Journal of Physics: Conference Series

PAPER • **OPEN ACCESS**

Multi Chaotic System to Generate Novel S-Box for Image Encryption

Multi Chaotic System to Generate Novel S-Box for Image Encryption

Hany Nasry[1], Azhaar A. Abdallah[2], Alaa K. Farhan[3], Hossam E. Ahmed[4], Wageda I.El Sobky[5,6]

[1] *Mathematical Departement ,Military Technecial Collage ,Cairo,Egypt[1]*
Department of Applied Sciences, University of Technology, Baghdad, Iraq[2,3]
Department of Communication Engineering, Benha Faculty of Engineering, Benha University, Egypt[4]
Department of *Basic* Engineering science, Behna Faculty of Engineering, Benha University, Egypt[5]
Department of Basic Science, Canidian International College (CIC), Egypt6.
Corresponding author[1]: hanynasry@mtc.edu.eg
Corresponding author[3]: 110030@uotechnology.edu.iq
Corresponding author[5]: wageda.alsobky@bhit.bu.edu.eg

Abstract. A novel method on the basis of multi chaos theory is suggested in the presented study. Also, the study used two different dimensions to generate S-Box to get a strong cipher that is difficult to break. The suggested image cryptosystem includes an identical (decryption and encryption) process, which involves a single keystream generator, shifting process (based on 3D Lorenz map) related diffusion operations, and generate S-Box (based on 2D Henon map) that related confusion operation. The comparative analysis and the simulate test show that the suggested image cryptosystem has a few properties, like high-sensitivity, fast encryption/decryption, large keyspace, excellent statistical properties related to the ciphertext, and so on. The suggested cryptosystem is considered as an alternative for practical secure communications.

Keywords: Chaos System, Image Encryption, S-Box, Shifting

1. INTRODUCTION

The research on image encryption is an important point in current encryption algorithm [1,2] after AES and DES became standards in terms of encrypting the text data. Also, the experts of cryptography attempt to identify the optimum algorithm of image encryption for serving as an algorithm for image encryption standard. In comparison to the text data, the properties of digital images, including strong correlation, large data amounts, big data redundancy, make it need a large quantity of pseudo-random numbers as a keystream, which is, simulating the researches on pseudo-random numbers. In addition, the chaotic systems are created via deterministic equations with vital benefits to create pseudo-random numbers since they were qualified with maximum sensitivity to the initial values as well as parameters, ergodicity, dense form, and so on. Currently, the chaotic systems were majorly utilized in the systems of image encryption as key stream generators [3,4], and extended with multiple images [5], in A.I also using the chaotic system to generated ranomen population and using in another application [6] might be categorized into 2 categories: 1D chaotic maps [7,8] and multi-dimensional (MD) chaotic maps [7,6]. Normally, 1D chaotic maps consist of a single variable [42-46] and a number of parameters. For instance, the Logistic, Sine, and Tent maps and can combine multiple chaotic maps as chaotic hybrid maps [9,10].

In this paper, to transfer the data into a perplexing type, such as block ciphers are using two major permutation and substitution operations. A substitution procedure uses a substitution table referred to as the substitution box (S-box) for replacing byte/block with another one [11,12]. On the other hand, in some linear methods, a permutation method shifts the input bits or bytes [13].

For producing strong S-boxes, researchers and academics have explored and examined different concepts [14]. The intensity was evaluated using some usual parameters, like non-linearity, lack of fixed points, differential and linear probabilities, the strict criterion of avalanche (SAC), the criterion of bit independence (BIC), and so on. [15]. In addition, section two is providing an overview of the chaos theory (2-D and 3-D). In Section 3, a novel approach for image encryption based on generated S-Box with shifting, also a performance evaluation as well as a comparison of encryption was performed. The research findings are provided in Section.

2. Chaotic Map

Chaos theory depends on (initial & condition) parameter sensitivity. This means that any small change gives different results.

A- 2D - The Hénon Map A discrete time dynamic system was often called Hénon-Pomeau attractor/map. It can be specified as a majorly examined example of chaotic behavior displaying dynamical systems. Furthermore, the Henon system is taking a point (x_n, y_n) in the plane and after that mapping it into a new point [1][16]. Introduced 2D-Henon system., as described in Eq. (1).

$$x_{i+1} = 1 - a x_i^2 + y_i \qquad (1)$$

$$y_{i+1} = b\, x_i$$

The map is based on 2 parameters, a and b, with values of a = 1.4 and b = 0.3 for the classical Hénon system [17].

B- 3D - Lorenz System the Lorenz system [18,19], which Edward Lorenz researched for the first time in 1960, is a dynamic system defined by the nonlinear system of ordinary equations:

$$X_{n+1} = \alpha(Y_n - Z_n) \qquad (2)$$

$$Y_{n+1} = RX_n + X_n Z_n - Y_n$$

$$Z_{n+1} = X_n Y_n - BZ_n$$

These variables (α, r, b) are referred to as control parameters, while (x, y, z) is referred to as status variables [20]. Equation (2) defines the control parameters, and the initial values x_0, y_0, z_0 are referred to as state variables, and they are 10, 8/3, and 28, respectively.

3. THE PROCESS OF ENCRYPTION & DECRYPTION

Because of the strong correlations amongst neighbour pixels of the plain image, this study suggests shifting the pixel positions related to plain image for solving such problem as well as breaking the pixels' correlations. Without a generality loss, the plain image dimensions are going to be N × N. The proposed method focuses on the principles (diffusion and confusion) for breaking the pixels' correlations. Design a new S-Box that gives a better way of Shifting to more confusion and diffusion.

4. S-Box Generator

There are several methods of generating S-Boxes [32-41].This work suggested designing a new S-Box depending on 2D-Henon map; this operation provides greater protection and complexity to generate new large ($\mathbf{16 \times 16}$). Initially, using initial value $\mathbf{X_0}$ to chaotic map and creating numbers, the range ($\mathbf{0 - 255}$), S-Box production mechanism by generating Henon system values, all S-Box values must be unique. If the value is greater than the appropriate area, then the rest of the section has been taken to that value, producing S-Box inverse at the same time depending on the result of S-Box, since the "responsive dependency on 5 initial states" with chaos theory changes the construction of S-Box and the result of dynamic S-Box inverse with every slight change in initial value.

5. Encryption Schema Steps

The details of image encryption are indicated in the following way **(as shown in fig. 1)**:

Step 1 Shifting columns based on the value of X_n that's generated from 3D-Lornez System then XORed the result matrix with the value of X_n

Step 2 Shift rows based on the value of Yi that's generated from 3D-Lornez System and the result matrix XORed with the value of Yi.

Step 3 To increase diffusion principle in pixel, replace rows with columns then XORed the result matrix with the value of Zi that generated from 3D-Lornez System.

Step 4 For more confusion, generate a new S-Box (16*16) depend on the 2D-Henon map in unique values and non-linearity, then inserting S-Box to the above matrix.

Step 5 Finally, we get cipher and ambiguous images.

6. Decryption Schema Steps

The details of image decryption are indicated in the following way:

Step 1 Substitute the image matrix based on inverse S-Box generated from 2D-Henon map.

Step 2 XOR result matrix with Zi that generated from 3D-Lorenze map then replace rows & columns.

Step 3 XOR result matrix with Yi then shifts columns based on Yi (Yi generated from 3D-Lorenz map).

Step 4 XOR result matrix with X_i then shifts columns based on X_i (X_i generated from 3D-Lorenz map).

Step 5 Finally, extract the plain image with a slight difference in resolution

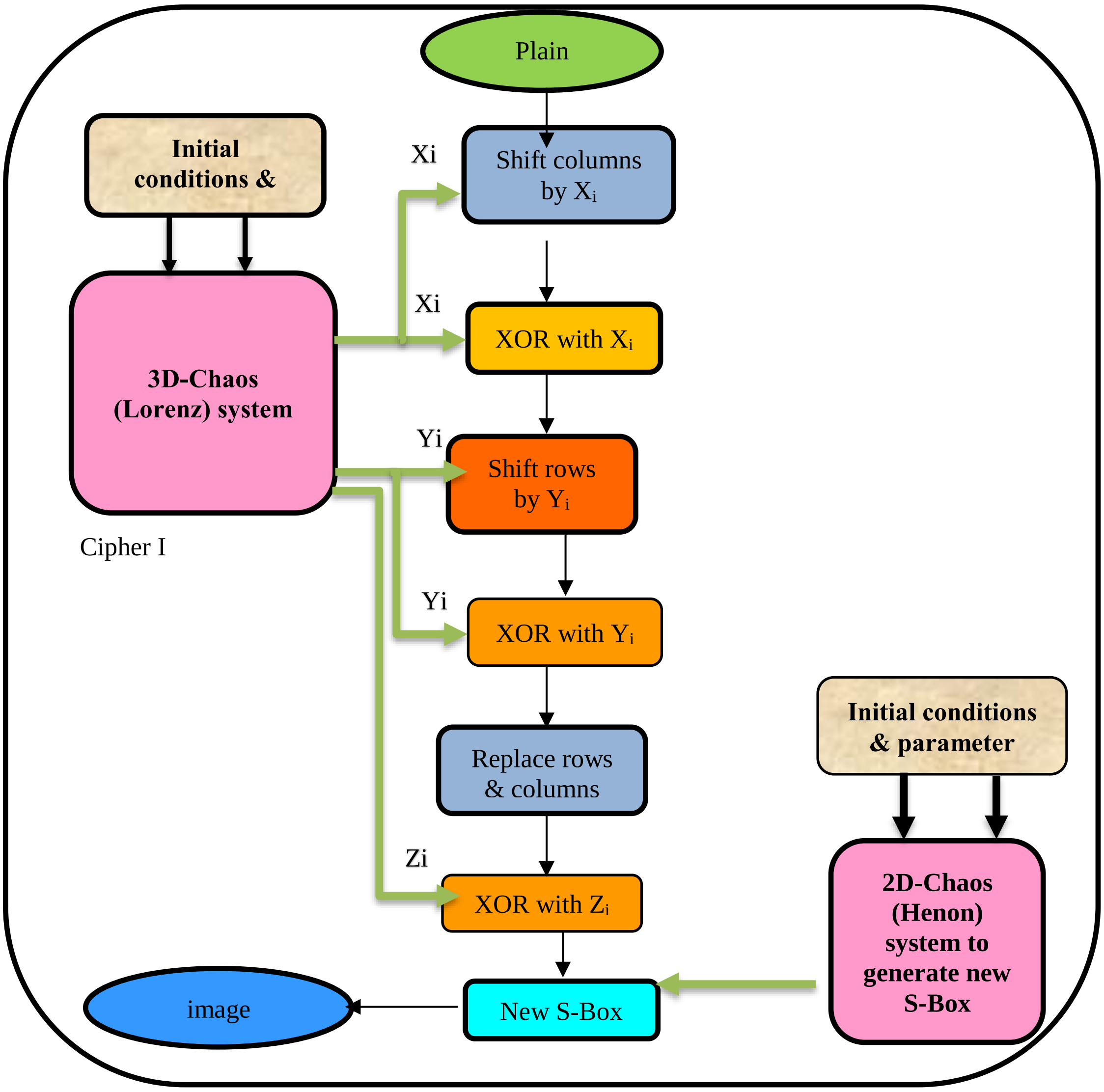
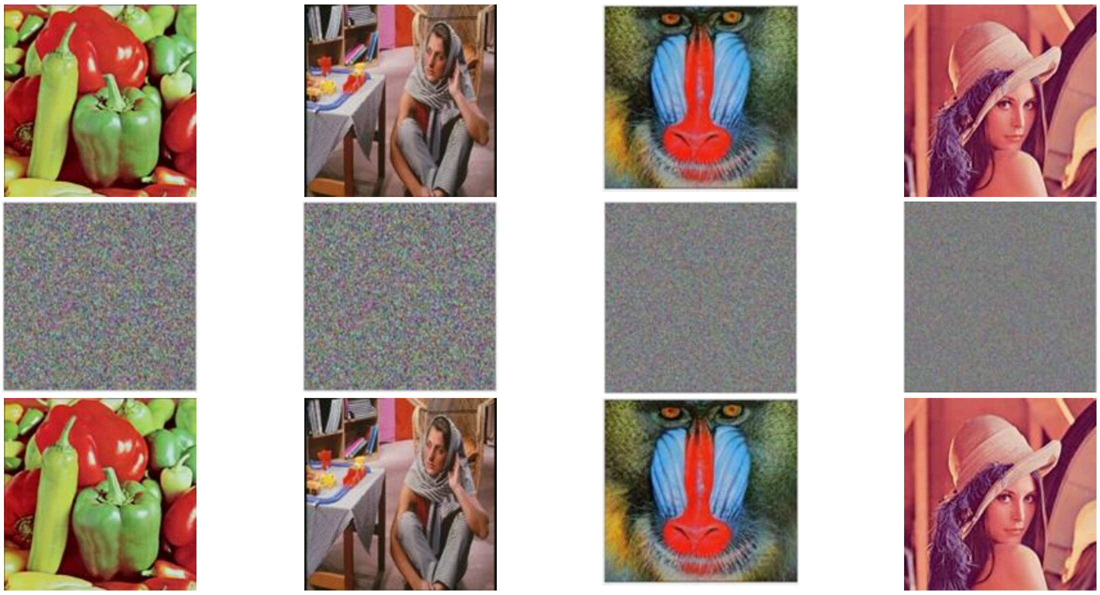


Figure (1): Diagram of Proposal Encryption algorithm

7. Simulation Analysis & Experiment Result

For the purpose of resisting brute-force attacks, the keyspace must be adequately large for securing the image cryptosystem. This segment discusses the results of the suggested encryption algorithm, also the new S-Box for statistical accuracy and analysis of the encrypted image. The base part of the cryptographic block cipher is confusion; each plain-image includes blocks that are transformed into cipher-image blocks, and this builds on the 2D Henon map key for XOR operation. Small changes in initial parameters or conditions lead to various results in final encryption image. Diffusion is the second part of Shift operation in the cryptography block cipher; several digits of the ciphertext can affect every digit of the plain image and every digit of the hidden key.

In terms of the image cryptosystem shown in **Figure 1,** we used the plain images Paper 256*256, Barbra 512*512, Baboon 560*560, Lenna 755*755, Goldhill 900*900 and all are color images and the test results are **as shown in Figure. 2**.



(a) (b) (c) (d)

Fig. 2. Simulation results. (a) Pepper (b) Barbra (c) Baboon (d) Lenna

In our proposed approach, we used different sizes and quality image tests for evaluating the efficiency and security of our proposed system. By Picture Quality Evaluation (PQE) [21], Histogram Analysis Randomness tests and evaluates Image Quality by Entropy.

8. Picture Quality Evaluation (PQE) Metrics

With regard to showing encoded and decoded image quality measurement, the PQE should be utilized as can be seen in the image indicated below, 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 the decryption image and the plain 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 the 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

Name	**MSE**	**PSNR**	**AD**	**MD**	**NC**	**MAE**	**NAE**	**SC**	**NSR**	**SIM**	**CC**	**EQ**
Pepper	10150.39	0.0047	4208.57	240	0.234	8417.59	0.2347	1.2601	2.0640	123.6	0.00568	13266
Barbra	8933.866	0.0053	4679.88	239	0.261	32.4567	0.2616	1.3690	1.9551	122.4	0.00235	14180
Baboon	9810.720	0.0049	4505.42	238	0.250	9011.28	0.2505	1.5090	1.9979	118.9	0.00644	13898
Lenna	9016.81	0.0053	3701.33	211	0.205	7403.39	0.2059	1.0429	2.2034	129.2	0.00263	12609

Encryption & Decryption Running Time

As can be seen in the Table 2, time complexity with all images, time take few milliseconds for encryption and decryption.

Table 2 - Encryption & Decryption Run Time

Name	**Diminution**	**Size**	**Encryption Time**	**Decryption Time**
Pepper	256*256	192KB	953MS	233MS
Barbra	512*512	768KB	100MS	289MS
Baboon	560*560	918KB	455MS	433MS
Lenna	755*755	1.63MB	175MS	867MS

9. S-Box Performance Analysis

Typical statistical criteria, including Balanced Criteria (BC), is the average allocation of 0 and 1 values, Avalanche Criteria (AC) that is an integral criterion that shows how a small shift in the input bits results in the main output change, Strict Avalanche Criteria (SAC) 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, and inevitability, are evaluated according to our proposed approach to designing a new S-box. **(as can be seen in Tables 3 & 4)**

Table 3 - AC, BC comparisons

	AC			**BC**	
	Min.	**Avg.**	**Max.**	**0's Avg.**	**1's Avg.**
Our proposed	0.33	0.570	0.8175	31	32
Ref[22]	0.25	0.5	0.75	32	32
Ref[23]	0.125	0.5	0.875	29	35
Ref[20]	0.25	0.875	0.56	31	33

Table 4 – SAC

	SAC		
	Min.	Avg.	Max.
Our proposed	0.33	0.570	0.8175
Ref[22]	0.25	0.5	0.75
Ref[25]	0.125	0.5	0.875
Ref[24]	0.25	0.875	0.56

10. Differential Attacks Analysis

The Number of Modifying Pixel Rate (NPCR) and Unified Average Adjusted Intensity (UACI) [26,27] were specified as 2 of the major quantities utilized for estimating the strength related to image encryption algorithms/coders for differential attacks, **as shown in Table 5**.

Table 5 - Randomness Tests

	NPSR	**UACI**
Pepper	76595	32747
Barbra	43758	43785
Boats	37489	43785
Lenna	57866	43875
Goldhill	32475	84397

As shown in Table 6, NPSR between our proposed and [28, 29, 30, 31] proposals, and in **Table 7** describe UACI between our proposed and [25, 32, 33, 34] proposals.

Table 6 - NPSR comparisons among different algorithms

	Barbra	**Lenna**
Our proposed	0.987	0.987
Ref[28]	Non	0.994
Ref[29]	Non	0.996
Ref[30]	Non	0.990
Ref[31]	0.996	0.996

Table 7 - UACI comparisons among different algorithms

	Barbra	**Lenna**
Our proposed	0.097	0.865
Ref[25]	Non	0.336
Ref[32]	Non	0.334
Ref[33]	Non	0.335
Ref[34]	0.996	0.335

11. 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 3** (a, b, c, d) depicts Lena, Pepper, Barbara, Baboon, and Pepper's regular and encrypted pictures. We evaluated from **Figure 3** (a, b, c, d) that the regular image histograms weren't precise, whereas the encrypted digital image histograms have been reliable. The uniformity of the pixel heights of the encrypted image histograms makes it hard to find an insight into the maximum information region for attackers.

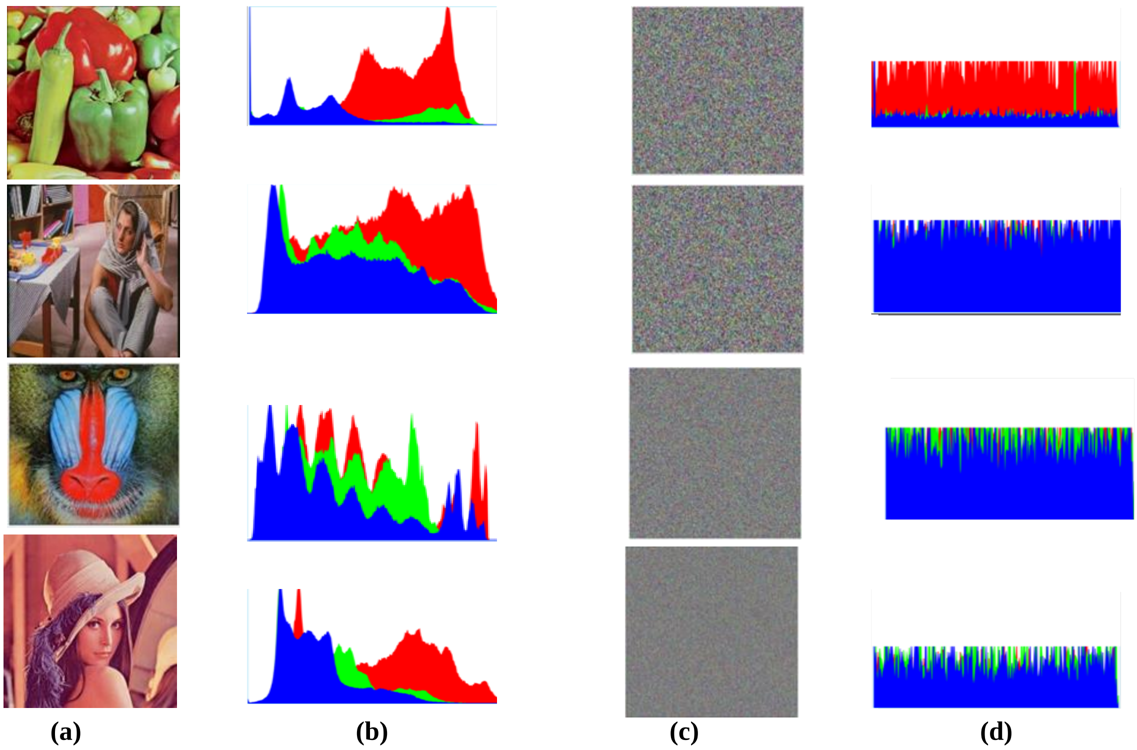


Figure 3: histogram of Lena, Pepper, Barbara, Baboon, and Pepper (a) plain image, (b) histogram of plain image, (c) cipher image, (d) histogram of cipher image

12. 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:

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

In which, p (s_i) corresponds to the probability related to s. Entropy would preferably be H(s) = 8 for a 2 - 1 gray cipher-8 picture displaying random knowledge, **as shown in Table 8**.

Table 8 - information entropy

Name	**Pepper**	**Barbra**	**Boats**	**Lenna**	**Goldhill**
Inf. Entropy	43646	43645	43546	65654	35656

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 comparisons among different algorithms

Image	**Our Proposed**	**Ref[30]**	**Ref[34]**	**Ref[33]**
Lenna	7.9973	7.997	7.997	7.997

13. REFERENCES

[1] Q. Liu, PY. Li, MC. Zhang. YX. Sui, H.J Yang, A novel image encryption algorithm based on chaos maps with Markov pro perties Commun Noilinear Sci. Numer. Simul. 20 (2) (2015) 506-515.

[2] X. Wu, D. Wang, J. Kurths, H. Kan, A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system, Inf. Sci. 349 (2016)

[3] X. Wang, H.L. Zhang, A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems, Nonlinear Dyn. 83 (1-2) (2016) 14021-14033.

[4] Y. Zhang, The image encryption algorithm with plaintext-related shuffling, IETE Tech. Rev. 33 (3) (2016) 310-322. Signal Processing, 147, 2000, pp. 167-175.

[5] Ahmed T., E.M.E.Mostafa, Yasser F. ,Ahmed B. 'Using Chaotic Maps to Enhance RSA Public Key Cryptography', Sci.Int.(Lahore), Vol. 30, PP. 711-715, Sep.2018.

[6] S. Rahma, Abdul Monem , M,Kadhem, Suhad, Engineering and Technology Journal,2012,volum 30,issue 9,pp 1625-1630

[7] Alaa Kadhim F, Hakeem Emad M. 'Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers' Diyala Journal For Pure Science, Vol. 13, PP. 24-39, Apr.2017.

[8] Shokouh Saljoughi, A., & Mirvaziri, H. 'A new method for image encryption by 3D chaotic map', Pattern Analysis and Applications, Vol. 22, PP. 243–257, Nov.2018.

[9] Zhou, N., Pan, S., Cheng, S., &Zhou, Z. 'Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing', Optics & Laser Technology, Vol. 82, PP.121–133, Feb.2016.

[10] Hua, Z., Jin, F., Xu, B., & Huang, H. '2D Logistic-Sine-coupling map for image encryption', Signal Processing, Vol. 149, PP. 148–161, Mar.2018.

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

[12] Alaa Kadhim, Rand Mahmoud MohamedAli. Visual cryptography for image depend on RSA & AlGamal algorithms, Conference in 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA).

[13] AT Sadiq, AK Farhan, SA Hassan. A proposal to improve RC4 algorithm based on hybrid chaotic maps, J. Adv. Comput. Sci. Technol. Res, 2016

[14] Alaa Kadhim Farhan, Rasha Subhi Ali, H Rashed Yassein, Nadia Mohammed Ghanim Al-Saidi, Ghassan Hameed Abdul-Majeed,feb. 2020. A NEW APPROACH TO GENERATE MULTI S-

BOXES BASED ON RNA COMPUTING. International Journal of Innovative Computing, Information and Control. Sci., vol. 16, no. 1, pp. 331–348.

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

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

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

[18] E. N. Lorenz 2017. Deterministic nonperiodic flow, in Universality in Chaos, Second Edition.

[19] A. Kadhim F. and Sura Khalaf. 2015. New Approach for Security Chatting in Real Time, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 4, issue. 3, pp. 30–36, doi: 10.24237/djps.1303.268b.

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

[21] Mrak, M., Grgic, S., & Grgic, M. ‘Picture quality measures in image compression systems’. The IEEE Region 8 EUR OCON. Computer as a Tool, PP. 233-237, Sep.2003.

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

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

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

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

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

[27] Hui L,Bo Z.,Linquan H. ‘Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling’, Entropy 2019, Vol.21, PP.343, Mar.2019.

[28] Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, A. ‘A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map’, Procedia Computer Science, Vol. 127, PP. 539–548, Mar.2018.

[29] Yong Z. ‘The unified image encryption algorithm based on chaos and cubic S-Box’, Information Sciences, Vol.450, PP.361–377, Mar.2018.

[30] Chai, X. ‘An image encryption algorithm based on bit level Brownian motion and new chaotic systems’. Multimedia Tools and Applications, Vol. 76, PP. 1159-1175,Nov.2015

[31] Liu, H., & Jin, C.‘A Novel Color Image Encryption Algorithm Based on Quantum Chaos Sequence’, 3D Research, Vol. 8, Jan.2017.

[32] Wageda Ibrahim Alsobky ,Abdelkader Esmail ,Ashraf S. Mohra, Ayman Abdelaziem “Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (2^8)” International Journal of Telecommunications, IJT’2022, Vol.02, Issue 01

[33] Medhat Mansour, Wageeda Elsobky, Ayman Hasan, Wagdy Anis." Appraisal of Multiple AES Modes Behavior using Traditional Enhanced Substitution Boxes ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020

[34] Eslam wahba afify, Wageda I. El sobky, Abeer T. Khalil, Reda Abo Alez." Algebraic Construction of Powerful Substitution Box", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020

[35] Eslam w. afify, Abeer T. Khalil, Wageda I. El sobky, Reda Abo Alez." Performance Analysis of Advanced Encryption Standard (AES) S-boxes ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9, Issue-1, May 2020

[36] Wageda Alsobky, Hala Saeed, Ali N.Elwakeil." Different Types of Attacks on Block Ciphers ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-3, September 2020

[37] Wageda I. El Sobky, Ahmed R. Mahmoud, Ashraf S. Mohra, T. El-Garf." Enhancing Hierocrypt-3 performance by modifying its S-Box and modes of operations ", Journal of Communications Vol. 15, No. 12, December 2020

[38] Abdel Halim A. Zikry, Ashraf Y. Hassan, Wageeda I. Shaban, Sahar F. Abdel-Momen.." Performance Analysis of LDPC Decoding Techniques ", International Journal of Recent Technology and Engineering (IJRTEISSN: 2277-3878, Volume-9 Issue-5, January 2021

[39] Mohamed G Abd Elfatah, Hany Nasry Zaky and Ahmed Shams" Mobile Robot Position Estimation using Milstein Algorithm" Journal of Physics: Conference Series, Volume 1970, 10th International Conference on Mathematics and Engineering Physics (ICMEP-10), 7-9 April 2020, Military Technical College, Kobry El-Kobbah, Cairo, Egypt

[40] Mohamed G Abd Elfatah1, Hany Nasry Zaky1 and M Gharib2" Mobile robot position estimation using Euler-Maruyama algorithm" IOP Conference Series: Materials Science and Engineering, Volume 610, 18th International Conference on Aerospace Sciences & Aviation Technology 9–11 April 2019, Military Technical College, Kobry Elkobbah, Cairo, Egypt.

[41] Hany Nasry." Coordinate Transformation In Unmanned Systems Using Clifford Algebra" Proceedings of the 5th International Conference on Mechatronics and Robotics EngineeringFebruary 2019 Pages 167–170https://doi.org/10.1145/3314493.3314496.

[42] Hassan R. Yassein, Nadia M. G. Al-Saidi & Alaa K. Farhan"A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure"Journal of Discrete Mathematical Sciences and Cryptography **,** May 2020

[43] Sameeh Abdulghafour Jassim, Alaa K. Farhan" Designing a Novel Efficient Substitution-Box by Using a Flower Pollination Algorithm and Chaos System" International Journal of Intelligent Engineering and Systems, Vol.15, No.1, 2022.

[44] Jolan Rokan Naif; Ghassan H. Abdul-Majeed; Alaa K. Farhan" Secure IOT System Based on Chaos-Modified Lightweight AES" 2019 International Conference on Advanced Science and Engineering (ICOASE), DOI: 10.1109/ICOASE.2019.8723807

[45] Omar Z. Akif , Sura Mazin Ali , Rasha Subhi Ali , Alaa Kadhim Farhan" A new pseudorandom bits generator based on a 2D-chaotic system and diffusion property" Bulletin of Electrical Engineering and Informatics Vol. 10, No. 3, June 2021, pp. 1580~1588 ISSN: 2302-9285, DOI: 10.11591/eei.v10i3.2610.

[46] F Alaa Kadhim, Ghassan H Abdul-Majeed, Rasha Subhi Ali" Enhancement CAST block algorithm to encrypt big data" 2017 Annual Conference on New Trends in Information &

Communications Technology Applications (NTICT),pages(80-85), **DOI:** 10.1109/NTICT.2017.7976119