International Journal of Computers and Informatics

Journal Homepage: https://www.ijci.zu.edu.eg

Int. j. Comp. Info. Vol. 7 (2025) 58–68

Paper Type: Original Article

New Image Encryption Algorithm Using 3D Logistics Map and Random Number Generator

Aisha M. Abdel-Raheem [1,*], Hanaa M. Hamza [1] and Khalid M. Hosny [1]

[1] Department of Information Technology, Faculty of Computer and Informatics, Zagazig University, Zagazig 44519, Egypt.
Emails: aishaeltaher7@gmail.com; hanaa_hamza2000@yahoo.com; k_hosny@zu.edu.eg.

Received: 17 Jan 2025 **Revised**: 09 Mar 2025 **Accepted**: 08 Jun 2025 **Published**: 11 Jun 2025

Abstract

This work presents a new algorithm for image encryption that utilizes a random number generator and the logistic map, generating keys with a large space and making them difficult to predict. This approach increases resistance to brute-force attacks, making the encryption more robust for secure applications and achieving low time complexity. The original image is confused in this algorithm, utilizing randomly generated numbers. Then, the permutated image is diffused using the sequence of the logistic map. The proposed image encryption algorithm was tested using noise and data cut attacks, histograms, and key space. Moreover, the proposed algorithm's performance is compared with several existing algorithms using entropy, correlation coefficients, and robustness against attacks. Security analysis indicates that the proposed algorithm is secure and resilient to attacks. It encrypts images using a large key space but is susceptible to slight changes in the security key. The histogram test is uniform, and the entropy is close to 8. Moreover, it consumes a very short time for encryption and decryption.

Keywords: Image Encryption; Random Number Generator; Logistic Map.

1 | Introduction

The transmission of digital images has become a fundamental part of modern communication across various platforms and networks. Users share personal images on social media but are often concerned about unauthorized access and privacy breaches. In the medical field, patient images, such as X-rays or MRI scans, hold sensitive information, and any unauthorized access or tampering could lead to incorrect diagnoses or compromised patient care. Similarly, military operations involve transmitting classified images, which require stringent security measures to prevent exposure to adversaries. Protecting the confidentiality and integrity of digital images is essential across all personal, medical, or governmental domains. Various security techniques address these concerns to ensure that image content remains inaccessible to unauthorized users, safeguarding sensitive data from potential misuse or compromise.

Image security approaches are divided into three main categories: data hiding [1,2], image watermarking [3–7], and encryption [8–11]. In data hiding techniques, a secret message is embedded within the cover image to remain undetectable. In image watermarking techniques, digital data is inserted into the image where the perceptibility of the original and watermarked images is similar. In image encryption techniques, the digital input image is converted into a noise image using a key that does not reveal or predict its content. Users cannot restore the encrypted image without knowing the key.

Corresponding Author: aishaeltaher7@gmail.com

2 | Literature Review

Many algorithms are built to encrypt images. Some rely on the chaos theory [6,7], while others utilize DNA [8,9]. The image encryption process consists of two main steps: confusion and diffusion. In the confusion step, the arrangement of image pixels changes. In diffusion, the pixel values of the image change. The encryption method based on chaos is characterized by non-periodic behavior, randomness, and sensitivity to control parameters and initial conditions, which enables it to achieve successful results. Many algorithms utilize chaos systems for encryption, such as [10, 11].

Liu and Ye [12] present an image encryption algorithm based on an improved 2D logistic map. Chaotic streams are constructed from the improved two-dimensional logistic map and used for confusion. The diffusion stage is achieved using the spatiotemporal chaos algorithm. Wu et al. [13] present an innovative image encryption algorithm anchored on the two-dimensional Logistic chaotic system, which enhances the speed and security of traditional Logistic chaotic systems. Wang et al [14] represent a new encryption method based on Quantum 3D Mobius for permutation and 3D Hyper-Chaotic Henon Map for changing pixel values. Hilmi et al [15] propose methods for encrypting images, first based on the Henon map to generate the permutation matrix for scrambling the plain image, secondly, by combining the Frobenius endomorphism and Tent chaotic map to create an encryption key, and then using the Exclusive-OR operation to diffuse the image. Khan et al [16] utilize a novel three-dimensional (3D) Chaotic map and an Enhanced Logistic Sine System in encryption. Li et al [17] developed an algorithm that encrypts images in three stages: first, generate the parameters and initial values of the dual chaotic system; second, the sequences generated by the dual chaotic system are used for dynamic DNA encoding and computation. In the third stage, the chaotic sequences generated by the improved Logistic chaotic system are used to perform row-column permutations, completing the scrambling. Zhu and Zhu [18] proposed a new encryption schema based on a newly constructed four-dimensional discrete chaotic map and the Chebyshev map. Benchikh et al [19] proposed a novel encryption method that combines image band scrambling with chaos and the Advanced Encryption Standard (AES) to protect critical and confidential satellite imagery. wang et al [20] Introduced a model based on the Arnold Coupled Logistic Map Lattices (ACLML). Wang et al [27] present a novel two-dimensional cross-hyperchaotic Sine-modulation-Logistic map (2D-CHSLM) based on the famous Sine and Logistic maps. Purwanto et al [28] employ complex mathematical algorithms and cryptographic keys to encrypt images, utilizing Fibonacci and Advanced Encryption Standard (AES)–Least Significant Bit (LSB) methodologies. Niu et al [29] present an improved algorithm for enhancing the image encryption using a four-dimensional chaotic system and evolutionary operators. Yu et al [30] present a new algorithm that combines DNA and a hyperchaotic system. First, a 256-bit secure hash algorithm (SHA-256) is employed to generate secret keys, and second, a hyperchaotic system is used to derive key streams. Then, the plaintext image can be encrypted using DNA encoding and DNA network encryption. Raghuvanshi [31] uses the Convolutional Neural Network (CNN) model and the logistic map to encrypt RGB images. They then use the logistic map to produce chaotic sequences that utilize permutation, Diffusion, and bit reversal, employing DNA rules to encode. Wang and Huang [32] present an encryption algorithm based on DNA and a meminductor chaotic systems to enhance image security and effectively prevent unauthorized access and decryption; first, they design an equivalent circuit model for the Meminductor and construct the corresponding chaotic system. Second, an artificial neuron is employed to perturb the original chaotic sequence generated by the system, resulting in a highly random mixed sequence. Finally, the original image is rearranged and encoded through Arnold transformation and dynamic DNA encoding techniques.

The authors can summarize the contributions as follows:

- An efficient encryption algorithm for RGB image encryption is introduced based on chaotic maps and a random number generator.
- The proposed encryption algorithm is tested using a set of RGB images from different modalities.

- Various security analysis parameters were evaluated, including information entropy, correlation coefficient, NPCR, and UACI.
- Various experiments are conducted to evaluate the proposed algorithm's performance in the presence of different attacks.
- The proposed method is superior to the existing methods.

3 | Mathematical Foundations

3.1 | 3D Logistics Map

The following equation represents the logistic map:

$$X_{n+1} = r.X_n(1 - X_n) \tag{10}$$

Here Xɳ is the system's state at iteration n (with Xn between 0 and 1); r is the control parameter determining the system's behavior (r is between 3.57 and 4). In this paper, the constant values selected are r=3.9

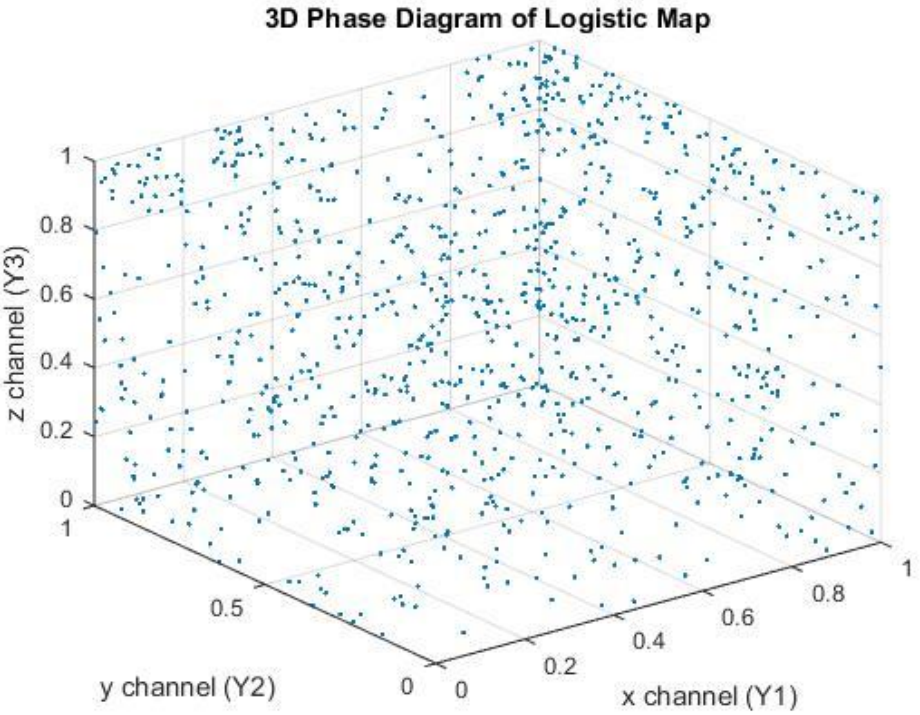

Figure 1. A phase diagram of a 3D logistic map for the RGB channel.

3.2 | Random Number Generator

The equation used to generate random numbers is:

$$x_{n+1} = (a.x_n + C) mod\ m$$

where a is multiplier, c is increment, m modulus, Xn is the current seed or state, Xn+1 is the updated seed.

4 | The Proposed Algorithm

The new algorithm utilized a 3D logistics Map and a Random number generator to encrypt the input image. Since the 3D logistics Map produces highly complex and chaotic behavior, it is easy to implement in both software and hardware systems. It is computationally efficient, which is crucial for real-time applications like encryption. Random numbers are essential for generating secure keys, as they provide unpredictable numbers

that ensure attackers cannot guess encryption keys or other security-critical values. This prevents predictable patterns in security systems, helping protect user data from attacks.

4.1 |Encryption

The encryption process consists of two steps: confusion and diffusion. The confusion step is based on a random number generator. First, we generate unique permutation indices for each channel using random number functions. Then, use it to permute each pixel in the plain image. Additionally, the permutation indices are XOR'd with the permuted image; after confusing the plain image, the diffusion step is performed to obtain the encrypted image. In our algorithm, the diffusion is based on a 3D logistic map. Each channel is defused by its key.

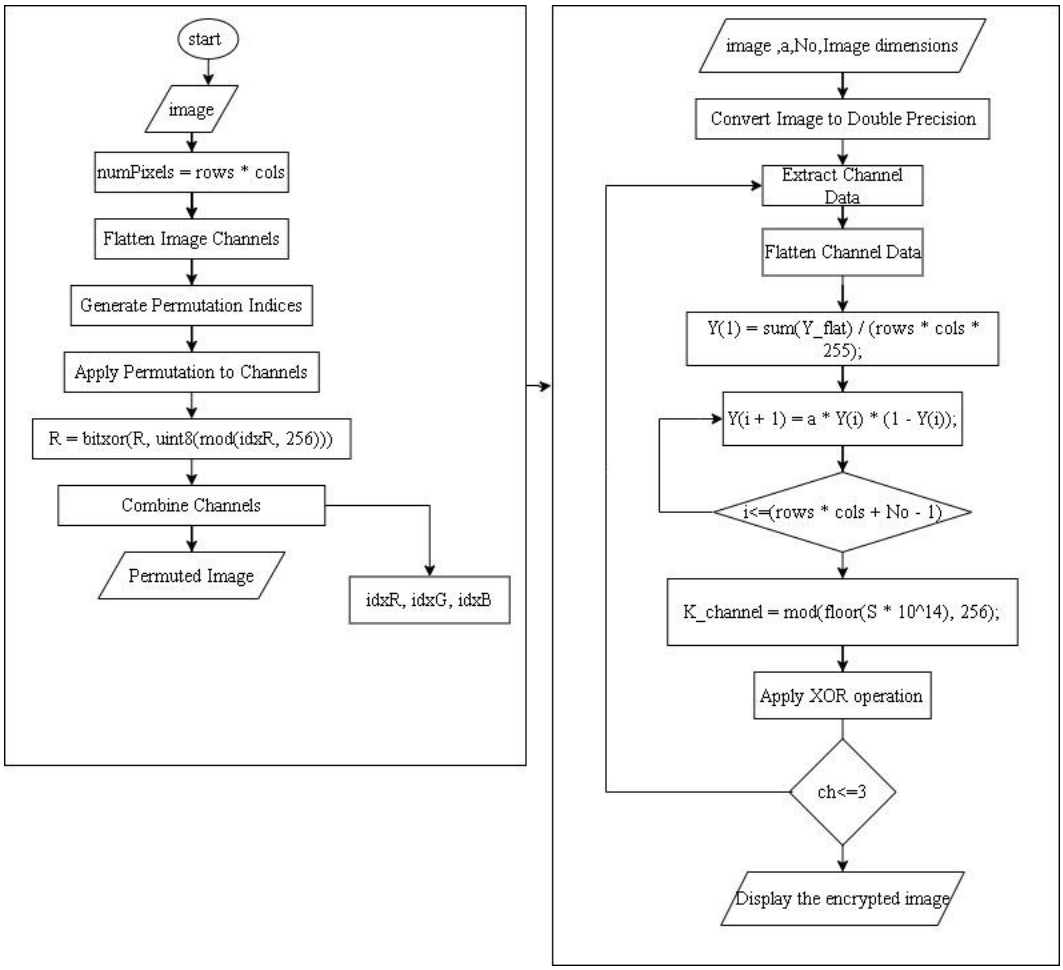

Figure 2. Flow chart of the proposed algorithm encryption process.

4.2 |Decryption

The decryption steps are performed on the encrypted image to retrieve the plain image. The following steps describe the decryption process:

- The encrypted image (C) is divided into RGB channels.
- The key generated in the encryption step is separate for each channel.
- Apply the XOR operation to decrypt each channel.
- The confused image obtained from the previous step is separated into its RGB Channels and reshaped for processing.
- The XOR Operation is applied using permutation indices.

- Invert the permutation indices.
- Each channel is Inverse Permuted using this equation:

$$ch_i = ch_i(\text{invIdx}\, ch_i) \quad i = 1{:}3$$

Combine the channels back into an RGB image

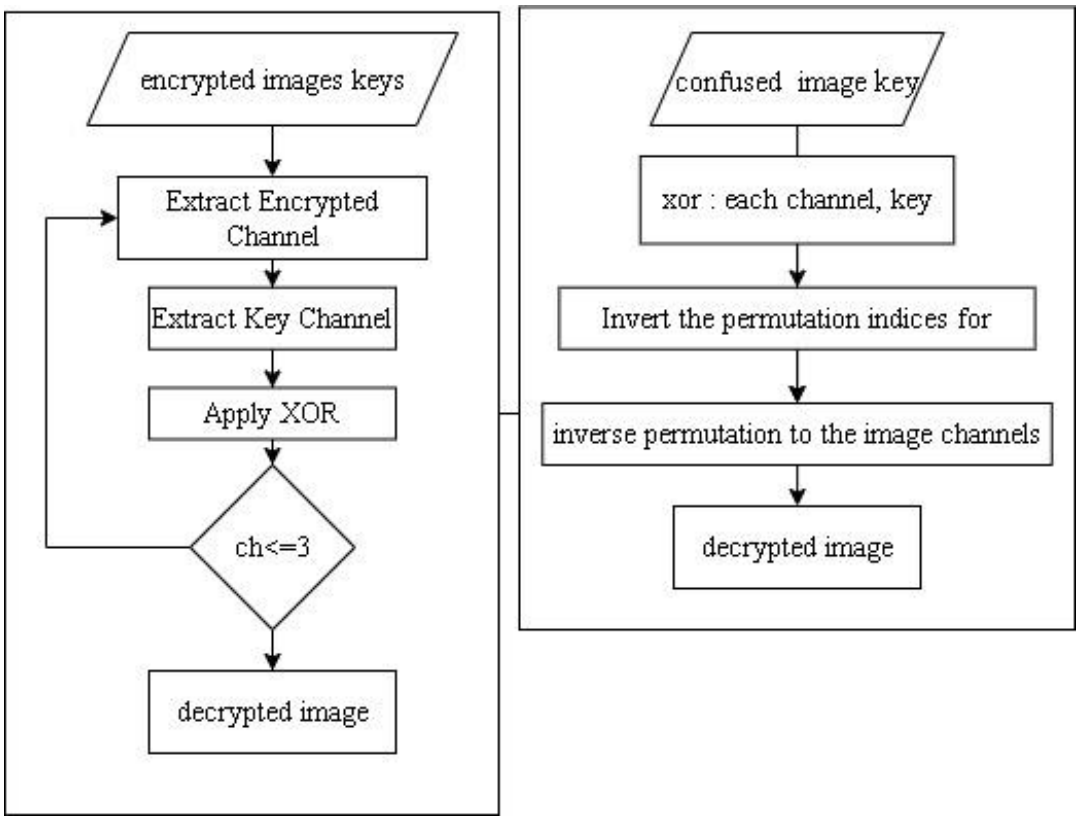

Figure 3. Flow chart of the proposed algorithm decryption process.

5 | Tests and Results

The proposed algorithm's effectiveness was tested using various standard RGB images (Baboon, Pepper, fruits, Airplane, and Lena) with a size of 256 × 256. Additionally, the proposed algorithm is compared with existing algorithms for image encryption. All experiments were conducted using MATLAB (R2015a) on a laptop computer equipped with a Core i5-4310U 2.00 GHz processor and 8 GB of RAM.

Eight experiments were performed to evaluate the proposed encryption algorithm using entropy, correlation coefficients, differential attacks, noise and data cut attacks, histograms, and keyspace Test.

5.1 | Entropy

The amount of unpredictability or disorder within a system is measured by entropy using the following equation:

$$\mathrm{H(m)} = \sum_{i=1}^{2^W-1} \mathrm{p(m}_i\mathrm{)log}_2 \frac{1}{\mathrm{p(m}_i\mathrm{)}} \tag{11}$$

Where P(mi) is the occurrence probability of mi, 2 w is the total number of mi, and w represents the total number of image pixels

The entropy of a few RGB images encrypted using the new and existing algorithms is shown in Tables 1 and 2.

Table 1. Entropy values of images with size 512 × 512 with our algorithm and other encryption algorithms.

Image	proposed	[11]	[21]	[22]	[23]	[24]	[25]	[26]
Lenna	7.9991	7.9975	7.9966	7.9972	7.9971	7.9972	7.9969	7.9974

Table 2. Entropy values of RGB encrypted images with size 512 × 512 with our algorithm.

Image	proposed
Baboon	7.9990
Pepper	7.9992
Fruits	7.9991
Airplane	7.9991

5.2 | Correlation Coefficient

Generally, the input images' adjacent pixels correlate highly in the diagonal, horizontal, and vertical directions. In a successful encryption algorithm, this correlation is weak. To calculate the correlation coefficient between two neighboring pixels x and y, we use this equation:

$$r_{x,y} = \frac{E((y - E(y))(x - E(x)))}{\sqrt{D(y)D(x)}} \tag{11}$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T} (x_i - E(x))^2$$

Where T refers to the total number of adjoining pixels, D(x) and E(x) are the variance and expectation of x, respectively. If the correlation between adjoining pixels approaches 0, this refers to a good and successful algorithm

Figures 4 and 5 show the original and encrypted Lena images' H-, V-, and D-correlation distributions. A strong correlation between the original image pixels is evident. However, the encrypted images have a weak correlation, as the pixels are uniformly distributed throughout the x-y space.

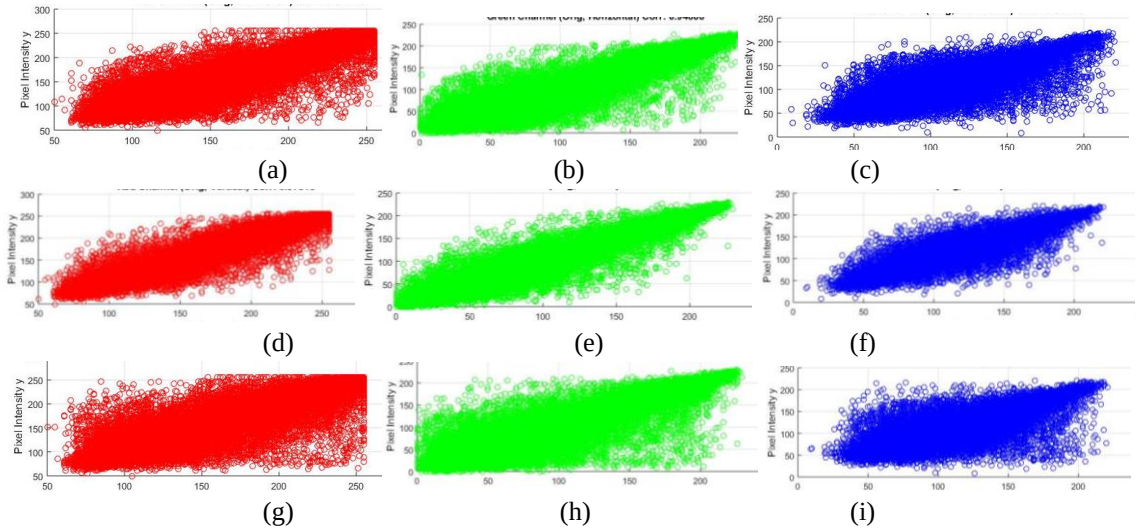

Figure 4. Correlation plots of Lena. a–c: Horizontal plots, d–f: vertical plots, and g–i: diagonal plots of RGB components, respectively.

Tables 3 and 4 present the absolute values of the calculated correlation coefficients for the encrypted images using the new and existing image encryption algorithms [11] [21–26]. All the results confirm that our proposed algorithm can effectively remove the correlation between adjacent pixels in the encrypted image. Figure 5 shows correlation plots of the encrypted image Lena.

Table 3. Correlation coefficients in three directions: horizontal (H), Vertical (V), and Diagonal (D) for the Lena image with a size of 512 × 512.

Algorithm	H			D			V		
	R	G	B	R	G	B	R	G	B
proposed	0.0007	-0.0029	-0.0030	0.0002	-0.0016	-0.0023	0.0007	-0.0005	-0.0030
[11]	−0.0007	0.0019	0.0002	0.0002	−0.0001	0.0013	0. 0010	−0.0003	−0.0002
[21]	0.00144			-0.00151			0.00055959		
[22]	0.0079784			-0.000125			0.001158		
[23]	0.0016			−0.0006			0.0046		
[24]	0.00206	-0.01386	-0.03479	0.01036	-0.00832	0.03226	-0.00643	-0.00663	-0.01286
[25]	0.0005	0.0013	-0.0005	0.0004	0.0001	0.0000	-0.0003	0.0004	-0.0001
[26]	0.9350			0.9111			0.9687		

Table 4. Correlation coefficients in three directions: Horizontal (H), Vertical (V), and Diagonal (D) for various RGB images with a size of 256 × 256.

Images	H			D			V		
	R	G	B	R	G	B	R	G	B
Baboon	-0.0000	-0.0044	0.0056	0.0009	-0.0002	0.0005	0.0013	-0.0013	0.0018
Pepper	-0.0006	0.0025	0.0019	-0.0003	0.0037	0.0006	-0.0012	0.0027	0.0016
Fruits	0.0014	0.0032	-0.0046	0.0001	0.0039	-0.0052	0.0018	0.0018	-0.0036
Airplane	0.0029	0.0033	0.0018	0.0041	0.0039	0.0009	0.0014	0.0019	0.0038

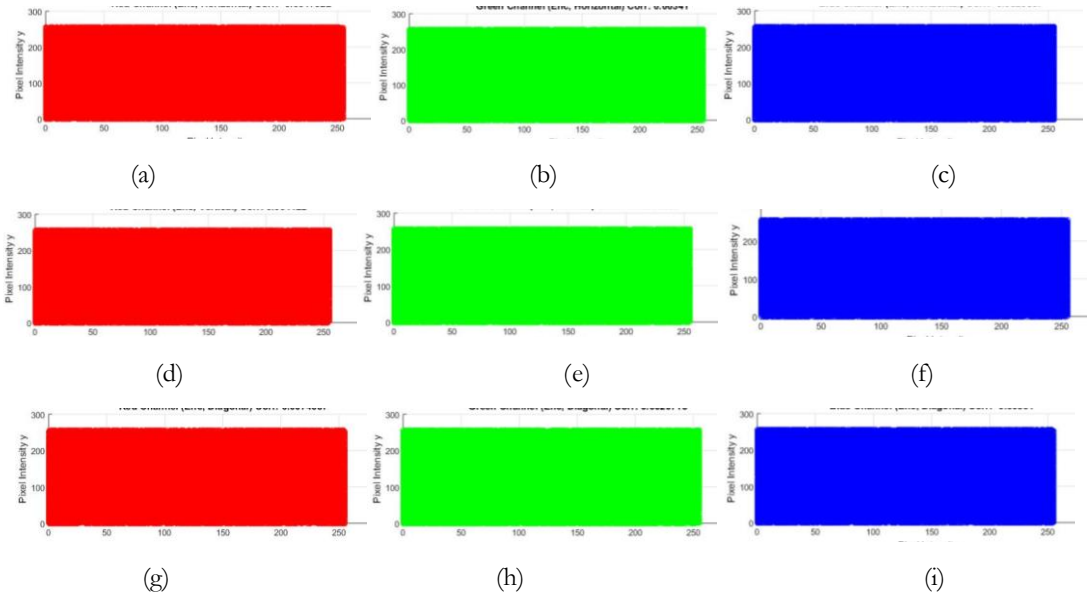

Figure 5. Correlation plots of encrypted Lena. a–c: Horizontal plots, d–f: vertical plots, and g–i: diagonal plots of RGB components, respectively.

5.3 | Differential Attack

We measure this type of attack by two parameters, the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI):

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} DIF(i,j) \times 100(\%) \qquad [11]$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_2(i,j) - C_1(i,j)|}{255} \times 100(\%) \qquad [11]$$

With

$$DIF(i,j) = \begin{cases} 0, & C_2(i,j) = C1(i,j), \\ 1, & C_2(i,j) \neq C1(i,j), \end{cases} \qquad [\mathbf{11}]$$

The symbol C2 refers to the chipper image encrypted from the original image by changing only one pixel. In contrast, C1 refers to the chipper image encrypted from the same plain image. Table 3 shows the computed values of the five RGB images encrypted using the proposed and existing image encryption algorithms.

Table 5. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) of the encrypted image using different encryption algorithms and our proposed algorithm.

Algorithm	**NPCR**			**UACI**		
	R	G	B	R	G	B
proposed	99.6231	99.6277	99.6292	32.9422	30.5143	27.7192
[11]	99.6277	99.6143	99. 6155	33.5638	33.4614	33.4924
[21]	99.6254	99.6254	99.6254	33.0704	30.7620	27.8720
[22]	99.636	99.591	99.638	33.097	30.723	27.701
[23]	99.6521	99.6292	99.6277	33.394	33.4283	33.5255
[24]	99.606	99.643	99.625	33.314	33.334	33.414
[25]	99.6368	99.6262	99.6338	33.5010	33.5307	33.5553
[26]	99.7401			33.4475		

Table 6. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) of the encrypted image using our proposed algorithm.

images	**NPCR**			**UACI**		
	R	G	B	R	G	B
baboon	99.5941	99.6033	99.6002	29.9511	28.7639	31.3245
Pepper	99.6017	99.6002	99.5911	28.6551	33.3979	34.2405
fruits	99.5605	99.6231	99.6292	30.2321	31.1718	37.0068
Airplane	99.5697	99.6002	99.5392	32.0967	33.0505	32.7595

5.4 |Noise and Data Cut Attacks

Images transmitted over a network can be susceptible to noise or data loss, such as cropping. Effective image encryption algorithms must demonstrate resilience against both noise and cropping attacks. A widely recognized metric, PSNR (peak signal-to-noise ratio), is employed to assess the quality of the decrypted image.

The following equation is used to calculate PNSR:

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right)(db) \qquad [17]$$

where MSE refers to the mean square error:

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|I_O(i,j) - I_D(i,j)|^2 \quad [17]$$

Effective algorithms have a high PNSR; if the PNSR exceeds 35, the original and decrypted images are indistinguishable.

This experiment assessed the robustness against noise and data cut attacks. In this experiment, an encrypted image is contaminated with "salt and pepper" noise of two levels, 0.002 and 0.005, and then decrypted using the new method. The encrypted images were also attacked by a data cut of 128 × 128 and 64 × 64, decrypted using the new algorithm. The PSNR for the five tested images with noise and data cut to a size of 512 × 512 is shown in Table 7.

Table 7. Peak signal-to-noise ratio (PSNR) (dB) values for noise and data cut attacks.

Standard RGB Images	Lena	Baboon	Peppers	fruits	Airplane
Salt and Pepper with noise level 0.002	35.089	35.8998	34.2821	35.2048	35.6755
Salt and Pepper with noise level 0.005	31.4046	31.7715	31.4834	31.2796	30.8225
Data cut with a block size of 128 × 128	14.6811	14.7891	14.1596	13.91	14.0354
Data cut with a block size of 64 × 64	22.1159	20.7846	20.14	20.02	19.9227

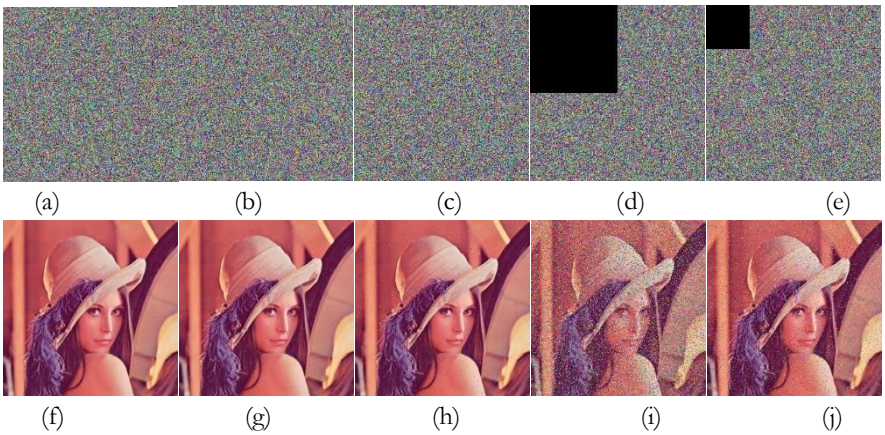

Figure 6. (a) The encrypted image, (b) noisy encrypted image with 0.002, (c) noisy encrypted image with 0.005, and (d) encrypted image with 128 × 128 data cut. (e) Encrypted image with 64 × 64 data cut. (f-j) Decrypted images of (a-e).

5.5 | Histograms

The histogram represents the distribution of image pixels; it is also a parameter for evaluating the encryption algorithm. The histogram should be uniform for a good and effective encryption algorithm. The standard RGB image of Lena is encrypted using the new algorithm. The histogram for each channel in the original and encrypted image is displayed in Figure 2.

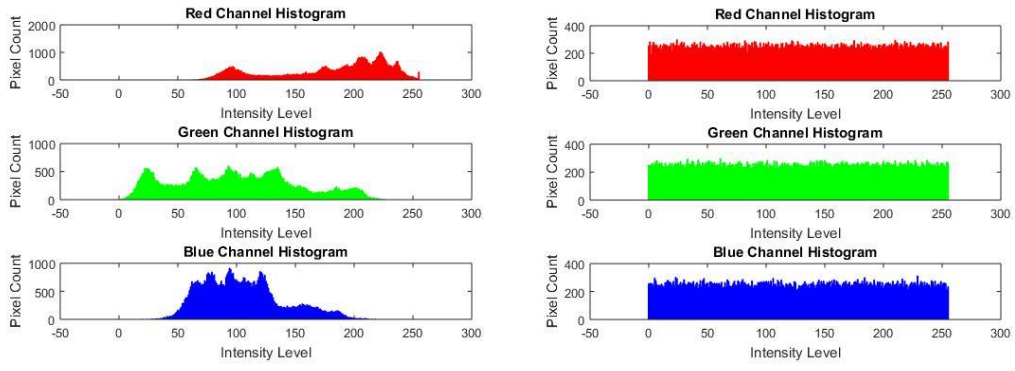

Figure 7. Histogram for each channel in encrypted and original image: (a) original "Lena", (b) encrypted "Lena."

5.6 | Keyspace

The Keyspace is an essential parameter for evaluating the algorithm's strength against brute force attacks; a successful and strong algorithm must have a keyspace size greater than 2^{100}. The proposed encryption algorithm utilizes two distinct keys: one for confusion and another for diffusion. The total keyspace size calculated for 256x256 RGB images equals $2^{,422,702,351}$, greater than 2^{100}; this improves our algorithm's robustness to the brute force attack.

5.7 | Computational Complexity

Time complexity reflects the growth in execution time with the input size. For a plain image of size M × N, the time complexity of the encryption steps in the proposed algorithm is O(M×N). Also, the time complexity of the decryption is O(M×N). Therefore, the total time complexity of the proposed algorithm is O(M×N). The encryption and decryption times for a color Lena image of size 256 × 256 are 7.236 s and 0.132 s, respectively, under this computer configuration

6 | Conclusion

The author proposed a new algorithm for RGB image encryption, utilizing the logistic map in conjunction with random number generators. First, we generate random numbers using random functions to permute each channel in the image. Then, we apply the logistic map to create a sequence and use it to defuse each channel in the image. The new algorithm successfully resists the differential attack, a type of brute force attack where the key space size is sufficiently large. Moreover, security performance was evaluated using information entropy, correlation coefficients, noise, data cut attack, and histogram.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability

This study is based on a conceptual framework, and no empirical data were generated or analyzed.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Hosny, K., Kamal, S., Darwish, M., & Papakostas, G. A. (2021). New image encryption algorithm using Hyperchaotic system and Fibonacci Q-matrix. Electronics 2021 (10): 1066.

[2] Abdel-Aziz, M. M., Hosny, K. M., & Lashin, N. A. (2021). Improved data hiding method for securing color images. Multimedia Tools and Applications, 80(8), 12641-12670.

[3] Li, N., & Huang, F. (2020). Reversible data hiding for JPEG images based on pairwise nonzero AC coefficient expansion. Signal Processing, 171, 107476.

[4] Hosny, K. M., Darwish, M. M., Li, K., & Salah, A. (2018). Parallel multi-core CPU and GPU for fast and robust medical image watermarking. IEEE Access, 6, 77212-77225.

[5] Hosny, K. M., & Darwish, M. M. (2018). Robust color image watermarking using invariant quaternion Legendre-Fourier moments. Multimedia Tools and Applications, 77, 24727-24750.

[6] Luo, Y., Zhou, R., Liu, J., Cao, Y., & Ding, X. (2018). A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. Nonlinear Dynamics, 93, 1165-1181.

[7] Yosefnezhad Irani, B., Ayubi, P., Amani Jabalkandi, F., Yousefi Valandar, M., & Jafari Barani, M. (2019). Digital image scrambling based on a new one-dimensional coupled Sine map. Nonlinear Dynamics, 97(4), 2693-2721.

[8] Chen, X., Mou, J., Cao, Y., & Banerjee, S. (2023). Chaotic multiple-image encryption algorithm based on block scrambling and dynamic DNA coding. International Journal of Bifurcation and Chaos, 33(16), 2350190.
[9] Meng, F. Q., & Wu, G. (2024). A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system. Expert Systems with Applications, 254, 124413.
[10] Zhao, M., Li, L., & Yuan, Z. (2024). An image encryption approach based on a novel two-dimensional chaotic system. Nonlinear Dynamics, 112(22), 20483-20509.
[11] Hosny, K. M., Elnabawy, Y. M., Elshewey, A. M., Alhammad, S. M., Khafaga, D. S., & Salama, R. (2024). New method of colour image encryption using triple chaotic maps. IET Image Processing, 18(12), 3262-3276.
[12] Liu, S., & Ye, X. (2024). Designing a novel image encryption scheme based on an improved 2D logistic map. Journal of Applied Physics, 136(12).
[13] Wu, Y., Chu, S., Bao, H., Wang, D., & Zhou, J. (2024). Efficient Image Encryption via 2D Logistic Chaos Mapping: Strengthening Security with Pixel-Level Dynamics. Int. Arab. J. Inf. Technol., 21(5), 915-924.
[14] Wang, L., Ran, Q., & Ding, J. (2023). Image Encryption Using Quantum 3D Mobius Scrambling and 3D Hyper-Chaotic Henon Map. Entropy, 25(12), 1629.
[15] Hilmi, A., Mezroui, S., & El Oualkadi, A. (2023). An image encryption based on confusion-diffusion using two chaotic maps and Frobenius endomorphism. SAIEE Africa Research Journal, 114(4), 98-105.
[16] Khan, S., Peng, H., Gu, Z., Usman, S., & Mukhtar, N. (2024). Integration of a novel 3D chaotic map with ELSS and novel cross-border pixel exchange strategy for secure image communication. Complex & Intelligent Systems, 10(6), 8433-8465.
[17] Li, R., Liu, T., & Yin, J. (2024). An encryption algorithm for color images based on an improved dual-chaotic system combined with DNA encoding. Scientific Reports, 14(1), 20733.
[18] Zhu, S., & Zhu, C. (2024). A visual security multi-key selection image encryption algorithm based on a new four-dimensional chaos and compressed sensing. Scientific Reports, 14(1), 15496.
[19] Benchikh, O., Bentoutou, Y., & Taleb, N. (2024). Satellite image encryption using 2D standard map and advanced encryption standard with scrambling. International Journal of Electrical & Computer Engineering (2088-8708), 14(5).
[20] Wang, G., Ye, X., & Zhao, B. (2024). A novel remote sensing image encryption scheme based on block period Arnold scrambling. Nonlinear Dynamics, 112(19), 17477-17507.
[21] Alexan, W., Elkandoz, M., Mashaly, M., Azab, E., & Aboshousha, A. (2023). Color image encryption through chaos and kaa map. Ieee Access, 11, 11541-11554.
[22] Alexan, W., Gabr, M., Mamdouh, E., Elias, R., & Aboshousha, A. (2023). Color image cryptosystem based on sine chaotic map, 4D chen hyperchaotic map of fractional-order and hybrid DNA coding. Ieee Access, 11, 54928-54956.
[23] Shraida, G., Younis, H. A., Al-Amiedy, T. A., Anbar, M., Younis, H. A., & Hasbullah, I. H. (2023). An efficient color-image encryption method using DNA sequence and chaos cipher. Comput. Mater. Contin, 75(2), 2641-2654.
[24] Meng, F., & Gu, Z. (2023). A color image-encryption algorithm using extended DNA coding and zig-zag transform based on a fractional-order laser system. Fractal and Fractional, 7(11), 795.
[25] Abed, Q. K., & Al-Jawher, W. A. M. (2024). Optimized color image encryption using arnold transform, URUK chaotic map and GWO algorithm. Journal Port Science Research, 7(3), 219-236.
[26] Alsahafi, Y. S., Khalid, A. M., Hamza, H. M., & Hosny, K. M. (2024). New optimized chaotic encryption with BCOVIDOA for efficient security of medical images in IoMT systems. Neural Computing and Applications, 36(14), 7705-7723.
[27] Wang, M., Teng, L., Zhou, W., Yan, X., Xia, Z., & Zhou, S. (2025). A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption. Expert Systems with Applications, 261, 125328.
[28] Purwanto, P., Marjuni, A., Astuti, E. Z., Sari, C. A., Rijati, N., Andono, P. N., & Sarker, M. K. (2024). An image encryption based on Fibonacci sequence and fusion of advanced encryption standard-least significant bit method. TELKOMNIKA (Telecommunication Computing Electronics and Control), 22(6), 1517-1528.
[29] Niu, Y., Zhou, H., & Zhang, X. (2024). Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. Scientific Reports, 14(1), 7033.
[30] Yu,J.; Peng,K.; Image encryption algorithm based on DNA network and hyperchaotic system. 2024,40, 8001–8021.
[31] Raghuvanshi, K. K., Kumar, S., Kumar, S., & Kumar, S. (2024). Image encryption algorithm based on DNA encoding and CNN. Expert Systems with Applications, 252, 124287.
[32] Wang, J., Huang, W., Wang, Z., Wang, J., & Chen, K. (2024). DNA dynamic coding image encryption algorithm with a meminductor chaotic system. Physica Scripta, 99(9), 095231.