A New Image Encryption Algorithm Based on Multi Chaotic System

Azhaar Akram Abdallah*, Alaa Kadhim Farhan

Computer Sciences Department, University of Technology, Baghdad, Iraq

Received: 30/11/2020 Accepted: 6/3/2021

Abstract:

In recent years, encryption technology has been developed rapidly and many image encryption methods have been put forward. The chaos-based image encryption technique is a modern encryption system for images. To encrypt images, it uses random sequence chaos, which is an efficient way to solve the intractable problem of simple and highly protected image encryption. There are, however, some shortcomings in the technique of chaos-based image encryption, such limited accuracy issue. The approach focused on the chaotic system in this paper is to construct a dynamic IP permutation and S-Box substitution by following steps. First of all, use of a new IP table for more diffusion of all image pixels based on a 1D logistic map to build IP table. Secondly, a new S-Box based on 2D-Henon chaos was created using more confusion to replace G-channel image data. Finally, design of a modern image encryption approach. This approach uses the key process confusion and diffusion operation and depend on IP and S-Box proposals in the encryption process and several shuffling operations using the 3D- Lornez chaos theory. Theoretical research and simulation suggest that starting sensitivity value of this method is high, has high protection, and encryption speed. Moreover, it also holds the value of the neighboring RGB close to zero. The studies show that the information security capabilities would be both safer and more efficient, as a result of our image quality assessment study. Number of Differential Pixel Rate Change Attacks (PSR), Unified Average Altered Intensity (UACI), are quality and strength of encryption processing are proved by pixel correlation, Entropy to be good results.

Keywords: Image Encryption, S-Box, IP, Chaos theory, RGB Channels, Entropy, UACI

خوارزمية تشغير صور جديده بالاعتماد على نظام فوضوي متعدد

أزهار أكرم عبدلله *, علاء كاظم فرحان
قسم علوم الحاسب، الجامعة التكنولوجية، بغداد، العراق

الخلاصة

في السنوات الأخيرة، تم تطوير تقنية التشغير بسرعة وتم طرح العديد من طرق تشغير الصور. تقنية تشغير الصور السبيطة على الفوضى هي نظام تشغير حديث لتشغير الصور ، تستخدم فوضى التسلسل العشوائي، وهي طريقة فعالة لحل المشكلة المستعصية لتشغير الصور السبيطة والمحمية للغاية. ومع ذلك، هناك بعض أوجه القصور في تقنية تشغير الصور السبيطة، مثل مشكلة الدقة الحميدة. يركز الهدف المقترح في هذا البحث على نظام الفوضى لإنشاء جدول تبديل (IP) وجداول ودستام بديل (S-Box) ويمكن نوضح مكونات المقترح في خطوات، أولًا وقبل كل شيء، استخدام جدول IP الجديد ودمجها.
1-Introduction

Data and information communication has become very crucial, an essential component of today's technological existence and considered to be a significant asset of an individual or organization. If the security of data is broken[1], then the data is compromised. For harmful purposes, it is possible to use information[2]. Current advances in information technology and its successful application in our lives have led to a massive rise in IT Industry. Private data is very sensitive especially if data being transmitted online[3]. Chaotic systems have initial values for sensitivity, pseudo randomness, and non-periodicity as a type of complex nonlinear system[4] which are consistent with characteristics needed for cryptography. As a random key, a chaotic sequence can be used, which can produce same encryption effect as first time, and it cannot, in principle, be broken[5]. In the field of information security, chaotic encryption technology has thus been widely used, especially in the field of image encryption[6][7]. The technology for image scrambling (shuffling) is to enhance the robustness of the hidden carrier by rearranging the matrix of the image pixel and removing the image matrix association[8]. Thus, image scrambling is a very common technique that uses IP table to hide information[9]. This method will allow information encryption to achieve the objective of secure transmission of images[10].

A stream cipher is one type of cryptography. In this form, the change of a bit-by-bit or byte-by-byte way, stream ciphers transform data [11]. Block ciphers, on the other hand, convert data into blocks comprising a large number of bits or bytes at a time. Block ciphers are regarded as one of the most powerful data protection techniques in modern symmetric encryption[12]. Examples of modern block ciphers are the Data Encryption Standard (DES), Blowfish, the Advanced Encryption Standard (AES), RC5, etc. The precise implementation of block ciphers is simple and more general than stream ciphers in nature[13][14]. As one class of prevalent block ciphers, the SP network-based block ciphers are classified. For the transformation of data into a perplexing type, these block ciphers use two main substitution and permutation operations. A substitution procedure uses a substitution table known as a substitution box or S-box to replace a byte/block with another byte/block[15][16]. On the other hand, in some linear fashion, a permutation method shuffles the input bits or bytes[17]. In addition to one or more S-boxes, block ciphers consist of several components[18]. Unlike other modules, the S-box is the sole non-linear block cipher feature that promotes data security enhancement. A block cipher typically uses either a static S-box or one or more dynamic S-boxes[19]. For any incoming data and secret key that is used in the block cipher repeatedly. In all its rounds, a block cipher based on a static S-box employs the S-box[20]. A static S-box allows an intruder to investigate its functionality, discover its fragility, and finally discover the possibility of obtaining plain text from the corresponding cipher text[21].

In order to produce strong cryptographic S-boxes, researchers and academics have explored and examined different concepts[14]. The intensity was evaluated using some usual

\[
\text{IP}(\text{1D}) \text{ for encryption, 2D-Henon} \text{ for linear block cipher feature that promotes data security enhancement. A block cipher typically uses either a static S-box or one or more dynamic S-boxes[19]. For any incoming data and secret key that is used in the block cipher repeatedly. In all its rounds, a block cipher based on a static S-box employs the S-box[20]. A static S-box allows an intruder to investigate its functionality, discover its fragility, and finally discover the possibility of obtaining plain text from the corresponding cipher text[21].}
\]

\[
\text{In order to produce strong cryptographic S-boxes, researchers and academics have explored and examined different concepts[14]. The intensity was evaluated using some usual}
\]
parameters, such as nonlinearity, absence of fixed points, Bit Independence Criterion (BIC), linear and differential probabilities, Strict Avalanche Criterion (SAC), etc[22]. Section 2 gives a description of the theory of chaos in 1D, 2D and 3D dimensions. Section 3, explains the proposal approach for image encryption based on generated IP and S-Box addition shuffling operation, performance evaluation and comparison of encryption is performed. In Section 4, the results of the research analysis are obtained. Finally, in section 5, Conclusion.

2- Chaotic Nonlinearity Systems

The biologist Robert May discovered the logistical map in 1976. The primary concept and its purpose were to study and explain the biological populations and their development, is a simple nonlinear polynomial mapping equation. The important parameters are defined as follows:[23][24].

A-1D logistic map is represented as:

\[ f(y_i) = ry_i(1 - y_i) \]  \hspace{1cm} (1)

Where the state variable is defined by the parameter r, r is [1,4], and the control parameter is considered. Figure1 shows the step plan for the logistic map.

![Figure 1-The Logistic map phase plane](image)

B- Hénon System: A discrete-time dynamic system is often called a Hénon-Pomeau attractor/map. It is one of the most studied examples of chaotic behavior displaying dynamical systems. The Henon system takes a point \((x_n, y_n)\) in the plane and maps it to a new point \([1]. [26]\)introduced the 2D-Henon system., as described in Eq.(2),

\[ f(X_{i+1}) = (1 - ax_i^2) \]

The map is based on two parameters, a and b, which have values of a = 1.4 and b = 0.3 for the classical Hénon system [27]. The Hénon map is chaotic in terms of classical principles. The map may be chaotic, sporadic, or converge into a periodic orbit for other a and b values. From its orbit diagram, an overview of the form of action of the map at different parameter values can be obtained[23].

C- Lorenz System: The Lorenz system [28][29], The dynamic system described by the nonlinear system of ordinary equations, which Edward Lorenz studied for the first time in 1960:

\[ Xn + 1 = a(Yn-Zn) \]

\[ Yn + 1 = RXn + XZn - Yn \]  \hspace{1cm} (3)

\[ Zn + 1 = XnYn - BZn \]

These variables \(a, R, B\) are referred to as control parameters, while \(X,Y,Z\) are referred to as status variables[30]. Equation (3) defines the control parameters defined, and the initial values
x0, y0, z0 are referred to as state variables. Fined 10, 8/3 and 28, respectively, respectively. However when these parameters are modified, various dynamical behaviors may be observed. Figure 2 (a, b, c) presents a typical chaotic attractor for the initial conditions (x, y, z) = (1.2, 1.3, 1.6). In the simulations, dt is adjusted as 0.005[31][32].

![Figure 2](image_url)

**Figure 2**-The projections of attractor on the planes (a) x-y, (b) x-z and (c) y-z[32].

3. Proposed Encryption Schema

Image data have strong correlations amongst adjacent pixels. For the purpose of disturbing high-correlations between pixels, pixel positions of plain image will be shifted. With no loss of generality, the dimension of the plain image will be N × N. In this suggested approach, we focus on principles as confusion and diffusion to break the correlation between the pixels. Design new dynamic S-Box and IP to more confusion and diffusion. The encryption does in steps and explains in Figure 1:

A. **New dynamic IP Base on logistic map**

The first operation of proposed design criteria for IP-Box development is based on concepts of chaos theory and for all data, the good IP must diffuse and reorder to minimize the correlation between pixels. Depending on the one-dimensional chaotic logistic map, IP includes two-dimensional (128X128), this operation generates more security and complexity.

B. **New dynamic S-Box Base on Henon system**

The second operation of suggested design criteria for creating a good S-Box based on principles of chaos theory showed that an S-Box that meets this criterion is resistant to differential cryptanalysis and used a new design paradigm to construct a new dynamic S-Box. The latest proposal provides new insights into the architecture of excellent S-Box. Depending on two-dimensional chaotic Henon system, this operation provides greater protection and complexity. To generate new large 16-16 S-Box by using Henon chaotic map 2D, at the beginning, use initial value X0 for chaotic system and numbers produced, range of numbers (0-255), the S-Box output method by producing the values of the Henon system, all values inside the S-Box must be unique and not repeated. If the value is greater than the corresponding range, then the remainder of the section has been converted to that value, producing S-Box inverse at the same time depending on the result of S-Box. Since the "responsive dependency on initial state" with chaos theory changes the construction of S-Box and the result of dynamic S-Box inverse with every slight change in initial value.

C. **Encryption Method**

The encryption process uses many stages. At the beginning, use new Permutation Box (IP)128*128 generated from 1D logistic map is illustrated in algorithm(1). We reorder each pixel in clear image, the operation to select each block IP of same size as repeated many
times. Fetch 128*128 block cells from image and reorder these cells based on IP map and repeated this process for each block image. **Second:** The image is broken into three channels as (R,G,B), after that each channel will be processed, R channel Xored with X_i and B channel Xored with Y_i, where X and Y generated from 2D Henon system in buffer equal size image. Also the G channel has special operation base in substitutions, this (S-Box as 16*16) for each data in G channel. This S-Box as new generation depends on 2D Henon system in unique values and nonlinearity. **Third:** To increase diffusion principle in pixels, shuffling in two style (channels and pixel) is performed. In channel shifting, apply on each R,G and B based in X_i, Y_i and Z_i as secret parameters. Those generated ones depend on 3D Lornez map chaos system, because it has sensitive parameters when modified. This process is periodic for each value in channels. After that, a construct an image using three channels (R,G and B). This image also shuffled in rows, columns and master diagonals, shifted and rotated to left in each rows value with X_i shifted and rotated to bottom in each columns value with Y_i also shifted and rotated to up in each master diagonals value with Z_i. Those shifted are used from generated ones depending on 3D Lornez system chaos system. Finally get cipher unclear image. The structure of the proposed approach schema in Figure 3. Encryption and decryption processes discuses in 1, 2 algorithms.
Figure 3- Encryption Schema proposal
### Algorithm (2): Decryption Algorithm

**Input:** *Cipher Image, Secrete Keys*

**Output:** *Clear Image*

**Begin**

**Step 1:** Inverse shuffling in cipher image pixels:
1.1: Shuffling diagonals in 8-bytes based on 64-bits $Z_i$ buffer // $Z$ generated from 3D chaos.
1.2: Shuffling column in 8-bytes based on 64-bits $Y_i$ buffer // $Y$ generated from 3D chaos
1.3: Shuffling rows in 8-bytes based on 64-bits $X_i$ buffer // $X$ generated from 3D chaos

**Step 2:** Split the image to (R,G,B) channel.

**Step 3:** Inverse Shift and Rotate operation for each channels:
3.1: Shifting and Rotate 8-Byte from (R) channel based on $X_i$ buffer in 8-Byte.
3.2: Shifting and Rotate 8-Byte from (G) channel based on $Y_i$ buffer in 8-Byte.
3.3: Shifting and Rotate 8-Byte from (B) channel based on $Z_i$ buffer in 8-Byte.

**Step 4:** For each channel Do:
4.1: Xor operation between (R) channel with $X_i$ buffer // $X$ generated from 2D chaos
4.2: Substation in (G) channel based in new inverse S-Box //for each pixels
4.3: Xor operation between (B) channel with $Y_i$ buffer // $Y$ generated from 2D chaos

**Step 5:** Using R, G and B channel to construct clear image.

**Step 6:** Reorder pixels in clear image using new dynamic inverse IP.

**Step 7:** Return clear image.

**End**

### Algorithm (1): Encryption Algorithm

**Input:** *Clear Image, Secrete Keys*

**Output:** *Encrypted Image*

**Begin**

**Step 1:** Reorder pixels in clear image using new dynamic IP

**Step 2:** Split the image to (R,G,B) channel

**Step 3:** For each channel Do:
3.1: Xor operation between (R) channel with $X_i$ buffer // $X$ generated from 2D chaos
3.2: Substation in (G) channel based in new inverse S-Box //for each pixels
3.3: Xor operation between (B) channel with $Y_i$ buffer // $Y$ generated from 2D chaos

**Step 4:** Shift and Rotate operation for each channels:
4.1: Shifting and Rotate 8-Byte from (R) channel based on $X_i$ buffer in 8-Byte.
4.2: Shifting and Rotate 8-Byte from (G) channel based on $Y_i$ buffer in 8-Byte.
4.3: Shifting and Rotate 8-Byte from (B) channel based on $Z_i$ buffer in 8-Byte.

**Step 5:** Using R, G and B channel to construct image.

**Step 6:** Shuffling in Image pixels:
6.1: Shuffling rows in 8-bytes based on 64-bits $X_i$ buffer // $X$ generated from 3D chaos
6.2: Shuffling column in 8-bytes based on 64-bits $Y_i$ buffer // $Y$ generated from 3D chaos
6.3: Shuffling diagonals in 8-bytes based on 64-bits $Z_i$ buffer // $Z$ generated from 3D chaos

**Step 7:** Return cipher image

**End**
4. Experiment Result
This section presents the results of the proposed encryption image systems and discusses new S-Box standards for statistical accuracy and analysis of encryption images. Confusion is an essential part of the cryptographic block cipher; each plain-image includes blocks that are transformed into cipher-image blocks, and this builds on the 2D Henon system key for Xor operation. Any change in the key leads to various results in the cipher picture. Diffusion is the second part of the shuffling process of the cryptographic block cipher; several digits of the cipher text can affect every digit of the plain image and every digit of the hidden key.

4.1 S-Box Performance Analysis
Typical statistical criteria, including Balanced Criteria (BC), Avalanche Criteria (AC), Strict Avalanche Criteria (SAC), and inevitability, are evaluated according to our proposed approach to designing a new S-box.

1) Balanced Criteria
In table 1, balanced distribution of 0 and 1 values in the generated output sequence is key requirement that S-Box should meet. As shown, BC's previous works define the average allocation of 0 and 1 values.

2) Avalanche Criteria
In the block cipher, avalanche property is an integral criterion that shows how a small shift in input bits lead to a major change in the output (avalanche). For a suitable value of 0.5, when designing a block cipher where a simple shift in a single input bit leads to a completely different output, The ref[30] shows how measured AC is better than reference in one-bit difference per input, and Table 1 shows that average value of proposed solution is better than reference, maintaining a perfect AC value. Usually want to take into account the avalanche effect. the result from our works in AC near to 0.5 and BC near to 1, that mean good result.

<table>
<thead>
<tr>
<th>Table 1- AC, BC comparisons</th>
<th>AC</th>
<th>BC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min.</td>
<td>Ave.</td>
</tr>
<tr>
<td>Our Proposed</td>
<td>0.33</td>
<td>0.57</td>
</tr>
<tr>
<td>Ref [33]</td>
<td>0.25</td>
<td>0.5</td>
</tr>
<tr>
<td>Ref [34]</td>
<td>0.125</td>
<td>0.5</td>
</tr>
<tr>
<td>Ref [30]</td>
<td>0.25</td>
<td>0.875</td>
</tr>
</tbody>
</table>

3) Strict avalanche criteria (SAC)
The SAC Criterion [30] is a condition for each and every cryptographic S-box to state that if an input bit is changed, half of the output bits will be changed. An S-box with a value of SAC equal to 0.5. Table 2 provides SAC average values for the proposed S-box. It is clear that the average SAC value in S-Box is 0.5 in Table 2 This SAC value means that a good enjoyment of the SAC land is provided by the proposed S-box.

<table>
<thead>
<tr>
<th>Table 2-SAC</th>
<th>SAC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min.</td>
</tr>
</tbody>
</table>

331
4.2 Image Encryption Performance Analysis

In order to determine the feasibility and security of a proposed method, our suggested solution used various sizes and quality image tests. By Picture Quality Evaluation (PQE)[34], Randomness Checks of Histogram Analysis and Image Quality Evaluation by Entropy.

1) Picture Quality Evaluation (PQE) Metrics

For Picture Quality Assessment (PQE) must be used to display experimental, encoded, and decoded image quality measurement, as shown below with our pictures. These metrics were implemented in our proposal, table 3 and table 4 show several measurements. The MSE should be large value because it shows differently between plain image and cipher image. The reason why PSNR results show these numbers to measure the ratio of maximum probable signal strength and noise power, AD shows the difference between plain and cipher image and divided by MSE, MD shows maximum error between plain and cipher image to convert both images to gray image with range (0-255). NC must be shown in all images equal to 1 between plain image and decryption image, but the result assessment shows less than one. NAE shows all-electric signals between plain and encryption image. SIM shows similar results between the original image and encoder image the same MSE idea. CC the correlation is very weak between images and EQ show encryption quality with all encrypted images this big values explain good encryption.

### Table 3-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>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>53388.40</td>
<td>10.8563</td>
<td>-3.4079</td>
<td>227</td>
<td>1</td>
<td>27.962</td>
</tr>
<tr>
<td>Barbara</td>
<td>56459.10</td>
<td>10.61346</td>
<td>-6.65866</td>
<td>235</td>
<td>1</td>
<td>25.803</td>
</tr>
<tr>
<td>Baboon</td>
<td>48398.40</td>
<td>11.28248</td>
<td>-24.5814</td>
<td>194</td>
<td>1</td>
<td>15.851</td>
</tr>
<tr>
<td>Lena</td>
<td>54171.20</td>
<td>11.28248</td>
<td>-31.5643</td>
<td>230</td>
<td>1</td>
<td>14.178</td>
</tr>
<tr>
<td>Monarch</td>
<td>46123.23</td>
<td>11.4916</td>
<td>-21.7716</td>
<td>225</td>
<td>1</td>
<td>16.738</td>
</tr>
</tbody>
</table>

### Table 4 - PQE Metrics

<table>
<thead>
<tr>
<th>name</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>0.431969</td>
<td>0.9699</td>
<td>-0.144</td>
<td>1.31946</td>
<td>0.0054</td>
<td>3150.23145</td>
</tr>
<tr>
<td>Barbara</td>
<td>0.521881</td>
<td>0.8955</td>
<td>-0.482</td>
<td>1.2905</td>
<td>0.00113</td>
<td>4532.44536</td>
</tr>
<tr>
<td>Baboon</td>
<td>0.448853</td>
<td>0.6612</td>
<td>-1.799</td>
<td>1.198218</td>
<td>0.00017</td>
<td>6879.4353</td>
</tr>
<tr>
<td>Lena</td>
<td>0.626411</td>
<td>0.5988</td>
<td>-2.227</td>
<td>1.162518</td>
<td>0.00235</td>
<td>3765.8879</td>
</tr>
</tbody>
</table>
2) Encryption and Decryption Runtime Images: In Table 5 indicates time complexity for all pictures, encryption and decryption time takes a few 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</td>
<td>213 KB</td>
<td>0.715</td>
<td>0.781</td>
</tr>
<tr>
<td>Barbara</td>
<td>512x512</td>
<td>777 KB</td>
<td>2.672</td>
<td>2.735</td>
</tr>
<tr>
<td>Baboon</td>
<td>560x560</td>
<td>960 KB</td>
<td>3.473</td>
<td>3.584</td>
</tr>
<tr>
<td>Lena</td>
<td>755x755</td>
<td>1.4 MB</td>
<td>6.794</td>
<td>6.893</td>
</tr>
<tr>
<td>Monarch</td>
<td>900x900 pixel</td>
<td>2.7 MB</td>
<td>9.695</td>
<td>9.852</td>
</tr>
</tbody>
</table>

3) Differential Attacks Analysis: The Number of Modifying Pixel Rate (NPCR) and Unified Average Adjusted Intensity (UACI)[35]. Ywo of the most common quantities used to estimate the strength of image encryption algorithms/coders for differential attacks, as stated in Table 6.- Randomness Tests

<table>
<thead>
<tr>
<th>Name</th>
<th>NPSR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>0.99696</td>
<td>0.3360</td>
</tr>
<tr>
<td>Barbara</td>
<td>0.99613</td>
<td>0.3361</td>
</tr>
<tr>
<td>Baboon</td>
<td>0.99690</td>
<td>0.3392</td>
</tr>
<tr>
<td>Lena</td>
<td>0.99620</td>
<td>0.3362</td>
</tr>
<tr>
<td>Monarch</td>
<td>0.99593</td>
<td>0.3363</td>
</tr>
</tbody>
</table>

To discus NPSR, the power in our proposal can comparison with many research [36, 37, 38, 39]. in Table 7 show them, and Table 8 describe UACI between our proposed and [31, 38, 39, 40]. proposals.

<table>
<thead>
<tr>
<th>Image</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lena</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Proposed</td>
<td>0.99613</td>
<td>0.99690</td>
<td>0.99620</td>
</tr>
<tr>
<td>Ref[36]</td>
<td>non</td>
<td>0.99620</td>
<td>0.99450</td>
</tr>
<tr>
<td>Ref [37]</td>
<td>non</td>
<td>0.99610</td>
<td>0.99610</td>
</tr>
<tr>
<td>Ref [38]</td>
<td>non</td>
<td>non</td>
<td>0.99000</td>
</tr>
<tr>
<td>Ref [23]</td>
<td>0.99617</td>
<td>0.99601</td>
<td>0.99620</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Image</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lena</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Proposed</td>
<td>0.3461</td>
<td>0.3392</td>
<td>0.3362</td>
</tr>
<tr>
<td>Ref [33]</td>
<td>non</td>
<td>0.3361</td>
<td>0.3361</td>
</tr>
</tbody>
</table>
4) Uniformity Analysis of Image Pixel
The diffusion measurements of pixel intensity for an image are expressed in a picture histogram. In order to withstand statistical attacks, a safe encryption scheme should include identical histograms. The histogram in Figure 4(a, b, c, d) depicts normal and encrypted photographs of Lena, Pepper, Barbara, Baboon and Butterfly. From Figure 4(a, b, c, d), we assessed that the histograms of standard images are not accurate, while the histograms of encrypted digital images 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:

5) Information Entropy
The entropy of knowledge is also one of the most essential characteristics of the cipher file's randomness measurement. For a $2^{-1}$ gray cipher-8 image showing random information, Table 9 Entropy will ideally be $H(s) = 8$.

<table>
<thead>
<tr>
<th>Image</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lenna</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Proposed</td>
<td>0.3461</td>
<td>0.3392</td>
<td>0.3362</td>
</tr>
<tr>
<td>Ref [38]</td>
<td>non</td>
<td>0.3346</td>
<td>0.3346</td>
</tr>
<tr>
<td>Ref [39]</td>
<td>non</td>
<td>non</td>
<td>0.3355</td>
</tr>
<tr>
<td>Ref [40]</td>
<td>0.3356</td>
<td>0.3320</td>
<td>0.3358</td>
</tr>
</tbody>
</table>

TABLE 9 - ENTROPY

<table>
<thead>
<tr>
<th>Paper</th>
<th>Barbara</th>
<th>Baboon</th>
<th>Lena</th>
<th>Monarch</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.9977</td>
<td>7.9972</td>
<td>7.9982</td>
<td>7.9980</td>
<td>7.9975</td>
</tr>
</tbody>
</table>

The entropy in Table 10 close to the ideal value 8. We thus assume that the algorithm suggested is strongly random.

TABLE 10 – COMPARSION ENTROPY WITH ALGORITHM
<table>
<thead>
<tr>
<th>Image</th>
<th>Our proposed</th>
<th>Ref [41]</th>
<th>Ref [42]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>7.9980</td>
<td>7.9979</td>
<td>7.9973</td>
</tr>
</tbody>
</table>

5- Conclusion
A new proposed approach for image encryption is developed with principles of confusion and diffusion. The confusion principle in new S-Box and the diffusion applicator in New IP. These tables are created based on multi chaotic system. The chaotic system is sensitive to initial values. Where any change in any value means a change in substation and permutation operations. Shuffling operations in our approach is used to increase distance between plain and cipher image. Results in tables above can show that the proposed approach is more secured from attackers when they try to retrieve plain image.

References
[17] F. A. Kadhim and H. I. Mhaibes, "Quantum Random Bits Generator based on Phase Noise of...
Dynamic System – Multiple Chaotic Map,

A new image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced Logistic-Tent Map,

Deterministic nonperiodic flow

An efficient image encryption scheme based on S-Boxes and Fractional-Order Differential Logistic Map,

A proposal to improve RC4 algorithm based on hybrid chaotic maps,

Dynamic S-BOX based on primitive polynomial and chaos theory,

A new hyperchaotic map and its application for image encryption,

Chaos and Cryptography: A new dimension in secure communications,

Deterministic nonperiodic flow,

A new partial image encryption method for document security analysis of blowfish algorithm,

An efficient image encryption scheme based on S-Boxes and Fractional-Order Differential Logistic Map,

A new chaos based image encryption system,

Chaos as an intermittently forced linear system,

"Difference equation of Lorenz system",

"Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes",

"A new chaos-based image encryption system",

"Design of an image encryption scheme based on a multiple chaotic map",

"A new image encryption system based on Hybrid Chaotic Maps",

"A New Image Encryption Scheme Based on Hybrid Chaotic Maps",

"Design of an image encryption scheme based on a multiple chaotic map",

"Chaotic Movement with 3D Chaotic Logistic Maps to Generate Random Numbers",

"A new image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced Logistic-Tent Map",

"A partial image encryption method for document images using variance based quad tree decomposition",

"A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation,”

"A new image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced Logistic-Tent Map,”

"A new image encryption scheme based on multi-level logistic map, skew tent map and S-Box,”

"A new image encryption scheme based on Henon map, skew tent map and S-Box,”

"Design of an image encryption scheme based on a multiple chaotic map,”

"A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation,”

"A new image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced Logistic-Tent Map,”

"A new image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced Logistic-Tent Map,”

"A new image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced Logistic-Tent Map,”