Available at https://www.iasj.net/iasj
Iraqi Academic Scientific Journals
Journal homepage:
https://journals.uokerbala.edu.iq/index.php/UOKJ

Research Article

Hindmarsh-Rose Model for Efficient Image Encryption

Estqlal Hammad Dhahi
Information Technology Center, University of Kerbala, Kerbala, Iraq

Article Info
Article history:
Received 6 -3-2025
Received in revised form19-3-2025
Accepted 22-12-2024
Available online 13 -4 -2025
Keywords: Image encryption, Image Decryption, Hindmarsh-Rose map, S-box, permutation

Abstract

Image is one type of multimedia data that is shared via networks and social media, to secure it needs an effective method for confidentiality. Image encryption is a powerful and effective tool for protecting visual data in an era of increasing reliance on technology and the propagation of security threats. With advances in encryption algorithms, it has become possible to secure images while maintaining system performance effectively. As the importance of visual data continues to grow, image encryption will remain a key component of information security strategies. An efficient method for color image encryption based on Hindmarsh-Rose map is proposed. The method used a dimension sequence for different stages of the encryption algorithm such as the first sequence used in block permutation, the second dimension used in S-boxes generation, and the third sequence used in the diffusion process. The proposed method results in accurate results in terms of visualization tests, objective tests, correlation tests, key space analysis, and randomness tests. The proposed method could be applied for audio and video encryption.

Corresponding Author E-mail : estqlal.h@uokerbala.edu.iq
Peer review under responsibility of Iraqi Academic Scientific Journal and University of Kerbala.

1. Introduction

Data security has become a prime concern in today's networking world since the rapid growth of network-enabled devices [1-3]. Keeping the data secured when transmitted over a network has become an utmost need. One of the best alternative ways is encryption to ensure security in data communication [4-6]. There are many encryption algorithms present today, the major drawbacks of the existing algorithms are that they are computationally intensive and consume more time to encrypt data. Hence there is a need to develop a new encryption algorithm, which is simple and efficient in terms of speed as well as security [7-9]. Images have become a vital part of communication in today's world. With the advancement of technology, various multimedia-based applications are available [10]. Users can send and receive images, video clips, audio clips, etc., through the networks. Digital images contain sensitive information that necessitates restricting unauthorized access. Hence protection of images during transmission has become a major concern. In recent years, many image encryption algorithms have been proposed and some of them are vulnerable to attacks [11]. The Internet of Things (IoT) includes smart items with limited energy, memory, and computational capacity. An efficient network structure is necessary for these devices to process multimedia data, which includes audio, video, and images. Lightweight encryption is requested to satisfy the limitation in the IoT networks [12]. Several lightweight encryption methods are available for safeguarding IoT devices, which makes choosing the best LWC algorithm difficult. AES, SIMON, PRESENT, and ASCON are a few popular lightweight encryption methods for IoT ecosystems that have demonstrated encouraging results in terms of effectiveness, security, and energy consumption [13].

2. Background Theory

The background theory is represented by the following concepts:

2.1. Hindmarsh-Rose Model

A strong framework for comprehending the intricate dynamics of neuronal firing is offered by the Hindmarsh-Rose model [14]. It is a useful tool for neuroscience simulations and theoretical research because it combines simplicity with the capacity to mimic physiologically significant actions. A mathematical model called the Hindmarsh-Rose model is used to explain the electrical activity of neurons, with an emphasis on bursting and spiking characteristics [15]. The intricate dynamics found in biological neurons are captured by this model. The Hindmarsh-Rose model consists of a system of three coupled ordinary differential equations:

$$\frac{dx}{dt} = y + a \cdot (b \cdot x - x^3) + I \quad \dots (1)$$

$$\frac{dy}{dt} = c - d.x - y \quad \dots (2)$$

$$\frac{dz}{dt} = r.(x - x_r) - z \quad \dots (3)$$

Where x: is the membrane potential of the neuron, y is the recovery variable that represents the activation of potassium currents, z is the adaptation variable linked to slow recovery processes, I is an input current, and the set (a, b, c, d, r) are parameters that influence the dynamics of the system [16]. The hind-Marsh behavioral model is explained in Figure 1.

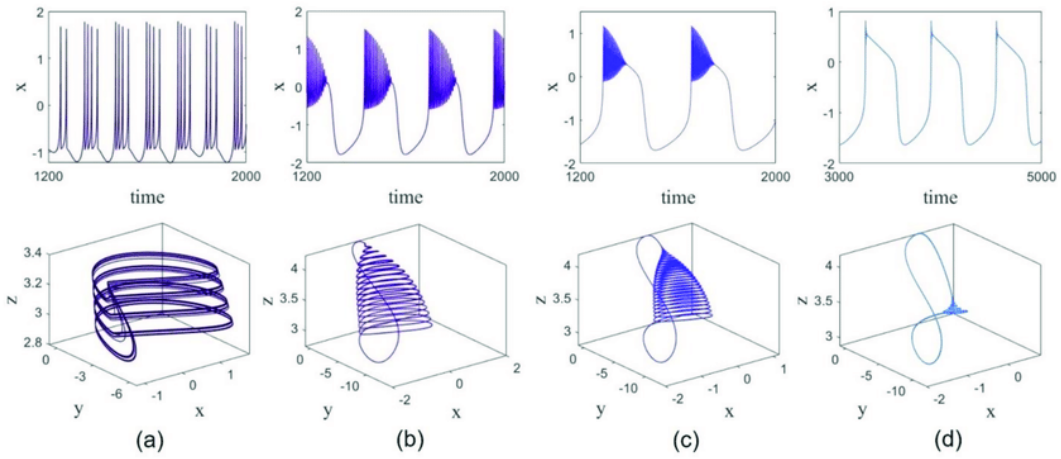

Figure 1: The Hind-Marsh chaotic behavior model [9]

The behavior of the Hindmarsh-Rose model can be exhibited based on parameters in neurons that produce discrete action potentials called spiking. The neuron fires a series of action potentials followed by periods of quiescence called dursting and chaotic dynamics through certain conditions [17].

2.2. Image Encryption

Color digital image encryption is the process of converting an image into a form that can only be read using the appropriate decryption key. Color images require additional processing compared to grayscale images because they contain multiple color channels (usually red, green, and blue RGB). Chaotic Image Encryption is a type of image encryption technique that relies on chaotic systems to generate random sequences used in the encryption process. This method is highly sensitive to initial conditions, making it suitable for secure cryptographic applications. Here is a detailed explanation of chaotic image encryption [18-20].

3. Related Work

The associated work of the suggested approach is essential to explain how it contributes to the subject, fills in knowledge gaps, and offers fresh application possibilities. Emphasizing the advancements and enhancements over earlier research will bolster the argument for the suggested approach and emphasize its importance in the field of chaotic systems and their uses:

Wu, Wanqing, and Qiao Wang [21] suggested the use of SHA-2 to generate the logistic map's initial parameters based on the plaintext image, a pre-shared key, and an initialization vector (IV). The confusion and diffusion are based on the random integers generated by the logistic map. The security, quality, and efficiency using a correlation coefficient, chi-square, entropy, mean square error, mean absolute error, peak signal-to-noise ratio, maximum deviation, irregular deviation, deviation from the uniform histogram, number of pixels change rate, unified average changing intensity, resistance to noise and data loss attacks, homogeneity, contrast, energy, and key space and key sensitivity analysis.

- **Elkandoz, Marwa Tarek, and Wassim Alexan. [22]** suggested. A shuffled image is first created by rearranging the pixels, and it is then spread by XORing its pixels with a secret key. A variety of chaotic maps are combined to create this key. Several indicators are used to assess the suggested scheme's

performance. It is demonstrated that the suggested strategy is resilient to both statistical and differential attacks. Its efficiency and adaptability for real-time applications are ensured by its extremely short running time.

- **Pourasad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani [23]** suggested a chaos sequence and wavelet transform value. As a result, an innovative method for encrypting digital images was put out, which enhanced earlier methods. Numerous performance indicators, including the Number of Pixels Change Rate (NPCR), Peak Signal to Noise Ratio (PSNR), Correlation coefficient, and Unified Average Changing Intensity (UACI). The efficiency of the suggested scheme is demonstrated by the simulation and theoretical analysis, which also demonstrates that this method is a good fit for real-world picture encryption.

- **Yan, Shaohui, et al. [24]** DNA coding, four-dimensional chaotic systems, and suggested two-dimensional chaotic mapping all raise the system's complexity and randomness while enhancing the encryption algorithm's security. It breaks the correlation of the RGB pixels of the three channels by increasing disorder organization, then uses the chaotic sequence created by the repeating of the four-dimensional chaotic system in the DNA encoding encryption. The algorithm is unaffected by the attack (brute-force) exhaustive attacks by examining the key space and key sensitivity. Test experiments demonstrate that this method is competitive with other algorithms and has a good level of security.

- **Girdhar, Ashish, Himani Kapur, and Vijay Kumar [25]** To attain a relatively high level of encryption, this research suggests a picture encryption technique that uses three chaotic sequences. The algorithm created to accomplish both the permutation and replacement procedures of picture encryption is what makes the suggested method novel. Ultimately, a comparison of the coefficient correlation values is made to assess how well the suggested method performs in comparison to several recently presented picture encryption schemes.

4. Proposed Methodology

The proposed method is designed to encrypt colored images based on generating keys using Hindmarsh-Rose Map, which is used to generate three-dimensional keys. Each dimension is used in the encryption stage (confusion and diffusion). The first dimension is used in the process of redistributing the blocks that are cut from the colored images. The second dimension is used in the process of building the substitution boxes (S-boxes). The third stage is used in the diffusion stage the exclusive-or process in the blocks. Then, these blocks are reassembled in matrices equal to the size of the input image from three layers. Then, these layers are combined to generate the encrypted small. The framework of the proposed method is explained in Figure 2.

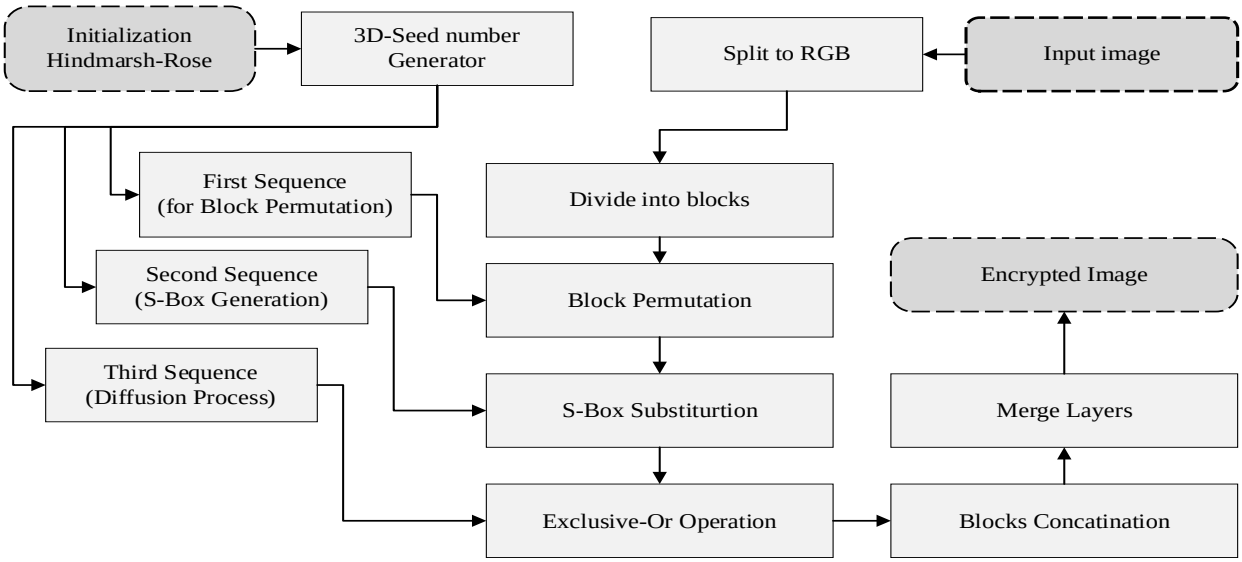

Figure 2: a general framework of the proposed method

- **3D-Seed number generation**

At this stage, the necessary keys are generated by encrypting the image through the equations of the proposed chaotic function, and the first dimension is for redistributing the blocks in the image. The second dimension is for generating the compensation tables in the proposed algorithm, and each table is for a specific block. The third dimension is for performing the X-O operation after completing the previous stages, the plotting of the dimension sequences is explained in Figure 3.

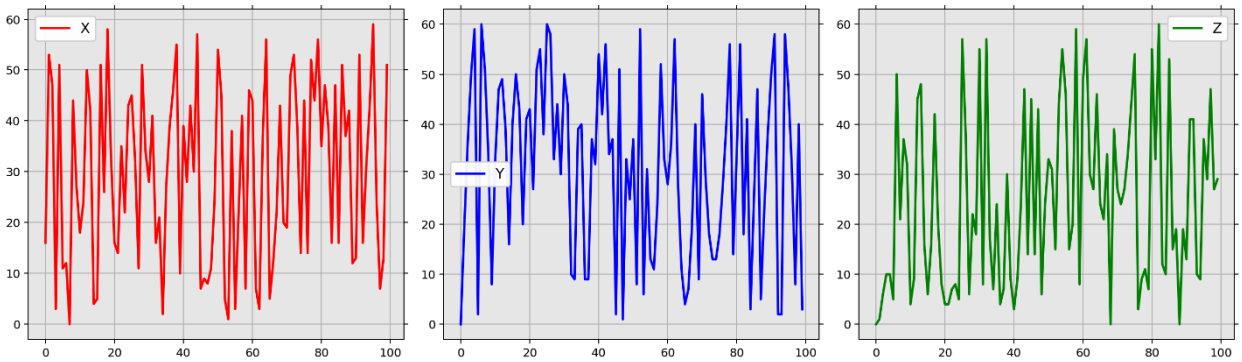

Figure 3: 3D-sequences generation based on Hindmarsh-Rose map

- **Split image into RGB**

In this step, the input color image is separated for the encryption process into its main layers, as shown in Figure 4. The image is divided into the main layers, red, green, and blue.

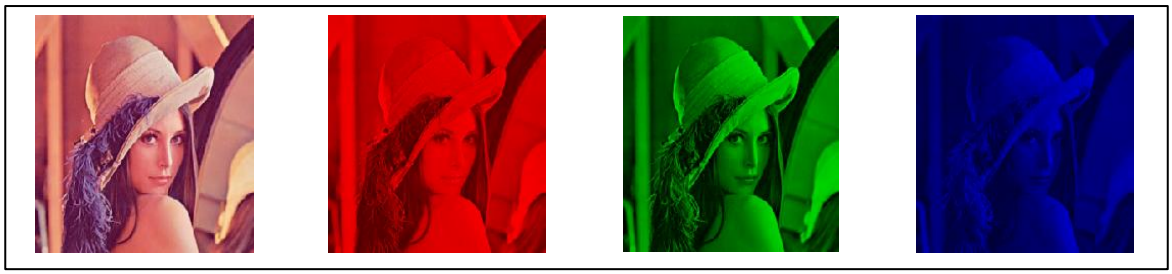

Figure 4: split color image into three band colors (RGB)

- **Dived image into blocks**

At this stage, each layer of the separated colored chest layers is cut into equal parts into equal blocks, which are 8, 16, or 32, depending on the choice used, as shown in Figure 5.

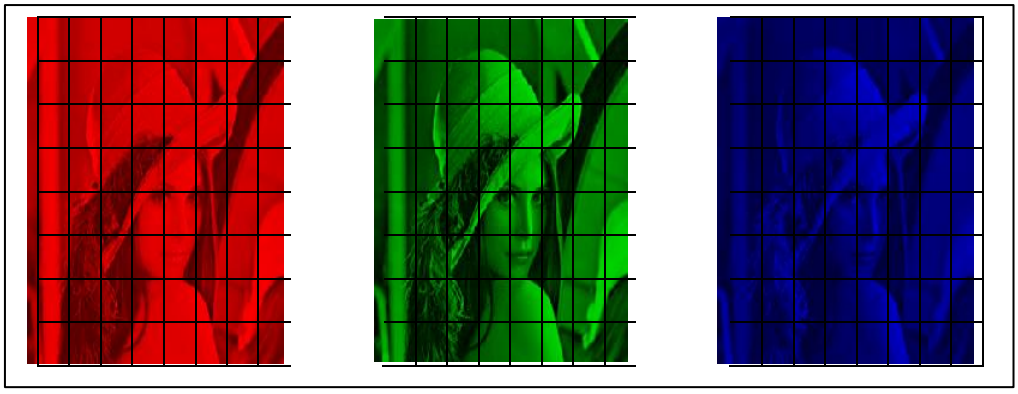

Figure 5: block partition of RGB color bands

- **Block Permutation**

At this stage, a set of numbers generated in India March Rose and the first dimension are taken, and the number of these numbers is equal to the number of blocks present in the soda. These numbers are arranged in ascending or descending order, and then the block number that enters the encryption process is assassinated through the location of the number present before the arrangement process. Thus, this process is the process of selecting blocks that enter the encryption process. It is not sequential, as the process.

- **S-Box Substitution**

At this stage, the image is taken. At this stage, the numbers generated from the second unit are taken to generate compensation tables. The method is to take the first 256 numbers and arrange them in ascending or descending order according to the user's choices. They are redistributed, and arranged in ascending or descending order, and the locations of these numbers are taken to convert them to the 16-bit format and placed in a table from two dimensions. These numbers are a 16-by-16 table (as explained in Table 1) that is used in the encryption process. To make this table unstable, the remaining numbers are relied upon in the process of moving this table to the right or the left according to the existing numbers. Each number is used to encrypt these numbers and obtain different tables. Each table is specific to one of the existing blocks.

Table 1: proposed Substitution Box S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	27	E4	C8	69	24	C5	A8	C	DD	B3	9B	4A	BE	23	CD	B9
1	F0	AB	D5	5D	7F	5C	45	63	51	D2	5A	94	D7	A0	E6	91
2	DF	41	2D	95	FF	3E	88	8	3B	49	1C	37	4B	54	A9	FB
3	52	D0	8B	B2	48	E	57	11	42	46	80	9	A1	F9	13	C0
4	6B	85	34	8A	D9	83	AA	38	2F	C2	E9	B6	43	59	40	100
5	AF	58	E5	7A	60	DB	7B	21	E8	4	D4	53	28	4E	F4	1B
6	6F	87	A7	61	18	ED	D3	31	F5	CA	50	E2	CE	93	AE	98
7	2	AC	4C	2C	8D	39	16	BF	EB	55	C3	6C	F2	F8	22	FC
8	67	BC	BD	C6	71	DE	72	44	5E	8E	7D	9A	33	7	30	A3
9	D1	EF	96	6E	99	76	6A	4D	FD	5	79	19	97	65	70	B4
A	BA	14	9D	32	1	73	C1	82	5B	EC	17	2A	6D	E3	12	89
B	29	E7	81	EE	FA	A6	A5	77	8C	B7	20	CC	64	2B	F	DA
C	84	F3	3	3C	86	7E	A4	10	F7	26	7C	8F	CB	B1	9C	66
D	92	15	3D	A	6	B0	EA	1E	CF	74	35	C4	F1	BB	56	3F
E	1A	75	C9	F6	D	3A	AD	FE	25	36	A2	9E	62	D6	5F	C7
F	78	1F	2E	4F	B	9F	B8	D8	1D	E0	B5	E1	68	DC	47	90

Shift(1)	Shift(2)	Shift(3)	Shift(4)	Shift(5)	Shift(6)	Shift(7)	Shift(8)	…	Shift(n)
42	90	3	1	76	65	41	73	…	89

- **Exclusive-Or generation**

At this stage, every single building of the flux inside the currency formation process is done by taking a set of numbers equal to the number of pixels present in the number of pixels present in the block and then working on the exploration to produce numbers different from the existing numbers.

- **Blocks Concatenation Merge Layers**

At this stage, the encrypted parts of the block image are combined horizontally and vertically to obtain a two-dimensional matrix representing one of the colors of the colored images. Three parts are formed, three halves, each representing the primary colors: red, green, and blue. The three matrix layers that represent the basic brigade are combined to form the encrypted image, which is stored in storage media or transmitted over networks.

5. Experimental Results

Testing the suggested method on a series of standard images, the images of Lenna, Baboon, Flight, Pepper, and Woman, respectively which represent the experiment outcomes. As seen in Figure 6, the first test is the histogram test, which is used on both plain and encrypted photos.

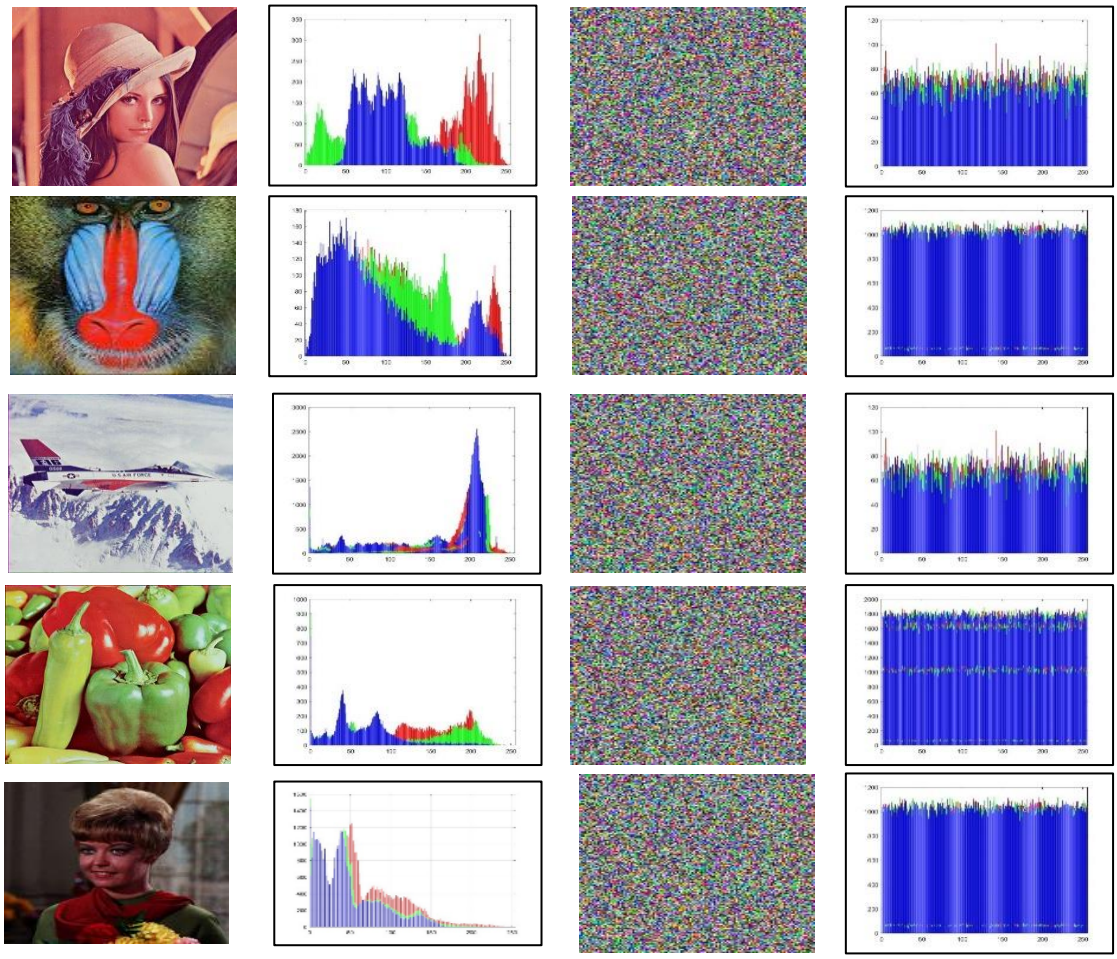

Figure 6: visual encryption test

The histograms of the results photos, which appear to have a uniform shape and simple photographs are contrasted in the preceding figure. The histogram's uniform shape indicates that there is no association between the results' values, no curve, and no superiority of one value over another. Applying the correlation test to the three-color band of an input image and an output image (encrypted image) is the second test.

The colors red, green, and blue were all subjected to the test. As seen in Figure 7, the correlation is used in three different ways: horizontally, to test a pixel with a neighbor in a row; vertically, to test a pixel with a neighbor in a column; and diagonally, to test a pixel with a neighbor in a diagonal.

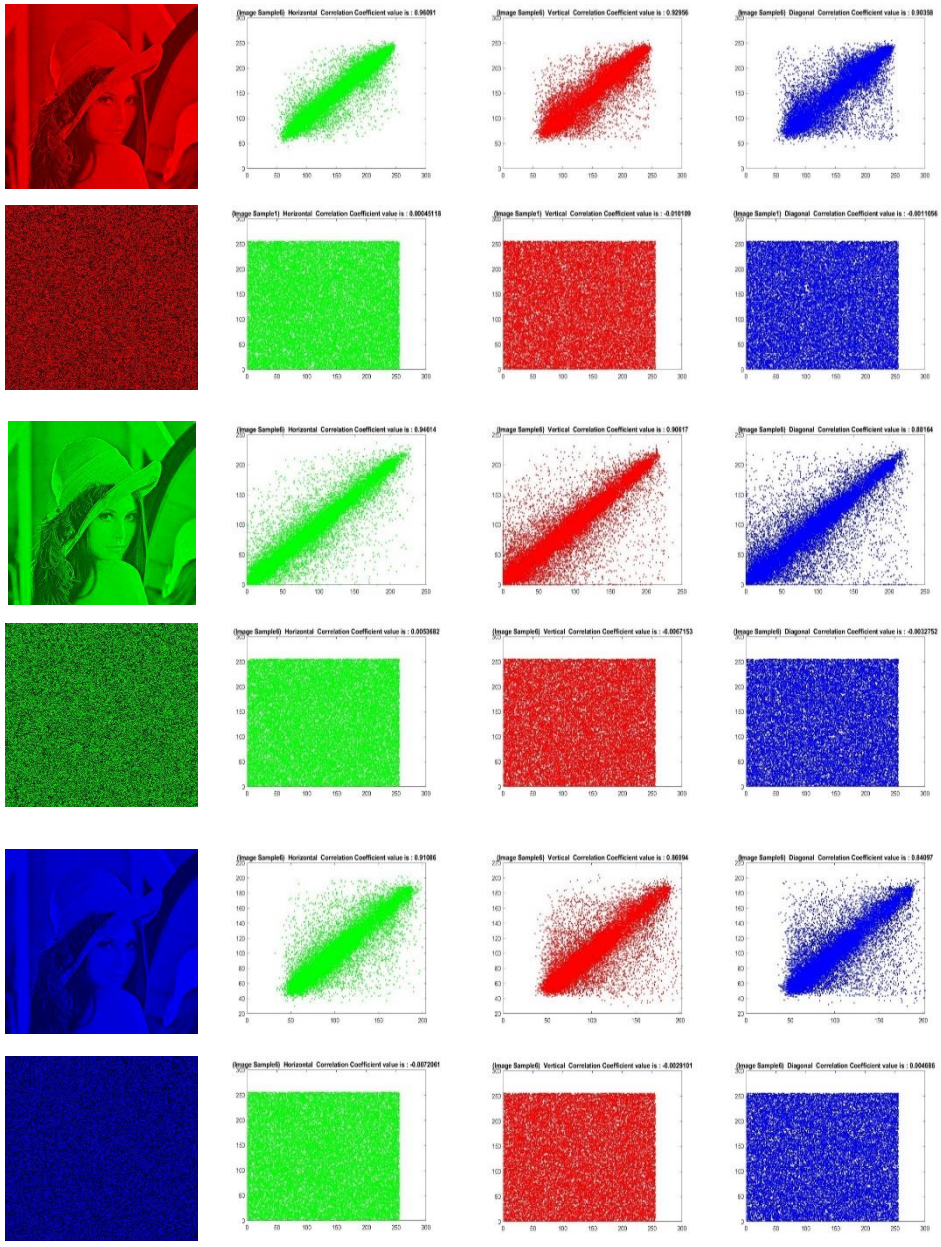

Figure 7: correlation test for Lenna image

The proposed encryption algorithm breaks the correlation in three directions of the three color bands, the input images have strong correlations in all bands and in all directions which means it resists brute force attack. Other tests are applied to the imaged dataset (objective tests) for analyzing the efficiency of a proposed method such as mean squared error MSE which measures the similarity between the plain image and encrypted image. Mean Squared Error (MSE) is one such commonly used metric, and it measures the average squared difference between the original (plain) image and the encrypted image as explained in Table 2.

Table 2: the measurement of the objective test (Image quality) of the test images

#	Entropy	MSE	PSNR	SNR	SIM
1	7.9921	7940.5606	0.0045	1.8886	109.4344
2	7.9973	7731.6393	0.0048	1.6307	102.6207
3	7.9917	9276.8136	0.0040	1.4510	136.8472
4	7.9916	8516.1755	0.0043	1.7553	109.7188
5	7.9913	8044.7967	0.0047	1.7651	120.8542
Av	7.9908	8301.9971	0.0045	1.6981	115.8950

The key test represented by several tests such as; key-space analysis is used for preventing the attack called brute force attack, the key-space should be greater than 2^{128}, and the key-space is found from the initial parameters of the Hindmarsh-Rose are (x_i, y_i, z_i, c_1, c_2, c_3), where the precision of each is 10^{10}, and the key-space is calculated as $(10^{10})^6 \approx 2^{199}$, demonstrating that the encryption system is resistant to brute force assaults and that the key-space is vast. This system may therefore be trusted to generate keys that are more resilient to the aforementioned threats, and for the same reason, it can be trusted to initiate encryption and decryption processes.

The measurement of the required time for the encryption and decryption method is depicted in Table 3, the time is calculated in seconds.

Table 3: The measurements of time for the proposed encryption/decryption method

	Time of image (128x128)		Time of image (256x256)		Time of image (512x512)	
#	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
1	0.00179	0.007141	0.004344	0.001784	0.015986	0.005107
2	0.001391	0.003588	0.004752	0.002012	0.011383	0.004405
3	0.001046	0.001705	0.004276	0.001596	0.009903	0.005306
4	0.001177	0.002766	0.005185	0.001587	0.016315	0.003811
5	0.001022	0.001994	0.004021	0.001897	0.011888	0.003041
Av.	0.001285	0.003439	0.004516	0.001775	0.013095	0.004334

Table 4 displays the results of the NIST tests, which were applied to the results of the proposed algorithm to confirm that the proposed key generation has high security and can withstand a variety of attacks. The proposed algorithm is passed in all NIST tests due to the modifications and keys used in each experimentally known test key.

Table 4: the randomness test of proposed method using NIST

#	Test	(P-Value)	Results
1	Run Test	0.099593	Success
2	Serial Test	0.022992	Success
3	random excursion variant test	0.684571	Success
4	random excursion test	0.686444	Success
5	Non-overlapping template matching test	0.748041	Success
6	Frequency Monobit Test	0.003198	Success
7	Maurer's universal statistical test	3.45E-05	Success
8	the longest run of ones in a block test	0.001069	Success
9	Linear complexity Test	0.021564	Success
10	Frequency test within a Block test	0.032982	Success
11	Discrete Fourier Transform test	0.788611	Success
12	Cumulative sums Test	0.004104	Success

The comparison results of the proposed method are explained in Table 5 in terms of the correlation value after the encryption of the image (in horizontal, vertical, and diagonal), entropy, NPCR, and UACI.

Table 5: The comparison of proposed method with other methods

References	Correlation	Entropy	NPCR	UACI
[26]	-0.0020 -0.0011 -0.002	7.997	99.59	33.031
[27]	-0.0016 -0.00031 -0.0021	7.999	99.61	33.4
[28]	0.0004 0.0061 -0.0012	7.999	99.62	33.2
[29]	-0.004 0.0017 0.004	7.996	99.625	33.4
[30]	0.0016 0.0067 0.0056	7.999	99.59	30.46
Proposed method	-0.0041 0.00013 -0.0011	7.9908	99.635	33.47

From the previous table, the proposed method result has been obtained from the experiments satisfying the standard of security measures and differential attacks.

6. Conclusion

In a time when security threats are growing and our reliance on technology is growing, digital picture encryption is a strong and efficient method for safeguarding visual data. It is now feasible to securely protect photos while preserving system efficiency thanks to advancements

in encryption methods. Image encryption will continue to be a crucial part of information security plans as the significance of visual data increases. A Hindmarsh-Rose map-based effective technique for color picture encryption is put forth. For various stages of the encryption technique, the method employed three-dimensional sequences: the first was utilized for block permutation, the second for the creation of S-boxes, and the third for the diffusion process. The suggested approach yields a precise visualization test result, objective. The generated number satisfies the NIST randomness test, the visualization test is accepted by producing a uniform histogram, the correlation is terminated between adjacent image pixels after encryption, and the quality of encrypted images is decreased after encryption. The proposed method could be developed to encrypt other types of multimedia such as audio and video.

References

[1]Shafiq, Muhammad, et al. "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT- Based Security Attacks." *Wireless Communications and Mobile Computing* 2022.1 (2022): 8669348.

[2]G. A. Sathishkumar, D. K. Bhoopathy bagan, and D. N. Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps," 2011.

[3]Mousavi, Seyyed Keyvan, et al. "Security of internet of things based on cryptographic algorithms: a survey." Wireless Networks 27.2 (2021): 1515-1555.

[4]I. El Hanouti, H. El Fadili, and K. Zenkouar, "Breaking an image encryption scheme based on Arnold map and Luca's series," 2019.

[5]Balsam A. Hameedi, Muntaha A. Hatem, and Jamal N. Hasoon "Dynamic Key Generation Using GWO for IoT" System" International journal of information Visualization. JOIV, Vol 8, No 2, 2024.

[6]Liu, He Zhang, Yiming He, Yeyin Xu, Independent continuous periodic firing series to chaos in the 3-D Hindmarsh–Rose neuron circuit, International Journal of Non-Linear Mechanics, Volume 155, 2023.

[7]Rasheed, Abdul Muhammed, and R. Mathusoothana S. Kumar. "Ultra-Lightweight Cryptographic Algorithm for Resource-Constrained Medical IoT Devices to Enhance Healthcare Security." (2025).

[8]Jain, Kurunandan, et al. "A lightweight multi-chaos-based image encryption Scheme for IoT Networks." *IEEE access* (2024).

[9]Usha, K., and P. A. Subha. "Energy feedback and synchronous dynamics of Hindmarsh–Rose neuron model with memristor." *Chinese Physics B* 28.2 (2019): 020502.

[10] Xingyuan Wang, Lin Teng, Xue Qin "**A novel color image encryption algorithm based on chaos"** Signal Processing, Volume 92, Issue 4, 2012, pp. 1101-1108.

[11] D. D. Salman, R. A. Azeez, and A.-M. J. Abdul-Hossen. "BUILD CRYPTOGRAPHIC SYSTEM FROM MULTI-BIOMETRICS USING MEERKAT ALGORITHM," Iraqi J. Comput. Informatics ijci, vol. 45, no. 2, pp. 1–8, 2019.

[12] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, "Rabbit: A new high-performance stream cipher," in International Workshop on Fast Software Encryption, 2003, pp. 307–329.

[13] S. Raizada, "Some results on analysis and implementation of HC-128 stream cipher." Indian Statistical Institute, Kolkata, 2015.

[14] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, Proc. Eurocrypt '93, volume 765

of LNCS, pages 386{397. Springer, 1993.
[15] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, Computer security: principles and practice. Pearson Education Upper Saddle River, NJ, USA, 2012.
[16] T. Gao and Z. Chen, “Image encryption based on a new total shuffling algorithm,” Chaos, solitons & fractals, vol. 38, no. 1, pp. 213–220, 2008.
[17] Li, S., Zheng, X., Mou, X. and Cai, Y. (2015). Chaotic Encryption Scheme for Real-Time Digital Video. Proceedings of SPIE. 4666:149-160.,
[18] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, “Rabbit: A New High-Performance Stream Cipher”, Proceedings of Fast Software Encryption (FSE’03), LNCS: 2887, pp. 307-329, Springer-Verlag, 2003.
[19] Ghanbari, Behzad, and J. F. Gómez-Aguilar. "Two efficient numerical schemes for simulating dynamical systems and capturing chaotic behaviors with Mittag–Leffler memory." *Engineering with Computers* (2020): 1-29.
[20] Yang Cao, "A New Hybrid Chaotic Map and Its Application on Image Encryption and Hiding", Mathematical Problems in Engineering, vol. 2013, Article ID 728375, 13 pages, 2013. https://doi.org/10.1155/2013/728375
[21] Wu, Wanqing, and Qiao Wang. "Block image encryption based on chaotic map and fractional fourier transformation." Multimedia Tools and Applications 82.7 (2023): 10367-10395.
[22] Elkandoz, Marwa Tarek, and Wassim Alexan. "Image encryption based on a combination of multiple chaotic maps." Multimedia Tools and Applications 81.18 (2022): 25497-25518.
[23] Pourasad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani. "A new algorithm for digital image encryption based on chaos theory." Entropy 23.3 (2021): 341.
[24] Yan, Shaohui, et al. "Development of an Image Encryption Algorithm Based on Compressed Sensing and Chaotic Mapping." IEEE MultiMedia (2024).
[25] M. S. Mahdi, and N. F. Hassan. "A SUGGESTED SUPER SALSA STREAM CIPHER." Iraqi Journal for Computers and Informatics ijci 44.2 (2018).
[26] M. Tanveer et al., "Multi-images encryption scheme based on 3D chaotic map and Substitution Box," IEEE Access, vol. 9, pp. 73924-73937, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3081362.
[27] B. Ge et al., "Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation," IEEE Access, vol. 9, pp. 137635-137654, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3118377.
[28] P. Parida et al., "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," IEEE Access, vol. 9, pp. 76191-76204, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3072075.
[29] S. Yan et al., "Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image," Integration, vol. 88, pp. 203-221, 2023. [Online]. Available: https://doi.org/10.1016/j.vlsi.2022.10.002.
[30] S. Deb and P. K. Behera, "Design of key-dependent bijective S-boxes for color image cryptosystem," Optik, vol. 253, p. 168548, 2022. [Online]. Available: https://doi.org/10.1016/j.ijleo.2021.168548.