Multi Chaotic Systems Based Pixel Shuffle for Image Encryption

H. H. Nien\textsuperscript{a} & C. K. Huang\textsuperscript{b}

\textsuperscript{a}Department of Electrical Engineering, Chienkuo Technology University, Changhua 500, Taiwan.
\textsuperscript{b}Department of Industrial Education and Technology, National Changhua University of Education, Changhua 500, Taiwan.

Abstract

This paper proposes a novel pixel shuffling method for image encryption. The output trajectory of chaotic system is very unpredictable because that the chaotic system is high nonlinearity and is sensitive to initial values and parameters of chaotic variables. Therefore, based on the unpredictable character, we use the chaotic sequences generated by chaotic systems as encryption codes and then implement the digital-color image encryption with high confidential security. The proposed method combined with 4 differential chaotic systems and pixel shuffling can fully banish the outlines of the original image, disorders the distributive characteristics of RGB levels, and dramatically decreases the probability of exhaustive attacks. The statistic methods involving FIPS PUB 140-1 and the correlation coefficient $r$ are adopted to test on the security analysis. Also NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) are proceeded for the proof of the distinguished characteristic of pixels in the encrypted image. Eventually, empirical images are conducted as illustrations and show that the proposed method has the great encryption performance and achieves the high confidential security.

Keywords—Pixel shuffling, Chaotic system, Correlation coefficient, NPCR, UACI
1. Introduction

Since the dynamic response of the chaotic system is sensitively to the initial values and parameters of the chaotic system, a great number of researches apply chaotic sequences to encrypt images for the purpose of communication security [1-5]. It is a convenient and fast method by conducting a first-order chaotic system to encrypt digital-color images [6]. Zhang and He created the encrypting matrix using a first-order chaotic sequence to encrypt the original matrix, and then conducted a second-order sequence to disguise the encrypted matrix with high security [7]. But there was report proposed that the communication security was insufficient [8].

Since the high security is the character of a high-order chaotic system, Zhu et al. proposed a digital-color image encryption based on a third-order chaotic system [9]. They confused the relation between the encrypted image and the original image by means of shuffling the position and varying the RGB levels of each pixel. Sun and Chen used Lorenz system to produce chaotic sequences, and combined chaotic mapping to encrypt image for promoting encryption security [10]. Sun et al. presented a shuffling method based on the third-order Chua system for enlarging the image space [11]. This method could avoid the localized distribution of grey levels. Kwok and Tang proposed a fast chaos based image encryption system with stream cipher structure [12]. The major core of the encryption system, which is a pseudo-random key stream generator based on a cascade of chaotic maps, serves the purposes of sequence generation and random mixing.

However, the insufficient key spaces are the major drawback of those methods with single chaotic system; moreover, the RGB levels are unchanged when only pixel shuffle is used. For this reason, this paper conducts chaotic variables with double scroll attractor [13], butterfly attractor [14], spiral attractor [15], and discrete time [16] characters to product encryption codes and applies them on pixel shuffling. Finally, a
high confidential security with a dramatically large key space and converted RGB-level spectrums is achieved.

2. Pixel-Chaotic-Shuffle method

A. Chaotic System

The third-order chaotic systems applied in this paper are shown below:

1. Hénon map (discrete time) [16]:

\[
\begin{align*}
    x(k+1) &= a - y^2(k) - bz(k) \\
    y(k+1) &= x(k) \\
    z(k+1) &= y(k),
\end{align*}
\]

where \( a = 1.76 \) and \( b = -0.1 \).

2. Lorenz (butterfly attractor) [14]:

\[
\begin{align*}
    \dot{x} &= -\sigma x + \sigma y \\
    \dot{y} &= -xz + \gamma x - y \\
    \dot{z} &= xy - bz,
\end{align*}
\]

where \( \sigma = 16 \), \( \gamma = 40 \), and \( b = -4 \).

3. Chua (double scroll attractor) [13]:

\[
\begin{align*}
    \dot{x} &= \alpha (y - x - h(x)) \\
    \dot{y} &= x - y + z \\
    \dot{z} &= -\beta y - \gamma z \\
    h(x) &= m_1 x + 0.5(m_0 - m_1)(|x + 1| - |x - 1|),
\end{align*}
\]

where \( \alpha = 10 \), \( \beta = 14.78 \), \( \gamma = 0.0385 \), \( m_0 = -1.27 \), and \( m_1 = -0.68 \).

4. Rössler (spiral attractor) [15]:

\[
\begin{align*}
    \dot{x} &= -(y + z) \\
    \dot{y} &= x + ay
\end{align*}
\]
\begin{equation}
\dot{z} = b + z(x - c),
\end{equation}

where \(a = 0.2\), \(b = 0.2\), and \(c = 5.7\).

B. Pixel-Chaotic-Shuffle (PCS)

As the color contrast of the original image’s outline becomes more distinct, the characteristic of the RGB levels will not be eliminated when only apply pixel shuffle on the image encryption. For this reason, this paper proposes a novel PCS encryption method. The proposed method can vary the RGB levels and positions of each pixel simultaneously.

Fig. 1 shows the flowchart of the proposed method. Four chaotic systems are applied to create chaotic codes individually.
The steps for the PCS can be outlined as follows:

Step 1: Select proper initial values and system parameters to create chaotic variable sets $X_1 \sim X_4, Y_1 \sim Y_4$ and $Z_1 \sim Z_4$.

Step 2: Prepare the chaotic sequences $f x_1 \sim f x_4$ generated from chaotic variable sets; that are

$$fx_1 = \text{sort}(X_{1,c_1}), \quad fx_2 = \text{sort}(X_{2,c_1}) \quad \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \}
Step 5: Shuffle bits within each pixel as shown in Fig. 3. We shuffle those separated 2-bit pairs by \( f_{x1} \sim f_{x4} \).

Step 6: Repeat from Step 1 to Step 5 for the G-level and B-level matrices respectively.

3. Example

In this paper, two color images are adopted as examples for the proof of the high security of the proposed method. The first one is the empirical color photo “Lena (256x256x3)”. Fig. 4 shows the original image and its RGB-level spectrums. Fig. 5 exhibits the encrypted image and its RGB-level spectrums by Zhu et al. [9].

Figure 2. Column shuffling and indexing for each pixel in the same column

Figure 3. 2-bit shuffling and indexing within a pixel
Figure 4. Lena and its RGB-level spectrums: (a) original image, (b) R-level spectrum, (c) G-level spectrum, (d) B-level spectrum.

Figure 5. Encrypted Lena using Zhu’s technique and its RGB-level spectrums: (a) encrypted image, (b) R-level spectrum, (c) G-level spectrum, (d) B-level spectrum.
Although the encrypted image has lost its outline completely, the RGB levels remain the same. Fig. 6 demonstrates the encrypted Lena using the proposed PCS technique. Not only the Lena’s outline but also the RGB levels are changed dramatically.

Figure 6. Encrypted Lena using the proposed PCS technique and its RGB-level spectrums: (a) encrypted image, (b) R-level spectrum, (c) G-level spectrum, (d) B-level spectrum.

Fig. 7 demonstrates the encryption effect of the another color image “Chienkuo badge”. From the encrypted Chienkuo, it revels that the proposed method is also effective for the design image.
4. Security analysis

Galton mentioned that two random variables \( x, y \) (\( x \) and \( y \) are grey-scale values of two adjacent pixels in the image) are defined as correlated if \( y \) changes as \( x \) changes, and changes with the same direction as \( x \) does. Correlation coefficient \( r \) is the measure of extent and direction of linear combination of two random variables. If two variables are closely related with stronger association, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related and cannot predict each other. The coefficient \( r \) can be calculated by the following formula [17]:

\[
    r = \frac{n(\sum_{i=1}^{n} XY_i) - (\sum_{i=1}^{n} X)(\sum_{i=1}^{n} Y)}{\sqrt{\left[n(\sum_{i=1}^{n} X_i^2) - (\sum_{i=1}^{n} X)^2\right]} \sqrt{\left[n(\sum_{i=1}^{n} Y_i^2) - (\sum_{i=1}^{n} Y)^2\right]}},
\]

(5)

in which, \( n(\sum_{i=1}^{n} XY_i) - (\sum_{i=1}^{n} X)(\sum_{i=1}^{n} Y) \) is called sample covariance, \( [n(\sum_{i=1}^{n} X_i^2) - (\sum_{i=1}^{n} X)^2] \) and \( [n(\sum_{i=1}^{n} Y_i^2) - (\sum_{i=1}^{n} Y)^2] \) are the standard deviations of \( X \) and \( Y \). According to the prescription of FIPS PUB 140-1 [18], a set of random numbers needs to satisfy these tests: monobit test, poker test, runs test, and long run...
test. Table 1 shows the test results of Lena and proves that the proposed PCS passes FIPS PUB 140-1 test.

<table>
<thead>
<tr>
<th>Table 1. Test results of Lena for FIPS PUB 140-1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monobit Test</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>$x: 9654 &lt; X = 9995 &lt; 10346$</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>$y: 9654 &lt; X = 9972 &lt; 10346$</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>$z: 9654 &lt; X = 10067 &lt; 10346$</td>
</tr>
<tr>
<td>Poker Test</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>$x: 1.03 &lt; X = 12.7232 &lt; 57.4$</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>$y: 1.03 &lt; X = 14.1440 &lt; 57.4$</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>$z: 1.03 &lt; X = 13.4400 &lt; 57.4$</td>
</tr>
</tbody>
</table>

In order to evaluate the variations between the original and the encrypted images, we conduct two additional tests: NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity). NPCR and UACI are performed as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100\%,$$  \hspace{1cm} (6)

$$UACI = \frac{1}{m \times n} \sum_{i=0}^{t-1} \sum_{j=0}^{m-1} \left( \frac{|A(i,j) - A_H(i,j)|}{255} \right) \times 100\%,$$  \hspace{1cm} (7)

for  $D(i,j) = \begin{cases} 0, & A(i,j) = A_H(i,j) \\ 1, & A(i,j) \neq A_H(i,j) \end{cases}$,

where $A$ and $A_H$ are RGB-level matrices of the original image and the encrypted image respectively. As shown in Table 2 and 3, the proposed method has great performances in $r$, NPCR and UACI tests. The correlation distribution of two
horizontally adjacent pixels in the original image and that in the cipher image: the correlation coefficients are 0.9597 and 0.1257. Similar results for diagonal and vertical axes are obtained. The results reveal that the proposed method dramatically randomized the pixels and varied the grey level of each pixel. Also, the NPCRs of the PCS encryption being all close to unity are evident. And that means almost all grey levels of pixels in the PCS encrypted image are changed.

Table 2. Comparisons of the correlation coefficient $r$ of Lena.

<table>
<thead>
<tr>
<th>Axis</th>
<th>Original $r$</th>
<th>PCS encryption $r$</th>
<th>Zhu (PS) $r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>0.9597</td>
<td>0.1257</td>
<td>0.3913</td>
</tr>
<tr>
<td>Vertical</td>
<td>0.9792</td>
<td>0.0581</td>
<td>0.3955</td>
</tr>
<tr>
<td>Diagonal</td>
<td>0.9570</td>
<td>0.0504</td>
<td>0.3973</td>
</tr>
</tbody>
</table>

Table 3. Results of NPCR and UACI tests of Lena.

<table>
<thead>
<tr>
<th>Test Method</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCS Encryption</td>
<td>R 99.42  G 99.60  B 99.54</td>
<td>R 27.78  G 27.66  B 24.94</td>
</tr>
</tbody>
</table>

5. Conclusions

This paper introduces a new pixel shuffle technique with multi chaotic systems for the image encryption. Since the chaotic system is highly sensitive to initial values and parameters of chaotic variables, meanwhile, has an enormous key space, the proposed method combined with 4 chaotic systems and pixel shuffle can fully banish the outlines of the original image, disorders the distributive characteristics of RGB levels, and dramatically decreases the probability of exhaustive attacks. We conduct FIPS PUB 140-1, the correlation coefficient $r$, NPCR, and UACI to test on the security analysis and the distribution of distinguished elements of variables for the encrypted image. The adopted examples show the highly confidential encrypted images and demonstrate a good potential in the application of the digital-color image encryption.
References


