An Novel Chaotic Image Encryption Algorithm based on Tangent-Delay Ellipse Reflecting Cavity Map System

HAN Feng-ying¹, ZHU Cong-xu²

¹Changsha Aeronautical Vocational And Technical College, Changsha Hunan 410014;
²School of Information Science and Engineering, Central South University, Changsha Hunan 410083

Abstract

In order to effectively protect digital image information, to improve the efficiency and security of the encrypted image, many effective and feasible image encryption algorithms have been proposed. The recovery is depended on the recovery value of pixel 8 bits plane; the incorrect from low to high pixel value of plane affect the incorrect of Index of all proportion to the pixel value, resulting in the restoration of image quality. Based on the study of digital image encryption technology, the essay proposes the image encryption algorithm based on TD-RECS chaotic system, and the decryption algorithm against attack on the basis of it.

Keywords: chaos sequences; image encryption; encrypted image anti-sheared recovery

1. INTRODUCTION

The literature [1] proposed a digital image encryption algorithm based on chaotic sequences pixel scrambling and the pixel value transform; the literature [2] proposed a method that embeds the important information of the image block in a least significant bit (LSB) of another image block which is decided by the chaotic system, in order to improve the anti-sheared capacity of encrypted image. This algorithm is unable to restore the area sheared of the image when the image is disturbed by a slight noise. When the block important information corresponding to the part is sheared, the block will not be restored; the literature [3] gives an image encryption algorithm based on image bit plane, and an anti-sheared recovery algorithm.

2. TD-ERCS CHAOTIC SEQUENCE
TD-ERCS system was developed by Professor Yuan Sheng Lee, who has proposed a two-dimensional chaotic systems [4] in 2004, the two-dimensional chaotic systems is a new domain-wide discrete chaotic system, with zero correlation and a stable probability distribution [4-5]. The mapping equation is

\[
\begin{align*}
    x_n &= -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2} \\
    k_n &= \frac{2k_{n-m} - k_{n-1} + k_{n-1}^2}{1 + 2k_{n-m}k_{n-m} - k_{n-m}^2}, n = 1, 2, 3, \ldots
\end{align*}
\]

(1)

where

\[
    k_{n-m} = \begin{cases} 
    \frac{-x_{n-1}}{y_{n-1}} & n < m \\
    \frac{-x_{n-m}}{y_{n-m}} & n \geq m
    \end{cases}
\]

(2)

\[
y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}
\]

(3)

\[
y_0 = \mu\sqrt{1 - x_0^2}
\]

(4)

\[
k_0' = -\frac{x_0}{y_0}
\]

(5)

\[
k_0 = -\frac{\tan \alpha + k_0'}{1 - k_0' \tan \alpha}
\]

(6)

On where, (μ,x_0,α,m) are the system seed parameters, system parameters μ ∈ (0,1], initial x_0 ∈ [-1,1], α ∈ (0, π ), tangent delay parameters m = 2,3,4,5, ...  

3. ENCRYPTION ALGORITHM

In order to improve the anti-sheared capacity and the ability to resist pixel characters statistic attacking of encrypted image, the algorithm adopts the pixel position change and the pixel value transform.

Let’s suppose the size of digital image A is m×n, the chaos sequence produced by TD-ERCS system is

\[
\{(X_i, K_i) | i = 1, 2, 3, \ldots, m \times n\}
\]

(7)

Sequence \{X_i|i=1,2,3,\ldots,m\times n\} and \{K_i|i=1,2,3,\ldots,m\times n\} are used to encrypt digital image’s pixel position and pixel value.

3.1. Pixel Position Change Based on Chaos Sequence

In order to achieve a better scrambling effect, we should use the chaos sequence’s pseudo-randomicity and ergodicity, the algorithm takes the original image pixels to a new place by chaos sequence.

1) To calculate conveniently, Matrix A is changed to one-dimensional vector B_t (1: m×n) in the order of ranks.
\[ B_i \left( (i-1)n + j \right) = A(i, j) \]  
(8)

where \( i=1,2,3,\ldots, m \), \( j=1,2,3,\ldots, n \).

2) Let the chaos sequence \( \{X_i|i=1,2,3,\ldots,m\times n\} \) sort ascending or descending, it achieves a new sequence \( \{cX_i|i=1,2,3,\ldots,m\times n\} \), use the \( cX(i) \)'s location index to produce a chaos random sequence \( \{sX_i|i=1,2,3,\ldots,m\times n\} \) that submit to \([1,m\times n]\), takes vector \( B_t \) to a new vector \( B \) according this sequence.

\[ B(i) = B_i \left( sX(i) \right) \]  
(9)

where \( i=1,2,3,\ldots, m \times n \).

If we make the new vector \( B \) reconstructs the image, it will all in a mess, such as the figure 1. Figure 1(a) is the grayscale image that only has two kinds of pixel value, figure 1(b) is the position encrypted image.

![Figure 1](image1.png)

(a) Original Image

(b) Position Encrypted Image

3.2. Pixel Value Change Based on XOR Operation

This algorithm uses chaos sequence to be XOR operand to encrypt image B’s pixel value.

1) Changing chaos sequence to unsigned integer as an XOR operand:

\[ mK(i) = \text{round} \left( K(i) \times 10^k \right) \mod 256 \]  
(10)

2) The new pixel value \( B(i) \) of vector B’s pixel value \( B(i) \) is

\[ B(i) = B(i) \oplus mK(i) \]  
(11)

In this list, \( i=1,2,3,\ldots, m \times n \).

Changing B to A, then we can achieve encrypted image. After image’s pixel values are changed randomly, it will change original image’s grayscale histogram, such as figure 2. Figure 2(a) is the image that pixel position and pixel value are encrypted. Figure 2(b) is its grayscale histogram.

![Figure 2](image2.png)

(a) Encrypted Image

(b) Encrypted Image Histogram

4. DECRYPTION ALGORITHM PROTECTING FROM SHEARING ATTACK
This essay’s encryption algorithm is a reversible algorithm, we can achieve lossless original image in the rule of encryption algorithm’s reversal algorithm. To resist the attack of malicious shearing, this paper put forwards an anti-sheared attack decryption recover algorithm. Encrypted image attacked by shearing or scrawling, their decrypted images just like figure 3.

(a)    (b)

Figure 3. The decryption effect of the sheared encrypted image: (a) the sheared image; (b) the decrypted image.

We can see from figure 3(b) that the sheared pixels uniformly distributed the whole image after being decrypted. According to neighboring pixel’s feature, the pixel can be almost recovered. But, this is based on the uniformly distributed characteristics of the encryption algorithm’s pixels scrambling and the pixel values diffusing.

4.1. Check The Sheared Image

Before decrypting, we should check the sheared pixels. After image pixels scrambling and pixel values diffusing, the image’s adjacent pixels hardly related. Such as 2 to 3 consecutive pixels of the same pixel value, then these pixels are supposed to be sheared or scribbled pixels. In the encryption algorithm of this paper, many experiments tell us, take 3 successive pixels values equal for judging condition is very reliable.

Suppose the algorithm uses flag $m \times n$ unsigned integer matrix signs encrypted image’s sheared pixels, also initializes to zero. From the first row’s first column, it starts to scan row by row and column by column. If there are 3 successive pixels values the same, then the pixels corresponding flag is set to 1. The flag bits must follow the image encryption to change to the flg bits of the original image distributed uniformly.

4.2. Anti-sheared Recovery Algorithm Based on the Neighboring Pixels Correlated Characteristic

This algorithm is called Np recovery algorithm. After image decrypting, sheared pixels have been distributed uniformly in the whole image already. Apply the 4 neighborhood adjacent pixels correlated characteristics, namely high correlation, sheared pixel values can be decided based on the neighboring pixel values. This algorithm is:

1) According to flg, the algorithm recovers the sheared pixel values from the first row, the first column, the m row and the n column, and takes the average value of neighboring pixel values or the neighboring pixel values.

2) From the pixel of the second row second column, according to flg, the algorithm calculate sheared pixel value row by row and column by column, if its right neighboring pixel isn’t sheared, its value should be equal to the average value of its left and right neighboring pixel value. Otherwise, if its lower neighboring pixel isn’t sheared, its value should be equal to the average value of its up ones and lower
ones’ pixel value. Still otherwise, if its lower neighboring pixel is sheared, its value should be equal to the average value of its left ones and up ones’ pixel value.

5. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed algorithm has done a lot of experiments. The experimental results show that the effectiveness of the proposed algorithm. For space reason, only some representative experiments which demonstrate and analysis the algorithm are given.

The experiment is using the platform of Matlab 2009b, 256-level grayscale lena image 256×256, TD-ERCS system parameters ($\mu$=0.5432, $x_0$=0.2535, $\alpha$=0.5868, $m$=3), iterations $n=100+256 \times 256$, $k=7$ in the Eq(10). The result of the experiment is shown in Figure 4. The original image and its histogram, the encrypted image and its histogram are given in the figures.

![Figure 4](image)

Figure 4. The results of lena image encrypted by the algorithm: (a)lena image; (b) the histogram of figure (a); (c)the encrypted image of figure (a); (d)the histogram of figure (c).

5.1. Key Security Analysis

The key space $k$ of the proposed algorithm is decided by TD-ERCS system parameters key=$($\mu$,x_0,\alpha,m)$, it can be calculated as

\[ k = k_n \times x_0 \times k_\alpha \times k_m \]

(12)

Where, $k_n, k_{x_0}, k_\alpha$ produces the double precision floating number $\mu, x_0, \alpha$; $k_m$ uses for producing integer $m$. Take the $m$ length this 12 bits, then values can be

\[
m = \begin{cases} 2 & (k_m = 0) \\ 4 & (k_m = 1) \\ k_m + 3 & (2 \leq k_m \leq 4095) \end{cases}
\]

(13)

Reckoning conservatively, we choose the precision of key which is $10^{-15}$, the size of the key space is over than $10^{48}$. The key space is large enough so that can resist the exhaustive attack effectively.

The key of the experiment, the revision of $\mu, x_0, \alpha$ only differs $10^{-16}$, got the decrypted image is still chaotic one. This indicates that the algorithm has high sensitivity to the key.

5.2. Statistic Characters Analysis
5.2.1. Histogram

The result of experiment shows that the pixel values’ distributed ability of the proposed is very strong. Random pixels values of the any encrypted image distributes uniformly in the whole range of values. And the pixel statistic values tends almost unanimous, completely change the statistic characters of the original image.

5.2.2. Correlation of adjacent pixels

In order to analysis the correlation of the image, we introduce the correlation coefficient of adjacent pixels. Its calculation formula is as follow:

\[ R_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}} \]  

Where \( x \) and \( y \) are grayscale value of two adjacent pixels in the image. \( \text{cov}(x,y) = E((x-E(x))(y-E(y))) \) is covariance between \( x \) and \( y \), \( D(x) = E((x-E(x))^2) \) is variance of variable, \( E(x) \) is mean.

The experiment has run the correlation of pixel test on each pair of all the adjacent pixels of lena image for experiment in horizontal, vertical and diagonal, their laboratory result of correlation coefficient are shown in table 1.

<table>
<thead>
<tr>
<th>TABLE 1. THE CORRELATION COEFFICIENT OF ADJACENT PIXELS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Image</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Horizontal</td>
</tr>
<tr>
<td>Vertical</td>
</tr>
<tr>
<td>Diagonal</td>
</tr>
</tbody>
</table>

The experimental data demonstrate that there is a significant relevance between the adjacent pixels of the original image. And the correlation coefficient of the encrypted image adjacent pixels is almost zero. The adjacent pixels are almost irrelevant.

6. Conclusion

Theory and experiment show that this algorithm has a better security and a strong anti-sheared capacity, anti-sheared recovery algorithm is really effective. But with the increase of the area to be shear, recovery accuracy of the pixels which are sheared decreased and it needs to be further improve the algorithm to improve the quality of recovery.

References