent map [28], that is

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

(2)

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

\[
T(x) = \begin{cases} 
(x-a_0)/(a_{2^i} - a_0), & \text{if } x \in [a_2, a_{2^i}], \\
(a_{2^i} - x)/(a_{2^i} - a_{2^{i+1}}), & \text{if } x \in (a_{2^{i+1}}, a_{2^{i+2}}],
\end{cases}
\]

(3)

where \(i = 0,\cdots, N-1\), \(0 = a_0 < a_1 < \cdots < a_{2^N-1} < a_{2^N} = 1\). See Fig. 1 for the case of \(N = 3\).

Fig 1: The diagram of a multimodal skew tent map.

A typical orbit of \(x_0 = 0.367\) derived from the dynamical system (3) is \(\{x_i = T^k(x_0), k = 0,1,\cdots\}\), which is shown in Fig. 2(a), for \(N = 3\), \(a = [0.16 0.3 0.51 0.68 0.78 1.0]\). Its waveform is quite irregular, indicating that the system is chaotic. The distribution of the points \(\{x_i : k = 0.1,\cdots,20000\}\) of a typical orbit of length 20000 is represented by the histogram of Fig. 2(b). It can be seen that the points of the orbit spread more or less evenly over the unit interval in the course of time. Multimodal skew tent map also possesses desirable auto-correlation and cross-correlation features. The iterated trajectory is used to calculate the correlation coefficients, which are shown
in Figs. 2(c)-(d) respectively. The cross-correlation coefficients are calculated by the orbits of $x_n = 0.367$ and $y_n = 0.368$. The control parameter $a_1, \ldots, a_{2N-1}$ and the initial condition $x_0$ can be regarded as cipher keys if the multimodal skew tent map is employed to design image encryption schemes.

Fig 2: Orbits derived from the considered multimodal skew tent map with $a = [0.1, 0.3, 0.5, 0.6, 0.8, 0.9, 1.0]$.

One can observe from Fig. 2(b) that the points of the orbit spread evenly over the unit interval. This property will also be shown in the sequel.

Definition 1 [28]:

A probability density $\rho(x)$ on $[0, 1]$ is invariant, if for each interval $[c, d] \subset [0, 1]$,\[\int_c^d \rho(x)dx = \int_{T^{-1}[c,d]} \rho(x)dx \tag{4}\]

where $T^{-1}([c, d]) = \{c \leq T(x) \leq d\}$.

Let $p_i = a_i - a_{i-1}, i = 1, \ldots, 2N$, then the unit interval is divided into $2N$ subintervals with length $p_i (i = 1, \ldots, 2N)$ such that $\sum_{i=1}^{2N} p_i = 1$. It is not difficult to see that for the multimodal skew tent map (3), (4) amounts to the following equation:

$$\rho(x) = p_1 \rho(p_1 x) + p_2 \rho(a_2 - p_1 x) + p_3 \rho(a_3 + p_1 x) + \cdots + p_{2N-1} \rho(a_{2N-2} + p_{2N-1} x) + p_{2N} \rho(1 - p_{2N} x). \tag{5}$$

It is easy to see that $\rho(x) = 1$ satisfies (5) and $\rho(x) = 1$ is the unique solution to (5) according to the uniqueness of invariant probability density function [28]. It then follows from Birkhoff’s ergodic theorem [29] that the asymptotic distribution of the points of almost every trajectory is uniform. This fact has been illustrated by Fig. 2(b). The existence and unique value of the Lyapunov exponent also follows from the following theorem.

Theorem 1 [28]:

Suppose $f : [0, 1] \to [0, 1]$ is continuously differentiable except for a finite number of points. Let $\rho(x)$ be the unique invariant probability density of the function. Then for (Lebesgue-) almost all initial
In this subsection, we propose a permutation process to confuse plain-image totally. Thanks to the chaotic nature of multimodal skew tent map on the unit interval [0,1] , one can easily get the chaotic orbit \( \{ x_k, k = 0, 1, \cdots \} \) of \( x_0 \) with given control parameters \( a_i (i = 1, \cdots, 2N - 1) \). We rearrange all the \( x_k \) values of the orbit to get a new sequence \( \{ x_k, k = 0, 1, \cdots \} \) according to the order from small to large. As a result, we also get an index order number for every \( x_k \). The index order number sequence can be applied to permute the image pixel positions and therefore can confuse the image to get a shuffled image. The permutation process is stated as follows.

**Step 1:** Set the values of the control parameters \( a_i (i = 1, \cdots, 2N - 1) \) and the initial condition \( x_0 \).

**Step 2:** Iterate the multimodal skew tent map (3) to get the truncated orbit of \( x_k \), say \( \{ x_k, k = 0, 1, \cdots, H \times W \} \) where \( H, W \) are the height and the width of the processed image respectively.

**Step 3:** Sort \( \{ x_k, k = 1, \cdots, H \times W \} \) to get one index order sequence \( \{ x_k, k = 1, \cdots, H \times W \} \).

**Step 4:** Reshape the grey-scale value matrix of the processed plain-image \( A \) sized \( H \times W \) to one vector \( U \) with length \( H \times W \); permute the vector \( U \) by \( Ix \) in the following way to get one new vector \( V \) :

\[
V_k = U_{i_k}, k = 1, \cdots, H \times W.
\]

**Step 5:** Reshape \( V \) back to one 2D matrix to yield the shuffled image \( B \).

### 3.2 Diffusion Process

As we know, a secure encryption algorithm should have a good mechanism of diffusion. The diffusion processing 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 permutation process has changed the pixel positions of the plain-image, it cannot change the statistical properties of the plain-image. The diffusion process will enhance the resistance to 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 plain-image. The opponent cannot find any useful clues between the plain-image and the cipher-image and so cannot break the cryptosystem even after they spend a lot of time and effort. A good diffusion process should yield key streams related to plain-images as well. When encrypting different plain-images (even with the same cipher keys), the encryption scheme should have a good mechanism of diffusion. The diffusion process is outlined as follows.

**Step 1:** Applying the permutation process to confuse the plain-image \( A \) and get a shuffled image \( B \). Set the values of the initial conditions \( y_0, z_0 \) and the control parameters \( h_i (i = 1, \cdots, 2N_1 - 1), c_j (j = 1, \cdots, 2N_2 - 1) \), for example, set \( y_0 = 0.761, b = [0.110.350.450.620.811] \), \( z_0 = 0.248, c = [0.0130.310.510.730.861] \), in the diffusion process.

**Step 2:** Let \( i = 0 \).

**Step 3:** Apply the following quantization formula to yield one 8-bit pseudo-random grey value \( d(i) \):

\[
d(i) = \text{floor}(L \times y_i)
\]
where $L$ is the color level (for a 256 grey-scale image, $L = 256$), the “floor” operation on $x$ returns the largest value not greater than $x$.

**Step 4:** Compute the pixel grey value in the cipher-image by a two-point diffusion transmission:

$$C(i+1) = \varphi(i+1) \oplus [(d(i) + C(i)) \mod L],$$

(8)

where $\varphi(i+1)$ is the grey value of the current operated pixel in the shuffled image which has been rearranged according to the order of row or column to a vector with length $H \times W$, $C(i)$ is the previous output cipher-pixel grey value. The diffusion process is well defined as the initial condition $C(0)$ is provided. $C(0)$ can be set to be part of the keys in the diffusion process or can just take the value of $d(0)$ for simplicity.

**Step 5:** Compute $s$ by $s = 1 + [C(i+1) \mod 2]$ to get the next $y_{i+1}$ by iterating the multimodal skew tent map with control parameters $b_j (j = 1, \ldots, 2N_j - 1)$ on $y_i$ for $s$ rounds, that is, $y_{i+1} = T'(y_i)$. This is the crucial step to generate a keystream depending on the plain-image since $s$ is related to $C(i+1)$, so is $y_{i+1}$. The encrypted image not only relates to the cipher keys, but also relates to the plain-image.

**Step 6:** Let $i = i + 1$ and return to Step 3 until $i$ reaches $H \times W$.

The above diffusion process implies that it cannot influence the pixels before the tampered pixel with a grey value change. As a remedy, we here add a reverse diffusion process as a supplement to the above diffusion process. Another multimodal skew tent map with control parameters $c_j (j = 1, \ldots, 2N_j - 1)$ is used here.

**Step 7:** Iterate the following multimodal skew tent map to produce another pseudo-random grey value sequence

$$z_{i+1} = T(z_i),$$

$$\psi(k+1) = \text{floor}(Lz_{i+1}), k = 0, 1, \ldots, H \times W - 1.$$  

**Step 8:** Execute the reverse diffusion process:

$$D(i) = D(i+1) \oplus [(C(i) + \psi(i)) \mod L], i = H \times W, \ldots, 2, 1,$$

(9)

where $D(i), i = 1, 2, \ldots, H \times W$ are the final encrypted vector consisting of the encrypted image pixel grey-scale values. The value of $D(H \times W + 1)$ should be provided to cipher out the sequence $D(i), i = 1, 2, \ldots, H \times W$. $D(H \times W + 1)$ can handled in the same way as $C(0)$.

The complete diffusion process is composed of Step 1 to Step 8. The permutation process and the diffusion process form the image encryption scheme. The Lena image is encrypted and the result is shown in Fig. 3(b).
4. SECURITY ANALYSIS

According to the basic principle of crypotlogy [8], 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.

4.1 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. In the permutation process, the control parameters \(a_i (i=1,\cdots,2N-1)\) and the initial condition \(x_0\) form the cipher keys. The cipher keys in the diffusion process consist of the initial conditions \(y_0, z_0\) and the control parameters \(b_j (i=1,\cdots,2N-1), c_j (j=1,\cdots,2N-2)\) for two multimodal skew tent maps. The sensitive tests with respect to all cipher keys have been carried out. To verify the sensitivity of parameter \(K\), the original plain-image \(I=(I(i,j))_{1\leq i,j \leq 8}\) 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 [5]:

\[
P_s(K) = \frac{1}{2 \times H \times W} \sum_{i,j} [N_s(I_1(i,j), I_2(i,j)) + N_s(I_2(i,j), I_3(i,j))] \times 100% \tag{10}
\]

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 tests where the initial key values are set to be the following (\(N=N_1=N_2=3\)):

\[
x_0 = 0.367, a = [0.160.30.510.680.781.0],
\]

\[
y_0 = 0.761, b = [0.0110.350.450.620.8110.0],
\]

\[
z_0 = 0.248, c = [0.0130.310.510.730.861.0].
\]

The variations \(\Delta \delta\) of the considered parameters are shown in below:

- Permutation process: \(x_0 = a_1 = a_2 = a_3 = a_4 = a_5 = 10^{-6}\),
- Diffusion process: \(y_0 = b_1 = b_2 = b_3 = b_4 = 10^{-6}\),
- \(z_0 = c_1 = c_2 = c_3 = c_4 = c_5 = 10^{-6}\).

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>
<thead>
<tr>
<th>Parameter</th>
<th>(x_0)</th>
<th>(y_0)</th>
<th>(z_0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(K)</td>
<td>0.9962</td>
<td>0.9957</td>
<td>0.9957</td>
</tr>
<tr>
<td>(P_s(K))</td>
<td>0.9961</td>
<td>0.9961</td>
<td>0.9961</td>
</tr>
</tbody>
</table>

The results in Table 1 imply that the control parameters \(a_i,b_j,c_i (i=1,\cdots,5)\) and the initial conditions \(x_0,y_0,z_0\) are all strongly sensitive. It also implies from the results that the key space is more than \(10^{28}\), which is large enough to make brute-force attack infeasible. As a matter of fact, the key space will become \(10^{32}\) times larger if \(N\) increased by 1 for one multimodal skew tent map. The proposed image encryption scheme promotes the key space significantly.

The sensitivity test can also be demonstrated visually, for example, see Figs. 4-5. In Fig. 4, the image encrypted by the key \(y_0 = 0.761\) has 99.57% of difference from the image encrypted by the key \(y_0 = 0.761+10^{-6}\); the encrypted image with the key \(c_5 = 0.31\) has 99.59% of difference from the encrypted image with the key \(c_5 = 0.31+10^{-6}\). Fig. 5 shows that the image encrypted by \(z_0 = 0.248, c_3 = 0.86\) is not correctly decrypted by the perturbed key \(z_0 = 0.248+10^{-6}, c_3 = 0.86\) and \(z_0 = 0.248, c_3 = 0.86+10^{-6}\).
Fig. 4: Key sensitive test: result 1.
4.2 Statistical Analysis

Shannon pointed out in his masterpiece [30] 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 Figs. 3(c)-(d), respectively. Fig. 3(d) 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 6000 pairs of two adjacent pixels randomly from an image and then calculate the correlation coefficient of the selected pairs using the following formulae:

\[
Cr = \frac{\text{cov}(x, y)}{\sqrt{D_x D_y}},
\]

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

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

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 the Table 2.

<table>
<thead>
<tr>
<th></th>
<th>plain-image</th>
<th>cipher-image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>0.9435</td>
<td>-0.0168</td>
</tr>
<tr>
<td>Vertical</td>
<td>0.9680</td>
<td>0.0010</td>
</tr>
<tr>
<td>Diagonal</td>
<td>0.9157</td>
<td>-0.0126</td>
</tr>
</tbody>
</table>

The correlation distributions of two horizontally adjacent pixels in the plain-image and that in the cipher-image are shown in Fig. 6.
(iii) Information entropy analysis. The entropy is the most outstanding feature of randomness. The entropy $H(m)$ of a message source $m$ can be measured by

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

where $L$ is the total number of symbols $m$, $p(m_i)$ represents the probability of occurrence of symbol $m_i$ and log denotes the base 2 logarithm so that the entropy is expressed in bits. For a random source emitting 256 symbols, its entropy is $H(m) = 8$ bits. For the encrypted image of Lena, the corresponding entropy is 7.9969 bits. This means that the cipher-image is close to a random source and the proposed scheme is secure against the entropy attack.

4.3 Differential Attack

In general, attackers 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 differential attack efficiently. To test the influence of only one-pixel change in the plain-image over the whole cipher-image, two common measures are used: number of pixels change rate (NPCR) and unified average changing intensity (UACI). They are defined as:

$$\text{NPCR} = \frac{1}{W \times H} \sum_{i,j} D(i,j) \times 100\%,$$

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

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 two cipher-images whose plain-images only have one-pixel difference. UACI measures the average intensity of differences between 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. We randomly select 10 pixels and change the grey values with a difference of 1, for example, we replace the grey value 107 of the pixel at position (220,243) by 108, and get the NPCR=100%, UACI=50.1961%. The numerical results are shown in Table 3. The mean values of the ten NPCR and UACI values are 99.8698% and 36.8921% respectively. We observe from Table 3 that the two measure values are exceptionally good undergoing only one round of encryption.
depends on the value of $y_i$; $y_i$ is related to the plain-image. Therefore the keystream depends on the processed image. When different plain-images are encrypted, the corresponding key streams are not the same. The attacker cannot obtain useful information by encrypting some special images since the resultant information is related to those chosen-images. Therefore, the attacks proposed in Refs. [16,17,19] become ineffective on this new scheme. The proposed scheme can desirably resist known-plaintext attack and chosen-plaintext attack.  

5. CONCLUSIONS

An efficient image encryption scheme based on multimodal skew tent maps is proposed in the paper. The proposed scheme can shuffle the plain-image efficiently in the permutation process. An effective two-way diffusion process is also presented to change the grey 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 scheme is easy to manipulate and it 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.

ACKNOWLEDGEMENT

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

REFERENCES


[16] C. Li, S. Li, G. Chen, W. A. Halang, Cryptanalysis of an image encryption scheme based on a

---

Table 3: Results of NPCR and UACI tests of Lena

<table>
<thead>
<tr>
<th>Position</th>
<th>NPCR(%)</th>
<th>UACI(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(220,243)</td>
<td>100.00</td>
<td>52.00</td>
</tr>
<tr>
<td>(90,58)</td>
<td>99.99</td>
<td>50.24</td>
</tr>
<tr>
<td>(133,138)</td>
<td>99.80</td>
<td>50.13</td>
</tr>
<tr>
<td>(20,52)</td>
<td>100.00</td>
<td>50.13</td>
</tr>
<tr>
<td>(19,6)</td>
<td>99.88</td>
<td>50.13</td>
</tr>
</tbody>
</table>

4.4 Resistance to Known-Plaintext and Chosen-Plaintext Attacks

In the diffusion process, a feedback from the cipher-image is employed to change the number of iterations of the multimodal skew tent map. In Step 3, $d(i)$ depends on the value of $y_i$; $y_i$ is related to the plain-image. Therefore the keystream depends on the processed image. When different plain-images are encrypted, the corresponding key streams are not the same. The attacker cannot obtain useful information by encrypting some special images since the resultant information is related to those chosen-images. Therefore, the attacks proposed in Refs. [16,17,19] become ineffective on this new scheme. The proposed scheme can desirably resist known-plaintext attack and chosen-plaintext attack.


AUTHOR PROFILES

Ruisong Ye received 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.

Weichuang Guo is a master degree candidate at department of mathematics in Shantou University.