Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 8, Issue 3, December 2025
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN:2789-7362

PERFORMANCE EVALUATION OF CHAOTIC IMAGE ENCRYPTION

Rania Ammar [1], **Hamsa A. Abdullah** [2]
[1,2] Department of Information and Communication Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq
raniahammar068@gmail.com[1], hamsa.abdulkareem@nahrainuniv.edu.iq[2]
Corresponding Author: **Hamsa A. Abdullah**
Received:03/09/2024; Revised:04/11/2024; Accepted:07/01/2025
DOI:10.31987/ijict.8.3.304

***Abstract*- Nowadays, data is the most valuable content in the world. Millions of data are generated every day in the form of text, images, videos, etc. Among them, images are widely used in daily communication. Due to the vulnerabilities of many data, it is difficult to transmit such images in a secure way. For this reason, a chaos-based data encryption algorithm is proposed where the image pixels are encrypted to generate a blurry image. In this paper, it is explained how to encrypt images using a 3D logistic chaotic map by generating chaotic keys where the image undergoes pixel scrambling and then XOR operation with the previously generated chaotic keys. To enhance the security and privacy of data, the proposed scheme uses different image sets to evaluate performance metrics such as Number of Pixel Change Rate (NPCR), Average Variable Intensity (UACI), correlation coefficients, and entropy in different attack scenarios. The proposed method achieved superior performance results in entropy (7.9993), key space, encryption pixel correlations, histogram contrast, UACI (35.2041%), and NPCR (99.6333%). The achieved results show that the proposed method can be used for image encryption with a high level of confidentiality.**

keywords: **Chaotic, 3D logistic key, Scrambling, Encryption.**

I. INTRODUCTION

There has been rapid development in multimedia including images, video and audio in recent years. The widespread use of digital information has been promoted in computer science and network technology. Images play an important role in our lives as an effective means of understanding colors among the categories of multimedia. For many reasons, including illegal eavesdropping, reviewing or eavesdropping, there has been a clear lack of security in terms of exchanging images over the network, especially medical and military images. Structurally, encryption is classified into two types, namely symmetric encryption and asymmetric encryption. According to the higher efficiency requirements and low computational requirements, preference is given to symmetric encryption systems in encryption. Thus, the preservation of privacy, safety, and security in photographs has drawn the attention of numerous researchers worldwide. Digital encryption techniques can be used to achieve this security [1]. Digital image encryption is the process of transforming an image into a human-unreadable format so that any potential.

Due to the massive amount of traffic that image data uploads and downloads generate online, sensitive data is more likely to be stolen and targeted by hackers. As a result, image encryption schemes a kind of image protection are desperately needed [2]. There are several techniques available for encrypting images by first dividing the neighboring pixels and then distributing the random replacement among the encrypted images, most of these techniques use the confusion-diffusion model. Specifically, this structure is supported by algorithms that use chaos. Researchers find it appealing because of its ramification structures and instability [3].

ISSN:2222-758X
e-ISSN:2789-7362

Because the properties of chaotic maps affect the security level of chaos-based algorithms, chaotic maps are becoming increasingly important in secure communications. Chaotic maps can often be divided into two categories: One Dimensional (1D) and Hyper Dimensional (HD). There is an urgent need to guarantee privacy and preserve this information, especially personal images and essential papers, given the growing frequency with which individuals use the internet to transmit personal and important information [4]. The complexity and length of time required for the process of applying these techniques to images are noteworthy. Both decoding and encryption. Consequently, crucial data and images were encoded using chaotic maps.

With the increasing volume and sensitivity of digital image content, there is a growing need for robust methods to ensure the security and confidentiality of image data during transmission and storage. Traditional encryption methods may face challenges in balancing security, and computational efficiency, motivating the exploration of alternative techniques.

II. RELATED WORKS

The development of new, effective methods for creating picture security schemes in response to the need for secure image transmission via communication channels was made possible by the chaos-based encryption algorithm.

An efficient encryption scheme was presented by [5] to protect IoT surveillance systems. There are three components to the proposed encryption framework. Key frames are first extracted from security footage using a fast histogram clustering method based on lightweight automated summarization methodology. Then, the proposed method uses the Discrete Cosine Transform (DCT) method to reduce the amount of recovered data. Finally, the proposed framework uses the Discrete Fractional Random Transform (DFRT) to implement an efficient image encryption procedure. The properties of the proposed encryption scheme are validated on surveillance systems through analysis and testing results where the value of Number of Pixel Change Rate (NPCR) is 99.5826% and Average Variable Intensity (UACI) is 33.4213%. By reducing transmission costs and storage requirements, the proposed architecture ensures fast, secure, and efficient real-time processing [5].

A secure method for encrypting and storing images has been proposed. This approach ensures the confidentiality and privacy of image data. This paper evaluates the robustness of the proposed image encryption method against differential attacks based on the analysis of information entropy, UACI = 33.4187% and NPCR = 99.6023%. The entropy levels reached are close to the optimal value of (8), which is believed to be secure against brute force attacks [6].

A proposed a new method for image encryption by combining chaotic maps and reversible cellular automata [7]. This proposed research shows that it relies on achieving high key sensitivity when using bidirectional chaotic maps as well as achieving a large key space which is done by swapping the image pixels at the byte level, while the cellular automata are used to propagate the images. It was found to be robust against attacks by evaluating the performance of the encryption method using statistical methods [7].

Due to the increasing use of the Internet in e-commerce, multimedia transmission and financial services, in [8] demonstrated how to use chaotic maps to generate pseudo-random numbers and perform multimedia encryption based on changing the initial values of the chaotic map. After carefully analyzing all the modern literature, it founds that the highest entropy is 7.999995 bits per byte using the chaotic map [8].

A new chaotic oscillator method was proposed [9]. The aim of this paper is to propose a viable encryption technique based

ISSN:2222-758X
e-ISSN:2789-7362

on a new chaotic oscillator around preposition multiples containing an attractor. The reliability of the proposed encryption scheme for a range of IoT applications, including image capture, has been confirmed by all investigations, with good results around NPCR (99.60556%) and UACI (33.49106%).

A new approach to a chaotic system has been introduced, a 3D chaotic system for color image encryption. A novel chaotic method is used to generate a basic key sequence for pixel encryption. The results are promising: a nearly uniform graph, nearly 0% inter-pixel correlation, and nearly perfect entropy. The proposed method includes graph uniformity, low pixel-to-pixel correlation close to zero, entropy close to ideal (8), and NPCR/UACI values close to ideal (99.7034%) and (33.0497%), respectively [10].

This work presents a method for improving the security of image encryption through the scrambling process using 3D logistic maps. The suggested system's performance evaluation tests have undergone statistical verification.

III. WORK STRUCTURE AND METHOD USED

In this paper, a new method of utilizing chaotic maps was presented, such as 3D logistic maps, to encrypt multimedia, including photographs. Using a 3D logistic map, chaotic keys are generated and the resultant image from the shuffling process is subjected to an XOR operation to create a fuzzy encrypted image. Through the scrambling process, the pixels in the image are swapped and the gray level settings are adjusted. The experimental results show that the proposed strategy is effective. Various values were computed to demonstrate the method's strength, including the values of NPCR that produced (99.6333%) a UACI value of (35.2041%) and the entropy values that produced a value of (7.9993%). From the experimental results, it was concluded that the proposed method can be used for image encryption with a high level of confidentiality. The main steps of proposed system are shown in Fig. 1.

A. Scrambling technique

Image scrambling is a process of randomly rearranging pixels to make an image visually unreadable and break the correlation between pixels, where the pixel values remain unchanged. The scrambling technique produces images with less correlation than the original image and is effective and straightforward. The image is split into four quadrants by the algorithm, which then performs a recursive quadrant transformation. The permutation matrix B is then used to permute each block [11]. The matrix permutation given in Eq. (1). After R iterations, the procedure is repeated.

$$\mathbf{B} = \begin{bmatrix} 57 & 49 & 58 & 41 & 50 & 59 & 33 & 42 \\ 51 & 60 & 25 & 34 & 43 & 52 & 61 & 17 \\ 26 & 35 & 44 & 53 & 62 & 9 & 18 & 27 \\ 36 & 45 & 54 & 63 & 1 & 10 & 19 & 28 \\ 37 & 46 & 55 & 64 & 1 & 11 & 20 & 29 \\ 38 & 47 & 56 & 3 & 12 & 21 & 30 & 39 \\ 48 & 4 & 13 & 22 & 31 & 40 & 5 & 14 \\ 23 & 32 & 6 & 15 & 24 & 7 & 16 & 8 \end{bmatrix} \quad (1)$$

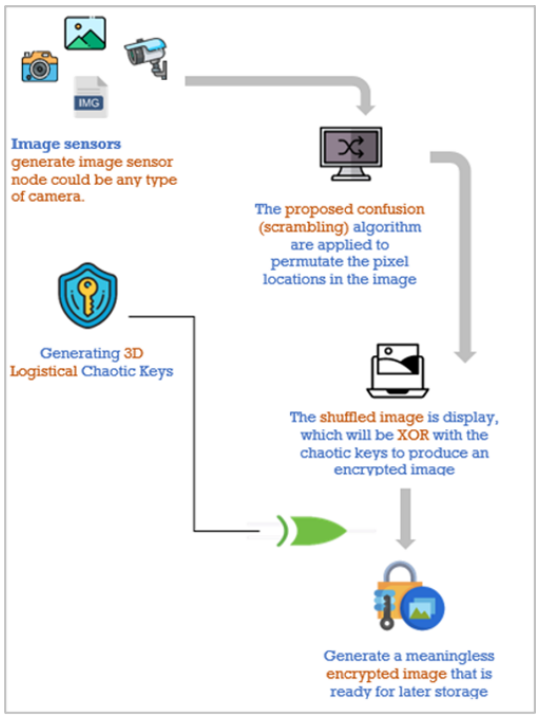

Figure 1: Main steps of the proposed method.

The algorithm of proposed scrambling method includes following steps:

Algorithm 1: Proposed Image Scrambling Algorithm

Step 1: *Input a random image of size* $(M \times N)$ *and calculate the midpoint of the image dimensions as* $S_1 = M/2$ *and* $S_2 = N/2$.

Step 2: *Divide the input image into four quarters, forming four sub-blocks* (B_1, B_2, B_3, B_4).

Step 3: *For each block, calculate* (Q_1, Q_2) *where* $Q_1 = S_1/2$ *and* $Q_2 = S_2/2$.

Step 4: *Divide each block into four quarters* (C_1, C_2, C_3, C_4) *and merge them into a new block defined as* $K = [C_4, C_3; C_2, C_1]$.

Step 5: *Create the intermediate image* $IM2$ *by reassembling the newly formed blocks as* $IM2 = [K_3, K_4; K_1, K_2]$.

Step 6: *Apply a recursive permutation by dividing the image into* 8×8 *blocks; extract each block, reshape it into a vector* $k = reshape(block, 1, 64)$, *and permute it according to the matrix* B *as* $block1(p) = k(B(p))$.

Step 7: *Reshape the permuted vector to form the block* $block2 = reshape(block1, 8, 8)$.

Step 8: *Return the final transformed (scrambled) image matrix as shown in Fig. 2.*

B. Diffusion Technique

Refers to changing the individual pixel grey values that leads to the reduction of correlation between image pixels and it is include the following steps:

ISSN:2222-758X
e-ISSN:2789-7362

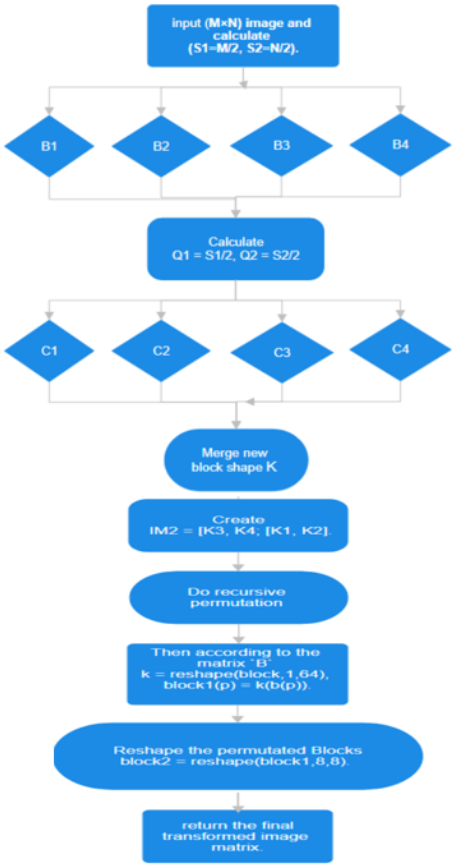

Figure 2: Flowchart of proposed scrambling method.

1) Preparing the 3D Logistics Map: 3D logistic maps can be defined by the following Eq. (2):

$$\begin{aligned} x_{i+1} &= \alpha x_i(1-x_i) + \beta y_i^2 x_i + \gamma z_i^3, \\ y_{i+1} &= \alpha y_i(1-y_i) + \beta z_i^2 y_i + \gamma x_i^3, \\ z_{i+1} &= \alpha z_i(1-z_i) + \beta x_i^2 z_i + \gamma y_i^3. \end{aligned} \tag{2}$$

Where α, β, and γ are control parameters. The control parameters of 3D logistic map rage are: $\alpha = [3.68, 3.99]$, $\beta = [0, 0.022]$, and $\gamma = [0.0.15]$ in order the system has a chaotic behavior. While the range values of system: x, y, and z are = $[0, 1]$.

2) Generating a series of random values: By iterating using the ternary logistic equations, it is possible to generate series of random values for each of (x), (y), and (z). For example, by iterating the equations for a number of steps (N) it was possible to generate series (X_i), (Y_i), and (Z_i) for each step (i).

3) Converting random values to pixel positions: After generating random strings, these values can be converted to pixel positions in the image. For example, (x) and (y) values can be used to specify the horizontal and vertical position of pixels

ISSN:2222-758X
e-ISSN:2789-7362

in the image, while (z) values can be used to specify the pixel intensity or pixel color, depending on the type of image (Gray or color).

4) Diffusion pixels: Using random strings, the pixels in the image are moved on so that the original pixel order is mixed up. For example, if the image is of size $(M \times N)$, the random values can be used to generate an array of pairs (i, j) that indicate the scrambled pixels at positions (i, j).

Consider an image of size (256×256):

- Set the starting values (x_0), (y_0), (z_0) and constants α, and β.
- Iterate the 3D logistic equations to get 65536 values (256×256).
- Arrange the values to form (x, y) pairs to determine the positions of the new pixels.
- An XOR operation is performed between the scrambled image and the chaotic keys to create a chaotic image.

These steps give an idea of how to use 3D Logistic Map with the scrambling image to encrypt images, which increases the complexity and impossibility of recovering the original image without knowing the key and scramble used as shown in Fig. 3.

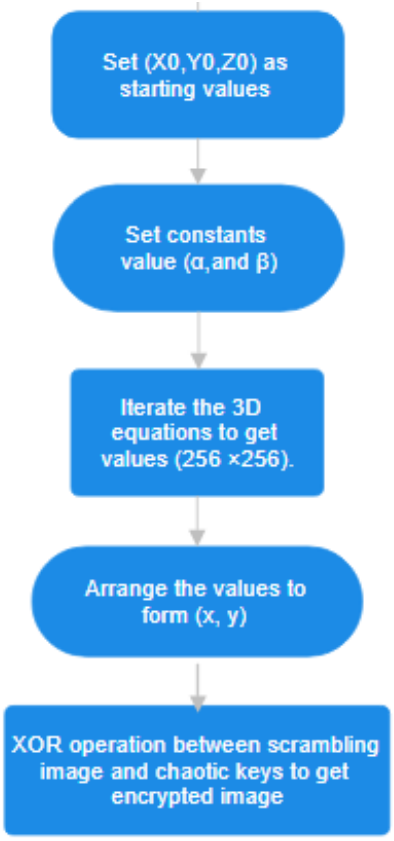

Figure 3: Steps of creating diffusion image.

ISSN:2222-758X
e-ISSN:2789-7362

C. Methodology

Steps to explain the applied algorithm:

1) Step 1: A random image is taken and after that the image is read and displayed using a specific algorithm after downloading the image from its storage location and is considered the original image.

2) Step 2: Determine the scrambling function where the image is divided into four quarters and then each quarter is divided separately and after completing the division process, scrambling is done on each color channel and displayed after the scrambling process as shown in Fig. 4.

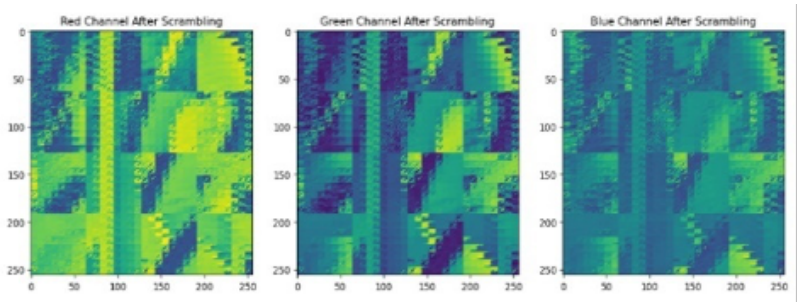

Figure 4: RGB channels before reconstructing pixel's location.

3) Step 3: After displaying each color channel separately before encryption using the method of determining the location of reconstruction pixels and then margining the channels to crate the scrambling image as shown in Fig. 5.

Figure 5: Scrambling image created.

4) Step 4: After collecting the color channels and creating the composite image, the encryption keys are now generated using the initial parameters $\alpha = 1.52$, $\beta = 0.05$ with the initial parameter values $x = 0.3$, $y = 0.2$, $z = 0.1$, $x_1 = 0.2$, $y_1 = 0.1$, $z_1 = 0.2$, and applied with the logistics system equations through the XOR operation with the encryption image in order to create the encrypted image as shown in Fig. 6.

ISSN:2222-758X
e-ISSN:2789-7362

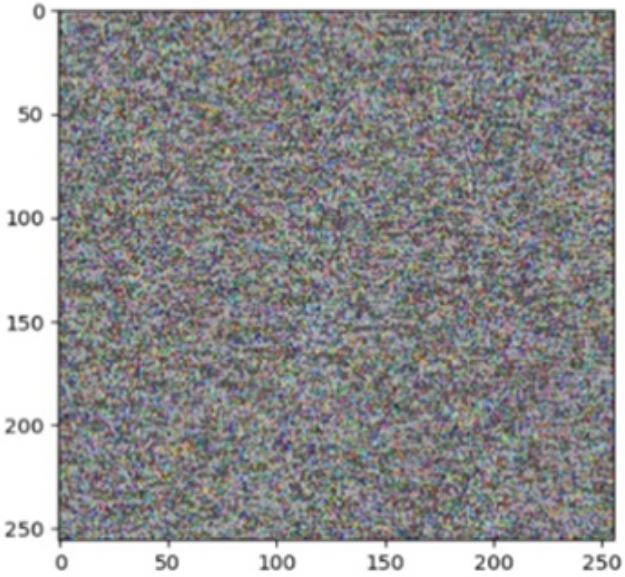

Figure 6: Encrypted image created using 3D Logistic Map.

5) Step 5: Decrypt the image using the same chaotic sequence and define the decrypted function, displaying the images using the revised function that handles images with or without alpha channels as shown in Fig. 7.

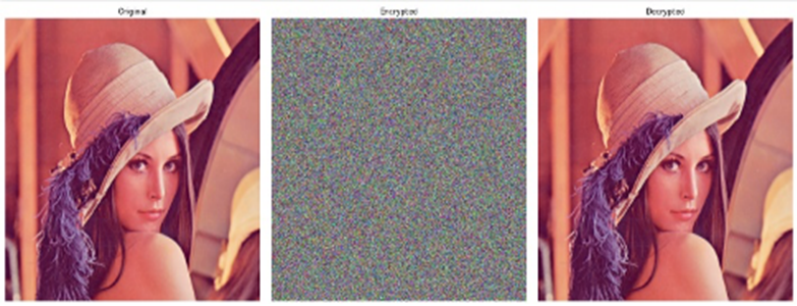

Figure 7: Encryption and Decryption Image: Original image, Encrypted image and, Decrypted image.

IV. PERFORMANCE ANALYSIS AND RESULTS

The stability is measured by statistical attacks, in this case Lena and Baboon images are chosen for testing. Some common security analyses are also used to evaluate the security of the proposed algorithm, histogram, entropy and correlation between pixels are calculated for statistical analysis, brute force analysis which includes key space analysis, key sensitivity, and finally differential calculus analysis (NPCR and UACI).

A. Statistical analysis

To test stability through statistical attacks, the histogram, entropy, and correlation between pixels of image are calculated.

ISSN:2222-758X
e-ISSN:2789-7362

1) Analysis of Histogram: A histogram is used to show the number of pixels for any Gray value in image [12]. Fig. 8 shows the histogram of original image, encrypted image and decrypted image, while in Fig. 9 shows histogram for each channel (RGB) for original and encrypted image.

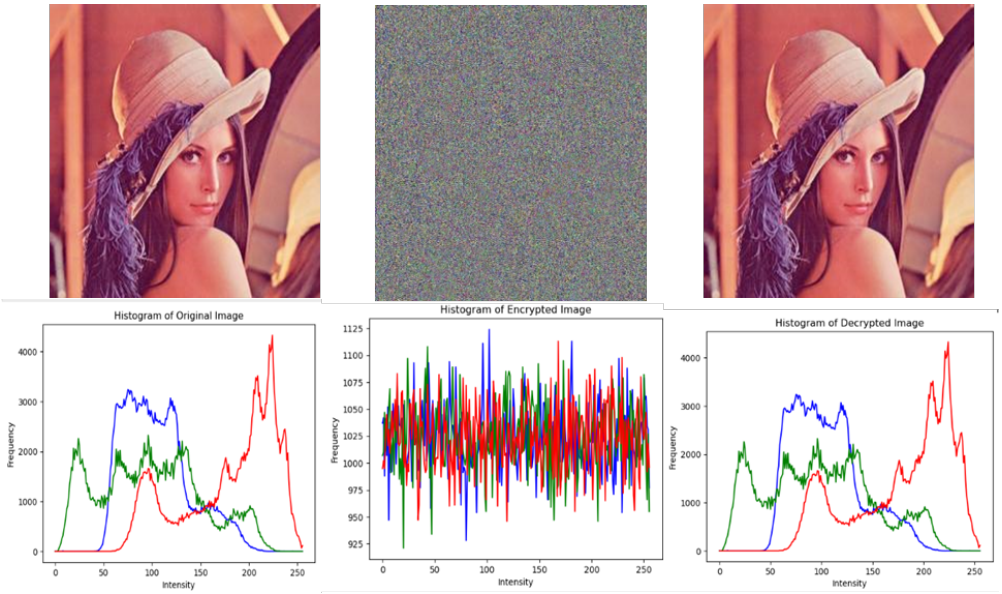

Figure 8: The difference values in the histogram for the original, encrypted and decrypted image.

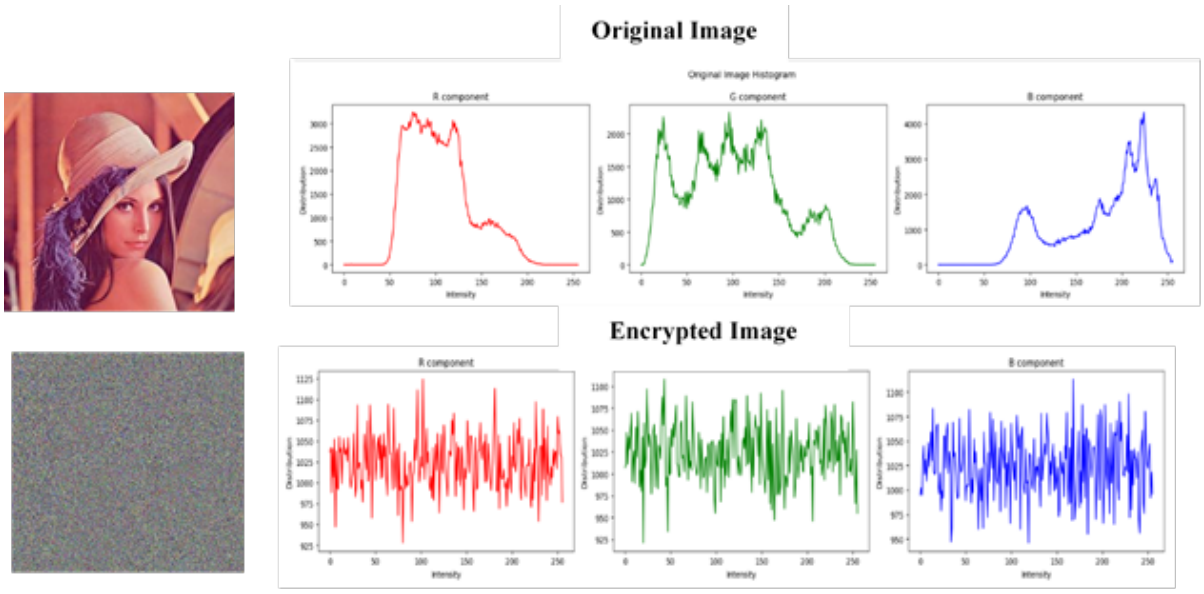

Figure 9: Histogram for each channel (RGB) for original and encrypted image.

2) Analysis of Correlation Coefficient: The effect of confusion and diffusion is examined in the proposed design; correlation coefficient analysis is used. In the cipher image, the correlation between adjacent pixels should be much lower than in the plain image. To determine whether the cipher image and the plain image are correlated. The horizontal average correlation coefficient of the pixels is studied. The Fig. 10 shows the Average Horizontal Correlation Coefficients (AHCC) of the original image, the cipher image, and the decipher image. Also, the correlation coefficient between original and encrypted image is 0.001.

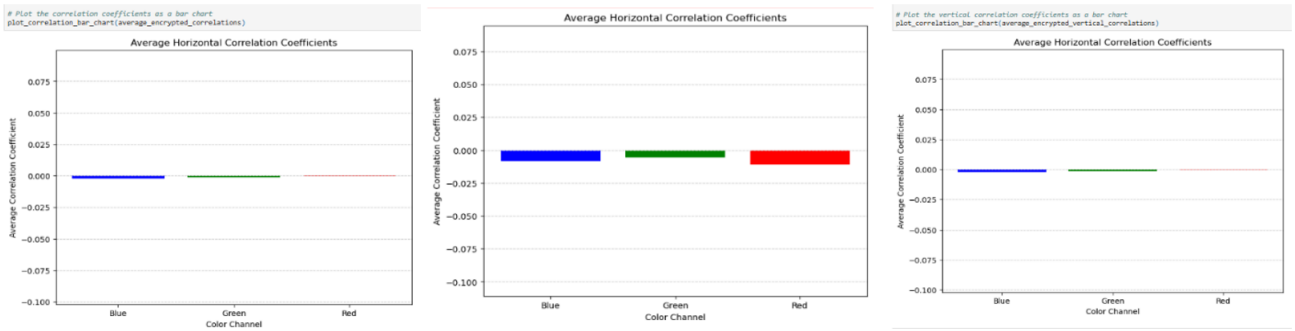

Figure 10: Average horizontal correlation coefficients (a) AHCC of original image, (b) AHCC of encrypted image (c) AHCC of decrypted image.

Using 256 neighbouring pixel pairs from the plain and encrypted images (vertical, horizontal, and diagonal), determine the correlation coefficients between two adjacent pixels using Eq. (3) adopted from [13]:

$$\text{corr.} = \frac{\sum_{i=1}^{w} (p_i - E(p))\,(q_i - E(q))}{\sqrt{\sum_{i=1}^{w} (p_i - E(p))^2}\sqrt{\sum_{i=1}^{w} (q_i - E(q))^2}} \tag{3}$$

Where, p_i and q_i are the pixel values in the original image as well as the encrypted image respectively. The correlation between two horizontally adjacent pixels in the plain image Lena and its ciphered image is displayed in Fig. 11, in the encrypted image, the correlation between neighbouring pixels is significantly lower.

3) Entropy analysis: Information entropy is used to measure and evaluate the degree of uncertainty and measure randomness or instability. The theory was first presented by Claude E. Shannon in 1949. The most famous formulas for information entropy in [14]:

$$H(S) = \sum_{i=0}^{2N-1} P(S_i)\,\log\left(\frac{1}{P(S_i)}\right) \tag{4}$$

In the (256*256) image for 8-bit, where N represents the number of Gray levels in the image while $P(S_i)$ represents the probability of the Gray level. For a perfect random image, the information entropy value is (8). The predictability of the method decreases when the information entropy goes to (8). In the proposed method, the information entropy of the encrypted image channel is obtained as blue = 7.993257%, green = 7.999279%, red = 7.999313% which is very close to the ideal value as shown in the Fig. 12. Table I shows that compared to the data obtained using the entropy values in the

ISSN:2222-758X
e-ISSN:2789-7362

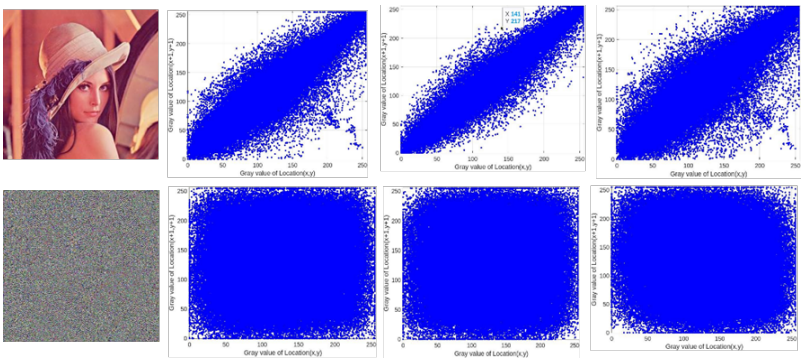

Figure 11: Pixels distribution for each original image correlation and encrypted image correlation.

3D logistic method, it is better compared to the literature.

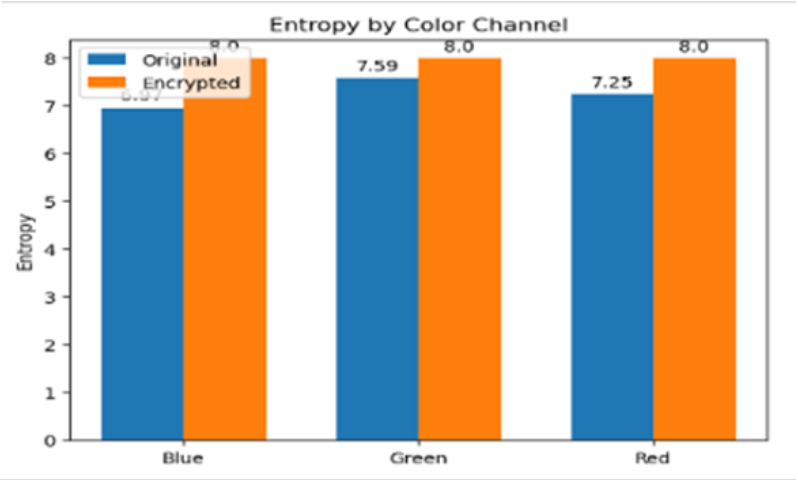

Figure 12: Entropy ratio of original and encrypted image.

TABLE I
Entropy Analysis

Proposed Method	Ref [11]	Ref [13]
7.9993	7.9978	7.9976

B. Brute-force attack Analysis

To make brute force attacks infeasible, the encryption algorithm must be sensitive to the encryption keys, and the key space must be large enough.

1) Analysis of key space: For the proposed method to be resistant to brute force attacks, the key space must be large enough. A value of 10^{96} shows that the method is resistant to brute force attacks [15].

ISSN:2222-758X
e-ISSN:2789-7362

2) Analysis of Key sensitivity: Regarding the secret key, the ideal image should be sensitive to the secret key, i.e. changing one bit in the key should produce a completely different cipher image. To test the key sensitivity of the proposed encryption scheme, the following steps were performed [16]:

Initially, the original image (Lena) was encrypted by changing the simple initial condition "x=0.3, y=0.2, z=0.1" to "x=0.31, y=0.2, z=0.1" where the resulting image was referred to as the encrypted image A with correlation value = 0.0640.

Step 1: For the image (Baboon) the same transformation process is applied to the image and also with a slight change of the initial condition "x=0.3, y=0.2, z=0.1" to "x=0.31, y=0.2, z=0.1" where the resulting image is referred to as the encrypted image B with a correlation value of 0.0638.

Step 2: Finally, the decrypted images A and B are displayed as shown in Fig. 13.

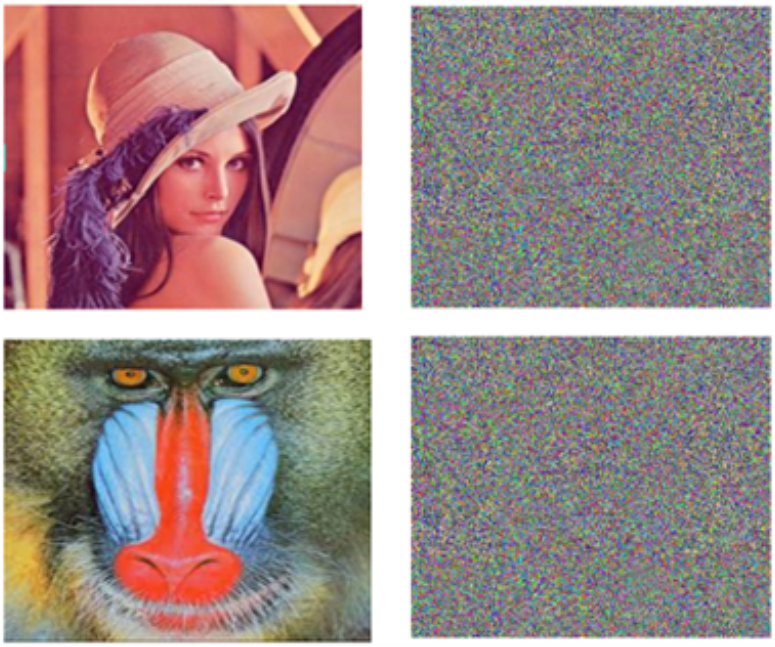

Figure 13: Result of change in initial values for each (Lena) and (Baboon) image.

C. Differential analysis

The encrypted image must be significantly different from its original form. This difference is measured by two criteria, NPCR and UACI [14] [15].

1) The Number of Pixel Change Rate (NPCR): The NPCR was defined as the rate at which a single pixel in the original image changes in an encrypted image. While the original photos had only one different pixel, the encrypted images' proportion of different pixel numbers is measured. The cryptosystem is more successful at fending off a plain-text attack the closer it gets to 100%. NPCR in Eq. (5) adopted from [17] :

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{5}$$

H is referred to as the height and W is the width of the encryption image. On the other hand, Table II shows that the proposed method has good performance with NPCR value= 99.6333%.

2) The Unified Average Changing Intensity (UACI): UACI is used to determine the average density difference between a cipher image and a plaintext image where the ability of a cryptosystem to withstand a differential attack increases with the size of UACI, mathematically in Eq. (6) as in [18] as follows:

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{6}$$

Table II shows that the proposed method has the better performance where the value of UACI is 35.2041%.

TABLE II
NPCR and UACI Analysis

Method	Image	NPCR	UACI
Proposed Method	Lena	99.6333%	35.2041%
Proposed Method	Baboon	99.6132%	33.5388%
Ref [10]	Lena	99.5826%	33.4213%
Ref [11]	Lena	99.6023%	33.4187%
Ref [13]	Baboon	99.7034%	33.0497%

V. DISCUSSION

In this section, the results of using 3D logistic chaotic maps to encrypt images will be explained. The experimental results demonstrate the strength of the proposed strategy against different types of attacks. Three logistic chaotic keys were used and the resulting image from the mixing process was subjected to an XOR process with the three chaotic keys and a completely encrypted image was produced. Also, through the values resulting from the performance analysis of the algorithm, which showed a high entropy value, which reached (7.9993) as well as high and good NPCR (99.6333%) and UACI (35.2041%) values compared to other algorithms, the strength of the proposed algorithm was concluded and it can be used against different types of attacks. The values obtained using this method are shown in Table III.

TABLE III
Comparison of proposed method with other chaotic system of Lena image

Method	NPCR	UACI	Entropy
3D Logistic map	99.6333%	35.2041%	7.9993
Arnold's cat map	99.6132%	33.5388%	7.9992

VI. CONCLUSION

In this paper, an approach to encrypt multimedia including images using 3D chaotic logistic maps is proposed. The image pixels are swapped and the Gray level settings are changed. Experimental results demonstrate the robustness of the proposed strategy, which changes the Gray value and is chaotically shuffled against various types of attacks. Compared with other proposed methods developed using Arnold-Cut map, it is also the best method. The results show that compared

with the data obtained using a different method, the entropy values, NPCR values and UACI values of the 3D logistic method are larger.

FUNDING

None.

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, "Analytic study of a novel color image encryption method based on the chaos system and color codes," Complexity, vol. 2021, no. 1, p. 5499538, 2021.
[2] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A color image encryption technique using block scrambling and chaos," Multimed Tools Appl, vol. 81, no. 1, pp. 505–525, 2022.
[3] Y. Bu, "Overview of image encryption based on chaotic system," in 2021 2nd International Conference on Computing and Data Science (CDS), IEEE, 2021, pp. 100–103.
[4] N. Chidambaram, P. Raj, K. Thenmozhi, and R. Amirtharajan, "Advanced framework for highly secure and cloud-based storage of colour images," IET Image Process, vol. 14, no. 13, pp. 3143–3153, 2020.
[5] R. Hamza, A. Hassan, T. Huang, L. Ke, and H. Yan, "An efficient cryptosystem for video surveillance in the internet of things environment," Complexity, vol. 2019, no. 1, p. 1625678, 2019.
[6] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," Entropy, vol. 22, no. 2, p. 175, 2020.
[7] M. A. Alkhonaini, E. Gemeay, F. M. Zeki Mahmood, M. Ayari, F. A. Alenizi, and S. Lee, "A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata," Scientific Reports, vol. 14, no. 1, p. 16701, 2024.
[8] R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," Annals of Data Science, vol. 11, no. 1, pp. 25-50, 2024.
[9] L. Li, A. A. Abd El-Latif, S. Jafari, K. Rajagopal, F. Nazarimehr, and B. Abd-El-Atty, "Multimedia cryptosystem for IoT applications based on a novel chaotic system around a predefined manifold," Sensors, vol. 22, no. 1, p. 334, 2022.
[10] Z. H. Thabit, S. A. Mehdi, and B. M. Nema, "Enhancing Color Image Security: Encryption with Dynamic Chaotic Three-Dimensional System and Robust Security Analysis," Al-Mustansiriyah Journal of Science, vol. 34, no. 4, pp. 87–95, 2023.
[11] G. Ye, K. Jiao, C. Pan, and X. Huang, "An effective framework for chaotic image encryption based on 3D logistic map," Security and Communication Networks, vol. 2018, no. 1, p. 8402578, 2018.
[12] R. M. Haris and S. Al-Maadeed, "Integrating blockchain technology in 5G enabled IoT: A review," in 2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT), IEEE, 2020, pp. 367–371.
[13] N. K. Pareek, "Design and analysis of a novel digital image encryption scheme," arXiv preprint arXiv:1204.1603, 2012.
[14] K. J. Aval, M. S. Kamarposhty, and M. Damrudi, "A simple method for image encryption using chaotic logistic map," Journal of Computer Science Computational Mathematics, vol. 3, no. 3, 2013.
[15] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," Signal Processing, vol. 128, pp. 155–170, 2016.
[16] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Opt Lasers Eng, vol. 88, pp. 197–213, 2017.
[17] G. Ye, K. Jiao, C. Pan, and X. Huang, "An effective framework for chaotic image encryption based on 3D logistic map," Security and Communication Networks, vol. 2018, no. 1, p. 8402578, 2018.
[18] C. Li, G. Luo, and C. Li, "An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map.," Int. J. Netw. Secur., vol. 21, no. 1, pp. 22–29, 2019.