 Iraqi Journal of Science, 2022, Vol. 63, No. 1, pp: 324-337
DOI: 10.24996/ijs.2022.63.1.31

ISSN: 0067-2904

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 (NPSR), 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

خوارزميه تشفير صور جديده بالاعتماد على نظام فوضوي متعدد

أزهار أكرم عبدالله *, علاء كاظم فرحان
قسم علوم الحاسوب, الجامعة التكنولوجية, بغداد, العرا ق

الخلاصة
في السنوات الأخيرة ، تم تطوير تقنية التشفير بسرعة وتم طرح العديد من طرق تشفير الصور. تقنية تشفير الصور المبنية على الفوضى هي نظام تشفير حديث لتشفير الصور ، تستخدم فوضى التسلسل العشوائي ، وهي طريقة فعالة لحل المشكلة المستعصية لتشفير الصور البسيطه والمحميه للغاية. ومع ذلك ، هناك بعض أوجه القصور في تقنية تشفير الصور القائم على الفوضى ، مثل مشكلة الدقة المحدودة. ركز النهج المقترح في هذا البحث على النظام الفوضوي لإنشاء جدول تباديل **(IP)** وجدول واستبدال ديناميكي **(S–Box)** ويمكن نوضح مكونات المقترح في خطوات، أولاً وقبل كل شيء ، استخدام جدول IP الجديد

*Email: cs.19.48@grad.uotechnology.edu.iq

لنشر كافة وحدات البكسل في الصورة بناءً على خريطة لوجستية **1D** لجدول **(IP)** الجديد ثانيًا ، تم إنشاء **(S–Box)** جديد استنادًا إلى فوضى **2D–Henon** لتقديم مزيد من الارتباك وستبدال بيانات صورة الموجوده في **G–channel** أخيرًا ، ان التركيب الداخلي للنهج المقترح ، يعتمد على عملية التشويش والانتشار الرئيسية ويعتمد على مقترحات **(IP)** و **(S–Box)** في عملية التشفير والعديد من عمليات الخلط , والتزحيف باستخدام نظرية الفوضى **3D– Lornez** . تشير الأبحاث والمحاكاة النظرية إلى أن حساسية قيمة البداية العالية لهذه الطريقة عالية وأن لها حماية عالية وسرعة تشفير. علاوة على ذلك ، فإنه يحمل أيضًا قيمة RGB المجاورة بالقرب من الصفر. تظهر الدراسات أن قدرات أمن المعلومات ستكون أكثر أمانًا وفعالية ، نتيجة لدراسة تقييم جودة الصورة ، وعدد هجمات تغيير معدل البكسل التفاضلي (NPSR) والمتوسط الموحد المتغير الكثافة (UACI) ، والجودة والقوة تم إثبات معالجة التشفير عن طريق الارتباط بالبكسل ، يظهر Entropy نتائج جيدة.

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 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:

$$f(y_i) = ry_i(1 - y_i) \quad \textbf{(1)}$$

Where the state variable is defined by the parameter r, r is [1,4], and the control parameter [25]. is considered. Figure1 shows the step plan for the logistic map.

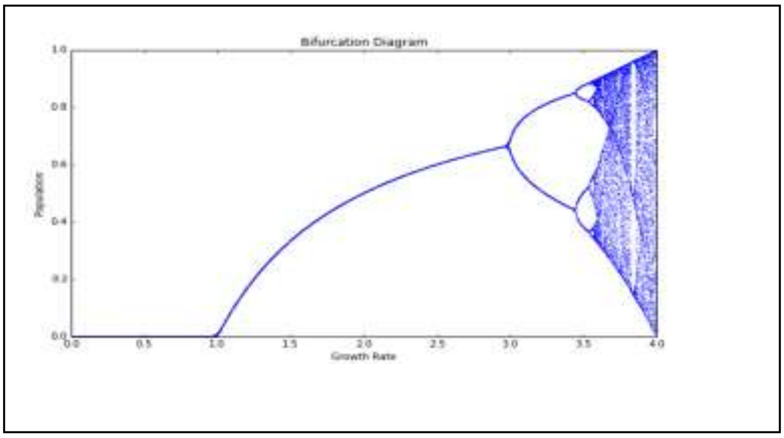

Figure 1-The Logistic map phase plane[25].

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).

$$f(X_{i+1}) = (1 - ax_{in}^2) \quad \textbf{(2)}$$

$$f(Y_{i+1}) = (bx_i)$$

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:

$$Xn + 1 = \alpha(Yn - Zn)$$

$$Yn + 1 = RXn + XZn - Yn \quad \textbf{(3)}$$

$$Zn + 1 = XnYn - BZn$$

These variables α, 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].

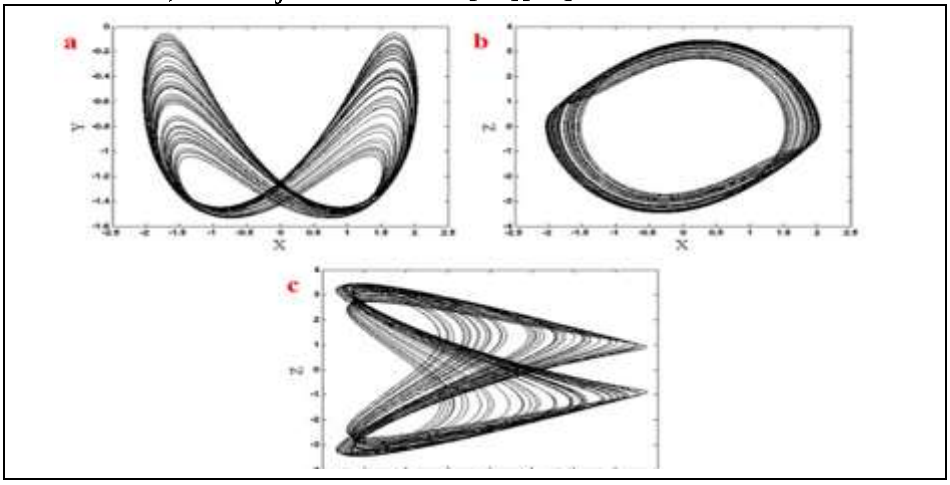

Figure 2-The projections of attractor on the planes (a) x-y, (b) x-z and (c) y-z[32].

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 $N \times N$. 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 dynmic 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 dynmic 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 Zi 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.

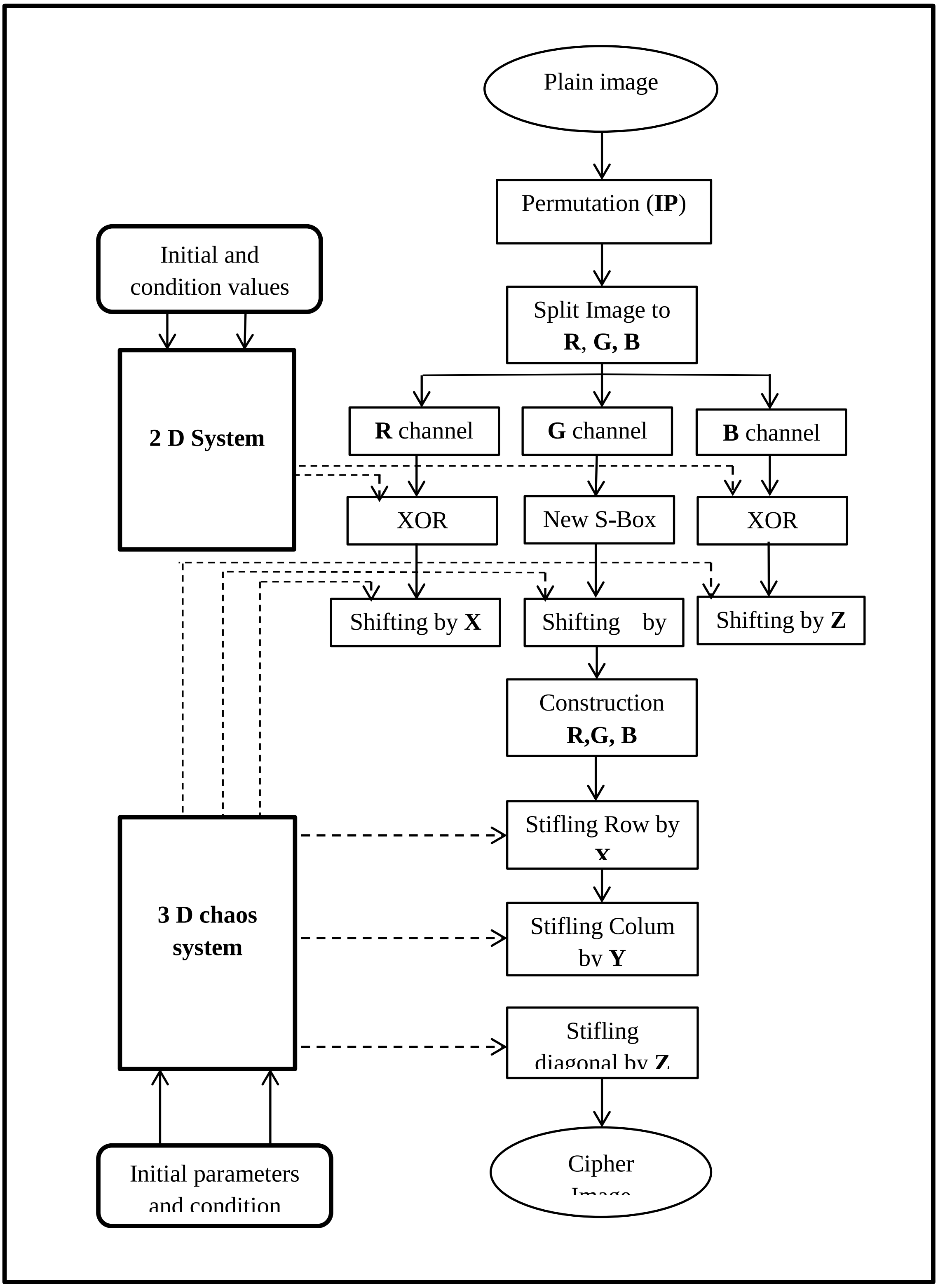

Figure 3- Encryption Schema proposal

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**:Shuffiling 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 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**:Shuffiling 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 1- AC, BC comparisons

	AC			**BC**	
	Min.	***Ave.***	***Max.***	***0's Avg***	***1's Avg***
Our Proposed	0.33	0.570	0.8175	31	32
Ref [33]	0.25	0.5	0.75	32	32
Ref [34]	0.125	0.5	0.875	29	35
Ref [30]	0.25	0.875	0.56	31	33

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 2-SAC

	SAC		
	Min.	*Ave.*	*Max.*

	SAC		
Our Proposed	0.416	0.502	0.588
Ref [30]	0.376	0.505	0.597
Ref [35]	0.421	0.503	0.593
Ref [33]	0.406	0.507	0.578

4.2 Image Encryption Performce 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. NAE shows 1 if plain and decryption have no deformation, but the result assessment shows less than one. NSR 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

name	*MSE*	*PSNR*	*AD*	*MD*	*NC*	*MAE*
Paper	53388.40	10.8563	-3.4079	227	1	27.962
Barbara	56459.10	10.61346	-6.65866	235	1	25.803
Baboon	48398.40	11.28248	-24.5814	194	1	15.851
Lena	54171.20	10.7931	-31.5643	230	1	14.178
Monarch	46123.23	11.4916	-21.7716	225	1	16.738

TABLE 4 - PQE METRICS

name	*NAE*	*SC*	*NSR*	*SIM*	*CC*	*EQ*
Paper	0.431969	0.9699	-0.144	1.31946	0.0054	3150.23145
Barbara	0.521881	0.8955	-0.482	1.2905	0.00113	4532.44536
Baboon	0.448853	0.6612	-1.799	1.198218	0.00017	6879.4353
Lena	0.626411	0.5988	-2.227	1.162518	0.00235	3765.8879

name	*NAE*	*SC*	*NSR*	*SIM*	*CC*	*EQ*
Paper	0.431969	0.9699	-0.144	1.31946	0.0054	3150.23145
Monarch	0.522711	0.6886	-1.622	1.208525	0.000061	5478.8889

2) Encryption and Decryption Runtime Images: In ***Table 5*** indicates time complexity for all pictures, encryption and decryption time takes a few milliseconds:

TABLE 5 – Time Complexity Milliseconds

name	*diminution*	*Size*	*Encryption time*	*Decryption time*
Paper	256x256	213 KB	0.715	0.781
Barbara	512x512	777 KB	2.672	2.735
Baboon	560x560	960 KB	3.473	3.584
Lena	755x755	1.4 MB	6.794	6.893
Monarch	900x900 pixel	2.7 MB	9.695	9.852

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

name	*NPSR*	*UACI*
Paper	0.99696	0.3360
Barbara	0.99613	0.3361
Baboon	0.99690	0.3392
Lena	0.99620	0.3362
Monarch	0.99593	0.3363

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 7 - NPSR COMPARISONS AMONG DIFFERENT ALGORITHMS

Image	**Barbara**	**Baboon**	**Lenna**
Our Proposed	0.99613	0.99690	0.99620
Ref[36]	non	0.99620	0.99450
Ref [37]	non	0.99610	0.99610
Ref [38]	non	non	0.99000
Ref [23]	0.99617	0.99601	0.99620

TABLE 8 - UACI COMPARISONS AMONG DIFFERENT ALGORITHMS

Image	**Barbara**	**Baboon**	**Lenna**
Our Proposed	0.3461	0.3392	0.3362
Ref [33]	non	0.3361	0.3361

Image	Barbara	Baboon	Lenna
Our Proposed	0.3461	0.3392	0.3362
Ref [38]	non	0.3346	0.3346
Ref [39]	non	non	0.3355
Ref [40]	0.3356	0.3320	0.3358

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:

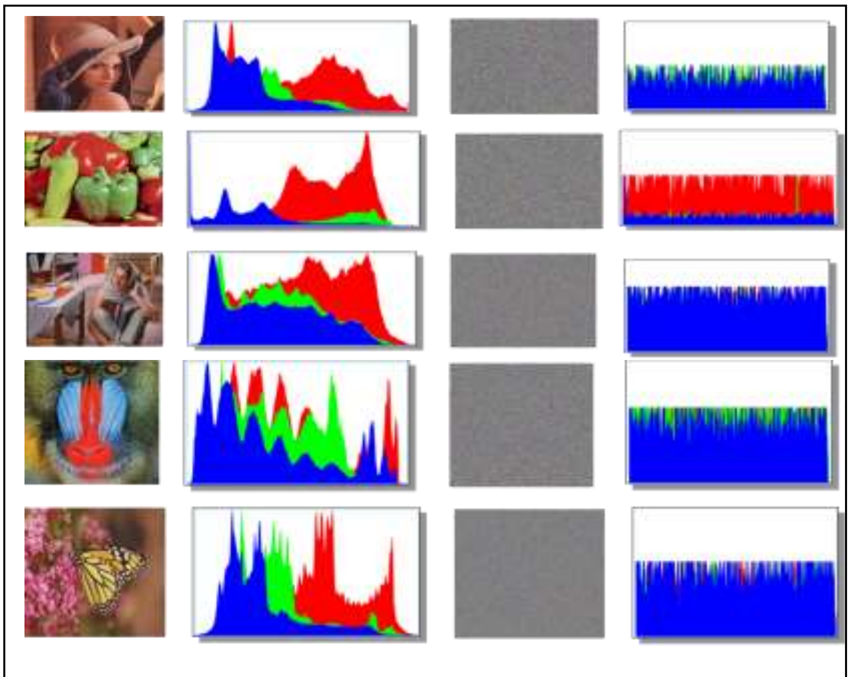

Figure 4-histogram of Lena, Pepper, Barbara, Baboon and Butterfly (a) plain image, (b) histogram of plain image, (c) cipher image, (d)histogram of cipher image

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 9 - ENTROPY

Paper	Barbara	Baboon	Lena	Monarch
7.9977	7.9972	7.9982	7.9980	7.9975

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 ALGORTHIM

Image	Our proposed	Ref [41]	Ref [42]
Lena	7.9980	7.9979	7.9973

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

[1] M. Li, M. Xu, J. Luo, and H. Fan "Cryptanalysis of an Image Encryption Using 2D Henon-Sine Map and DNA Approach," *IEEE Access*, 2019. doi: 10.1109/ACCESS.2019.2916402.

[2] J. M. Liu *et al.*, "Chinese internet searches provide inaccurate and misleading information to epilepsy patients," *Chin. Med. J. (Engl).*, 2015. doi: 10.4103/0366-6999.171425.

[3] Deye, N., Vincent, F., Michel, P. , Ehrmann, S., Da Silva, D., Piagnerelli, M., … Laterre, P.-F 6, "Changes in cardiac arrest patients' temperature management after the 2013 "*TTM*" trial: results from an international survey," *Annals of Intensive Care*, vol. 6, no. 1, 2016. http://doi.org/10.1186/s13613-015-0104-6.

[4] A. K. Farhan, N. M. G. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder," *Entropy*, vol. 21, no. 10, p. 958, 2019, doi: 10.3390/e21100958.

[5] A. K. Farhan and M. A. A. Ali, "Database Protection System Depend on Modified Hash Function," In Conference of Cihan University-Erbil on Communication Engineering and Computer Science, 2017.

[6] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu, "A Survey on True Random Number Generators Based on Chaos," *Discret. Dyn. Nat. Soc.*, 2017,doi: 10.1155/2019/2545123.

[7] S. M. Cho, E. Hong, and S. H. Seo, "Random Number Generator Using Sensors for Drone," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2972958.

[8] H. W. Pang, "The Technology of Digital Image Hiding Based on Discrete Wavelet Transform," *Appl. Mech. Mater.*, 2015, doi: 10.4028/www.scientific.net/amm.740.718.

[9] R. Pakshwar, V. Trivedi, and V. Richhariya, "A survey on different image encryption and decryption techniques," *Int. J. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 113–116, 2013.

[10] H. A. Lee *et al.*, "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study," *J. Med. Internet Res.*, 2020, doi: 10.2196/16748.

[11] B. Schneier, "*Applied Cryptography,"* First Edition. 1996 John Wiley & Sons 784 Pages

[12] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov, "Triathlon of lightweight block ciphers for the Internet of things," *J. Cryptogr. Eng.*, 2019, doi: 10.1007/s13389-018-0193-x.

[13] B. Schneier, *"Applied Cryptography Second Edition,"* John Wiley & Sons, Inc, 1996.

[14] A. Kadhim and S. Khalaf, "New Approach for Security Chatting in Real Time," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 4, no. 3, pp. 30–36, 2015.

[15] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *Journal of Cryptographic Engineering*, 2018, doi: 10.1007/s13389-017-0160-y.

[16] F. Alaa Kadhim, G. H. Abdul-Majeed, R. S. Ali, F. A. Kadhim, G. H. Abdul-Majeed, and R. S. Ali, "Enhancement CAST block algorithm to encrypt big data," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, pp. 80–85, 2018 doi: 10.1109/NTICT.2017.7976119.

[17] F. A. Kadhim and H. I. Mhaibes, "Quantum Random Bits Generator based on Phase Noise of

Laser," *J. Eng. Appl. Sci.*, vol. 13, no. 3, pp. 629–633, 2018. .

[18] D. M. Morens, P. Daszak, and J. K. Taubenberger, "Escaping Pandora's Box — Another Novel Coronavirus, *N. Engl. J. Med.*, 2020, doi: 10.1056/nejmp2002106.

[19] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A NEW APPROACH TO GENERATE MULTI S-BOXES BASED ON RNA COMPUTING," *Int. J. Innov. Comput. Inf. Control*, vol. 16, no. 1, pp. 331–348, 2020, doi: 10.24507/ijicic.16.01.331.

[20] R. Hosseinkhani, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System," *Int. J. Comput. Sci. Secur. (IJCSS), Vol. Issue 2012*.

[21] A. Alabaichi, F. Ahmad, and R. Mahmod, "Security analysis of blowfish algorithm," 2013, doi: 10.1109/ICoIA.2013.6650222.

[22] Y. Q. Zhang, J. L. Hao, and X. Y. Wang, "An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map," *IEEE Access*, 2020, Doi: 10.1109/ACCESS.2020.2979827.

[23] H. Zhu, Y. Zhao, and Y. Song, "2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2893538.

[24] A. T. Sadiq, A. K. Farhan, and S. A. Hassan, "A proposal to improve RC4 algorithm based on hybrid chaotic maps," *J. Adv. Comput. Sci. Technol. Res.*, vol. 6, no. 4, pp. 74–81, 2016.

[25] F. Alaa Kadhim and Z. A. Kamal, "Dynamic S-BOX base on primitive polynomial and chaos theory," *Int. Iraqi Conf. Eng. Technol. its Appl. IICETA 2018*, pp. 7–12, 2018, doi: 10.1109/IICETA.2018.8458093.

[26] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *Eur. Phys. J. Plus*, 2018, doi: 10.1140/epjp/i2018-11834-2.

[27] B, S., Kurths, J., "Chaos and Cryptography: A new dimension in secure communications," Eur. Phys. J. Spec., 2014, Top. 223, 1441–1445. https://doi.org/10.1140/epjst/e2014-02208-9.

[28] Lorenz, E.N., "Deterministic nonperiodic flow," Journal of atmospheric sciences, 20(2), pp.130-141, 1963.

[29] A. Kadhim F. and H. Emad M., "Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers," *Diyala J. Pure Sci.*, vol. 13, no. 3, pp. 24–39, 2017, doi: 10.24237/djps.1303.268b.

[30] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Process. Image Commun.*, 2016, doi: 10.1016/j.image.2015.10.004.

[31] S. L. Brunton, B. W. Brunton, J. L. Proctor, E. Kaiser, and J. Nathan Kutz, "Chaos as an intermittently forced linear system," *Nat. Commun.*, 2017, doi: 10.1038/s41467-017-00030-8.

[32] W. Song and J. Liang , "Difference equation of lorenz system," *Int. J. Pure Appl. Math.*, 2013, doi: 10.12732/ijpam.v83i1.9.

[33] X. P. Zhang, R. Guo, H. W. Chen, Z. M. Zhao, and J. Y. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chinese Phys. B*, 2018, doi: 10.1088/1674-1056/27/8/080701.

[34] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," *Complexity*, 2020, doi: 10.1155/2020/9597619.

[35] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and S-Box,", 2015, doi: 10.1109/ICMSAO.2015.7152261.

[36] X. J. Tong, "Design of an image encryption scheme based on a multiple chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, 2013, doi: 10.1016/j.cnsns.2012.11.002.

[37] H. Liu, A. Kadir, X. Sun, and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and S-boxes," *Multimed. Tools Appl.*, 2018, doi: 10.1007/s11042-016-4288-z.

[38] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using Enhanced Logistic-Tent Map," *Entropy*, 2019, doi: 10.3390/e21070656.

[39] C. R. Revanna and C. Keshavamurthy, "A new partial image encryption method for document images using variance based quad tree decomposition," *Int. J. Electr. Comput. Eng.*, 2020, doi: 10.11591/ijece.v10i1.pp786-800.

[40] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," *Neural Comput. Appl.*, 2018, doi:

10.1007/s00521-017-2970-3.
[41] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling," *Entropy*, 2019, doi: 10.3390/e21040343.
[42] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, 2019, doi: 10.1016/j.sigpro.2018.09.029.