ANEW ARCHITECTURE OF KEY GENERATION USING DWT FOR IMAGE ENCRYPTION WITH THREE LEVELS ARNOLD TRANSFORM PERMUTATION

Qutaiba K. Abed 1, Waleed A. Mahmoud Al-Jawher 2

1 Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq.
2 College of Engineering, Uruk University, Baghdad, Iraq.

phd202130682@iips.icci.edu.iq

Abstract The security of image transmission is an important issue in digital communication. As well as it is necessary to preserve and protect important information for several applications like military, medical and other services related to high confidentiality over the Internet or other unprotected networks. In this paper a proposed encryption scheme was introduced that using Lorenz system with a circular convolution and discreet cosine transform (DCT). The diffusion process was achieved using three levels of Arnold transform permutation: - namely, block level, inside each block and pixel level. The image was divided into blocks of sizes 8x8 pixels and shuffle by applying Fisher-Yates permutation image pixels. The DCT was applied to each block and multiplied by the H kernel matrix to achieve the circular convolution. Next the logistic map is used for diffusion to get the cipher image. A new key generation method is applied in order to produce the key values for generating the chaos numbers sequence. Finally applying the discreet wavelet transform (DWT) to the image will produced four quarters (LL, LH, HL and HH). The cosine of each pixel in the LL and HH quarters were computed. The sine of each pixel in the LH and HL quarters were also computed in order to generate the keys for the chaos sequence. By using this way of keys generation in every image, the differential attack possibility will be negligible.

Keywords: Convolution diffusion, Fisher Yate permutation, Sine and Cosine function, Arnold transform, permutation for Pixel level, DCT and DWT

1. INTRODUCTION

Nowadays, image security is becoming increasingly important as more and more confidential images are transmitted over public Internet or stored in a third party. In this respect, various image cryptosystems have been suggested because encryption is recognized as an effective and direct technique to keep private information safe. With the rapid development of digital image processing technology, people pay more and more attention to improve the security of information [1]. Chaotic systems have many features suitable for cryptography, including pseudo randomness, initial value sensitivity, parameter sensitivity, periodicity, and unpredictability. Therefore, in recent years, the use of chaotic systems to study encryption algorithms has become one of the hot spots in the field of computer science and cryptography [2].

Chaotic system has many excellent intrinsic properties, such as ergodicity, aperiodicity, high sensitivity to initial conditions and control parameters and random-like behaviors. Therefore, researchers have proposed many image encryption algorithms based on chaotic systems [2–21]. The typical ciphers based on chaotic map can be partitioned into two stages, permutation and diffusion [3].

From several research works, it has been inferred that performing permutation only within a sub block alone cannot give acceptable security. Chaotic sequence provides better randomness to improve security. N time’s permutation and M times’ diffusion will decrease the potential in cryptanalysis. Both permutation and diffusion are important processes in increasing the security of the cipher. With these facts, the following steps have been taken for image security which are cited as contributions to this work, an actual image-related key generation technique is used to reduce the risk of differential attack [4].

In [5], an image encryption based on one-time keys is proposed. In [6], a novel chaotic block image encryption algorithm based on dynamic random growth technique is proposed. Although the schemes adopt some measures in the encryption process to improve security, but they cannot resist chosen plaintext attack and chosen-ciphertext attack totally. To avoid attackers crack cryptosystems by using the order from top to bottom and from left to right, Wang et al. propose dynamical pixel order for diffusion and sub-images.
division method [7]. Belazi et al. [8] proposed a new chaos-based partial image encryption scheme which encrypts only the requisite parts of the sensitive information in frequency domain of Lifting-Wavelet Transform (LWT) based on hybrid of chaotic maps and a new S-box. Liu et al. [9] proposed a fast image encryption algorithm. In this algorithm, the confusion and diffusion processes are combined for one stage. Wang et al. [10] proposed a novel hybrid color image encryption algorithm using two complex chaotic systems to enhance the security and enlarge key space of color image encryption. In [11–16], a variety of image encryption algorithms using bit-level permutation have been proposed due to the advantages of bit-level permutations, which can change the position and value of a pixel simultaneously. In [6], a new bit-level encryption algorithm based on the spatiotemporal non-adjacent coupled map lattices which makes it possible for any bit in pixels to break the limit of its bitplane without extra space in permutation process.

Take the DWT to the input image and apply computation to get the initial keys for Lorenz chaos and logistic map[31–40]. Three layered, pixel level of Arnold transform and Fisher-Yates scrambling method is employed to randomize the pixel values. A circular convolution is performed to improve security, multiplication operation is applied in frequency domain to get the result of the circular convolution, and logistic map is used to apply diffusion to get the final cipher image.

2. CHAOTIC MAPS

Chaotic maps are non-linear dynamical systems that behave chaotically in a manner under certain parameters and initial values. The randomness in the chaos sequence is needed for image encryption to randomize the image by permutation/diffusion. It mainly secures the image from the possibility of pattern attacks [18, 4]. Chen chaotic system can be described by

\[
\begin{align*}
\frac{dx}{dt} &= \sigma (y - x) , \\
\frac{dy}{dt} &= x (\rho - z) - y \\
\frac{dz}{dt} &= x \cdot y - \beta \cdot z 
\end{align*}
\]

Where \(\sigma\), \(\rho\) and \(\beta\) are control parameters, when \(\sigma = 35\), \(\rho = 3\), \(\beta = 28\), the system represents chaotic characteristics. The Logistic chaotic map is a degree 2 polynomial and exhibits chaotic behavior under certain parametric values. The equation for the map sequence generator is expressed in Equation (2)

\[
K_{n+1} = r \cdot K_n \cdot (1 - K_n)
\]

Where \(K_n\) is the value between 0 and 1. \(r\) is the parameter within the interval [0,4].

![Image Scrambling Diagram](image.png)
3. THE PROPOSED ENCRYPTION SYSTEM

In this encryption method the Discreet Wavelet Transform (DWT) is first calculated for the input natural image, where as a result of applying the Discreet Wavelet Transform (DWT), we will obtain four divisions of the image, which are LL, LH, HL and HH, and then operations are applied to these four parts. Sine for LL, HH and Cos for LH, HL are calculated, in order to compute the calculation to obtain the five keys K1, K2, K3, K4, K5 that can use as keys for Lorenz chaotic and logistic map. Then the same as the original natural image have been divided into 8x8 blocks. Three levels of Arnold transform permutation have been performed in order to ensure security. In the first level, Arnold transform permutation is applied inside each block. In the second level, Arnold transform permutation is performed on all blocks in order to scramble the 8x8 blocks into another places. Then, the blocks have been masked into a single image and on the whole Arnold transform permutation is applied in the third level. Each Level is permuted by Arnold transform manner for n times. Fisher-Yates is performed for all pixels to scramble all image. Divide the image to blocks each 8*8 pixels and the apply DCT to each block after that convolute the each block with the H kernel matrix then apply IDCT to get the result. Applying diffusion to get the final cipher image. This can be describe the following procedure.

1- Input a natural image size (256*256)
2- Obtain the DWT which result into four quarters namely; LL, LH, HL and HH.
3- calculate the sine of each pixel in LH and HL quarters
4- calculate the cosine of each pixel in LL and HH quarters
5- select 64 octal values from the result of step 4 above using the following set of equations

\[
\begin{align*}
    n1 &= f_1 + f_5 + f_9 + \ldots + f_{61} \\
    n2 &= f_2 + f_6 + f_{10} + \ldots + f_{62} \\
    n3 &= f_3 + f_7 + f_{11} + \ldots + f_{63} \\
    n4 &= f_4 + f_8 + f_{12} + \ldots + f_{64} \\
    n5 &= f_1 + f_3 + f_5 + \ldots + f_{63} \\
    n6 &= f_2 + f_4 + f_6 + \ldots + f_{64} 
\end{align*}
\]

Where fi represent the value of the pixel from the processed image

6- Calculate the following parameters

\[
\begin{align*}
    W &= ((n1+n2)/256) + (n5/n3) \\
    X &= ((n3+n4)/256) + (n6/n2) \\
    Y &= ((n1+n3)/256) + (n5/n4) \\
    Z &= ((n2+n3)/256) + (n6/n1) 
\end{align*}
\]

7- Calculate the five initial keys necessary as initial keys necessary for Lorenz chaos and logistic map generation

\[
\begin{align*}
    K1 &= \text{mod} (W+X, 256)/256 \\
    K2 &= \text{mod} (Y+Z, 256)/256 \\
    K3 &= \text{mod} (W+X+Y, 256)/256 \\
    K4 &= \text{mod} (X+Y+Z, 256)/256 \\
    K5 &= \text{mod}(X+Y, 3) 
\end{align*}
\]

Where the K1,K2,K3,K4 and K5 represent the keys for the Lorenz chaos

Figure 2: depict the process of the keys generation
8- Divide the image into 8*8 blocks
9- Applying three levels of permutation using Arnold transform as following:
   a- applying Arnold transform on the wavelet coefficient within each block
   b- Applying Arnold transform on the index of the blocks.
   c- Applying Arnold transform on an image wavelet coefficient of 256*256 dimension.

![Diagram showing three level Arnold Transform scrambling]

Figure 3: Show the three level Arnold Transform scrambling

10- applying fisher yates permutation for pixel shuffling randomly using the following procedure:
   a- In each position starting from the end of the vector
   b- The position index is taken in every loop
   c- The map sequence value is taken as a random value and change with end position to get the new sequence.
   d- Shift to the next position and new value is taken as another position.
   e- Repeat the process to all position to get the scrambled image

![Diagram showing Fisher Yates permutation]

Figure 4: Depicts the Fisher Yates permutation

11- Apply the convolution on the H kernel matrix using the following steps:
   a- H kernel matrix size (8*8) generated by Lorenz chaotic
   b- Divide the input image into many blocks each size 8*8 bytes
   c- Apply DCT to each block
   d- Multiply each block with the H kernel matrix size 8*8 to get the new block
   e- apply IDCT for the blocks
   f- Repeat this process for all blocks in order to get the cipher image

12- Quantify the result to make it between [0-255].
13- Diffuse the result with the logistic map number Cipgher=im xor logistic_map (i, j)

Figure 5: Convolution with the H kernel matrix

Figure 6: The overall flowchart of the proposed encryption system.
The Decryption Method

The decryption way of the system can be performed by reversing the order of the encryption process. Inverse the diffusion, then Inverse circular convolution is applied. After that, inverse Fisher-Yates permutation is applied. Then Inverse Arnold transform permutation is performed to get the decrypted image. Figure 7 shows permuted image, diffused image and decrypted image.

![Figure 7: shows permuted image, diffused image and decrypted image.](image)

4. The Results of the proposed system

This part discusses the results obtained from the simulation of the proposed encryption system. As shown in Figure 7, the effects of encryption and decryption are visually displayed. Five 256x256 greyscale Lena, Baboon, peppers, Barbara and Gold-hill are used as original images. It is all the plain images are encrypted into cipher images. The cipher images are noise-like images without carrying any visual information. Besides, the decrypted images look much the same visually as their original counterparts.

4.1 The Analysis of the Key Length

The security level of the cryptosystem mainly depends on the key. The key length of the system must be as large as to prevent an exhaustive attack. In the proposed algorithm, five initial keys are needed to generate chaotic sequences. $10^{-15}$ is the precision of these numbers then a total of $10^{90}$ which is greater than $2^{100}$. Hence brute force attack cannot be attempted.

4.2 Analyzing the Correlation Coefficient

The relationship between the nearby pixel values is one of the ways to get the information from the encrypted image. In normal images, the correlation coefficient value is close to 1, whereas in encrypted images, the correlation coefficient value is close to 0. If it is nearer 0, then the possibility of getting any information through the correlation among pixels is very low. The Correlation Coefficient (CC) is measured using Equation (3)

$$CC = \frac{D1(x-D1(x))(y-D1(y))}{\sqrt{D1(x)D1(y)}}$$

Where D1(x) and U1(y) are the gray level expectation and variance, respectively. Figure (3) illustrates the close statistical relationship between the pixels in the original image in all directions, where all pixels are concentrated in one area. The pixels are dispersed throughout the region. Table 1 shows the CC values of cipher images. Table 2 compares the CC value of the proposed solution with existing solutions. H1, V1 and D1 in Tables 1 and 2 denote the horizontal, vertical and diagonal correlation values, respectively. Obtained results of CC outperform the existing solutions.
Table 1 shows the CC values of cipher images

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Vertical</th>
<th>Horizontal</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>0.9850</td>
<td>0.0071</td>
<td>0.9719</td>
</tr>
<tr>
<td>Baboon</td>
<td>0.7586</td>
<td>0.0034</td>
<td>0.8665</td>
</tr>
<tr>
<td>peppers</td>
<td>0.9783</td>
<td>-0.0006</td>
<td>0.9810</td>
</tr>
<tr>
<td>Barbara</td>
<td>0.9619</td>
<td>-0.0001</td>
<td>0.9415</td>
</tr>
<tr>
<td>Gold-hill</td>
<td>0.9743</td>
<td>-0.0006</td>
<td>0.9710</td>
</tr>
</tbody>
</table>

Table 2: compares the CC value of the proposed solution with existing solutions

<table>
<thead>
<tr>
<th>Direction</th>
<th>Vertical</th>
<th>Horizontal</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref[19]</td>
<td>-0.0296</td>
<td>-0.0050</td>
<td>-0.0230</td>
</tr>
<tr>
<td>Ref[20]</td>
<td>-0.0299</td>
<td>-0.0121</td>
<td>-0.0477</td>
</tr>
<tr>
<td>Ref[21]</td>
<td>0.0016</td>
<td>-0.0088</td>
<td>-0.0254</td>
</tr>
<tr>
<td>proposed</td>
<td>0.0071</td>
<td>-0.0001</td>
<td>0.0056</td>
</tr>
</tbody>
</table>

4.3 The Pixels Distribution

Histogram analysis is one of the most crucial statistical tests for evaluating the resistance of encryption algorithms to statistical analysis attacks. Graphically describing the distribution of pixel density, the histogram provides a comprehensive description of the image's content. Consequently, the normal image histogram and the encrypted image histogram must be fundamentally distinct, with the normal image histogram containing multiple peaks and vertices and the encrypted image histogram being flat, which helps to conceal the pixel density distribution information from attackers [22-25]. Figure 9 depicts the histogram of the normal and encrypted images generated by the proposed method, which demonstrated an effective outcome.
4.4 Local Entropy

Local entropy values are calculated to analyze the strength of the diffusion with the blocks of the encrypted image. Information entropy can be used as an indication of randomness for the plain and scrambling images. Its value should be larger for scrambled images. Ideally, it should be equal to 8 for every channel of an RGB color image [26]. A signal’s information entropy can be calculated as in equation (4).

\[
\text{entropy} = -\sum_{m=0}^{2N-1} q(m)\log_2 q(m) \tag{4}
\]
The degree of irregularity is measured using PSNR and MSE values. PSNR value should be as low as possible to get the encryption to be effective. Similarly, the MSE value should be as high as possible. The PSNR and MSE are calculated using Equations (5) and (6),

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}}$$

$$\text{MSE} = \frac{1}{K \times L} \sum_{i=1}^{K} \sum_{j=1}^{L} (p(i,j) - c(i,j))^2$$

Where K, L is the size of original image, p(i, j) is the original image, and c(i, j) is the encrypted image. The higher value of MSE represents better encryption quality. This MSE analysis is a useful test for a plain image and encrypted image with pixel values in the range of [0–255]. The PSNR (expressed in logarithmic scale and decibels) determines the ratio between the maximum possible power of a signal and the power of distorting noise that affects the quality of its representation.

The Mean Structural Similarity Index (MSSIM) indicates the degree of similarity between two images, and it is closer to 1 means the more similar the images are. MSSIM can be calculated by

$$\text{SSIM}(P, D) = \frac{2\mu_p\mu_d + c_1}{\mu_p^2 + \mu_d^2 + c_1} \frac{2\sigma_p\sigma_d + c_2}{\sigma_p^2 + \sigma_d^2 + c_2} \frac{\sigma_{pd} + c_3}{\sigma_{pd} + c_3}$$

$$\text{MSSIM}(P, D) = \frac{1}{W} \sum_{i=1}^{W} \text{SSIM}(P_i, D_i)$$

where W = 64, P and D are sequences of the original and decrypted images. $\mu_p$ and $\mu_d$ are the mean values of P and D, $\sigma_p$ and $\sigma_d$ are the variances of P and D, $\sigma_{pd}$ is the covariance between P and D. Additionally, $c_1$, $c_2$, $c_3$ are three constants $c_1 = (k_1*\mu)^2$, $c_2 = (k_2*\mu)^2$, $c_3 = \mu/2$, $\mu = 255$, $k_1 = 0.01$ and $k_2 = 0.03$.

Table 3: Entropy information examination results for five test images using the proposed system.

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>7.9974</td>
</tr>
<tr>
<td>Baboon</td>
<td>7.9971</td>
</tr>
<tr>
<td>peppers.png</td>
<td>7.9976</td>
</tr>
<tr>
<td>Barbara</td>
<td>7.9974</td>
</tr>
<tr>
<td>Gold-hill</td>
<td>7.9975</td>
</tr>
</tbody>
</table>

Table 4: Comparing the evaluation results of the proposed chaotic map to those of other method

<table>
<thead>
<tr>
<th>Image</th>
<th>Lena</th>
<th>Peppers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref[27]</td>
<td>7.9973</td>
<td>7.9975</td>
</tr>
<tr>
<td>Ref[28]</td>
<td>7.9972</td>
<td>7.9974</td>
</tr>
<tr>
<td>Ref[29]</td>
<td>7.9976</td>
<td>7.9973</td>
</tr>
<tr>
<td>Ref[30]</td>
<td>7.9993593</td>
<td>7.9994499</td>
</tr>
<tr>
<td>Proposed</td>
<td>7.9974</td>
<td>7.9976</td>
</tr>
</tbody>
</table>

4.5 Quality Metrics Analysis (PSNR, MSE and MSSIM)

4.6 Noise attack analysis

Images are susceptible to various kinds of noise pollution during transmission. “Lena” and “Pepper” were used to test the resistance of this scheme to Salt and Pepper Noise (SPN) and Speckle Noise (SN) attacks. The decrypted images after adding SPN with the intensity of 0.00001, 0.00003, 0.0005 and 0.0007, respectively, Table 10 shows the corresponding PSNR values for these decrypted images. Both images had a fine PSNR values when exposed to SPN from 0.0001 to 0.00007. It means that our scheme has strong defense ability against SPN. On the other hand, the visual effect of decrypted

Table 5: Entropy information examination results for five test images using the proposed system.

<table>
<thead>
<tr>
<th>Image</th>
<th>PSNR</th>
<th>MSE</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>45.9317</td>
<td>7772.05</td>
<td>0.9915</td>
</tr>
<tr>
<td>Baboon</td>
<td>25.4270</td>
<td>6867.86</td>
<td>0.9707</td>
</tr>
<tr>
<td>peppers</td>
<td>40.2647</td>
<td>9723.7</td>
<td>0.9930</td>
</tr>
<tr>
<td>Barbara</td>
<td>31.3811</td>
<td>10264.66</td>
<td>0.9917</td>
</tr>
<tr>
<td>Gold-hill</td>
<td>33.0163</td>
<td>9280.47</td>
<td>0.9935</td>
</tr>
</tbody>
</table>
images is distinctly impacted when attacked under SN. But under SN attacks of limited intensity, the main information can be recognized from decrypted images. Therefore, it can be concluded from the experimental results that this algorithm can resist noise attacks.

Table 6 shows the PSNR values

<table>
<thead>
<tr>
<th></th>
<th>intensity</th>
<th>Lena</th>
<th>Baboon</th>
<th>Lena</th>
<th>Baboon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salt and pepper</td>
<td>0.00001</td>
<td>0.00003</td>
<td>0.00005</td>
<td>0.00007</td>
<td></td>
</tr>
<tr>
<td>Lena</td>
<td>45.9317</td>
<td>45.9317</td>
<td>26.9207</td>
<td>28.6046</td>
<td></td>
</tr>
<tr>
<td>Baboon</td>
<td>24.0800</td>
<td>40.7771</td>
<td>28.8744</td>
<td>30.5872</td>
<td></td>
</tr>
<tr>
<td>Speckle</td>
<td>0.00001</td>
<td>0.00003</td>
<td>0.00005</td>
<td>0.00007</td>
<td></td>
</tr>
<tr>
<td>Lena</td>
<td>27.3732</td>
<td>28.5419</td>
<td>28.2337</td>
<td>27.0075</td>
<td></td>
</tr>
</tbody>
</table>

5. CONCLUSION

An encryption scheme to protect the image files has been proposed. The versatility of the proposed scheme, the Algorithm has been tested with standard analyses and tests such as Correlation coefficient, Histogram analysis, PSNR and MSE. The results obtained from the analysis of the cipher image are satisfactory and outperform when compared with existing encryption schemes. Fisher-Yates used for permutation in order to add further security. In this proposed system, three-layer permutation is performed to enhance security. Circular convolution layer are used for additional security, which is employed in substitution. And the last process is diffusion with keys to get the last encrypted image. Moreover, the used security measurements and computer simulation confirmed that the system are able to provide better protection against statistical, differential, and brute force attacks, where the algorithm based on circular convolution, Lorenz and logistic map Secret Keys has strong encryption procedures and high computational speed, and can overcome common weaknesses found in encryption algorithms based on other chaotic systems

REFERENCES


