A Highly Secure Image Encryption Scheme using Compound Chaotic Maps

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

ABSTRACT

During the last two decades various chaotic image encryption algorithms have been proposed, but most of them encountered some defects like small key space, low speed, lack of robustness and weak security. This paper proposes a chaos-based image encryption scheme with a permutation–diffusion mechanism, where six skew tent maps and one six-dimensional Arnold map are utilized to generate one hybrid chaotic orbit applied to disorder the pixel positions in the permutation process, while four skew tent maps and one Arnold map are employed to yield two random gray value sequences to change the gray values by a two-way diffusion process. The major merits of the proposed image encryption scheme include a huge key space, desirable computation overhead, good statistical nature resisting statistical attack, differential attack and satisfying robustness against malicious attacks on cipher-images, such as cropping, noising, JPEG compression. Experimental results have been carried out with detailed analysis to show that the proposed scheme can be a potential candidate for practical image encryption.

Keywords: chaotic system, skew tent map, Arnold map, image encryption scheme

1. INTRODUCTION

Chaos theory is a blanket 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 has many practical applications to the real world, including synchronization, control, communication, cryptography, etc. [1-4]. The applications of chaos in communication and cryptography have been an attractive research field since the beginning of 1990s. Chaos has been introduced to cryptography thanks to its ergodicity, pseudorandomness and sensitivity to initial conditions and control parameters, which are close to confusion and diffusion in cryptography. These properties make chaotic systems a potential candidate for constructing cryptosystems [5-12]. There exist two main approaches of designing chaos-based cryptosystems: analog model and digital model. This paper mainly focuses on the chaotic digital encryption techniques. In the digital world nowadays, thanks to the rapid developments in digital image processing and network communication, more and more electronic publishing and wide-spread dissemination of digital multimedia data have been communicated over the Internet and wireless networks. Therefore the security of digital images and the performance speed have 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 [13], 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. Among the chaos-based encryption schemes, one-dimensional and two-dimensional chaotic systems, such as logistic map [14-16], skew tent map [17], Arnold map[6, 18], baker map[5, 7], piecewise linear chaotic map [19-21], piecewise nonlinear chaotic maps [22, 23] and standard map [9-11], were applied widely owing to the advantage of simple implementation. However, there are fundamental drawbacks in these chaotic systems, such as small key space, slow performance speed and weak security. As a matter of fact, some chaos-based image encryption algorithms have been broken recently [24-30].

To overcome these drawbacks, we construct a novel chaos-based image encryption scheme in this paper. The proposed scheme consists of a permutation process and a diffusion process, in which six skew tent maps and one six-dimensional Arnold map are utilized to generate one chaotic orbit applied to scramble the pixel positions in the permutation process while four skew tent maps and two classical Arnold maps are employed to yield two pseudo-random gray value sequences to change the gray values by a two-way diffusion process. Thanks to the simplicity of skew tent maps, we choose them as the candidates of the chaotic maps in both the permutation process and the diffusion process. Although six skew tent maps are used in the permutation process, the computation overhead is almost the same as that caused by one skew tent map. The reason is that the total iteration times for the six skew tent maps are the same as those for one skew tent map if the transient iteration times are not considered. The advantage of using multiple chaotic maps is obvious. The key space is enlarged greatly and it is six times as large as that in the cryptosystem based on one single chaotic map. Therefore the security is improved significantly to resist brute-force attack. To improve the sensitivity of the control parameters and initial conditions, one six-dimensional Arnold map is employed to integrate the chaotic effects of the six skew tent maps. The yielded chaotic orbit in the permutation process is not just a simple rearrangement of the six chaotic orbits, it is a hybrid one derived by six orbits of skew tent maps. The six-dimensional Arnold map is employed to realize this combination effect. As for the diffusion effect, a two-way diffusion process is presented, where another four skew
tent maps are utilized to generate two pseudo-random gray value sequences. The two sequences are then used to modify the pixel gray values sequentially. We note that two skew tent maps are coupled by two-dimensional Arnold map in the diffusion process to strengthen the security as well as the sensitivity of control parameters and initial conditions. Thanks to the good permutation–diffusion mechanism, the proposed image encryption scheme possesses a huge key space, therefore efficiently frustrating brute-force attack. The key space capacity will be $10^{30}$ in the case of tent skew tent maps are employed and can increase as long as the number of skew tent maps increases. As a matter of fact, the key space will become $10^{21}$ times larger generally if the number of skew tent maps increased by 1. 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, differential attacks. An additional merit for the proposed scheme is its robustness against malicious attacks on the cipher-images. As far as we know, many image encryption schemes are vulnerable to image processing, such as cropping, noising, compression, etc. The robustness against such a kind of image processing is also important for cryptosystems. The opponents would rather tamper the cipher-images than analyze them as they are not able to perform the cryptanalysis. The robustness test of the proposed scheme against malicious attacks, like cropping, noising, JPEG compression, is also performed. The proposed image encryption scheme provides a potential candidate for practical image encryption thanks to its satisfactory properties.

The rest of the paper is organized as follows. In Section 2, skew tent map and Arnold map are reviewed. Section 3 proposes a novel image encryption scheme composed of one permutation process and one diffusion process based on skew tent maps and Arnold maps. The security of the proposed scheme is evaluated via detailed analysis and experiments in Section 4. Section 5 draws some conclusions.

2. SKEW TENT MAP AND ARNOLD MAP

2.1 Skew Tent Map Skew Tent Map

We consider the skew tent map $T : [0,1] \rightarrow [0,1]$ given by

$$x_{n+1} = T(x_n) = \begin{cases} x_n / a, & \text{if } x_n \in [0,a] \\ (1-x_n) / (1-a), & \text{if } x_n \in (a,1] \end{cases}$$

(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 $a = 0.5$, $T$ 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 $-1/(1-a) < -1$. A typical orbit of $x_0$ derived from the dynamical system is $\{x_k = T^k(x_0), k = 0, 1, \cdots \}$, which is shown in Fig. 1(a), for $a = 0.4$. Its waveform is quite irregular and indicates that the system is chaotic. For any $a \in (0,1)$, the piecewise linear map (1) has a Lyapunov exponent $-a \ln a - (1-a) \ln(1-a)$, which is larger than 0, implying that the map is chaotic. So the control parameter $a$ and the initial condition $x_0$ can be regarded as cipher keys. There exist some good dynamical features in the skew tent map. It has been verified that the density $\rho(x)$ of the skew tent map is the same as the regular tent map [1], that is

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

The distribution of the points $\{x_k : k = 0, 1, \cdots, 6000\}$ of a typical orbit of length 6000 is represented by the histogram of Fig. 1(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. Skew tent map also possesses desirable auto-correlation and cross-correlation features. The iterated trajectories are used to calculate the correlation coefficients, which are shown in Figs. 1(c)-(d) respectively.

(a) A typical orbit of skew tent map

(b) Histogram of the points of a typical orbit of length 6000
June

PROPOSED

new orbits where

harmful

T

IMAGE

0 4

Cross

with given control parameters

- -

image

dimensional Arnold map (mod 1) to improve the sensitivity of the six skew
centers
c15

x

Auto

1
to the nearest integer towards infinity.

is confined in the

{( ( ) 1 ,

-

fore the absolute

1 }

2

2013

be extended to

are then mapped

chaotic orbits

capacity

enhance

N

3

by the

1

and let

correlation
-

(s) can

). We rearrange all the

orbit points of each

- -

mod 1

Permutation P
dimensional Arnold map (2)

s in the permutation process.

in all the

2

0

and

N

W H-

- -

or process

to form a combined

3

by adding or subtracting an

correlation
-

(3 5) 1 (3 5) 1

(3)

2

dimensional Arnold map (2) can be extended to N -
dimensional one in the following way

\[
\begin{pmatrix}
 y_1 \\
 y_2 \\
 \vdots \\
 y_{N-1} \\
 y_N
\end{pmatrix} = T_A
\begin{pmatrix}
 x_1 \\
 x_2 \\
 \vdots \\
 x_{N-1} \\
 x_N
\end{pmatrix} \mod 1
\]

where

\[
T_A = \begin{pmatrix}
 1 & 1 & \cdots & 1 & 1 \\
 1 & 2 & 2 & \cdots & 2 & 2 \\
 1 & 2 & 3 & \cdots & 3 & 3 \\
 \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
 1 & 2 & 3 & \cdots & N-1 & N-1 \\
 1 & 2 & 3 & \cdots & N-1 & N
\end{pmatrix}
\]

The determinant of the matrix for N -
dimensional Arnold map is 1, therefore the absolute
values of some eigenvalues should be greater than 1 and
the derived system is chaotic. In this paper, we utilize the
six-dimensional Arnold map (3) and the two-dimensional
Arnold map (2) to improve the sensitivity of the six skew
tent maps in the permutation process and the four skew
tent maps in the diffusion process. We will show the
integration process in Section 3.

3. THE PROPOSED IMAGE
ENCRIPTION SCHEME

3.1 Permutation Process

A permutation process to confuse plain-image
totally is proposed. Assume the processed plain-image
sized \( W \times H \) and let \( L = \lceil W \times H / N \rceil \), where \( \lceil x \rceil \) rounds
x to the nearest integer towards infinity. In order to
improve the key space capacity and enhance the
sensitivity of the control parameters and initial conditions,
we generate \( N = 6 \) chaotic orbit sequences by six skew
tent maps and then integrate the six chaotic orbits by one
six-dimensional Arnold map (3) to form a combined
sequence. In more details, we set the initial conditions
\( x(i,0), i=1,\cdots,N \), and iterate the skew tent maps (1) to
yield \( N \) chaotic orbits \( \{ (x(i,k), k=0,1,\cdots, i=1,\cdots N) \} \)
of
\( x(i,0), i=1,\cdots,N \) with given control parameters
\( a_i, i=1,\cdots,N \). The beginning \( L_0 \) orbit points of each
orbit are then deleted to avoid the harmful transient effect,
where \( L_0 \) is a constant, for example, \( L_0 = 15 \) in all the
experiments. The truncated parts \( \{ (x(i,k), k=L_0 + 1,\cdots, i=1,\cdots N) \} \) are then mapped
to \( N \) new orbits \( \{ (y(i,k), k=1,\cdots, i=1,\cdots, N) \} \) by the
\( N \)-dimensional Arnold map (3). We rearrange all the
\( y(i,k) \) values of the orbits to get one new combined orbit

Fig 1: Properties for the skew tent map with \( a = 0.4 \) and
\( x_0 = 0.367 \).

2.2 Arnold Map

Arnold map was proposed by V. I. Arnold in the
research of ergodic theory; and it is commonly known as
cat face transform [31]. The map is a process of clipping
and splicing that realign the pixel matrix of digital image.
The classical Arnold map is an invertible map described by

\[
\begin{pmatrix}
 x_{n+1} \\
 y_{n+1}
\end{pmatrix} = T_A
\begin{pmatrix}
 x_n \\
 y_n
\end{pmatrix} = \begin{pmatrix}
 1 & 1 \\
 1 & 2
\end{pmatrix} \begin{pmatrix}
 x_n \\
 y_n
\end{pmatrix} \mod 1
\] (2)

where the notation “\( x \mod 1 \)” refers to the fractional part
of a real number \( x \) by adding or subtracting an
appropriate integer. Therefore \( (x_n, y_n) \) is confined in
the unit square \( [0,1]^2 \). The Arnold map is area preserving
since the determinant of its linear transformation matrix
is equal to 1; its Lyapunov characteristic exponents are the
two eigenvalues \( \sigma_1 \) and \( \sigma_2 \) of the coefficient matrix in
(2), given by

\[
\sigma_1 = \frac{1}{2}(3+\sqrt{5}) > 1, \quad \sigma_2 = \frac{1}{2}(3-\sqrt{5}) < 1.
\]

It implies that the map is chaotic since one of the
Lyapunov characteristic exponents is larger than 1. The

\( x_{n+1} = T_A x_n \mod 1 \)}

\( T_A \)}

\( \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{N-1} \\ x_N \end{pmatrix} \)

\( \begin{pmatrix} \sigma_1 \\ \sigma_2 \end{pmatrix} \)
{(z(j), j = 1,⋯, L×N} in the manner

\[ z((k - 1)\times N + i) = y(i, k), \quad i = 1,\cdots, N, k = 1,2,\cdots, L. \]

A truncated combined orbit \( z(k), k = 1,\cdots, 600 \) is depicted in Fig. 2. The truncated sequence \( z(k), k = 1,2,\cdots, H \times W \) is sorted according to the order from small to large. As a result, we get an index order number for each \( z(k) \). 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 initial conditions \( x(i,0), i = 1,\cdots, N \) and of the control parameters \( a_i, i = 1,\cdots, N \).

**Step 2:** Iterate the skew tent map (1)

\[ x(i,k + 1) = T(x(i,k)) \]

to get the orbit of \( x(i,0) \), say \( \{x(i,k), k = 0,1,\cdots, L_0 + L\} \). We choose the truncated orbits \( \{y(i,k), k = L_0 + 1,\cdots, L + L_0\} \) and map them to be \( \{y(i,k), k = 1,\cdots, L\} \) by the \( N \)-dimensional Arnold map (3)

\[
\begin{pmatrix}
y(1,k) \\
y(2,k) \\
\vdots \\
y(N,k)
\end{pmatrix} = T_A
\begin{pmatrix}
x(1,k + L_0) \\
x(2,k + L_0) \\
\vdots \\
x(N,k + L_0)
\end{pmatrix} \mod 1.
\]

**Step 3:** Rearrange all the values of \( \{y(i,k), k = 1,\cdots, L, i = 1,\cdots, N\} \) to get one combined orbit \( \{(z(j), j = 1,\cdots, N \times L) \} \) given by

\[ z((k - 1)\times N + i) = y(i, k), i = 1,\cdots, N, k = 1,2,\cdots, L. \]

**Step 4:** Sort \( \{z(k), k = 1,\cdots, H \times W\} \) to get one index order sequences \( \{IZ(k), k = 1,\cdots, H \times W\} \).

**Step 5:** Reshape the gray-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 \( IZ \) in the following way to get one new vector \( V \)

\[ V(k) = U(IZ(k)), k = 1,\cdots, H \times W. \]

**Step 6:** Reshape \( V \) back to one 2D matrix to yield the shuffled image \( P \).

3.2 Diffusion Process

It is well-known that diffusion process can strengthen the resistance to statistical attack and differential attack efficiently. The histogram of the cipher-image encrypted by a efficient diffusion process is fairly uniform and is significantly different from that of the plain-image. 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 spend a lot of time and effort. The diffusion process is outlined as follows.

**Step 1:** Set the values of the control parameters \( b_i, i = 1,\cdots, 4 \), and the initial conditions \( x_i(i,0), i = 1,\cdots, 4 \). Let \( L_i = \left\lfloor \frac{H \times W}{b_i} \right\rfloor + 1 \).

**Step 2:** Iterate the skew tent map \( x_i(i,k + 1) = T(x_i(i,k)) \) using (1) to get the orbit of \( x_i(i,0) \), say \( \{x_i(i,k), k = 0,1,\cdots, L_0 + L_i\} \). We choose the truncated parts of the orbits, \( \{x_i(i,k), k = L_0 + 1,\cdots, L_0 + L_i\} \), and map them to be \( \{y_i(i,k), k = 1,\cdots, L_i\} \) by the two-dimensional Arnold map (2)

\[
\begin{pmatrix}
y_i(1,k) \\
y_i(2,k) \\
y_i(3,k) \\
y_i(4,k)
\end{pmatrix} = T_A
\begin{pmatrix}
x_i(1,k + L_0) \\
x_i(2,k + L_0) \\
x_i(3,k + L_0) \\
x_i(4,k + L_0)
\end{pmatrix}, k = 1,\cdots, L_i.
\]

The two sequences \( y_i(1,k), y_i(2,k) \) are then piled together to form a new sequence by

\[ TY(2 \times k - 1) = y_i(1,k), \quad TY(2 \times k) = y_i(2,k), \quad k = 1,\cdots, L_i, \]

while \( y_i(3,k), y_i(4,k) \) are integrated to yield another sequence

\[ TZ(2 \times k - 1) = y_i(3,k), \quad TZ(2 \times k) = y_i(4,k), \quad k = 1,\cdots, L_i. \]
TY, TZ are truncated to obtain two pseudo-random gray value sequences \( \varphi_1(k), \varphi_2(k), k = 1, 2, \cdots, H \times W \) by

\[
\varphi_1(k) = \left\lfloor TY(k) \times 255 \right\rfloor, \varphi_2(k) = \left\lfloor TZ(k) \times 255 \right\rfloor,
\]

where \( k = 1, 2, \cdots, H \times W \).

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

\[
C(k) = \varphi_1(k) \oplus \{(P(k) + \varphi_1(k)) \mod 256 \} \oplus C(k - 1),
\]

where \( P(k) \) is the gray 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 \( H \times W \). \( C(k-1) \) is the previous output cipher-pixel gray value. The diffusion process is well defined as the initial condition \( C(0) \) is provided. \( C(0) \) can be set to be part of the keys in the diffusion process or can just take the value of \( C(0) = \varphi_1(1) \) for simplicity. Note that the inverse diffusion function is

\[
P(k) = \{\varphi_1(k) \oplus C(k) \oplus C(k - 1) - \varphi_1(k)\} \mod 256,
\]

where \( k = 1, 2, \cdots, H \times W \).

The above diffusion process can not influence the pixels before the tampered pixel. As a remedy, we here add a reverse diffusion process as a supplement to the above diffusion process. \( \varphi_2(k), k = 1, 2, \cdots, H \times W \) are utilized to perform the reverse diffusion process on the sequence \( C(k), k = H \times W, \cdots, 2, 1 \) by step 4.

**Step 4:** The following diffusion function is utilized to achieve more diffusion effect.

\[
D(k) = \varphi_2(k) \oplus \{(C(H \times W - k + 1) + \varphi_2(k)) \mod 256 \} \oplus D(k - 1),
\]

where \( D(0) \) can be handled as \( C(0) \), it can be set to be part of the keys or can just take the value of \( \varphi_2(1) \) for simplicity.

**Step 5:** Reshape \( D(k), k = 1, 2, \cdots, H \times W \) to be a matrix \( Q \) with height \( H \) and width \( W \). \( Q \) is the resulted cipher-image.

The permutation process and the diffusion process constitute the complete image encryption scheme. The Lena image is encrypted and the resulted cipher-images are shown in Fig. 3.
permutation process and \( b = (0.6, 0.36, 0.41, 0.66) \) and \( x_i(0) = (0.3, 0.23, 0.72, 0.73) \) in the diffusion process.

4. PERFORMANCE AND SECURITY ANALYSIS

According to the basic principle of cryptography [13], a desirable encryption scheme requires sensitivity to cipher keys, i.e., the cipher-text should have close correlation with the 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 attack, differential attack, etc. Some security analysis will be performed on the proposed image encryption scheme, including the most important ones like key sensitivity test, key space analysis, statistical analysis, and differential attack analysis. All the analysis shows that the proposed image encryption scheme is highly secure thanks to its high sensitivity of the control parameters and initial conditions of the skew tent maps, large key space, and satisfactory permutation-diffusion mechanism.

4.1 Key Sensitivity Analysis and Key Space

The high sensitivity of the cipher-image to initial conditions and control parameters is inherent to any chaotic system. 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 \( a, i = 1, \ldots, N \) and the initial conditions \( x_i(0), i = 1, \ldots, N \) form the cipher keys. The cipher keys in the diffusion process consist of the initial conditions \( x_i(j, 0), j = 1, \ldots, 4 \) , the control parameters \( b_j, j = 1, \ldots, 4 \) for the four skew tent maps. The sensitivity tests with respect to all cipher keys have been carried out. The sensitivity is generally measured by means of two criteria, namely, 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 cipher keys with a minor change or two plain-images with only one pixel difference, \( D \) is a bipolar array with the same size as image \( C \). \( D(i,j) \) is determined as: if \( C_1(i,j) = C_2(i,j) \), then \( D(i,j) = 0 \), otherwise \( D(i,j) = 1 \).

To verify the sensitivity of key parameter \( K \), the original plain-image \( I = (I(i,j))_{H \times W} \) is encrypted with \( K = p, K = p - \Delta K \) and \( K = p + \Delta K \) respectively while keeping the other key parameters unchanged. Here \( \Delta K \) is the perturbing value. The corresponding encrypted images are denoted by \( I_1, I_2, I_3 \) respectively. The NPCR and UACI values are calculated for the cipher-image couples \((I_1, I_2)\) and \((I_1, I_3)\). The greater value of NPCR and UACI, the more sensitive is for the key \( K \). Tables 1-2 show the results of the sensitivity test where the initial key values are set to be the following.

**Permutation process:**
- initial conditions \( x(0) = (0.4, 0.44, 0.23, 0.64, 0.236, 0.73) \),
- control parameters \( a = (0.2, 0.7, 0.56, 0.12, 0.371, 0.251) \);

**Diffusion process:**
- initial conditions \( x_0(0) = (0.3, 0.23, 0.72, 0.73) \),
- control parameters \( b = (0.6, 0.36, 0.41, 0.66) \).

The variations \( \Delta K \) of the considered parameters are all set to be \( 10^{-16} \) in the tests. 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 1: Results regarding the sensitivity to cipher keys,

<table>
<thead>
<tr>
<th>( K )</th>
<th>( a_1 )</th>
<th>( a_4 )</th>
<th>( a_5 )</th>
<th>( a_6 )</th>
<th>( a_7 )</th>
<th>( x(1,0) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>UACI(%)</td>
<td>33.63</td>
<td>33.45</td>
<td>33.62</td>
<td>33.44</td>
<td>33.43</td>
<td>33.42</td>
</tr>
<tr>
<td>( K )</td>
<td>( x(2,0) )</td>
<td>( x(3,0) )</td>
<td>( x(4,0) )</td>
<td>( x(5,0) )</td>
<td>( x(6,0) )</td>
<td>( b_1 )</td>
</tr>
<tr>
<td>UACI(%)</td>
<td>33.53</td>
<td>33.43</td>
<td>33.44</td>
<td>33.44</td>
<td>33.45</td>
<td>33.46</td>
</tr>
</tbody>
</table>

### Table 2: Results regarding the sensitivity to cipher keys,

<table>
<thead>
<tr>
<th>( K )</th>
<th>( b_1 )</th>
<th>( b_2 )</th>
<th>( x(i,0) )</th>
<th>( x(i,3) )</th>
<th>( x(i,4) )</th>
<th>( x(i,5) )</th>
<th>( x(i,6) )</th>
<th>( x(i,7) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>UACI(%)</td>
<td>33.55</td>
<td>33.50</td>
<td>33.59</td>
<td>33.47</td>
<td>33.36</td>
<td>33.41</td>
<td>33.49</td>
<td></td>
</tr>
<tr>
<td>( K )</td>
<td>( b_1 )</td>
<td>( b_2 )</td>
<td>( x(i,0) )</td>
<td>( x(i,3) )</td>
<td>( x(i,4) )</td>
<td>( x(i,5) )</td>
<td>( x(i,6) )</td>
<td>( x(i,7) )</td>
</tr>
<tr>
<td>UACI(%)</td>
<td>33.54</td>
<td>33.33</td>
<td>33.50</td>
<td>33.43</td>
<td>33.41</td>
<td>33.40</td>
<td>33.40</td>
<td></td>
</tr>
</tbody>
</table>

**Part 1:** calculated based on the cipher-images \( I_1, I_2 \).

**Part 2:** calculated based on the cipher-images \( I_1, I_3 \).
We also set the perturbing value $\Delta K$ from $10^{-1}$ to $10^{-16}$ and perform the sensitivity tests. The results are depicted in Fig. 4 which are the simulation results for $a_x, x(5,0), b_y$ and $x_1(2,0)$ . The results in Tables 1-2 and Fig. 4 imply that all the control parameters and the initial conditions are strongly sensitive. Although the initial conditions and the control parameters for the four skew tent maps in the diffusion process are less sensitive than those in the permutation process, the resulted NPCR values are all more than 99.1%.

We can conclude from the results that the key space is $(10^6)^20 = 10^{320}$, which is huge enough to make brute-force attack infeasible. As a matter of fact, the key space increases as long as the number of skew tent maps increases. The key space will generally become $10^{32}$ times larger if the number of skew tent maps increased by 1. The sensitivity test can also be demonstrated visually, for example, see Figs. 5-6. In Fig. 5, the image encrypted by the key $a_i = 0.2, x(3,0) = 0.23$ has 99.60% of difference from the image encrypted by the key $a_i = 0.2, x(3,0) = 0.23 + 10^{-16}$. Fig. 6 shows the encrypted image with $a_i = 0.2, x(5,0) = 0.236, b_j = 0.41, x_1(4,0) = 0.73$ can not be decrypted with only one of the keys $a_i = 0.2, x(5,0) = 0.236, b_j = 0.41, x_1(4,0) = 0.73$ perturbed by a minor variation $10^{-16}$. For example, Fig. 6(c) shows that the image encrypted by $b_j = 0.41$ is not correctly decrypted by using the perturbed key $b_j = 0.41 + 10^{-16}$.
(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 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:

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

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

where \( x, y \) are the gray-scale values of two adjacent pixels in the image and \( T \) is the total pairs of pixels randomly selected from the image. The correlations of two adjacent pixels in the plain-image and in the cipher-image are shown in Table 3. The correlation distribution of two horizontally adjacent pixels in the plain-image and that in the cipher-image are shown in Fig. 7.

<table>
<thead>
<tr>
<th>Table 3: Correlation coefficients of two adjacent pixels in two images</th>
</tr>
</thead>
<tbody>
<tr>
<td>plain-image</td>
</tr>
<tr>
<td>Horizontal</td>
</tr>
<tr>
<td>Vertical</td>
</tr>
<tr>
<td>Diagonal</td>
</tr>
</tbody>
</table>

Fig 5: Key sensitive test: result 1

4.2 Statistical Analysis

Shannon pointed out in his masterpiece [32] 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 robust against any statistical attack. In order to prove the security of the proposed encryption scheme, the following statistical tests are performed.
Fig 6: Key sensitive test: result 2

(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

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

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 7.9971 bits. This means that the cipher-image is close to a random source and the proposed algorithm is secure against the entropy attack.
Fig 7: 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.

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 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 NPCR and UACI, given by Eq. (4) and Eq. (5) respectively, are used [6]. In this case, 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. They indicate the sensitivity of the cipher-images to the minor change of plain-image. 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 gray values with a difference of 1, for example, we replace the gray value 93 of the pixel at position (13,115) by 94, and get the NPCR=99.77%, UACI=40.70%. The numerical results are shown in Table 4. The mean values of the ten NPCR and UACI values are 99.81% and 33.79% respectively. We observe from Table 4 that the two measure values are exceptionally good undergoing only one round of encryption.
Table 4: Results of NPCR and UACI tests of Lena

<table>
<thead>
<tr>
<th>Position</th>
<th>(13,115)</th>
<th>(240,194)</th>
<th>(142,114)</th>
<th>(204,93)</th>
<th>(143,173)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPCR(%)</td>
<td>99.77</td>
<td>99.69</td>
<td>99.86</td>
<td>99.91</td>
<td>99.80</td>
</tr>
<tr>
<td>UACI(%)</td>
<td>40.70</td>
<td>30.83</td>
<td>44.15</td>
<td>45.44</td>
<td>29.84</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Position</th>
<th>(242,158)</th>
<th>(200,236)</th>
<th>(121,230)</th>
<th>(97,100)</th>
<th>(243,144)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPCR(%)</td>
<td>99.96</td>
<td>99.86</td>
<td>99.85</td>
<td>99.63</td>
<td>99.82</td>
</tr>
<tr>
<td>UACI(%)</td>
<td>25.27</td>
<td>44.77</td>
<td>15.47</td>
<td>32.33</td>
<td>29.12</td>
</tr>
</tbody>
</table>

4.4 Resistance to Cipher-Image Attacks

Cipher-image attacks mean that the opponent performs image processing like cropping, noising, compression, etc. on the cipher-image. The opponent can just damage the cipher-images if he does not need to know the secret. In such a case, the cryptosystem’s robustness against such a kind of malicious attacks is very important. A secure encryption scheme should consider the robustness against cipher-image attacks. The results of tests to cipher-image attack are shown in Fig. 8, demonstrating that the proposed image encryption scheme is strongly robust against cropping, salt & pepper noising, JPEG compression. Especially the proposed scheme resists cropping attack effectively.
5. CONCLUSIONS

An efficient image encryption scheme based on multiple skew tent maps and Arnold 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 designed to change the gray values of the whole image pixels. Security analysis including key sensitivity analysis, key space analysis, statistical attack analysis and differential attack analysis are performed numerically and visually. The robustness test of the proposed scheme against malicious attacks, like cropping, noising, JPEG compression, is also performed. All the experimental results show that the proposed encryption scheme is secure thanks to its huge key space, its highly sensitivity to the cipher keys and plain-images and its strong robustness resisting malicious image processing. All the desirable 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


AUTHOR PROFILES

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.