Engineering and Technology Journal
Journal homepage: https://etj.uotechnology.edu.iq

New S-Box Design for Image Encryption Based on Multi-Chaotic System

Azhaar A. Abdallah*, Alaa K. Farhan

Computer Sciences Dept., University of Technology-Iraq, Alsina'a street, 10066 Baghdad, Iraq.
*Corresponding author Email: cs.19.48@grad.uotechnology.edu.iq

HIGHLIGHTS

- A novel encryption scheme was proposed based on a multi-chaotic system for secure communications.
- The scheme employs a strong cipher generated from a 2D Henon map for the S-Box and a 3D Lorenz map for key generation.
- The proposed encryption method demonstrates high performance, offering efficiency and robustness against attackers.

ARTICLE INFO

Handling editor: Rana F.Ghani

Keywords:
2D-Henon map;3D-Lorenz map;Color Image Encryption;S-Box; Shuffling.

ABSTRACT

Image encryption is a crucial area for researchers in information security, which protects digital images from unauthorized access. This paper proposes a novel image encryption scheme based on the multi-chaotic system. This paper is about encrypting color images based on a 2D Henon map and a 3D Lorenz map. We used the 2D Henon map equation to generate a new S-Box, thus creating a solid cipher that is difficult to break (for the confusion operation). We then generate keys from the 3D Lorenz map for the shifting process (for diffusion operation). A comparative analysis and the simulation test show that the suggested image cryptosystem has some excellent properties, including high sensitivity, fast encryption/decryption, a large keys-pace, excellent statistical properties related to the ciphertext, etc.

1. Introduction

Defending information from any illegal access via various media, such as the rapid development of the internet and communication, makes it essential to secure the transmitted data over the internet, including text and images, audio, and video. Furthermore, digital information privacy and secrecy of information has become one of the most pressing issues, compelling Information Technology (IT) experts to devise new methods to protect and secure those data. Image Encryption is essential to provide security to the information that should not be used by other users, as well as providing the integrity, privacy, confidentiality, and authenticity of images. At the same time, they are transmitted and stored through networks. Chaos theory is one of the common approaches mainly used in current cryptographic algorithms because it generates vital keys against attackers, the speed of the encryption algorithm. Also, it is easy to implement [1].

During the last few years, Chaos Theory has attracted researchers in different fields, specifically cryptography. The secret behind chaos theory is the characteristics like its deterministic behavior, unpredictability, random appearance, and sensitivity to the initial value [2]. Currently, chaotic systems are mainly utilized in image encryption as keystream generators [3] and extended with multiple images [4]. The dispersal of the initial region via whole phase space due to the chaotic map repetitions. This can be obtained in algorithms of encryption through the construction process of the algorithm, which depends on rounds, chaotic systems, and cryptographic algorithms that are differed from each of these differences in that encryption transformations are determined on limited groups. In contrast, chaotic systems have a sense of real numbers.

Chaotic maps can be categorized into 1D chaotic maps and multi-dimensional ones [5]. Typically, 1D chaotic maps consist of a single variable and several parameters. For instance, there are Logistic, Sine, and Tent maps, which can be combined into multiple chaotic or chaotic hybrid maps [6].

This paper proposed a new image encryption based on a multi-chaotic map (2D - Henone map, 3D - Loreze system) to transform the data into perplexing-type data, such as a block cipher, and produce a scheme in two fundamental principles (confusion and diffusion).

http://doi.org/10.30684/etj.2023.139076.1416
Received 08 April 2023; Received in revised form 10 June 2023; Accepted 16 June 2023; Available online 16 July 2023
2412-0758/University of Technology-Iraq, Baghdad, Iraq

A substitution procedure uses a substitution table called a substitution box (S-box) to replace a byte/block with another [7]. On the other hand, in some linear methods, a permutation method is used to shift the input bits or bytes. Researchers have examined different concepts for producing strong S-boxes [8]. The intensity of such a box can be evaluated using some usual parameters, such as non-linearity, lack of fixed points, differential and linear probabilities, the strict criterion of avalanche (SAC), the measure of bit independence (BIC), and so on.

The major aim of this paper is to build a cryptographic system capable of getting good statistical test results. and encrypt the data to prevent the unauthorized person from accessing it or sending it through the internet; get a high degree of complexity to increase security. This can be worked chaos theory to generate keys to be used as secret numbers in the internal processes and can work depending on the principle of "confusion " and " diffusion" as a process to break the colored connection to get the encrypted image, to achieve secure protection for information (image).

This paper is divided into sections as follows. Section 2 will overview chaos theory (2-D and 3-D). Section 3 examines an approach for image encryption based on generating an S-Box via shifting. In addition, a performance evaluation, as well as a comparison with other encryption methods, is presented. The research findings are provided in Section 4. In final section presented Conclusions and Recommendations.

2. Related Work

In this section, we considered and explaind briefly three of state of the art work of the proposed image encryption algorithms:

Yasser and et al. [9], proposed a perturbation algorithm for image encryption based on double chaotic systems. The proposed chaotification algorithm is a hybrid technique which combin Discrete Wavelet Transform (DWT) with both permutation and diffusion properties are attained using the chaotic states and parameters of the proposed maps. The proposed algorithm was tested using dynamical analysis and sample entropy algorithms showing that the proposed map is overall hyperchaotic with the high sensitivity and high complexity.

Khan and et al. [10], proposed a chaos-based image encryption algorithm using 2D Henon chaotic map and skew tent map. Both chaotic maps play a key role in the permutation and diffusion mechanism. Authors used Extensive security analysis and resistance to statistical attack to prove the security of proposed algorithm.

Liu and et al. [11], Proposes a lossless quantum image encryption scheme based on substitution tables (S-box) scrambling, mutation operation and general Arnold transform with keys. Testing the proposed algorithms shows the ciphered image has a uniform histogram, low correlation coefficients, high information entropy and the proposed algorithm in general is resistant to various existing attacks.

3. Chaotic Map

Chaos theory depends on (initial and conditional) parameter sensitivity, meaning that any small changes in the system will provide different results. The issue may be solved by distributing light.

3.1 2D - The Hénon Map

The 2D- Hénon Map is a two-dimensional nonlinear map that describes a chaotic system. It was introduced by Michel Hénon, a French astronomer, in 1976. The Hénon Map has been studied extensively in the fields of physics, mathematics, and engineering due to its fascinating properties and applications . The Hénon system takes a point (xn, yn) in the plane and maps it into a new point. A 2D Hénon system is described in Equation 1 [12, 13].

$$(X\mathrm{n}+1) = (1 - ax2\mathrm{n})+\mathrm{yi} \qquad (1)$$
$$(Y\mathrm{n}+1) = (bx\mathrm{n})$$

where x[n] and y[n] are the state variables at time step n, and a and b are parameters that control the behavior of the system [12, 13].

The map is based on two parameters, a and b, where a = 1.4 and b = 0.3 in the classical Hénon system. Figure 1 shows the step plan for the Hénon map.

Figure 1 Plot the trajectory in the x-y plane to visualize the behavior of the system can. Note that the behavior of the Hénon map is highly sensitive to the initial conditions and the values of a and b. Small parameter changes can lead to drastically different trajectories, including chaotic behavior.

3.2 3D - Lorenz System

The Lorenz system is a set of differential equations that describe the behavior of a simple model for atmospheric convection. It was introduced by Edward Lorenz in 1963 as a simplified model for the weather system. The Lorenz system is Notable for its chaotic behavior, meaning that small changes in the initial conditions can lead to vastly different outcomes [14]. The 3D-Lorenz system extends the original Lorenz system to three dimensions. It is given by the following set of differentials system 2:

$$\mathrm{X}n + 1 = \alpha\ (\ \mathrm{Y}n - \mathrm{Z}n\ )$$
$$Yn + 1 = RXn + XZn - Yn \qquad (2)$$
$$Zn + 1 = XnYn - BZ\mathrm{n}$$

where x, y, and z are the system variables, and σ, ρ, and β are parameters. The system exhibits chaotic behavior for certain values of the parameters.

The first equation describes the rate of change of x, which is proportional to the difference between y and x, with the proportionality constant σ. The second equation describes the rate of change of y, which depends on x, y, and z. The third equation describes the rate of change of z, which depends on x, y, and z, with the proportionality constant β [15].

When plotting the Lorenz system in 2D phase space, one can choose two of the state variables and plot them against each other. For example, one could plot x against y, or y against z. The resulting plot will show the trajectory of the system in 2D and will reveal the complex and chaotic behavior of the Lorenz system, as shown in Figure 2 (a,b,c). This figure defines the control parameters, and the initial values x0, y0 and z0 are state variables with values 10, 8/3, and 28, respectively.

Figure 2 plot the system trajectories in the x-y, x-z, and y-z planes. These are known as the Lorenz attractor phase planes. In the x-y plane, the attractor takes on the form of a distorted figure-eight shape. In the x-z and y-z planes, the attractor appears as two "wings" spiral towards the center.

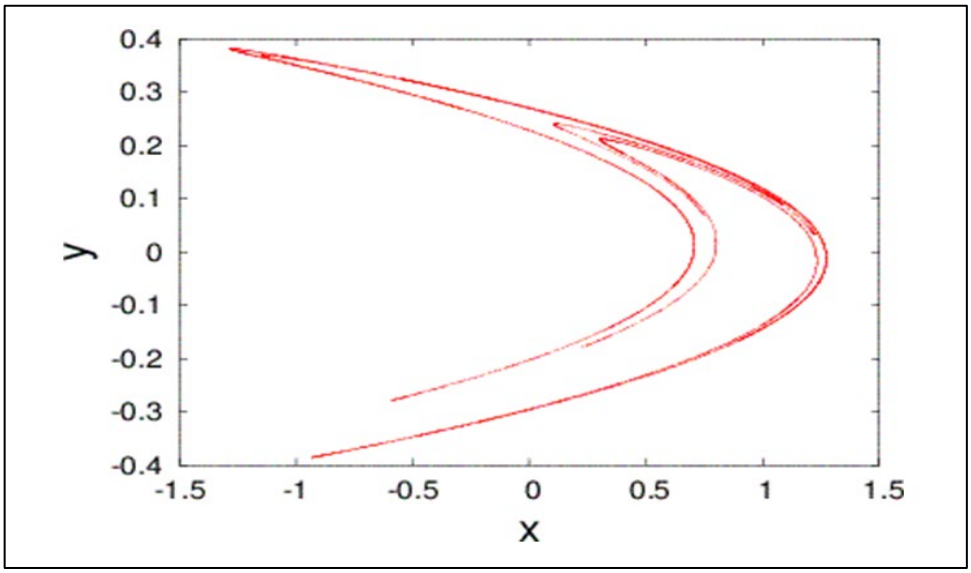

Figure 1: Phase Plot of the Henon map with a = 1.4, b = 0.3

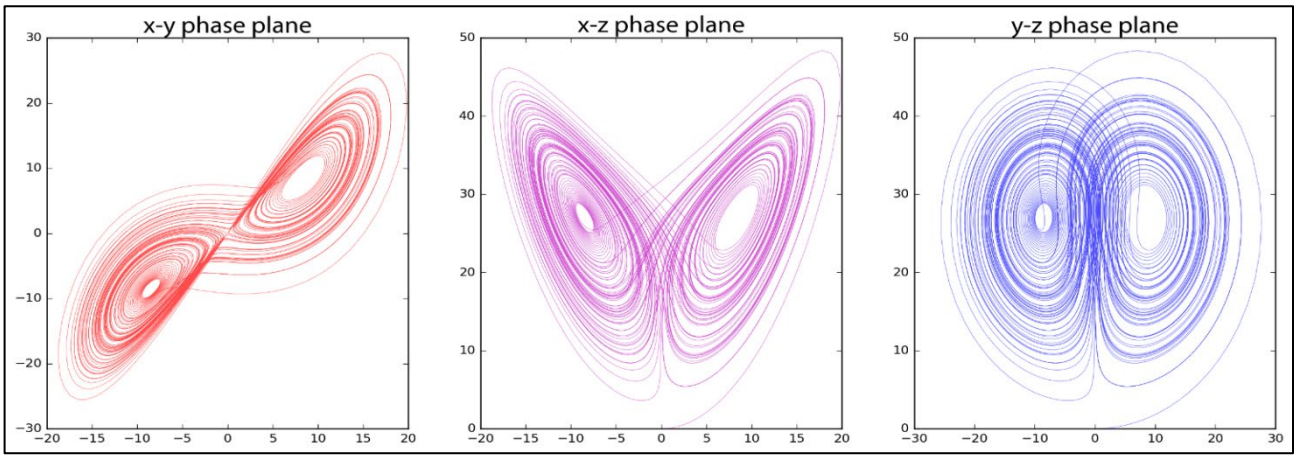

Figure 2: The projections of attractor on the planes (a) x-y, (b) x-z and (c) y-z

4. The Encryption and Decryption Process

Due to the strong correlations amongst neighboring pixels in the plain image, this study suggests shifting the pixel positions in such images to solve such problems and breaking the pixels' correlations. The 2D-Henon map and 3D-Lorenze Map generated a huge number of random keys (about 20,000 random numbers) used in the encryption/decryption process. Without loss of generality, a plain image's dimensions will be set as N × N. The proposed method focuses on diffusion and confusion principles to break the pixels' correlations. A new S- Box design will increase the confusion.

4.1 S-Box Generator

This work suggests designing a new S-Box using a 2D Hénon map; this operation provides more excellent protection and complexity to generate a new large S-Box [16 X 16] by using a 2D Henon Map, first using initial value X_0 to chaotic map and

creating numbers with (0-255), S-Box production mechanism by generating Henon system values, all values within the S-Box must be unique. Suppose the value is greater than the appropriate area. In that case, the rest of the section has been taken to that value. It produces the S-Box inverse simultaneously since the "responsive dependency on initial state" with chaos theory changes the construction of the S-Box and the result of dynamic S-Box inverse with every slight change in initial value.

4.2 Encryption Algorithm

The details of the image encryption are indicated below in Figure 3:

Step 1 Shift the rows based on the value of Yi (generated by the 3D-Lornez System), then XORed the resulting matrix with Yi value.
Step 2 Replace the rows with columns, then XORed the resulting matrix with Zi value (generated by 3D-Lornez System).
Step 3 Shifting columns based on Xi (generated by 3D-Lornez System), then XORed the resulting matrix with Xi value.
Step 4 To increase confusion, generate a new S-Box (16 × 16) that depends on the 2D Hénon map for its unique values and non-linearity, then insert this S-Box into the matrix generated above.
Step 5 Finally, the cipher and ambiguous images are created.

4.3 Decryption Algorithm

The details of the image decryption are as follows:

Step 1 Substitute in the image matrix based on the inverse S-Box generated from the 2D Hénon map.
Step 2 XORed the resulting matrix with Zi (generated by 3D-Lornez System), then replaced rows and columns.
Step 3 XORed the resulting matrix with Yi value (generated by 3D-Lornez System), then shifted columns based on Yi value.
Step 4 XORed the resulting matrix with Xi value (generated by 3D-Lornez System), then shifted columns based on Xi value.
Step 5 Finally, extract the plain image with a slight difference in resolution.

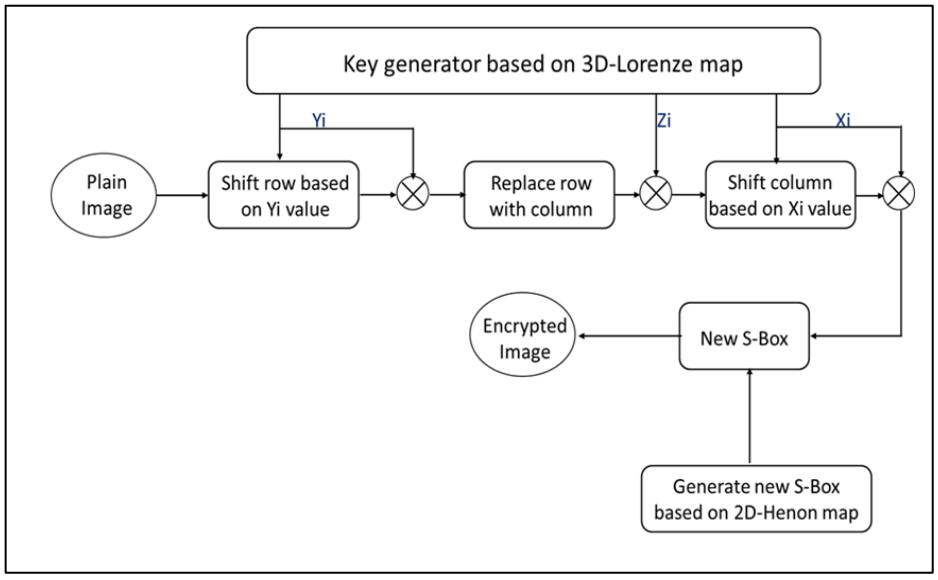

Figure 3: Diagram of Proposal Encryption algorithm

5. Results and Discussion

The simulation results in proposals in this section were implemented on a Lenovo laptop computer with the following specifications: Intel (R) Core (TM) i7-8565U @1.80GHz 1.99GHz, installed RAM 8.00 GB, hard disk SSD 256 GB, Windows 10 Enterprise 64 Bits, and Visual Studio 2019 with C# programming software. To evaluate the proposed method, eight images of varying sizes and types of bitmap (BMP) are used; to resist brute-force attacks, the keyspace utilized to secure the image cryptosystem must be adequately large. This section discusses the results of the suggested encryption algorithm with its new S-Box in terms of statistical accuracy and the encrypted image. The base of the cryptographic block cipher is confusion; the plain image blocks are transformed into cipher-image blocks, building on the 2D Hénon map key for the XOR operation. Small changes in initial parameters or conditions lead to changes in the final encryption image. Diffusion is then used to shift the

cryptographic block cipher; several digits in the ciphertext can affect every digit of the plain image and every digit of the hidden key.

Figure 4 shows the plain images of Goldhill (256 × 256), Airplain (512 × 512), boat (560 × 560), and Lenna (755 × 755) Figure 4 is used in the proposed approach, with different image sizes and quality tests for evaluating the efficiency and security of our proposed system. In particular, we used Picture Quality Evaluation (PQE), randomness tests, and an Image Quality by Entropy evaluation. The pixel strength diffusion measurements for a picture are represented in a histogram. A secure encryption system should provide evenly balanced histograms in order to survive statistical attacks. The histograms in Figure 4 (a, b, c, d) are for the Goldhill, Airplane, Boat, and Lenna pictures in their original and encrypted forms. It can be seen that the histograms of the regular images could be more well-balanced, whereas the histograms created from the encrypted digital images are evenly balanced.

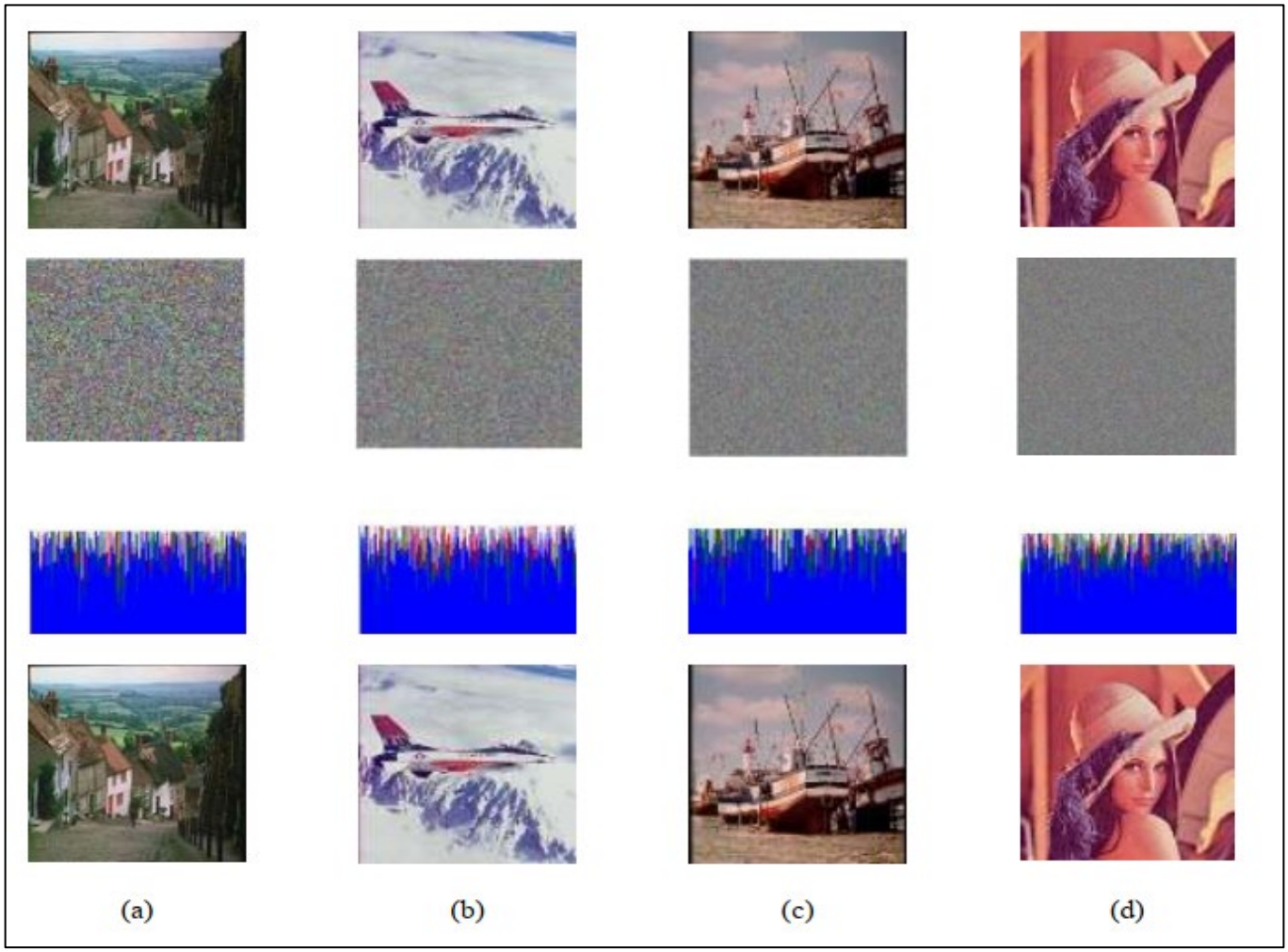

Figure 4: Simulation results. (a) Goldhill (b) AirPlain (c) Boat (d) Lenna

5.1 Picture Quality Evaluation (PQE) Metrics

With regard to encoded and decoded image quality measurements, the Picture Quality Evaluation (PQE) should be utilized. As shown in the image below, these metrics have been implemented in this study. Table 1 shows the twelve Mean Square Error (MSE) measurements. A Mean Square Error (MSE) value should be significant because it indicates the difference between the plain and cipher images [16], and all images have large values. The Peak Signal to Noise Ratio (PSNR) formula then uses these Mean Square Error (MSE) values to calculate the maximum probable signal and noise powers ratios. Furthermore, the Average Difference (AD) shows the difference between the plain and cipher images, and when it is divided by the Mean Square Error (MSE), the resulting Maximum Difference (MD) shows the maximum error between the plain and cipher images after both images have been converted to grey images with ranges 0-255. The Normalized Cross-Correlation (NC) between the decryption and the plain image should be significant because it shows the difference between the plain and cipher images. In contrast, the Mean Absolute Error (MAE) provides the same information provided by the MSE. However, instead of using the squared differences between the plain and decrypted images, the Mean Absolute Error (MAE) will be one of the plain and decrypted images with no differences and less than one otherwise. The Signal-To-Noise Ratio (SNR) includes all electric signals between the plain and encrypted images, the Similarity Measure (SIM) conveys the same information conveyed by the MSE, and the Encryption Quality (EQ) measures the encryption quality. All the images show good results.

Table 1: PQE Metrics for Encrypted Images

Name	MSE	PSNR	AD	MD	NC	MAE	NAE	SC	NSR	SLM	CC	EQ
Goldhill	9745.84	0.0049	5954.69	224	0.331	11909.38	0.3310	1.4302	1.7378	118.2	0.00468	16248
Airplane	10327.98	0.0046	6494.38	214	0.360	12988.77	0.3605	0.5194	1.6655	155.7	0.00265	70167
Boats	9041.214	0.0053	5125.18	247	0.284	10250.37	0.2848	1.0131	1.8737	133.4	0.00544	69582
Lenna	9016.81	0.0053	3701.33	211	0.205	7403.39	0.2059	1.0429	2.2034	129.2	0.00026	12609

5.2 Encryption and Decryption Running Time

As can be seen in Figure 5, it takes a few milliseconds for the encryption and decryption of each image. We used different sizes of images (Goldhill=256*256, Airplane=512*512, Boats 560*560,
Lenna 755*755).

The running time is 1 second when the plain and decrypted images have no differences and less than 1 second otherwise. The SNR includes all electric signals between the plain and encrypted images, the SIM conveys the same information the MSE conveys, and the EQ measures the encryption quality. All the images show good results.

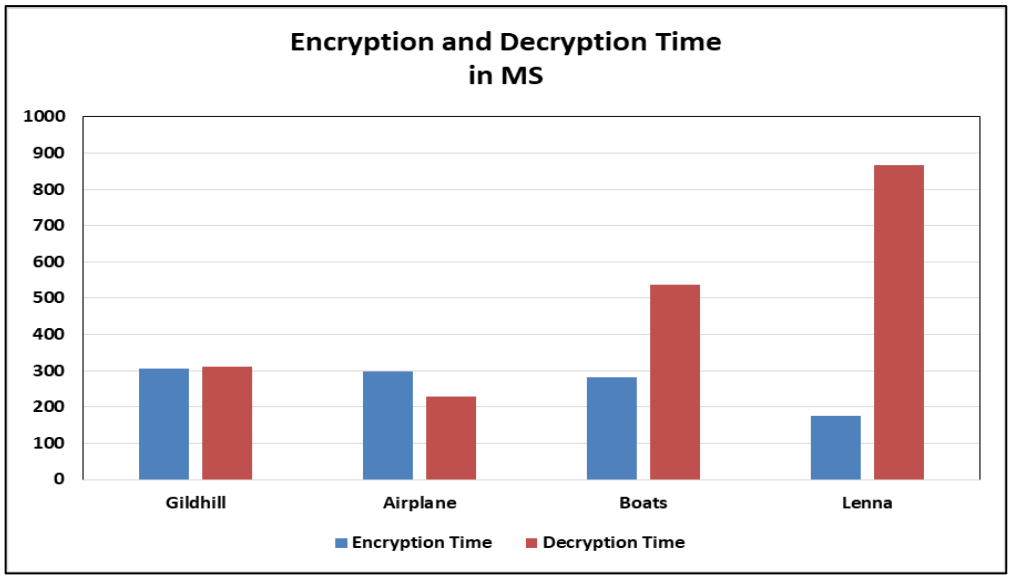

Figure 5: Encryption and Decryption Running Time of the proposed algorithm

5.3 S-Box Performance Analysis

Typical statistical criteria include the Non-Linear Stage, Correlation Immunity, Algebraic Degree, Algebraic Complexity, Bijection, Strict Avalanche Criteria (SAC), Non-Linearity, Differential Uniformity, Power Mapping, Balanced Criteria (BC), and the Avalanche Criteria (AC) [17]. This paper evaluates the new S- box with three criteria, shown in Table 2.

Table 2: AC, BC, and SAC comparisons

System	AC			BC		SAC		
	0.33	0.570	0.8175	32	32	0.33	0.57	0.817
	0.25	0.5	0.75	32	32	-	-	-
	0.125	0.5	0.875	29	35	0.125	0.5	0.875
	0.25	0.875	0.56	31	33	0.25	0.5	0.75

5.4 Differential Attack Analysis

The Number of Modifying Pixel Rates (NPCR) and Unified Average Adjusted Intensity (UACI) are utilized to estimate the strength of the image encryption algorithm/code in terms of differential attacks [14,15]. The results are shown in Table 3.

Table 3: Randomness Tests

Picture	NPSR	UACI
Goldhill AirplaneBoats	0.9941	0.341
Lenna	0.9961	0.356
	0.9950	0.332
	0.9961	0.336

5.5 Information Entropy

The entropy of information also is important when calculating the randomness of the cipher file. The H (s) entropy is given by Equation 3:

$$(S) = -\sum_{i=0}^{2^{n-1}} p(s_i) log_2 2\, p(s_i) \quad (3)$$

Here, p (si) is the probability of s. H (s) should be 8 for a 2-1 grey cipher-8 picture displaying random knowledge. As shown in Table 4.

Table 4: Information entropy

Name	Inf. Entropy
Our proposed	7.9953
Goldhill	7.9971
Barbra	7.9936
Boats	7.9961
Lenna	7.9973

5.6 Comparison with Other Researchers

This section shows the comparison image of Lenna with other papers. For calculating correlation coefficients between a plain image and a cipher image and its corresponding cipher image, the result for the image (Lenna) is listed in Table 2. Clearly, our algorithm has the smallest value of (CC) than the algorithms explained in section 2, as shown in Table 5.

Table 6 shows the NPSR values for our proposed system and other systems [16,17,14], and Table 7 shows the UACI values for our proposed system and other systems [9,10,11].

Table 5: Correlation Coefficients (CC) comparisons among different algorithms

System	Lenna
The proposed algorithm	0.00026
Ref [9]	0.00032
Ref [10]	0.00114
Ref [11]	0.0055

Table 6: NPSR comparisons among different algorithms

System	Lenna
The proposed algorithm	0.9961
Ref [9]	0.996
Ref [10]	0.990
Ref [11]	0.996

Table 7: UACI comparisons among different algorithms

System	Lenna
The proposed algorithm	0.336
Ref [9]	0.335
Ref [10]	0.335
Ref [11]	0.334

The entropy values in Table 8 are close to this ideal value. Thus assume that the proposed algorithm is strongly random.

Table 8: Information entropy comparisons among different algorithms

Image	Lenna
The proposed algorithm	7.9973
Ref [9]	7.997
Ref [10]	7.997
Ref [11]	7.997

In this study, we have comprehensively analyzed the proposed image encryption method based on a chaotic map and a new S-Box, considering several significant limitations. Firstly, we conducted a thorough security analysis; our results indicate that the proposed method demonstrates robustness against these attacks. Secondly, we ensured the encryption method accommodates a large key space, making it resilient to exhaustive key search attacks. Moreover, we assessed the sensitivity of the encryption scheme to variations in the encryption key and found that minor changes have minimal impact on the security of the encryption. Furthermore, we conducted extensive performance evaluations, confirming that the proposed method exhibits reasonable computational complexity and execution speed, making it practical for real-time applications. Additionally, we

conducted a statistical analysis of the generated encryption keys and cipher texts, demonstrating the randomness and absence of biases, correlations, or patterns that could compromise the security of the encrypted images. Lastly, we compared our proposed method with existing encryption techniques, identifying and addressing vulnerabilities based on known cryptanalytic techniques. By addressing these limitations, our study contributes to developing a secure and efficient image encryption method.

6. Conclusions

In this paper, we have implemented a high-performance and efficient image security encryption method that is based on a chaotic system and shuffling scheme; the first step is the shifting process, then XOR after that replaced rows with columns then shifting process then XOR for more diffusion and more confusion the S-Box process. The security analysis performed was sensitive with initial value and a high speed in encryption processing. Compared with some other encryption schemes, the NPCR and UACI show high efficiency and ideal entropy, where the histograms of the cipher image indicate the robustness of the encryption method to withstand the attackers.

Author contributions

Conceptualization, A. Abdallah. and A. Farhan; methodology, A. Abdallah. and A. Farhan; software, A. Abdallah. and A. Farhan; validation, A. Abdallah. and A. Farhan; formal analysis, A. Abdallah. and A. Farhan; investigation, A. Abdallah. and A. Farhan; resources, A. Abdallah. and A. Farhan; data curation, A. Abdallah. and A. Farhan; writing—original draft preparation, A. Abdallah. and A. Farhan; writing—review and editing, A. Abdallah. and A. Farhan; visualization, A. Abdallah. and A. Farhan; supervision, A. Farhan; project administration, A. Abdallah. and A. Farhan. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability statement

The data supporting this study's findings are available on request from the corresponding author.

Conflicts of interest

The authors declare that there is no conflict of interest.

References

[1] X. Wu, D. Wang, J. Kurths, H. Kan, A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system, Inf. Sci., 349–350 (2016) 137-153. https://doi.org/10.1016/j.ins.2016.02.041

[2] E. A. Albahrani, A new audio encryption algorithm based on a chaotic block cipher, Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, Iraq, 2017, 22-27. https://doi.org/10.1109/NTICT.2017.7976129

[3] X. Wang, H.L. Zhang, A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems, Nonlinear Dyn., 83 (2016) 333–346. https://doi.org/10.1007/s11071-015-2330-8

[4] T. Ahmed, E.M.E.Mostafa, F. Yasser, B. Ahmed, Using Chaotic Maps to Enhance RSA Public Key Cryptography, Sci.Int. (Lahore), 30 (2018) 711-715.

[5] Z. Xiaoqiang, W. Xuesong, Multiple-Image Encryption Algorithm Based on the 3D Permutation Model and Chaotic System, Symmetry, 10 (2018) 660. https://doi.org/10.3390/sym10110660

[6] A. Shokouh Saljoughi, and H. Mirvaziri, A new method for image encryption by 3D chaotic map, Pattern Anal. Appl., 22 (2018) 243–257. https://doi.org/10.1007/s10044-018-0765-5

[7] Z. Hua, F. Jin, B. Xu, and H. Huang, 2D Logistic-Sine-coupling map for image encryption, Signal Process., 149 (2018) 148–161. https://doi.org/10.1016/j.sigpro.2018.03.010

[8] A.T Sadiq, A.K. Farhan, S.A .Hassan. A proposal to improve the RC4 algorithm based on hybrid chaotic maps, J.Adv. Comput. Sci. Technol. Res., 6 (2016) 74-81.

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

[10] J. Khan, J. Ahmad, and S. O. Hwang , An efficient image encryption scheme based on: Henon map, skew tent map and S-Box, 6th Int. Conf. Model., Simulation, Appl. Optim., 2015,1-6.https://doi.org/10.1109/ICMSAO.2015.7152261

[11] H. Liu, B. Zhao, L. Huang ,Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling, Entropy, 21 (2019) 343.https://doi.org/10.3390/e21040343

[12] 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, 8 (2020) 54175-54188.https://doi.org/10.1109/ACCESS.2020.2979827

[13] 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, 21 (2019) 656.https://doi.org/10.3390/e21070656

[14] 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, 6 (2018) 133. https://doi.org/10.1140/epjp/i2018-11834-2

[15] A. Kadhim F. and H. Emad M. 2017. Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers, Diyala J. Pure Sci., 13 (2017) 24–39. https://doi.org/10.24237/djps.1303.268b

[16] M. Hassan, and A. Kadhim, New Image Encryption Based on Pixel Mixing and Generating Chaos System, Al Qadisiyah J. Pure Sci., 25 (2020) 1-14. https://doi.org/10.29350/qjps.2020.25.4.1182

[17] 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, 27 (2018) 080701. https://doi.org/10.1088/1674-1056/27/8/080701