Image encryption using random permutation algorithm and based on a new hyperchaotic system

Abstract

Because of ample using images in the transmission process, it is important to protect the confidential image data from unauthorized access. Cryptography plays a major role in the field of network security. The available encryption algorithms which are mainly used for text data may not be adequate for multimedia data like images. Most of the encryption techniques have some security and performance issues. Due to the random-like property and high sensitivity for initial values and parameters, chaotic systems are usually proposed as a solution to image encryption. This work deals with the encryption of a color image using a new hyperchaotic system. To demonstrate its application in image processing, the system is applied with an algorithm based on key generation based on initial conditions for encryption and decryption. Experimental results show that the algorithm can provide a high level security and it can restore the image as same as the original one, which reaches to the purposes of image safe and reliable transmission.

Keywords: chaotic/hyperchaotic systems, histogram, image encryption, decryption, correlation

Introduction

Recently, security of multimedia data is receiving more and more attention due to the transmission over various communication networks. In order to protect personal information, many image encryption algorithms are designed and proposed such as two-dimensional cellular automata based method,\(^1\)\(^2\) Henon chaotic map,\(^3\)\(^4\) Chen’s hyperchaotic system,\(^5\)\(^6\) Arnold transform.\(^7\)\(^8\) Chaotic functions are blessed with properties like sensitivity to the initial conditions, and ergodicity which make them very desirable for encryption.

In general, there are two types of encryption schemes namely symmetric encryption and asymmetric encryption. Symmetric key otherwise known as secret key or shared key or private key is one of the encryption methods\(^5\) which use one key for encryption as they do for decryption process. Asymmetric cryptography\(^9\)\(^10\)\(^11\) uses different encryption keys for encryption and decryption. Traditional ciphers methods are less efficient in securing real-time multimedia data encryption systems and exhibit some drawbacks and weakness in high stream data encryption.\(^12\)\(^13\) Contrariwise, the chaos-based image encryption algorithms have many advantages for the random properties of chaotic systems, such as sensitivity to initial conditions and state ergodicity.

Current research into the development of new chaotic and hyperchaotic systems is highlighting the benefits of real-time encryption and communication applications. They show that chaotic systems are good schemes for designing cryptosystems. For these prominent features, this paper introduces a new four dimensional hyperchaotic system have been explored and utilized in the design of the color image encryption algorithm. The paper is divided into five parts. In Section II, the image encryption using proposed hyperchaotic system is presented. Then in Section III, the four hyperchaotic system is introduced and its chaotic property has also observed. Simulation results and security analysis are shown in Section IV and In Section V, a conclusion will be reached.

Proposed encryption scheme

This section introduces a chaos-based image encryption algorithm. It is based on the permutation pixel position only without changing the pixel value. The initial conditions for each system allow generating the output chaotic encryption sequence. Thereafter the image encryption steps are quoted. The image decryption is done by simply reversing the process using the same key. This encryption algorithm contains five steps:

1. Step 1: Load the original image I \([M, N]\);
2. Step 2: Initializing the chaotic/hyperchaotic system;
3. Step 3: Generating the chaotic sequences at length of M*N, then starts to generate the chaotic sequences for image encryption;
4. Step 4: Calculating the new index pixel position based on key sequence;
5. Step 5: Permute the pixel positions on the original image then get the encrypted one.

The proposed hyperchaotic system

The hyperchaotic system consists of an encryption chaotic sequence generator. In the part of the chaotic sequence generator, the system is used to generate the output chaotic sequence. The function in Eqn. (1) represent the four dimensional chaotic system.

New four dimensional hyperchaotic system

The four hyperchaotic system is described by the following equations and his attractor is represented in Figure1.
Simulation results

The encryption and decryption algorithms are implemented in MATLAB. The simulation results demonstrate that the proposed algorithm shows good performances in image encryption. For the performance evaluation of the proposed method, we used “Moon.jpg” image of size 338x450. The initial conditions for 4D hyperchaotic system is \( x_0^{4D} = [0.1; 0.02; 0.2; 0.06] \). The encrypted image in Figure 3A is completely different from the original image and cannot be recognized. The decrypted image in Figure 3B, getting from the decryption process, is the same as the original image in Figure 3C. This shows the success of the encryption and decryption algorithm for color image.

Statistical analysis

In order to resist attacks, the encrypted images should possess certain random properties. To prove the robustness of the proposed algorithm, a statistical analysis has been performed by calculating the histograms, the correlation coefficients, PSNR, NPCR and UACI. For the image that has been tested, it has been determined that her quality is good.

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. The experimental results of the original image and its corresponding encrypted image and their histograms are shown in Figure 4. It is clear that the histogram of the encrypted image is significantly different from the respective histograms of the original image.

The experimental results of the original image and its corresponding encrypted image and their histograms are shown in Figure 4. It is clear that the histogram of the encrypted image is significantly different from the respective histograms of the original image.

The results of the correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the original image and its encrypted image show that there is very good correlation between adjacent pixels in the image data, while there is only a small correlation between adjacent pixels in the encrypted image.

PSNR analysis

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

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

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

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

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:

$PSNR(Original/Decrypted) = \infty$

$PSNR(Original/DecryptedNoise) = \infty$

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 shown in Table 2. The result is much closed with the correlation coefficient.

Table 2 PSNR coefficient for “ALICE” color image

<table>
<thead>
<tr>
<th>PSNR(:,:,1)</th>
<th>PSNR(:,:,2)</th>
<th>PSNR(:,:,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo/Encrypted</td>
<td>11.3249</td>
<td>14.3677</td>
</tr>
<tr>
<td>Photo/Decrypted</td>
<td>Inf</td>
<td>Inf</td>
</tr>
<tr>
<td>Photo/Decrypted Noise</td>
<td>34.3291</td>
<td>Inf</td>
</tr>
</tbody>
</table>

i. The correlation coefficients for the original and decrypted image are identical. The value of PSNR (Original/Decrypted) means that the decrypted image is identical to original image.

ii. The correlation coefficients 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.

**NPCR and UACI analysis**

NPCR stands for the number of pixels change rate while one pixel of plain image changed. UACI stands for the average intensity of differences between the plain image and ciphered image. The NPCR and UACI measure tested the different range between two images. Calculate using the following formulas:

\[
NPCR_{R,G,B} = \frac{\sum_{i,j} D_{R,G,B}(i,j) \times 100\%}{W \times H}
\]

\[
UACI_{R,G,B} = \frac{1}{W \times H} \left[ \sum_{i,j} |C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)| \right]
\]

Where \( W, H \) are the width and height of the image, \( C_{R,G,B}(i,j) \) and \( C'_{R,G,B}(i,j) \) are the two encrypted images before and after one pixel of the plain image is changed respectively. \( D_{R,G,B}(i,j) \) is determined by the following rule: when \( C_{R,G,B}(i,j) = C'_{R,G,B}(i,j) \), then \( D_{R,G,B}(i,j) = 0 \); otherwise it is 1. The results are shown in Table 3. We can find that the NPCR is over 99% and the UACI is over 30%; the results show that the algorithm was very sensitive to tiny changes in the plain image, even if there is only one bit difference between the plain images, the decrypted image will be different completely. Thus, the algorithm is robust against differential attack.

<table>
<thead>
<tr>
<th>Table 3 NPCR and UACI result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPCR %</td>
</tr>
<tr>
<td>Image</td>
</tr>
</tbody>
</table>

**Error decrypted image**

To recover image, we apply the inverse of the algorithm proposed in section 2. For a good decryption, we used the same key as the encryption. The result is already shown in section 4.1. But in the practical case we find situation where the encrypted image will be attacked. In this part of work we present two cases.

**Cannel attack: white noise**

In practice, the transmission of information is done through the Channel with noise. So to analysis the performance of our algorithm and our chaotic systems, we have added a white noise to the encrypted image, then we have decrypted it with the same key in the encryption. The results are shown in Figure 5. We observe that the decrypted image is the same as the original one. That is confirmed by the PSNR value equal to Inf.

**Unauthorized access: error in initial conditions**

Another case is when an unauthorized person tries to decrypt the image with another key. In our key, we have chosen a decryption key with an error of 10\(^{-6}\). The results show that the decrypted images are totally different of the original image as shown in Figure 6. These results confirm performance of our algorithm using hyperchaotic system sensitive to initial conditions.

**Table 4 time encryption and decryption (color image)**

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>4D</td>
<td>0.21136</td>
</tr>
<tr>
<td></td>
<td>0.23161</td>
</tr>
</tbody>
</table>

**Conclusion**

In this paper, an algorithm for color image encryption was designed utilizing the proposed new four hyperchaotic system. The simulation results showed that this algorithm was capable of achieving in terms of encryption and decryption process. The proposed scheme provides sensitivity to very small change in the initial conditions (10\(^{-6}\)).
analyzed the basic dynamic characteristics of the proposed system. The chaotic sequence of the proposed system is generated based on the initial conditions. Then we proposed image encryption based on permutation. The security analysis, including histogram, Correlation of two adjacent pixels, PSNR, NPCR and UACI shows that the proposed system has good security and complexity. It is observed that image encryption using this technique given good results.

Acknowledgments

None.

Conflict of interest

Author declares there is no conflict of interest.

References