New Image Encryption Based on Pixel Mixing and Generating Chaos System

Mohaimen Hassan  
*Computer Science Department, University of Technology, Baghdad, Iraq, cs.19.61@grad.uotechnology.edu.iq*

Alaa Kadhim  
*Computer Science Department, University of Technology, Baghdad, Iraq, 110030@uotechnology.edu.iq*

Follow this and additional works at: https://qjps.researchcommons.org/home

Part of the Computer Sciences Commons

**Recommended Citation**  
DOI: 10.29350/qjps.2020.25.4.1182  
Available at: https://qjps.researchcommons.org/home/vol25/iss4/12

This Article is brought to you for free and open access by Al-Qadisiyah Journal of Pure Science. It has been accepted for inclusion in Al-Qadisiyah Journal of Pure Science by an authorized editor of Al-Qadisiyah Journal of Pure Science. For more information, please contact bassam.alfarhani@qu.edu.iq.
New Image Encryption Based on Pixel Mixing and Generating Chaos System

Authors Names
a. Mohaimen Hassan
b. Alaa Kadhim

ABSTRACT
This paper presents new encryption by utilizing the image dispersion principle, depending on the Lorenz chaotic Map, the chaos theory is unpredictability and vulnerable initial states as one of the dynamic cryptography methods as suitable for using cryptographic applications, to disengage the color of pixels (Red, Green, Blue). The encryption process is divided into three basic steps. The first step is the process of mixing pixels for each color channel vertically and horizontally. The second step is to split the image into four regions for each color channel where the color pixels are mixed for each region (horizontal, vertical, main diameter, and secondary diameter) finally was used the XOR process. Because the three-channels (R, G, B) encryption process is simultaneous, the process takes only Milliseconds to encryption and decryption images. The experiments demonstrate that the information security capabilities will be both safe more efficient, the result of our analysis of picture quality evaluation, differential attacks number of changing pixel rate (NPSR) and unified averaged changed intensity (UACI), Pixels correlation shows the quality and strength of encryption processing, Entropy show good results.

1. Introduction
The security of information is an enduring topic. In ancient times, when valuable text content was spread over a long period to other individuals, it became a complicated and necessary task to avoid a leak of original text information. Many steganographic and encryption approaches have been suggested to deal with this problem. However, the visual image, a media file, is increasingly used, stored, and interacted with the advancement of new technologies, For eg, medical image, grayscale, color, binary image, etc. Hence it is an important and urgent task to secure this sort of information [5, 14]. Chaos structures provide several features for cryptographing, including pseudo-randomness [13], flexibility to the initial value, responsiveness to parameters, ergodicity, and unpredictability [10]. Encryption algorithms that incorporate the properties of chaos processes have thus been one of the highlights in informatics and cryptography over the last few years. Encryption applications like DNA [21] and hash function [3] also can using for encryption images. In addition, the system of space-time chaos has better properties than those of low-dimensional chaos, to protect digital images, researchers have developed a number of techniques, such as data hiding [31], watermarking [15], and encryption [18,31]. And protracted with multiple images [29], existing chaotic maps [2] can be divided into two categories: one-dimensional (1D) chaotic maps [4,25] and multi-dimensional (MD) chaotic maps [27,2,4]. 1D chaotic maps normally include one variable and a number of parameters. For instance, the Logistic, Sine, and Tent maps, and can combine multiple chaotic maps as hybrid chaotic maps [33,16,17].

According to Mohamed et al. [12] proposed new confusion and diffusion method depending on skew tenet map, he separates the plain image in sectors each sized 1×256 pixel and encrypted the MSE and PSNR show good result. Finally, according to Priya et al. [26] suggested a new way for image encryption she makes a new chaotic
map by enhanced logistic map and scrambled and zigzagged RGB image (255×255x3) by rotated anti-clockwise 90 degrees PSNR and UACI has been good results.

Here, in this paper shows how to create a new proposal in the image encryption process, and this proposal distracting pixels after separating the image into three channels and rotated each channel, rotated operation based on the sequence of three-dimensional Lorenz map outcome, this proposed added a higher degree of security and more accurate encoding, in time analysis experimental of proposal recorded only take few milliseconds for image encryption and decryption, the differential attacks’ analysis NPCR and UACI show fair result, and the MSE and PSNR has shown also good results, our proposal make the parameters of the permutation and diffusion process related with cipher image so that the encryption algorithm can resist with the plain image so that the encryption algorithm can resist chosen ciphertext attack.

the rest of paper shown as following, Section 2 show the methods using contain methods that used in our algorithm, Section 3 described our algorithm for encryption image processing, Section 4 represent show experimental results of our proposed method and compare with previous works, finally discussion a conclusion remarked in Section 5.

2. Chaos Theory

Chaos theory depend on initial conditions sensitively. This means that when two copies of the system differ very small, the two systems will will differ and become very distinct after a reasonably short period of time.

• Lorenz map

The Lorenz system [24], which Edward Lorenz researched for the first time in 1960, is a dynamic system defined by the nonlinear system of ordinary equations:

\[
\begin{align*}
  x_{n+1} &= \alpha(y_n - z_n), \\
  y_{n+1} &= r x_n + x_n z_n - y_n, \\
  z_{n+1} &= x_n y_n - b z_n
\end{align*}
\]

these variables \( \alpha, r, b \) is referred to as control parameters while \( x, y, z \) is referred to as status variables, Equation (1) is describe a specified control parameters and initial values \( x_0, y_0, z_0 \) of the state variables; other methods that also apply.

3. Proposal algorithm for image Encryption

Our proposal contains and extracting the three channels from the image and rotate each channel difference directions as see illustrate in figures and algorithms.

• Encryption Method

In encryption process pike plain image, in figure 1, the work encryption technique was illustrated, every pixel in an image was divided into three channels for the purpose of increasing dispersion in the image to achieve the principle of diffusion after that each channel present (red, green, and blue), after that entered to the first step of the process. Dispersing each row or column was rotated sequentially so that the rotation of the first column was dependent on the output of the first-row rotation this process is done until the end of all rows and columns as shown in figure 3, then in the second step the image was divided equally into four regions for each channel Chromatic (left upper, right upper, right lower, left lower) so that the first region all row ware rotated the left, and the second region all the secondary diameter is rotated to the left, and the third region all the columns are rotated upward and finally the fourth part are all the main diameter is rotated towards the left as shown in figure 4. Finally, xor was done with all channels to increase the dispersion strength as shown in figure 5. Finally, the three channels are reconfigured into a color image to be the encoded image. As figure 6 shows all the steps where the original image 6.a and 6.b the step one and tow,6.c show the third step and 6.d The encoded images represent the final encryption image. The decoding process is the same mechanism, but the sequence of steps
from bottom to top show in figure 2, algorithm 1 shows the encryption system and algorithm 2 shows a decryption system.

![Encryption System Diagram](image-url)
Algorithm (1): Encryption System

Input: Plain Image.
Output: Cipher Image.

Begin

Step 1: Get image.

Step 2: Split image to three channels (R, G, B).

Step 2.1: Shift rotate row column

1. Take $X$ sequential from Lorenz chaotic 3D (each channel using different value).
2. Shift rotate left first row by take first value from Lorenz map and shift rotate.
3. Shift rotate up first column by take second value from Lorenz map and shift rotate (using the result from row shifting).
4. Do these shift processing until end image from each channel.

Step 2.2: Shift rotate left the four regains

1. Split image four areas for each channel.
2. Take $Y$ sequential from Lorenz chaotic 3D (each channel using different value).
3. First area shift rotates left row by take values from Lorenz map and shift rotate.
4. Second area shift rotates left second diagonal by take values from Lorenz map and shift rotate.
5. Third area shift rotates up columns by take values from Lorenz map and shift rotate.
6. Fourth area shift rotates left main diagonal by take values from Lorenz map and shift rotate.
7. Do these shift processing for all areas and channels until ending size.

Step 2.3: XORed image

1. Take $Z$ sequential from Lorenz chaotic 3D (each channel using different value).
2. With using XOR operation every pixel with Z map, to each channel using different Z map.

3. The cipher image is final step now the cipher image is ready.

**Step 3:** Merge all three channels (R, G, B).

**Step 4:** Get cipher image.

End

**Fig. 2:** Decryption System
Algorithm (2): Decryption System

Input: cipher Image.
Output: plain Image.

Begin

Step1: Get cipher image

Step2: Split image to three channels (R, G, B).

Step2.1: XORed image

1. Take Z matrix from Lorenz chaotic 3D (each channel using different value)
   using same initial value with using in encryption processing.

2. Using XOR operation every pixel with Z map, to each channel using
   different Z map.

Step2.2: Shift rotate left the four regains

1. Take Y sequential from Lorenz chaotic 3D (each channel using different
   value) same way that using in encryption.

2. First area shift rotates right row by take values from Lorenz map and
   shift rotate.

3. Second area shift rotates right second diagonal by take values from
   Lorenz map and shift rotate.

4. Third area shift rotates down columns by take values from Lorenz map
   and shift rotate.

5. Fourth area shift rotates right main diagonal by take values from Lorenz
   map and shift rotate.

6. Do these shift processing for all areas and channels until ending size.

7. Concatenation the four areas and send to next step.
4. Experimental results

This segment discusses the effects of the systems suggested and analyzes the encryption pictures. Confusion is an important feature of the cryptographic block chip; any picture has blocks translated into cipher blocks of the message and is thus focused on the key. Each primary change indicates the output of each cipher. The diffusion is the block cryptographic cipher; by digit of the plaintext and by hidden key digit, those ciphertext numbers can be calculated. The two models are very common and casual. Initial condition and controller parameters on Lorenz map $\alpha=10$, $r=28$, and $\beta=8/3$.

As see in figure 3 use first encryption step and figure 4 and 5 show second and third step, all steps show and how each channel processing for each step, in figure 6 show all steps of Encryption Image

<table>
<thead>
<tr>
<th>Step2.3: Shift rotate row column</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Take X sequential from Lorenz chaotic 3D (each channel using different value), same generate chaotic map way.</td>
</tr>
<tr>
<td>2. Shift rotate right last column by take last value from Lorenz map and shift rotate.</td>
</tr>
<tr>
<td>3. Shift rotate last row by take before last value from Lorenz map and shift rotate (using the result from column shifting).</td>
</tr>
<tr>
<td>4. Do these shift processing until first column and row in image from each channel.</td>
</tr>
</tbody>
</table>

**Step3:** Merge all three channels (R, G, B).

**Step4:** Get plain image.

End

![Fig. 3: Encryption Image (first step), (a) red channel, (b) green channel, (c) blue channel and (d) color image](image1)

![Fig. 4: Encryption Image (second step), (a) red channel, (b) green channel, (c) blue channel and (d) color image](image2)
In figure 6, the encryption bitmap image has size 755*755 pixels and 1.7 Mb, consuming only 5,251 seconds to encrypt and 5,357 seconds in decrypt an image, because a big difference between plain and cipher image MSE between plain image (a) and decryption image (c) equal to 5498.22 that lead to PSNR equal to 10.72858, NC equal 1 because there is no deformation in the decoded image between plain image (a) and decryption (d), and entropy between plain image (a) and cipher image (c) equal to 7.9940, NPSR and UACI are 0.99309, 0.3310 between plain image (a) and cipher image (c), other encryption and decryption result can see in figure 7, the size of a paper image is (256x256) pixel, Barbara image(512x512) pixel, Baboon image(560x560) pixel and finally monarch image(900x900) pixel.

Fig. 6: (a) first step, (b) second step, (c) third step and (d) encryption image

Fig. 7: Encryption and decryption (a) Paper, (b) Barbara, (c) Baboon and (d) Monarch
Our proposed approach used different sizes and quality images tests for evaluated the efficiency and security of a proposed system. by Picture Quality Evaluation (PQE) [23], Histogram Analysis Randomness Tests and Evaluation of Image Quality by Entropy.

4.1. Picture Quality Evaluation (PQE) Metrics

For show experimental an encoded and decoded image quality measurement, The picture quality evaluation (PQE) must be used, as shown below with our images, these metrics implemented applied our proposal, table 1 show twelve measurements in MSE should be big number because it shows differently between plain image and cipher image with all images show big numbers, the reason PSNR results show with these numbers to calculate ratio max probable signal power and noise power, AD show the difference between plain and cipher image and divided by MSE, MD show maximum error between plain and cipher image convert both images to gray image with rang (0-255), NC must be shown in all images 1 between plain image and decryption image should be big number because it shows differences between plain image and cipher image, MAE show absolute same idea MSE instead of the square difference between plain and decryption image calculate absolute, NAE show 1 if plain and decryption have no deformation but the result evaluation show less one, SNR Show all-electric signals between plain and encryption image, SIM show similar results between the original image and encoder image the same idea MSE, and EQ show encryption quality with all images show big results.

Table 1 - PQE Metrics

<table>
<thead>
<tr>
<th>name</th>
<th>MSE</th>
<th>PSNR</th>
<th>AD</th>
<th>MD</th>
<th>NC</th>
<th>MAE</th>
<th>NAE</th>
<th>SC</th>
<th>NSR</th>
<th>SIM</th>
<th>CC</th>
<th>EQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>7217.26</td>
<td>9.54708</td>
<td>-2.24890</td>
<td>238</td>
<td>1</td>
<td>33.48825</td>
<td>0.562332</td>
<td>0.89521</td>
<td>-0.49811</td>
<td>1.35E+02</td>
<td>0.004093</td>
<td>1.77E+04</td>
</tr>
<tr>
<td>Barbara</td>
<td>7369.17</td>
<td>9.45661</td>
<td>-5.99177</td>
<td>241</td>
<td>1</td>
<td>31.954</td>
<td>0.59543</td>
<td>0.851694</td>
<td>-0.06994</td>
<td>1.30E+02</td>
<td>0.01467</td>
<td>7.16E+04</td>
</tr>
<tr>
<td>Baboon</td>
<td>4944.42</td>
<td>11.18965</td>
<td>-14.8767</td>
<td>188</td>
<td>1</td>
<td>20.89631</td>
<td>0.552606</td>
<td>0.73598</td>
<td>-1.3366</td>
<td>1.16E+02</td>
<td>0.000917</td>
<td>6.94E+04</td>
</tr>
<tr>
<td>Lena</td>
<td>5148.70</td>
<td>11.01382</td>
<td>-19.4692</td>
<td>231</td>
<td>1</td>
<td>19.264423</td>
<td>0.606295</td>
<td>0.693848</td>
<td>-1.58098</td>
<td>1.12E+02</td>
<td>0.002805</td>
<td>1.74E+05</td>
</tr>
<tr>
<td>Monarch</td>
<td>4351.23</td>
<td>11.74468</td>
<td>-14.3720</td>
<td>212</td>
<td>1</td>
<td>18.997913</td>
<td>0.495405</td>
<td>0.763527</td>
<td>-1.17439</td>
<td>1.17E+02</td>
<td>-0.001486</td>
<td>1.66E+05</td>
</tr>
</tbody>
</table>

4.2. Running time of Encryption and Decryption Image

Table 2 and figure 8, shows time complexity with all images, time take few milliseconds for encryption and decryption.

Table 2 - time complexity milliseconds

<table>
<thead>
<tr>
<th>name</th>
<th>diminution</th>
<th>size</th>
<th>Encryption time</th>
<th>Decryption time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>256x256 pixel</td>
<td>201 KB</td>
<td>0.462</td>
<td>0.541</td>
</tr>
<tr>
<td>Barbara</td>
<td>512x512 pixel</td>
<td>786 KB</td>
<td>2.226</td>
<td>2.273</td>
</tr>
<tr>
<td>Baboon</td>
<td>560x560 pixel</td>
<td>941 KB</td>
<td>2.913</td>
<td>3.013</td>
</tr>
<tr>
<td>Lena</td>
<td>755x755 pixel</td>
<td>1.7 MB</td>
<td>5.251</td>
<td>5.357</td>
</tr>
<tr>
<td>Monarch</td>
<td>900x900 pixel</td>
<td>2.4 MB</td>
<td>7.725</td>
<td>7.853</td>
</tr>
</tbody>
</table>

Fig.8: Encryption and decryption time
And in table 3 show the compare encryption speed in milliseconds with other proposed system, we see our proposed is faster than others for difference image sizes.

4.3. Differential Attacks Analysis

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) [19] are two farthest popular quantities used to estimate the strength of image encryption algorithms/ciphers with respect to differential attacks, can describe in table 4.

<table>
<thead>
<tr>
<th>name</th>
<th>NPSR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>0.992</td>
<td>0.333</td>
</tr>
<tr>
<td>Barbara</td>
<td>0.996</td>
<td>0.336</td>
</tr>
<tr>
<td>Baboon</td>
<td>0.996</td>
<td>0.336</td>
</tr>
<tr>
<td>Lena</td>
<td>0.997</td>
<td>0.337</td>
</tr>
<tr>
<td>Monarch</td>
<td>0.993</td>
<td>0.332</td>
</tr>
</tbody>
</table>

With table 5 show NPSR between our proposed and [12,32,18,19] proposals, and table 6 describe UACI between our proposed and [12,32,18,19] proposals.

<table>
<thead>
<tr>
<th>Image</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lenna</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Proposed</td>
<td>0.996</td>
<td>0.996</td>
<td>0.997</td>
</tr>
<tr>
<td>Ref [27]</td>
<td>non</td>
<td>0.996</td>
<td>0.994</td>
</tr>
<tr>
<td>Ref [32]</td>
<td>non</td>
<td>0.996</td>
<td>0.996</td>
</tr>
<tr>
<td>Ref [12]</td>
<td>non</td>
<td>non</td>
<td>0.990</td>
</tr>
<tr>
<td>Ref [26]</td>
<td>0.996</td>
<td>0.996</td>
<td>0.996</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Image</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lenna</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Proposed</td>
<td>0.996</td>
<td>0.996</td>
<td>0.336</td>
</tr>
<tr>
<td>Ref [27]</td>
<td>non</td>
<td>0.996</td>
<td>0.336</td>
</tr>
<tr>
<td>Ref [32]</td>
<td>non</td>
<td>0.996</td>
<td>0.334</td>
</tr>
<tr>
<td>Ref [12]</td>
<td>non</td>
<td>non</td>
<td>0.335</td>
</tr>
<tr>
<td>Ref [26]</td>
<td>0.996</td>
<td>0.996</td>
<td>0.335</td>
</tr>
</tbody>
</table>
4.4. Uniformity Analysis of Image Pixel

The pixel strength diffusion measurements for a picture are represented in a histogram from a picture. A secure encryption system should provide identical histograms to survive statistical attacks. The histogram in Figure 9(a, b, c, d) depicts Lena, Pepper, Barbara, Baboon and Pepper's regular and encrypted pictures. We evaluated from Figure 9(a, b, c, d) that the histograms of regular images are not accurate, while the histograms of the digital images that have been encrypted are reliable. The uniformity of the pixel heights of the histograms of the encrypted image makes it hard to find an insight into the maximum information region for attackers.

Fig. 9: histogram of Lena, Pepper, Barbara, Baboon and Pepper (a) plain image, (b) histogram of plain image, (c) cipher image, (d) histogram of cipher image

4.5. Pixels Correlation Analysis

Adjacent pixels have a rather strong correlation in the images. The existence of neighboring pixels in an image will be removed by a high-security encryption algorithm. The formula for calculating the association of neighboring pixels is the correlation coefficient. The smaller the absolute value, the lower the correlation across adjacent pixels, in table 7 show calculate correlation coefficients between an original image and an encoded image and its corresponding encoded image the result for Lena image is listed in table 7.

Table 7- CC comparisons among different algorithms

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>0.009426</td>
<td>0.531</td>
<td>0.000249</td>
<td>0.005497</td>
<td>-0.00114</td>
<td>0.000329</td>
</tr>
</tbody>
</table>
4.6. Information Entropy

The entropy of information also is one of the most significant characteristics for calculating the randomness of the cipher file. The $H(s)$ entropy in a source is given by:

$$H(s) = - \sum_{i=0}^{2^n-1} p(s_i) \log_2 p(s_i)$$

where $p(s_i)$ corresponds to the probability of the $s$. Entropy would preferably be $H(s) = 8$ for a 2–1 gray cipher-8 picture displaying random knowledge, table 8.

Table 8- information entropy

<table>
<thead>
<tr>
<th>Paper</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lena</th>
<th>Monarch</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.993</td>
<td>7.994</td>
<td>7.995</td>
<td>7.997</td>
<td>7.994</td>
</tr>
</tbody>
</table>

The entropy in table 9 close to the ideal value 8. We thus assume that the algorithm suggested is strongly random.

Table 9 - information entropy for cipher image among different algorithms

|-------|--------------|----------|----------|----------|

5. Conclusion

This paper implemented a high performance and efficient image security encryption method that based on a chaotic system and shuffling scheme. It consists of three steps for dispersion principle to disengage the color points, the color point divided to three colors (red, green, and blue) and scrambled all color channel with all directions, this process depended on Lorenz chaotic map three-dimensional, first step shifting and rotate (row and column in series) each pixel in each channel, the second step split to four regions shift rotate each region with different directions, final step xored operation. The security analysis performs was sensitive with initial value speed in encryption processing, compared with some other encryption schemes the NPSR and UACI show high efficiency, also the entropy analysis, and the histograms of the encrypted image makes it hard to find an insight into the maximum information region for attackers. Because of the high efficacy of our suggested encryption method, we will explore its implementations in more methods like using high dimensional chaotic maps and using with videos.

References


