Novel Chaotic System for Color Image Encryption Using Random Permutation

S. N. Lagmiri\(^1\), N. Elalami\(^2\) and J. Elalami\(^3\)

\(^1\) Information and Production System, Mohammadia School Engineering, Mohamed V University in Rabat, Morocco

\(^2\) LAII, Mohammadia School Engineering, Mohamed V University in Rabat, Morocco

\(^3\) LASTIMI, Higher School of Technology of Sale, Mohamed V University in Rabat, Morocco

\(^1\)najoua.lagmiri@gmail.com, \(^2\)prelalami@gmail.com, \(^3\)alamijamila1@gmail.com

ABSTRACT

The recent researches of image encryption algorithms have been more and more interested to combine the encryption methods and the complex behavior of chaotic signals, in order to reach higher security performance. A digital image can be represented by two dimensional arrays which have numeric value called pixel, and can be encrypted by various combination of those pixels. There are various encryption methods to secure image from unauthorized parties. This paper is an implementation of a color image encryption algorithm based on a novel three dimensional chaotic system using a random permutation technique.

Keywords: Encryption, Decryption, Chaotic System, Permutation, Histogram, Correlation Coefficient.

1 INTRODUCTION

With the ever-increasing growth development of image transmission through computer networks, especially the Internet, the security of digital images has become more important. So it is necessary to encrypt image data before transmission over the network to preserve its security and prevent unauthorized access. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption.

In recent years, plenty of color image encryption approaches have been proposed, such as DES, AES, RSA, etc. However, due to bulk volume of data, high correlation among adjacent pixels, high redundancy and real time requirement [4], these ciphers may not be the most desired candidates for image encryption, particularly for fast and real-time communication applications [5].

In order to overcome image encryption problems, in recent years, many scientists and engineers have designed image encryption algorithms based on chaotic random permutation [6, 9]. Due to desirable properties of nonlinear dynamical systems such as high sensitive dependence on initial conditions and control parameter, ergodicity, unpredictability, mixing, etc., which are analogous to the confusion and diffusion properties of Shannon [1], the chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption [2].

Our proposed work focused on the image encryption using random permutation technique. The current pixel is moved to calculated new position using chaos theory.

The rest of paper is organized as follows. Section 2 presents the novel chaotic system. Section 3 details the chaotic permutation techniques for encryption image. The simulation results are presented in section 4 while section 5 is devoted to the conclusion.
2 PROPOSED SYSTEM

The first step in designing an encryption algorithm is to choose the adequate chaotic system. Choosing systems for encryption algorithms is not an easy task and one should consider only ones with good cryptographic properties. In this section, a novel chaotic system is constructed by combining two others. Then the dynamic behaviors of this system are presented.

2.1 Nosé-Hoover system

A classical example of a conservative chaotic system is the Nosé-Hoover system [3, 6], which is modeled by the system of differential equations:

\[
\begin{align*}
\dot{x}_1 &= x_2 \\
\dot{x}_2 &= -x_1 + x_2 x_3 \\
\dot{x}_3 &= 1 - x_3^2
\end{align*}
\]  

(1)

The Nosé-Hoover system (1) has the Lyapunov exponents \( L_1 = 0.014, L_2 = 0 \) and \( L_3 = -0.014 \). The system (1) is chaotic as it has a positive Lyapunov exponent and is conservative as the sum of the Lyapunov exponents is zero. Thus, the system (1) is volume-conserving.

2.2 Tang & al system

The following 3D chaotic system which was introduced by Tang et al. [9] in 2012 is considered:

\[
\begin{align*}
\dot{x}_1 &= -ax_1 + bx_2 + x_2 x_3 \\
\dot{x}_2 &= cx_1 - dx_2 - x_1 x_3 \\
\dot{x}_3 &= ex_1 - fx_3 + gx_1 x_2
\end{align*}
\]  

(2)

Where \( x_1, x_2, x_3 \in \mathbb{R} \) are state variables and \( a, b, c, d, e, f, g \in \mathbb{R}^+ \). Every state equation has two one-order terms and one quadratic cross-product term. System (2) has complex dynamic behaviors and several larger chaotic coefficient’s regions. It has a typical chaotic attractor when \( a = 25, b = 16, c = 40, d = 4, e = 5, f = 5 \) and \( g = 7 \).

2.3 Novel chaotic system

The novel chaotic system introduced in this paper is described as the following autonomy differential equations:

\[
\begin{align*}
\dot{x}_1 &= -25x_1 + 17x_2 + x_2 x_3 \\
\dot{x}_2 &= 39x_1 - 4x_2 - x_1 x_3 + x_2 x_3 \\
\dot{x}_3 &= 5(x_1 - x_3) + 7x_1 x_2 + 1 - x_2^2
\end{align*}
\]  

(3)

Fig. 1. Novel chaotic 3D attractor

2.3.1 Lyapunov exponent

By linearizing the Jacobian matrix \( J_E \) round the equilibrium point \( E \) and solving the following equation:

\[
|\lambda - J_E| = 0
\]

(4)

Therefore, the novel chaotic system (3) has three eigenvalues shown in figure 1.

\[
\lambda_1 = 40.051, \lambda_2 = -5.039, \lambda_3 = 0.828
\]
2.3.2 Sensitivity to initial conditions

Sensitivity to initial conditions means that each point in a chaotic system is arbitrarily closely approximated by other points with significantly different future paths, or trajectories. Thus, an arbitrarily small change, or perturbation, of the current trajectory may lead to significantly different future behavior. The next figure compares the time series for two slightly different initial conditions. The two time series stay close together, but after that, they are pretty much on their own.

![Time Series](c)

Fig.3. Sensitivity to two initial conditions $[5, -2, 1]$ and $[6, -1, 3]$ (a): $x_1$ (b): $x_2$ (c): $x_3$

3 PROPOSED ENCRYPTION SCHEME

3.1 Encryption algorithm

The random permutation of the pixel positions will achieve global encryption of the image pixel position, in such a way as to break the correlation of the adjacent pixels. We only permute the location of the image, without changing the pixel value. The following algorithm permutes the indices of bits of each pixel using the chaotic value. The technique used at the permutation stage is based on the ascending sorting of the chaotic sequence.

The encryption algorithm is composed of eight steps.

Step 1: Load the original image $I[M, N]$;

Step 2: Separation of the image for RGB three-color block;

Step 3: Reshape the original image $I$ into 1-D signal $A1$ (reshape each block);

Step 4: Sort $X$ and get $lx$ then, generate the permutation key;

Step 5: Permute the pixels of the whole 1-D signal $A1$ with the generated key (using $lx$) to obtain the 1-D signal $A2$. 
**Step 6:** Repeat step 5 until reaches $M \times N$, the length of the whole 1-D signal;

**Step 7:** Reshape the 1-D signal into the 2-D block;

**Step 8:** Recombine the three-color bloc and get encrypted image $I'$;

---

### 3.2 Decryption algorithm

The decryption involves reconstructing color levels of the original image from the encrypted image. It is a simple inverse process of the proposed encryption algorithm. Therefore, it is a symmetric key encryption algorithm in which the same keys are used in the retrieval process. The use of chaos provides the lossless encryption and decryption.

---

### 4 SIMULATION RESULTS AND SECURITY ANALYSIS

The proposed encryption algorithm is implemented in MATLAB for computer simulations. We take a color “baby” image of 384x384 in size for experimental purposes. The Figure 5 shows the encrypted image using the proposed method.

---

**4.1 Histogram analysis**

An image histogram is a commonly used method of analysis in image processing. The advantage of a histogram is that it shows the shape of the distribution for a large set of data. Thus, an image histogram illustrates how pixels in an image are distributed by plotting the number of pixels at each
color intensity level. It is important to ensure that the encrypted and original images do not have any statistical similarities.

Fig. 6. Original image histogram in three channels RGB

Fig. 7. Encrypted image histogram in three channels RGB
The experimental results of the original image and its corresponding encrypted image and their histograms are shown in Figures 6 and 7. The histogram of original image illustrates how the pixels are distributed by graphing the number of pixels at every color of RGB [8]. As shown, it is obvious that the histograms of the encrypted image are nearly uniform and significantly different from the histograms of the original image.

4.2 Correlation analysis

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image respectively.

First, randomly select 3000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following formulas:

\[
C_r = \frac{N \sum_{i=1}^{N} (x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{(N \sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2) \times (N \sum_{i=1}^{N} y_i^2 - (\sum_{i=1}^{N} y_i)^2)}}
\]

where \(x\) and \(y\) are the intensity values of two adjacent pixels in the image and \(N\) is the number of adjacent pixels selected from the image to calculate the correlation. Results for the correlation coefficients of two adjacent pixels are shown in Table 1.

The results of the correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the original images and its encrypted images are given in Figures 8 and 9. There is very good correlation between adjacent pixels in the image data [10, 11], while there is only a small correlation between adjacent pixels in the encrypted image.

Fig. 8. Horizontal, vertical and diagonal correlation of original image
3 PSNR

Peak Signal to Noise Ratio (PSNR) criterion is used to test the unobservable factor. This measure dictates the degree of similarity between the watermark images and a watermark images. PSNR expressed mathematically in the following form:

$$PSNR[\text{dB}] = 10 \log_{10} \left( \frac{255^2}{EQM(I_o,I_R)} \right)$$

where $EQM$ is the mean square error between the images ($I_o$ original, $I_R$ recovered).

$$EQM(I_o,I_R) = \frac{1}{mn} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} (I_o(x,y) - I_R(x,y))^2$$

4 DECRYPTED IMAGE

To recover the "Baby" image, we apply the inverse of the proposed algorithm in Figure 4. The result is shown in figure 10.

By modifying the initial conditions of the novel chaotic system with $10^{-7}$ the decrypted image is totally wrong, as shown in figure 11.

This result shows the performance of using a chaotic system to secure image transmission.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>0.9890</td>
<td>0.9889</td>
<td>0.9838</td>
</tr>
<tr>
<td>Encrypted</td>
<td>-0.0540</td>
<td>-0.0795</td>
<td>-0.0252</td>
</tr>
<tr>
<td>Decrypted</td>
<td>0.9890</td>
<td>0.9889</td>
<td>0.9838</td>
</tr>
</tbody>
</table>

Fig. 9. Horizontal, vertical and diagonal correlation of encrypted image

Fig. 10. Decrypted image
PSNR high means: Mean square error between the original image and reconstructed image is very low. It implies that the image been properly restored. In the other way, the restored image quality is better; in our case, the value of PSNR is as follow:

\[
\text{PSNR (Original/Decrypted)} = \text{Inf}
\]

Contrariwise, a low PSNR means: Mean square error between the original image and encrypted image is very high. It implies that the image been correctly encrypted. In our case the value of PSNR is as follow:

\[
\text{PSNR (Original/Encrypted)} = 16.9466
\]

The result is much closed with the correlation coefficient.

- The correlation coefficient for the original and decrypted image are identical. The value of PSNR (Original/Decrypted) means that the decrypted image is identical to original image.
- The correlation coefficient for the original and encrypted image are very different. The PSNR(Original/Encrypted) means that the encrypted image is totally different of the original image.

5 CONCLUSION

In this paper, we construct a novel three-dimensional chaotic system by adding the Nosé-Hoover system to the Tang & al system. Then we analyze the basic dynamic characteristics of the proposed system. The chaotic sequences of the proposed system are generated. The security analysis, including histogram, Correlation of two adjacent pixels and PSNR, shows that the proposed system has good security and complexity. Then we proposed image encryption base on permutation. The different combination of the permutations for image encryption has been performed. It is observed that image encryption using this technique given good results.

8 REFERENCES