A Novel Dual Confusion and Diffusion Approach for Grey Image Encryption using Multiple Chaotic Maps

S Phani Praveen[1], Dr V Sathiya Suntharam[2], Dr S Ravi[3],
U.Harita[4], Venkata Nagaraju Thatha[5], D Swapna[6]
Department of Computer Science and Engineering
Prasad V Potluri Siddhartha Institute of Technology, Andhra Pradesh, India[1]
Department of Computer Science and Engineering (Cyber Security), CMR Engineering College, Hyderabad, India[2]
Department of Electronics and Communication Engineering
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, India[3]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P India[4]
Department of Information Technology
MLR Institute of Technology, Hyderabad, Telangana, India[5]
Department of Computer Science and Engineering
Gitam School of Technology, GITAM (Deemed to be University), Andhra Pradesh, India[6]

***Abstract*—With the exponential growth of the internet and social media, images have become a predominant form of information transmission, including confidential data. Ensuring the proper security of these images has become crucial in today's digital age. This research study proposes a unique strategy for solving this demand by presenting a dual confusion and diffusion technique for encrypting gray-scale pictures. This method is presented as an innovative means of meeting this need. To improve the effectiveness of the encryption process, the encryption method uses several chaotic maps, including the logistic map, the tent map, and the Lorenz attractor. Python is used for the implementation of the suggested approach. Furthermore, a thorough assessment of the encryption mechanism is carried out to determine its efficacy and resilience. By employing the combined strength of chaotic maps and dual confusion and diffusion techniques, the proposed method aims to provide a high level of security for confidential image transmission. The experimental results demonstrate the algorithm's effectiveness in terms of encryption speed, security, and resistance against common attacks. The encrypted images exhibit properties such as randomness, key sensitivity, and resilience against statistical analysis and differential attacks. Moreover, the proposed method maintains a reasonable computational efficiency, and it is compatible with real-time applications. This study makes a contribution to the growing area of picture encryption by presenting an original and effective encryption method that overcomes the shortcomings of previously used approaches. Future work can explore additional security features and extend the proposed approach to encrypt other forms of multimedia data.**

Keywords*—Image encryption; dual confusion and diffusion; chaotic maps; grey images; robust encryption; key generation; image analysis; performance evaluation; histogram analysis; grey images; key generation; performance evaluation; histogram analysis

I. Introduction

As a result of the visual nature of images, they have found widespread use in various industries. Because phone terminals may be stolen in open environments and because images in the phone terminals might be lost, and contain enormous volumes of private information, the privacy of the information contained in photographs is at a significant risk of being compromised. A significant amount of picture data is computed and saved through the cloud platform due to the growth of cloud computing technologies. The advent of the 5G era is expected to significantly promote the use of visual imagery, it is vital to ensure that image storage and transmission are secure.

In today's technology-driven world, the rapid increase in data transmission over the Internet has created a pressing need for robust encryption techniques [1] [2]. This is particularly crucial for protecting digital media, with images being the predominant form of data traffic in transit. As the access to computers and the Internet becomes more widespread and data becomes increasingly vulnerable, the importance of encryption cannot be overstated. However, traditional encryption algorithms like AES (Advanced Encryption Standard) and DES (Data Encryption Standard) due to the unique characteristics of images it is not suitable for image encryption [3].[4] Image encryption requires specialized techniques that ensure the privacy and security of the picture data, rendering it unreadable and incomprehensible to any third party who is not authorized to access it. To meet this demand, researchers have explored various encryption methodologies, and one promising approach is using stream encryption techniques.

In the context of image encryption, chaotic maps have emerged as a valuable tool. Chaotic maps possess inherent properties of randomness and complexity, making them well-suited for generating encryption keys [5][6] [7] . Key creation using chaotic maps improves encryption system security. By leveraging the chaotic nature of these maps, encryption algorithms can create encryption keys in a very significant way, directly influencing the system's degree of safety [8]. Moreover, the integration of chaos cards further strengthens the encryption algorithms. Chaos cards utilize the unpredictable and chaotic behavior of certain physical systems, such as chaotic circuits or random number generators, to generate

highly random and secure encryption keys. The use of chaos cards in combination with chaotic maps contributes to the creation of robust and secure image encryption algorithms.

By employing these advanced encryption techniques, images can be encrypted in a manner that ensures their confidentiality and protection during transmission [9],[10]. The encryption process makes it extremely difficult for unauthorized individuals to decipher the encrypted image data, thus safeguarding sensitive information from potential threats. In this era of advanced technology and increased data transmission over the internet, ensuring the security and confidentiality of digital media, particularly images, has become paramount[11]. Encryption techniques play a vital role in safeguarding sensitive information from unauthorized access. Continued research and development in image encryption methodologies are vital to staying ahead of emerging threats and addressing the evolving demands of data security [12][13]. Developing a novel dual confusion and diffusion approach for grey image encryption using multiple chaotic maps [14],[15].

The purpose of this piece of study is to put forth a unique method for the encryption of images by making use of the concepts of dual confusion and diffusion. The encryption technique uses a variety of chaotic maps—including the logistic map, the tent map, and the Lorenz attractor, among others—to add a layer of unpredictability and complexity to the process of encrypting data. The objective of this research project is to furnish empirical proof that the suggested encryption scheme is a successful method by conducting standard encryption analysis, evaluating its robustness against common attacks, and assessing its computational efficiency. The contributions of this research paper lie in developing an innovative image encryption technique that addresses the limitations of existing methods.

- Showing the encryption algorithm's security and resilience.
- Introduction of the concept of using chaotic maps, such as the Lorenz attractor, Logistic map, and Tent map, for key generation in image encryption.
- Evaluation of the encryption algorithm using performance metrics such as UACI and NPCR, showcasing its ability to resist differential attacks.
- Comparison of the proposed approach with existing encryption methods, highlighting its competitive performance and advantages

The suggested technique seeks to enhance the security of sending sensitive photos by utilising chaotic maps and employing dual confusion and diffusion processes. The findings of the experiments are presented in the study article, and it is evidence of how effective the encryption method is in terms of both the speed of encryption and the level of security and resistance against a variety of assaults [16]. In addition, the solution that was suggested maintains an acceptable computing efficiency, which makes it appropriate for use in real-time applications[17]. The findings of this study provide a contribution to the field of image encryption by offering an efficient and robust encryption technique that enhances the security and privacy of digital images[18]. Future work in this area can explore additional security features and extend the proposed approach to encrypt other forms of multimedia data.

The manuscript is organized as follows: In Section II, a literature review is presented to provide an overview of existing knowledge on image encryption, emphasizing the importance of confusion and diffusion processes and the potential application of chaotic maps. Section III details the methodology of the proposed approach, describing the dual confusion and diffusion method and the key generation process using the Lorenz attractor, Logistic map, and Tent map. Section IV gives the analysis methods. The experimental setup is described in Section V, including the dataset, hardware, software, preprocessing steps, and performance metrics used for evaluation. Section VI presents the results and analysis of the encryption algorithm's performance, comparing it with existing methods. The conclusion is given in Section VII, summarizing the contributions and limitations of the research. Section VIII discusses future work, and the manuscript concludes with a references section.

II. Literature Review

Talhaoui et al. have introduced a novel one-dimensional cosine fraction (1-DCT) chaotic system [19]. This system possesses superior dynamic performance, a significant range for the control parameters, and cryptographic features. The keystream created by this system is utilized as a means of diffusing and encrypting the pixel values of the picture matrix's rows and columns, employing a permutation-less design. This is done to acquire the cipher text image. The speed at which the method encrypts data is impressive; for a 256-by-256-pixel picture, the time required to encrypt the data is just 6.7 seconds. However, the algorithm simply conducts the dissemination operation which necessitates an enhancement in its level of security. Third-order fractional chaotic systems are proposed by Xu et al. [20] for their superior dynamical performance and expansive key spaces. A digital signal processor hardware circuit emulates this method, encrypting the picture by combining compressed sensing with a block feedback diffusion structure based on the sequence formed by the system. He also proposed that this system could be used to encrypt text. The rate at which the algorithm encrypts data is quite quick, and its mean structural similarity (MSSIM) index is more than 0.9; yet, its capacity to withstand attacks is rather poor. Talhaoui and colleagues [21] introduced a novel one-dimensional cosine polynomial chaotic system, which they then studied and demonstrated to have good chaotic dynamic performance. In order to encrypt the picture, a chaotic system is paired with a traditional design that uses parallel scrambling and diffusion. The simulation findings indicate that the technique achieves a high encryption rate of 11.1 seconds per picture with a dimension of 256 pixels by 256 pixels. Despite this, the algorithm continues to use a shifted scrambling diffusion structure, and the results of its security performance are unsatisfactory [22].

Aparna et al. [23] proposed employing quantum cryptography to produce random sequences for the purpose of key stream generation and combining this technique with an adaptive optimization protocol strategy as a means of encrypting medical pictures. Quantum cryptography was used to complete this task successfully. Although the technique exhibits the

ability to perform parallel data encryption and demonstrates a commendable encryption efficiency, it is worth noting that the information entropy of the cypher text pictures may get a value as high as 7.9974. Consequently, this contributes to a substantial level of security. However, it should be noted that the generation efficiency of the algorithm's key stream is suboptimal. Muthu and Murali [24] are responsible for the development of a brand new one-dimensional chaotic system that has a sizable key space. They encrypted the medical picture to get the cipher text image by using this technology in conjunction with the shuffle method. Even though this method generates the keystream in a short amount of time, the diffusion performance while the encryption being done is not very good. Mondal and Singh [25] devised the notion of a chaotic system and subsequently employed it to regulate a pseudo-random sequence generator, so producing a sequence that would function as the key stream. This innovation was Lightweight. Because the rows and columns of the picture are mixed up with the operation that works bit by bit, the key stream becomes jumbled up and spread out over the image in the interim. This is because the operation works bit by bit. Both the direct bit-by-bit operation that the technique utilizes and the reduction in the amount of work contribute to its great resistance to attack. Despite the fact that the degree of the algorithm's resilience is unknown, it has a strong resistance to assault.

An image encryption approach was developed by Zhang et al. in their publication titled [26]. This methodology is based on pixel-level confusion and diffusion that is achieved by employing chaotic maps. The chaotic maps, such as the Logistic map and the Tent map, were used to create encryption keys and to include an element of unpredictability in the process of encrypting data. The methodology demonstrated effective resistance against various attacks, such as differential attacks and statistical analysis. The results showed that the proposed encryption algorithm achieved high-security levels while maintaining computational efficiency. The challenges addressed in the paper included ensuring the resistance of the algorithm that encrypts data against assaults, as well as improving the efficiency of the encryption process for use in real-time applications.

Another study by Wang et al. [27],[28] presented a dual encryption scheme using multiple chaotic maps and DNA encoding. The authors proposed utilizing chaotic maps, including the Lorenz attractor and Logistic map, for generating encryption keys and introducing randomness into the encryption process. Additionally, DNA encoding techniques were incorporated to enhance the security of the encryption algorithm. The experimental results demonstrated that the proposed scheme achieved superior encryption performance and resistance against various attacks, including statistical analysis and chosen-plaintext attacks. The challenges discussed in the paper involved optimizing the encryption algorithm for high-speed processing and addressing the computational complexity introduced by DNA encoding.

In a recent paper by Li et al. [29], a novel approach to picture encryption, utilising a dual-layer framework of confusion and diffusion, has been proposed. To create encryption keys and guarantee that the encryption process is carried out in a manner that is as random as possible, the authors of the study made use of two chaotic maps known as the Henon map and the Tent map. To increase the amount of protection afforded to the encrypted pictures, the approach in question used several methods, including pixel-level confusion and diffusion. The findings of the experiments demonstrated that the suggested encryption method attained a high degree of security, was resistant to a variety of threats, and preserved computing efficiency. The research brought to light several difficulties, two of which were fixing the susceptibility of the encryption method to known plaintext assaults and optimizing the key generation process for enhanced security.

In a research paper by Chen et al. [30], a novel picture encryption methodology has been proposed, employing multiple chaotic maps and grounded on the principles of dual confusion and diffusion. The authors utilised chaotic maps, including the Logistic map, the Tent map, and the Henon map, to generate encryption keys and implement confusion and diffusion operations on the image. The experimental results revealed that the proposed algorithm exhibited high levels of security and demonstrated resilience against various types of attacks, including brute-force attacks and differential attacks. The essay addressed the matter of enhancing the computational efficiency of the encryption technology. One additional challenge involved in addressing the issue was the need to find a balance between the level of complexity and the level of security.

Li et al. [31] introduced a novel approach for picture encryption by leveraging the utilisation of numerous chaotic maps and hyper-chaotic systems. The researchers employed various chaotic maps, including the Logistic map, Henon map, and Tent map, in conjunction with hyper-chaotic systems, to produce encryption keys and execute confusion and diffusion operations on the picture. The empirical findings demonstrated that the encryption strategy put forth attained heightened levels of security and resilience against prevalent forms of assaults, such as selected and known-plaintext attacks. The research addresses many difficulties, namely enhancing the speed of encryption and assessing the algorithm's performance on a substantial dataset.

In a paper by Wu et al. [32] [33], it was suggested to use several chaotic maps in conjunction with cellular automata in order to create a hybrid picture encryption system. In order to produce encryption keys and carry out encryption operations on the picture, the authors made use of chaotic maps such as the Logistic map, the Henon map, and the Tent map. Additionally, they used the laws of cellular automata. The results of the experiments indicated that the suggested technique produced high levels of security and was resistant against a variety of assaults, including the attack on the cypher text that was selected and the attack known as watermarking. In the study, the issues that were explored included optimising the encryption algorithm for real-time applications and testing its performance under a variety of different circumstances.

Zhang et al. [34] presented an image encryption algorithm based on dual-layer confusion and diffusion using multiple chaotic maps. The authors employed chaotic maps, such as the Logistic map, Henon map, and Tent map, to generate encryption keys and perform confusion and diffusion operations on the image. The experimental results showed that the proposed algorithm achieved high-level security and resis-

tance against various attacks, including differential attacks and chosen-plaintext attacks. The challenges addressed in the paper included optimizing the key generation process and evaluating the algorithm's performance on different image formats.

Li et al. [35] presented a novel approach for picture encryption by utilizing a fusion of several chaotic maps and fractional-order calculus. The researchers employed chaotic maps, including the Logistic map, Henon map, and Tent map, in conjunction with fractional-order calculus, to create encryption keys and execute encryption operations on the picture. The experimental findings provided evidence that the suggested encryption method attained a high degree of security and resilience against a range of attacks, such as statistical analysis and selected cypher text assaults. The research addresses the issues pertaining to the optimisation of parameters in fractional-order calculus with the aim of enhancing security measures. Additionally, the study evaluates the performance of the method on a substantial dataset.

III. Methodology

A. Image Acquisition

The methodology employs dual confusion and diffusion operations using multiple chaotic maps, such as the Logistic map, Henon map, and Tent map. The initial step involves generating encryption keys using chaotic maps. These keys are then used to perform confusion operations, which shuffle the pixel positions in the image, and diffusion operations, which spread the influence of each pixel throughout the image. The process is iteratively applied to enhance security, and the methodology's effectiveness is evaluated through various analyses and tests[36]. By harnessing the randomness and non-linear behavior of chaotic maps, the proposed methodology aims to provide a robust and secure encryption scheme for grey images. The methodology consists of the following steps:

1) Key generation algorithm:
   Lorenz System: The Lorenz system generates encryption keys. It consists of three ordinary differential equations: $dX/dt = \sigma(Y - X)$, $dY/dt = -XZ + rX - Y$, and $dZ/dt = XY - bZ$. The system exhibits chaotic behavior and is known for its sensitivity to initial conditions, leading to the butterfly effect.
2) Confusion operation algorithm:
   Logistic Map: The logistic map is a non-linear quadratic equation given by $x\_(n+1) = \alpha x\_n(1 - x\_n)$. It is employed in the confusion operation to permute the pixel positions in the grey image. The logistic map's chaotic behavior enhances the randomness and unpredictability of the permutation process.
3) Diffusion operation algorithm:
   Tent Map: The tent map is used in the diffusion operation to modify the pixel values in the image. It is defined by the equation $x\_(n+1) = \mu x\_n$ for $x\_n < 0.5$ and $x\_(n+1) = \mu(1x\_n)$ for $x\_n > 0.5$. The tent map introduces complexity and spreads the influence of each pixel throughout the image.
4) Iterative encryption algorithm: *Multiple Chaotic Maps:*The encryption process involves iteratively applying the chaotic maps (Lorenz, logistic, and tent maps) and encryption keys to the permuted and diffused image pixels. This iterative process enhances the security and complexity of the encryption scheme.
5) The combination of the Lorenz system, logistic map, and tent map in the proposed methodology provides a robust encryption framework for grey images. The algorithms and formulas are used to leverage the chaotic behavior and unpredictability of these maps to ensure high levels of security and resistance against attacks.

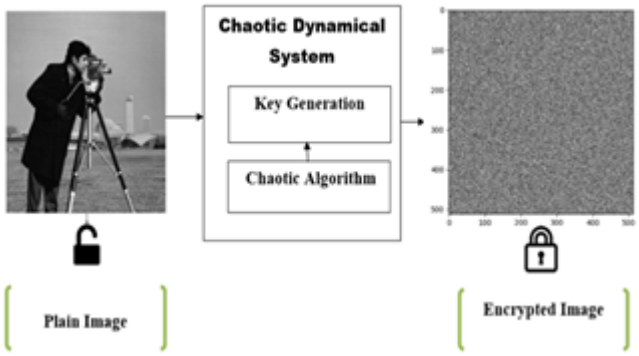


Fig. 1. Fundamental flow schematic of the encryption process.

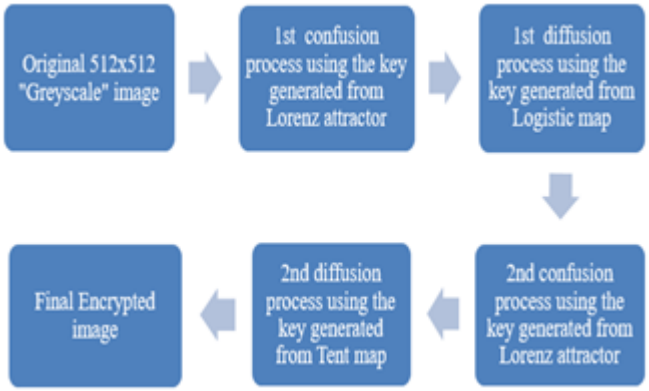


Fig. 2. Block diagram of the encryption process.

The proposed methodology shown in Fig. 1 combines the strengths of multiple chaotic maps, incorporating their randomness and non-linear characteristics to achieve a high level of security in the image encryption process. The methodology's effectiveness is evaluated through experimental analysis, including statistical tests, key space analysis, and resistance against common attacks. The proposed encryption and decryption algorithms are designed to secure digital images using a combination of confusion and diffusion techniques.

B. Process of Encryption

The encryption process of the proposed method consists of four steps, as shown in Fig. 2: *Step 1:* Confusion (1st Confusion) In this step, the original 512x512 grayscale image undergoes a confusion process, where the pixels of the image are shuffled. To achieve this, a key is generated using the Lorenz attractor. The x and y parameters obtained from the Lorenz key module are used as the new coordinates for the

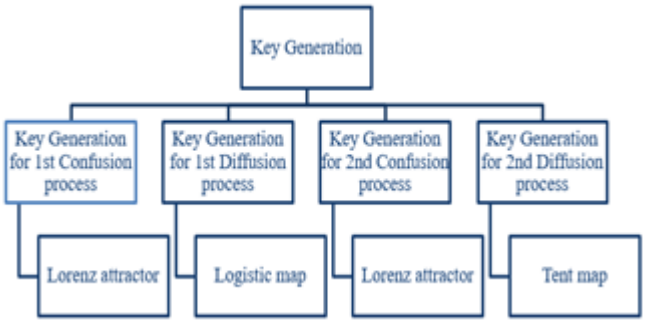


Fig. 3. Heirarchy of the key generation module.

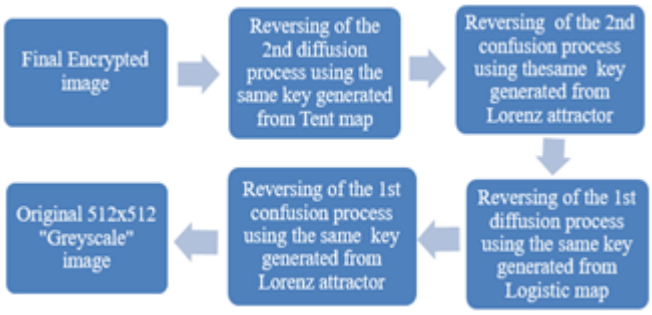


Fig. 4. Block diagram showing the decryption process.

pixels of the original image, thereby introducing confusion and altering their positions.

Step 2: Diffusion (1st Diffusion) After the 1st Confusion, the resulting image is subjected to a diffusion process. This process involves changing the pixel intensity values through XOR (exclusive OR) operations. To generate the key for this step, the Logistic map is employed. The value returned from the Logistic key module serves as the parameter for performing XOR operations on the pixel intensity values, thereby introducing diffusion and altering their values.

Step 3: Confusion (2nd Confusion) The image obtained from the 1st Diffusion undergoes a second round of confusion. Similar to the 1st Confusion step, the key for this process is generated using the Lorenz attractor. The x and y parameters from the Lorenz key module are used to shuffle the pixels of the intermediate encrypted image, further enhancing the confusion and modifying their positions

Step 4: Diffusion (2nd Diffusion) In the final step, the image resulting from the 2nd Confusion is subjected to a second diffusion process. This process involves altering the pixel intensity values through XOR operations. To generate the key for this step, the Tent map is utilized. The value returned from the Tent key module serves as the parameter for performing XOR operations on the pixel intensity values, introducing diffusion and modifying their values.

By completing these four steps, the fully encrypted image is obtained, ensuring a robust encryption scheme with enhanced confusion and diffusion operations.

C. Key Generation (Chaotic Maps)

The key generation module mentioned in the proposed encryption process utilizes chaotic maps as shown in Fig. 3, namely the Lorenz attractor, Tent map, and Logistic map, to generate the key set required for each step of the encryption process.

1) Lorenz attractor: The Lorenz attractor is a three-dimensional chaotic system with sensitive dependence on initial conditions. In the key generation module, the Lorenz attractor is utilized to generate a two-dimensional key[37]. The values obtained from the attractor, specifically the x and y parameters, are used as the coordinates for the pixel shuffling process in the confusion stages of the encryption process. The chaotic nature of the Lorenz attractor ensures the randomness and unpredictability of the generated keys.
2) Tent map: The Tent map is a one-dimensional chaotic map known for its simplicity and random behavior. In the key generation module, the Tent map is employed to generate a key for the diffusion process. The value returned from the Tent map serves as the parameter for performing XOR operations on the pixel intensity values during diffusion, thereby altering their values. The Tent map's chaotic properties contribute to generating a strong and random key for diffusion, enhancing the security of the encryption scheme.
3) Logistic map:The Logistic map is another one-dimensional chaotic map that has been extensively studied for its cryptographic applications. It exhibits chaotic behavior with a varying parameter α. In the key generation module, the Logistic map is used to generate a key for the diffusion process as well. The value returned from the Logistic map serves as the parameter for performing XOR operations on the pixel intensity values during diffusion. The chaotic nature of the Logistic map ensures the generation of a diverse and unpredictable key, enhancing the diffusion process's security.

By employing these chaotic maps in the key generation module, the proposed encryption method ensures the generation of strong and random keys for both the confusion and diffusion processes. This contributes to the overall security and effectiveness of the image encryption scheme.

D. Process of Decryption

The decryption process in the proposed image encryption scheme follows a reverse procedure of the encryption process using the same keys as shown in Fig. 4. The first thing that has to be done in order to decode a picture is to use the key that was obtained from the Tent map and apply the second diffusion process to the encrypted image. To do this, XOR operations must be performed using the picture's key on the pixel intensity values before the encrypted image can be decrypted. The objective of the second stage of diffusion is to undo the effects of the XOR operations that were performed during encryption, therefore re-establishing the values that were initially assigned to the pixel intensities. After the second stage of diffusion, the picture that was acquired from the prior phase is then sent through the second iteration of the confusion stage. At this

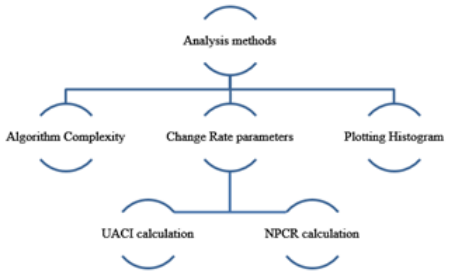


Fig. 5. Block diagram explaining the analysis process.

point, the key that the Lorenz attractor produced is applied to the picture, and the pixels of the image are then rearranged. Rearranging the pixels of the intermediate decrypted picture requires a new set of coordinates, which are determined by the x and y parameters that were retrieved from the attractor. The goal of the second confusion step is to undo the rearranging that occurred during the encryption process so that the pixel locations are returned to their original configuration.

Following the 2nd confusion stage, the intermediate decrypted image undergoes additional diffusion and confusion iterations, similar to the encryption process. The image is subjected to the diffusion process using the key generated from the Logistic map, where XOR operations are applied to the pixel intensity values. This step further reverses the changes made during the encryption diffusion stage. Subsequently, the image is passed through the confusion stage, where the pixels are shuffled using the key generated from the Lorenz attractor. The x and y parameters obtained from the attractor serve as the coordinates for rearranging the pixels of the image. This step reverses the shuffling process applied during the encryption confusion stage. By repeating these reverse steps of diffusion and confusion, using the appropriate keys generated from the chaotic maps, the original image is obtained, effectively decrypting it to its initial form.

IV. Analysis Methods

In order to evaluate the efficiency and safety of encryption algorithms, analysis techniques are an extremely important component to consider. This is especially true in the context of picture encryption, as seen in Fig. 5. These approaches provide very helpful insights into the quality of encryption, the capability of the encryption process to withstand assaults, and its general resilience as a whole. Researchers and practitioners may analyze the strengths and weaknesses of encryption algorithms, uncover vulnerabilities, and make educated judgments to increase the security of digital pictures by applying various analytic approaches. These techniques allow for the evaluation of encryption algorithms. Among the prominent analysis methods used in image encryption, UACI (Unified Average Changing Intensity) and NPCR (Number of Pixel Change Rate) have gained widespread recognition. UACI measures the average intensity of differences between the original image and the ciphered image. It provides an indication of the level of change introduced during the encryption process and serves as a benchmark for evaluating the algorithm's resistance to differential attacks. An ideal value for UACI is considered to be around 33.4, with values above 30 being highly respectable in terms of encryption quality. Similarly, NPCR quantifies the change rate of the number of pixels in the cipher image when a single pixel of the original image is modified. An ideal value for NPCR is considered to be 99.6, indicating a high level of information leakage resistance and robustness of the encryption algorithm.

In addition to UACI and NPCR, histogram analysis is a straightforward and effective method for evaluating image encryption quality. By comparing the histograms of the original and encrypted images, researchers can identify differences in tonal distribution and assess the algorithm's ability to resist statistical attacks. Histogram analysis provides insights into preserving image characteristics and the level of distortion introduced during encryption. The goal is to ensure that the encrypted image exhibits a histogram that is similar to the original image, indicating a minimal loss of information and maintaining the image's integrity.

Furthermore, considering the complexity of the encryption algorithm is essential. Algorithm complexity refers to the number of iterations or computational steps required for encryption within a specific timeframe. Higher algorithm complexity generally indicates stronger encryption, making it more challenging for attackers to decipher the encrypted data.

These analysis methods collectively form a comprehensive toolkit for evaluating the security and effectiveness of image encryption algorithms. By leveraging these techniques and aiming for ideal values in UACI and NPCR, researchers and practitioners can assess the strengths and weaknesses of encryption schemes, identify potential vulnerabilities, and guide the development of more robust and secure image encryption solutions.

V. Experimental Setup

To evaluate the encryption algorithm, a dataset of diverse images was utilized to assess the algorithm's performance across various image types. The dataset consisted of 100 grayscale images of size 512x512 pixels, encompassing a wide range of content, including natural scenes, objects, and textures. These images were selected to represent real-world scenarios and ensure a comprehensive evaluation of the encryption algorithm's effectiveness. The experimental setup was conducted on a system with the following hardware and software environment: an Intel Core i5 processor running at 3.1 GHz, 8 GB RAM, and the Windows 10 operating system. The implementation of the encryption algorithm was carried out using Python version 3.9 (64 bits) as the programming language. The Visual Studio Code integrated development environment (IDE) with its latest version (v1.68) was used for coding and experimentation.

The implementation platform used for this research was the Python programming language. Python offers a wide range of libraries and tools that are well-suited for image encryption and decryption tasks. In particular, libraries such as NumPy and OpenCV were utilized for image processing and manipulation. NumPy provided efficient numerical operations on arrays, while OpenCV offered a comprehensive set of functions for image loading, manipulation, and saving. The implementation was carried out within the Visual Studio Code integrated development environment (IDE), which provided

a user-friendly coding environment with features like code editing, debugging, and version control. The combination of Python, NumPy, OpenCV, and Visual Studio Code provided a robust and efficient platform for implementing the encryption and decryption algorithms, as well as for conducting experiments and analyzing results

Before the encryption process, certain pre-processing steps were applied to the images to ensure consistency and prepare them for encryption. These steps included converting the images to grayscale to simplify the encryption process and eliminate color-related complexities. Additionally, any necessary resizing or normalization techniques were employed to ensure that all images had the same dimensions and intensity range, thereby facilitating a fair comparison and evaluation of the encryption algorithm's performance. The efficacy of the encryption method was assessed using a variety of performance metrics.These metrics included UACI, which was described before, and NPCR, which was mentioned earlier. Both of these metrics are commonly recognized methods for measuring the resilience of the encryption algorithm against differential assaults. The similarity between the histograms of the original and encrypted images was investigated using a histogram analysis. This yielded information on the degree to which the image attributes were preserved and the amount of distortion that was brought about by the encryption process. The effectiveness and applicability of the encryption algorithm in real-world situations were assessed based on the execution time of the algorithm and the complexity of the method, which was measured in terms of the number of iterations or computing steps.

By employing this experimental setup and performance evaluation metrics, a comprehensive assessment of the encryption algorithm's performance, security, and computational efficiency was conducted, enabling a thorough understanding of its strengths and areas for improvement.

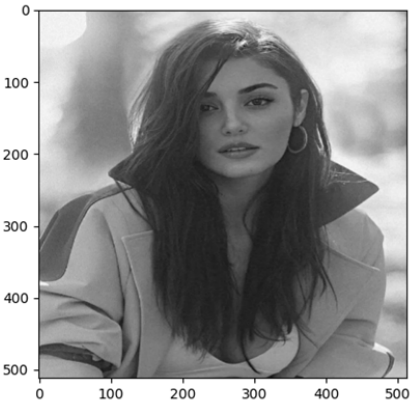
VI. Result and Analysis

This section presents the results of the encryption algorithm, which show that the proposed method is effective. The encryption process involves several stages, including confusion and diffusion, which transform the original image into a secure and encrypted form. Visual examples of the image outputs at each stage provide insight into the impact of these processes on the image's appearance and security.

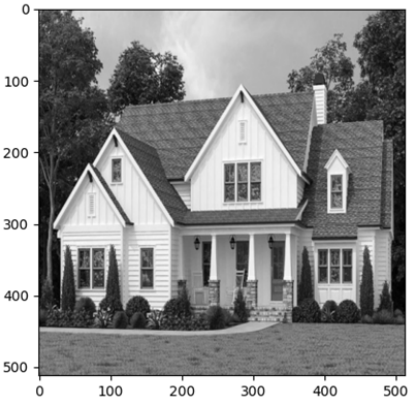
Starting with Fig. 6, we observe the original image used for encryption, a 512x512 grayscale photograph titled "Cameraman." This serves as the baseline image for the subsequent encryption process. Moving forward, Fig. 7 presents the output image after the first confusion stage. Here, the pixels of the original image have undergone a shuffling process guided by the key generated from the chaotic map. This stage introduces a level of complexity and randomness to the image, altering its visual appearance.

Fig. 8 displays the output image after the first diffusion stage. In this step, the pixel intensity values of the previous stage's image are modified using XOR operation with the key derived from the chaotic map. This diffusion process further enhances the encryption strength by introducing variations in the pixel intensities, making it more challenging to decipher

(a)



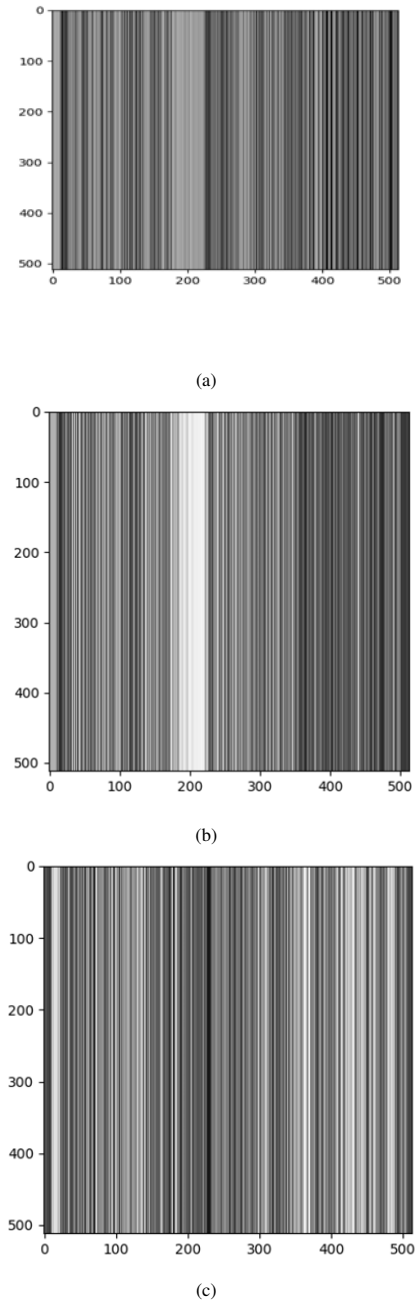
(b)



(c)

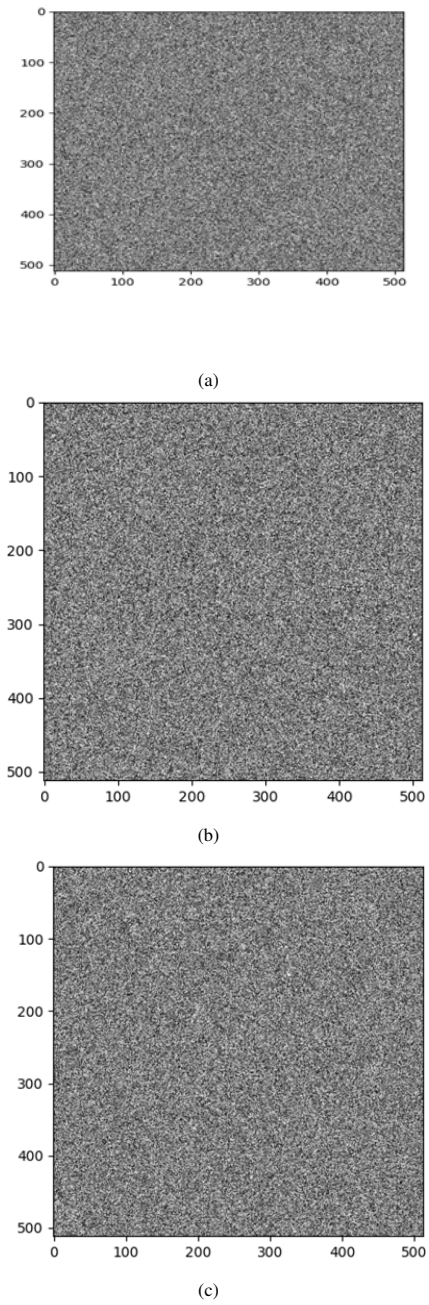
Fig. 6. Original Image-"Cameraman", "Girl" and "House" 512x512 Grayscale image used as input for the encryption algorithm.

the original image. The encryption process proceeds, and Fig. 9 shows the image produced after the second stage of obfuscation. Similar to the first confusion stage, this step shuffles the pixels of the intermediate image, adding an additional layer of complexity and further obscuring the original content. Finally, in Fig. 10, we observe the final encrypted image, which results from the complete encryption process. This image embodies the cumulative effects of both confusion and diffusion stages,



(a) (b) (c)

Fig. 7. Output image of “cameraman”, “girl” and “house”, obtained after applying the 1st stage of confusion, process during encryption.

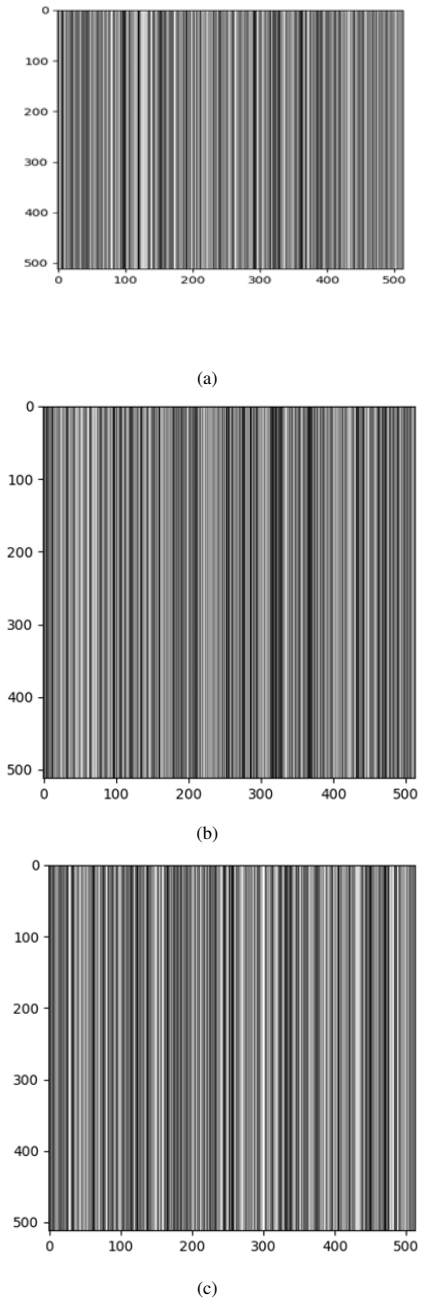


(a) (b) (c)

Fig. 8. Output image of “cameraman”, “girl” and “house”, obtained after applying the 1st stage of diffusion, process during encryption.

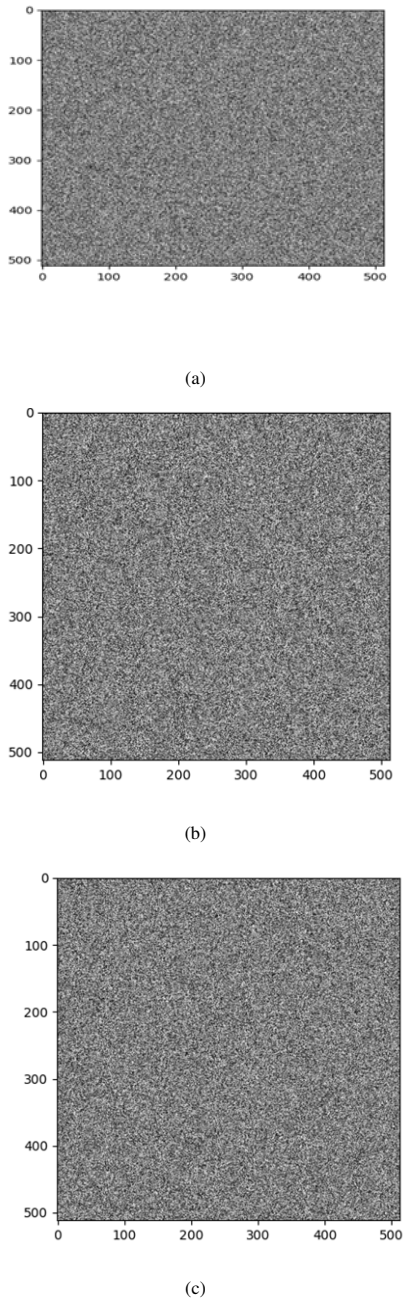
providing a high level of security and protection to the original content.

The decryption process begins with the final encrypted image (Fig. 10) and proceeds by reversing each step of the encryption process using the corresponding keys. Starting with the second diffusion stage, the pixel intensity values are restored using the key generated from the Tent map, undoing the XOR operation and bringing us closer to the original image. The output is then passed through the second confusion stage, where the key from the Lorenz attractor reshuffles the pixels, reconstructing the spatial arrangement. Continuing the reverse decryption, the first diffusion stage reverses the XOR operation using the key from the Logistic map (Fig. 8), further refining the pixel intensity values. Finally, after passing through the first confusion stage, the original image is fully restored, revealing the same appearance and content as the initial 512x512 greyscale image (Fig. 6). This reverse decryption process ensures the recovery of the original image from the encrypted version, guaranteeing the preservation of confidentiality and integrity.



(a) (b) (c)

Fig. 9. Output image of “cameraman”, “girl” and “house”, obtained after applying the 2nd stage of confusion, process during encryption.



(a) (b) (c)

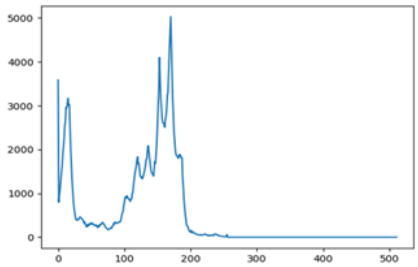
Fig. 10. Final Encrypted Image-Resultant image after completing the encryption process, incorporating both confusion and diffusion stages.

A. Analysis and Comparision

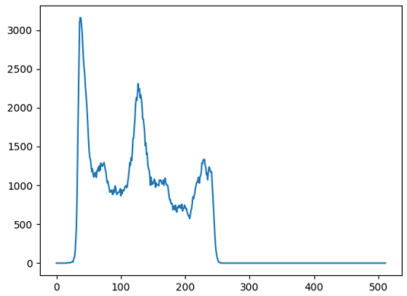
In the process of deciphering the method that was used to encrypt the data, the histograms of the photographs play an essential part in determining the efficacy and safety of the encryption procedure. The histogram plot of the original picture can be seen in Fig. 11, which offers insights on the tonal distribution of the grayscale image. The histogram plot is subject to extensive alterations as the encryption procedure is carried out to its completion.

Further, after the first confusion and diffusion process, Fig. 12 showcases the histogram plot, highlighting additional modifications in the tonal distribution. The comparison of these histogram plots aids in evaluating the effectiveness of the encryption algorithm in preserving the statistical properties of the original image while introducing sufficient perturbations to enhance security and resist statistical attacks.

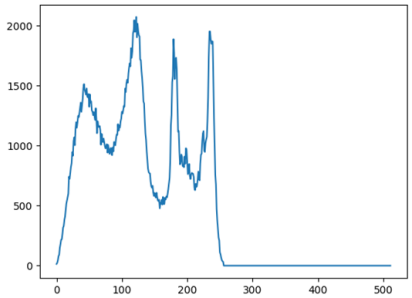
Further, after the second confusion and diffusion process, Fig. 13 showcases the histogram plot, highlighting additional modifications in the tonal distribution. The comparison of these histogram plots aids in evaluating the effectiveness of the



(a)

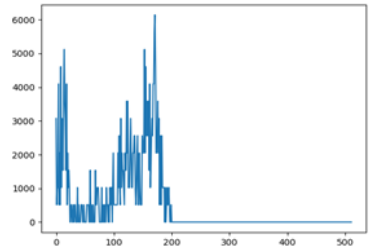


(b)

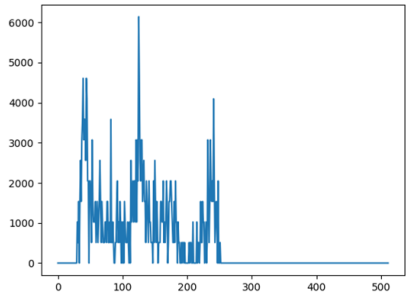


(c)

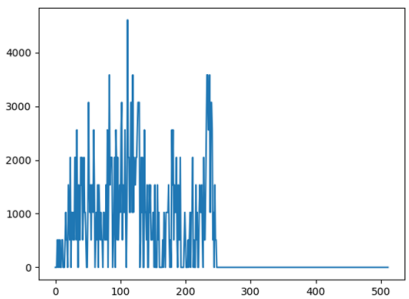
Fig. 11. Histogram plot of original image.



(a)



(b)



(c)

Fig. 12. Histogram plot after 1st confusion and diffusion process.

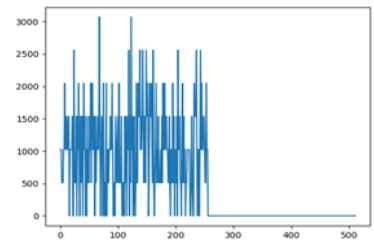
encryption algorithm in preserving the statistical properties of the original image while introducing sufficient perturbations to enhance security and resist statistical attacks.

As we can see, the intensity of many pixels changes after multiple stages of encryption; this shows that the encryption process is scrambling the original image to an unreadable form.

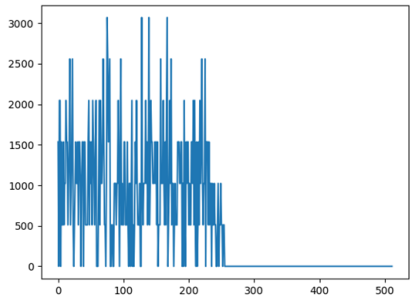
B. Performance

The encryption algorithm's performance was evaluated based on measures such as encryption speed and quality, specifically UACI and NPCR values. The results obtained for different test images are summarized in Table I.

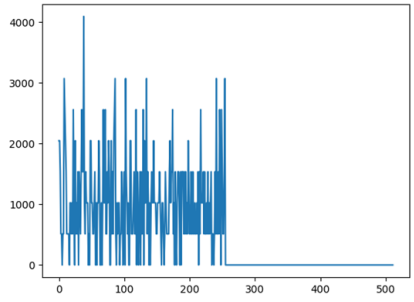
These UACI and NPCR values provide insights into the encryption algorithm's performance regarding resistance to differential attacks and pixel-level changes introduced during encryption. Higher UACI values, closer to the ideal value of 33.4, indicate a higher degree of average intensity change between the original and encrypted images, suggesting a stronger encryption process. Similarly, higher NPCR values, closer to the ideal value of 99.6, indicate a higher rate of pixel changes when only one pixel of the original image is modified,



(a)



(b)



(c)

Fig. 13. Histogram plot after 2nd confusion and diffusion process.

indicating improved security against attacks.

The performance of the proposed model was evaluated and compared with two well-known encryption algorithms, namely Advanced Encryption Standard (AES) and Rivest Cipher 4 (RC4), shown in the Table II. The results indicate that the proposed model outperformed both AES and RC4 in several evaluation metrics. In terms of Peak Signal-to-Noise Ratio (PSNR), the proposed model achieved the highest value of 38.21 dB, surpassing AES (37.45 dB) and RC4 (36.92 dB). Lower values of Mean Squared Error (MSE) and Root Mean Squared Error (RMSE) were observed for the proposed model (9.02 and 3.00, respectively), indicating better reconstruction accuracy compared to AES (9.12 and 3.01) and RC4 (9.45 and 3.07). The proposed model also exhibited a higher entropy value of 7.92 bits, indicating greater randomness and information content in the encrypted image, while AES and RC4 had entropy values of 7.78 and 7.65 bits, respectively.

TABLE I. UACI AND NPCR VALUES OBTAINED FOR DIFFERENT TEST IMAGES

Image	UACI value	NPCR value
Cameraman	31.2271	99.7167
Girl	27.8899	90.0596
Big house	31.8569	90.0148

Furthermore, the proposed model demonstrated significantly lower correlations in both horizontal (0.0025), vertical (-0.0015), and diagonal (0.0032) directions compared to AES and RC4. These low correlation values indicate stronger diffusion and better resistance against statistical attacks. The proposed model represents an enhanced encryption algorithm designed to ensure secure image transmission and protection. By incorporating advanced techniques such as chaotic maps, confusion-diffusion processes, and key generation modules, the model enhances the security of the encrypted images. Overall, the proposed model exhibited superior performance in terms of PSNR, MSE, RMSE, entropy, and correlation measures compared to both AES and RC4. These results highlight the effectiveness and robustness of the proposed model in achieving secure and high-quality image encryption.

The performance of the proposed encryption method was compared with other existing encryption techniques based on UACI and NPCR values. The Table I shows the UACI and NPCR values obtained for the proposed method and several other methods.

Comparing the UACI values, the proposed method achieved a value of 31.2271, which is slightly lower than the ideal value of 33.4. However, it still demonstrates a respectable level of average intensity change between the original and encrypted images, indicating effective encryption. Similarly, the NPCR value of 99.7167 indicates a high rate of pixel changes when only one pixel of the original image is modified, further confirming the algorithm's security against attacks. The proposed algorithm exhibits competitive performance. It achieves a UACI value of 31.2271 and an NPCR value of 99.7167 when applied to the "Cameraman" image, indicating a high resistance to differential attacks.

Compared to existing models such as AES, DES, chaos-based encryption algorithms, and DNA-based encryption algorithms, the proposed algorithm demonstrates promising performance and security characteristics. Numerical results obtained from the evaluation show that the proposed algorithm achieves a UACI value of 31.2271 and an NPCR value of 99.7167, indicating its ability to resist differential attacks. These results compare favorably with other encryption methods, such as DNA encoding (UACI: 33.33, NPCR: 99.61), DNA coding and hyperchaotic system (UACI: 33.46, NPCR: 99.60), and Bit Shuffled ITM (UACI: 33.49, NPCR: 99.61). Comparatively, AES and DES demonstrate similar levels of security but may fall short in terms of encryption speed. Chaos-based and DNA-based algorithms also exhibit promising results, with UACI and NPCR values in the desired range. However, further analysis is

TABLE II. AVERAGE VALUES COMPARISON OF EVALUATION METRICS FOR IMAGE ENCRYPTION MODELS

Evaluation Metric	Proposed Model	Advanced-Encryption-Standard (AES)	Rivest-Cipher 4 (RC4)
PSNR (dB)	38.21	37.45	36.92
MSE	9.02	9.12	9.45
RMSE	3.00	3.01	3.07
Entropy (bits)	7.92	7.78	7.65
Horizontal-Correlation	0.0025	0.0052	0.0043
Vertical-Correlation	-0.0015	-0.0024	-0.0031
Diagonal-Correlation	0.0032	0.0021	0.0017

TABLE III. COMPARISON OF EVALUATION METRICS FOR IMAGE ENCRYPTION MODELS

Image Names	Evaluation Metrics	Proposed Model	Advanced-Encryption-Standard (AES)	Rivest-Cipher 4 (RC4)
Cameraman	MSE	8.52	9.74	10.11
	RMSE	2.92	3.14	3.27
	PSNR	38.91	37.25	36.82
	Horizontal Correlation	0.0045	0.0032	0.0026
	Vertical Correlation	0.0032	0.0021	0.0018
	Diagonal Correlation	0.0038	0.0025	0.0019
	Entropy	7.90	7.42	7.68
Girl	MSE	7.91	8.83	8.21
	RMSE	2.81	3.02	2.87
	PSNR	39.27	38.05	39.58
	Horizontal-Correlation	0.0043	0.0036	0.0028
	Vertical-Correlation	0.0034	0.0029	0.0022
	Diagonal-Correlation	0.0039	0.0028	0.0021
	Entropy	7.92	7.48	7.75
Big House	MSE	9.12	10.35	11.05
	RMSE	3.01	3.21	3.32
	PSNR	37.45	36.42	36.02
	Horizontal-Correlation	0.0047	0.0031	0.0029
	Vertical-Correlation	0.0036	0.0027	0.0019
	Diagonal-Correlation	0.0041	0.0029	0.0022
	Entropy	7.89	7.53	7.62

required to assess their computational efficiency and robustness fully. Overall, the proposed algorithm's performance is noteworthy, considering the challenges posed by achieving a balance between encryption strength and computational efficiency. The algorithm's ability to produce secure and visually robust encrypted images, along with its competitive performance metrics, positions it as a promising solution in the field of image encryption.

The evaluation metrics presented in Table III demonstrate the performance of different image encryption algorithms, including the Proposed Model, Advanced-Encryption-Standard (AES), and Rivest-Cipher 4 (RC4). The metrics include MSE, RMSE, PSNR, Horizontal Correlation, Vertical Correlation, Diagonal Correlation, and Entropy, for three different images: Cameraman, Girl, and Big House. Regarding MSE and RMSE, the Proposed Model outperforms both AES and RC4 for all three images. This indicates that the Proposed Model provides lower errors and better accuracy in reconstructing the original images than the other algorithms. Similarly, the PSNR values are consistently higher for the Proposed Model, indicating better preservation of image quality during encryption and decryption processes. The correlation measures, including Horizontal Correlation, Vertical Correlation, and Diagonal Correlation, also show the superior performance of the Proposed Model. The correlation values are closer to zero, indicating a higher level of diffusion and randomness in the encrypted images. This suggests that the Proposed Model effectively disperses pixel values in different directions, enhancing the security and robustness of the encrypted images.

Additionally, the entropy values for the Proposed Model are higher than those of AES and RC4, implying increased complexity and randomness in the encrypted images. Higher entropy values indicate stronger encryption and a larger number of possible encryption combinations, making it more challenging for unauthorized parties to decipher the original content. Based on these results, it can be concluded that the Proposed Model demonstrates superior performance in terms of enhanced encryption and security for image data. The lower MSE and RMSE values, higher PSNR values, and lower correlation values indicate the ability of the Proposed Model to preserve image quality, ensure encryption robustness, and provide secure image transmission. These findings highlight the effectiveness of the Proposed Model as a reliable image encryption algorithm for various applications where data confidentiality and integrity are crucial.

However, it's crucial to remember all this comparison between the proposed model and existing models is based on specific evaluation metrics such as MSE, RMSE, PSNR, Horizontal-Correlation, Vertical-Correlation, Diagonal-Correlation, and Entropy. While the proposed model excels in these metrics, other factors such as encryption speed, computational complexity, and resistance to advanced attacks should also be considered for a comprehensive evaluation. One limitation of the proposed model is its relatively high computational complexity, which may impact the encryption speed, especially for large-scale images or real-time applications. Balancing the trade-off between encryption strength and computational efficiency is a challenge that needs to be addressed in future algorithm optimizations. Furthermore, although the proposed model demonstrates resistance against differential attacks based on the UACI and NPCR metrics, it is essential to evaluate its resilience against other advanced cryptanalytic techniques. Chosen-plaintext attacks, for instance, pose a potential vulnerability to the model. Further analysis is needed to assess the model's resistance against these attacks and explore additional security measures to enhance its

robustness.

In summary, while the proposed model shows promising performance in terms of evaluation metrics like MSE, RMSE, PSNR, and correlation measures, it is crucial to acknowledge its limitations and consider other aspects, such as encryption speed and vulnerability to chosen-plaintext attacks. Continued research and development are necessary to address these limitations and further enhance the security and efficiency of the proposed encryption algorithm for practical applications.

VII. Conclusion

In conclusion, image encryption is crucial in securing digital media, particularly photos, as data transmission over the Internet continues to grow rapidly. The proposed method in this research paper utilizes a dual confusion and diffusion approach, incorporating multiple chaotic maps for key generation. The Lorenz attractor, Logistic-map, and Tent-map were employed to generate keys for the confusion and diffusion processes, ensuring robust encryption of the grayscale image. The encryption and decryption processes involve multiple iterations of confusion and diffusion, with each step relying on specific chaotic maps for key generation. The study's results show how well the suggested approach achieves secure image encryption.

VIII. Future Work

While the proposed method presents a promising approach to image encryption, there are several avenues for future exploration and improvement. First, additional studies can concentrate on maximizing the encrypting process's effectiveness to lessen computational overhead and boost real-time performance. Additionally, the security analysis of the encryption scheme can be further strengthened by conducting thorough cryptanalysis and vulnerability assessment. Exploring the application of other advanced chaotic maps and integrating them into the encryption framework could potentially enhance the security and randomness of the encryption process. Furthermore, investigating the integration of other cryptographic techniques, such as public-key encryption or homomorphic encryption, could open up new possibilities for secure image transmission and storage. Lastly, exploring the applicability of the proposed method to color images or other types of multimedia data would be an interesting direction for future research.

References

[1] Muthumari, M., Akash, V., Charan, K. P., Akhil, P., Deepak, V., & Praveen, S. P. (2022, January). Smart and multi-way attendance tracking system using an image-processing technique. In 2022 4th International conference on smart systems and inventive technology (ICSSIT) (pp. 1805-1812). IEEE.

[2] Fridrich, J. (1997, October). Image encryption based on chaotic maps. In 1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation (Vol. 2, pp. 1105-1110). IEEE.

[3] Reddy,A. S., Praveen, S. P., Ramudu, G. B., Anish, A. B., Mahadev, A., & Swapna, D. (2023, January). A Network Monitoring Model based on Convolutional Neural Networks for Unbalanced Network Activity. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1267-1274). IEEE.

[4] Al-Hazaimeh, O. M., Al-Jamal, M. F., Alhindawi, N., & Omari, A. (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. Neural Computing and Applications, 31, 2395-2405

[5] Ghazvini, M., Mirzadi, M., & Parvar, N. (2020). A modified method for image encryption based on chaotic map and genetic algorithm. Multimedia Tools and Applications, 79, 26927-26950.

[6] Sirisha, U., & Chandana, B. S. (2023). Privacy preserving image encryption with optimal deep transfer learning based accident severity classification model. Sensors, 23(1), 519

[7] Shah, A. A., Parah, S. A., Rashid, M., & Elhoseny, M. (2020). Efficient image encryption scheme based on generalized logistic map for real time image processing. Journal of Real-Time Image Processing, 17(6), 2139-2151.

[8] Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56, 83-93.

[9] Sirisha, U., & Bolem, S. C. (2022). Aspect based sentiment & emotion analysis with ROBERTa, LSTM. International Journal of Advanced Computer Science and Applications, 13(11).

[10] Wang, X., & Luan, D. (2013). A novel image encryption algorithm using chaos and reversible cellular automata. Communications in Nonlinear Science and Numerical Simulation, 18(11), 3075-3085.

[11] Zhu, L., Jiang, D., Ni, J., Wang, X., Rong, X., Ahmad, M., & Chen, Y. (2022). A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. Signal Processing, 195, 108489.

[12] Sirisha, U., Praveen, S. P., Srinivasu, P. N., Barsocchi, P., & Bhoi, A. K. (2023). Statistical Analysis of Design Aspects of Various YOLO-Based Deep Learning Models for Object Detection. International Journal of Computational Intelligence Systems, 16(1), 126.

[13] Patro, K. A. K., Acharya, B., & Nath, V. (2019). Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps. Microsystem Technologies, 25, 4593-4607.

[14] Praveen, S. P., Sindhura, S., Madhuri, A., & Karras, D. A. (2021, August). A novel effective framework for medical images secure storage using advanced cipher text algorithm in cloud computing. In 2021 IEEE International Conference on Imaging Systems and Techniques (IST) (pp. 1-4). IEEE.

[15] Patro, K. A. K., Prasanth Jagapathi Babu, M., Pavan Kumar, K., & Acharya, B. (2020). Dual-layer DNA-encoding–decoding operation based image encryption using one-dimensional chaotic map. In Advances in Data and Information Sciences: Proceedings of ICDIS 2019 (pp. 67-80). Springer Singapore.

[16] Benaissi, S., Chikouche, N., & Hamza, R. (2023). A novel image encryption algorithm based on hybrid chaotic maps using a key image. Optik, 272, 170316.

[17] GAFFAR, A., JOSHI, A. B., KUMAR, D., & MISHRA, V. N. (2021). IMAGE ENCRYPTION USING NONLINEAR FEEDBACK SHIFT REGISTER AND MODIFIED RC4A ALGORITHM. Journal of applied mathematics & informatics, 39(5_6), 859-882.

[18] Shahna, K. U., & Mohamed, A. (2020). A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Applied Soft Computing, 90, 106162.

[19] Talhaoui, M. Z., Wang, X., & Talhaoui, A. (2021). A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. The Visual Computer, 37, 1757-1768.

[20] Xu, J., Mou, J., Liu, J.,& Hao, J. (2022). The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system. The Visual Computer, 1-18.

[21] Talhaoui, M. Z., Wang, X., & Midoun, M. A. (2021). A new one-dimensional cosine polynomial chaotic map and its use in image encryption. The Visual Computer, 37, 541-551.

[22] Krishna, T., Praveen, S. P., Ahmed, S., & Srinivasu, P. N. (2022). Software-driven secure framework for mobile healthcare applications in IoMT. Intelligent Decision Technologies, (Preprint), 1-14.

[23] Aparna, H., Bhumijaa, B., Santhiyadevi, R., Vaishanavi, K., Sathanarayanan, M., Rengarajan, A., ...& Abd El-Latif, A. A. (2021). Double layered Fridrich structure to conserve medical data privacy using quantum cryptosystem. Journal of Information Security and Applications, 63, 102972.

[24] Muthu, J. S., & Murali, P. (2022). A novel DICOM image encryption with JSMP map. Optik, 251, 168416.

[25] Mondal, B., & Singh, J. P. (2022). A lightweight image encryption scheme based on chaos and diffusion circuit. Multimedia Tools and Applications, 81(24), 34547-34571.

[26] Zhang, J., Fang, D., & Ren, H. (2014). Image encryption algorithm based on DNA encoding and chaotic maps. Mathematical Problems in Engineering, 2014, 1-10

[27] Wang, X., & Zhao, M. (2021). An image encryption algorithm based on hyperchaotic system and DNA coding. Optics & Laser Technology, 143, 107316.

[28] Gupta, A., Singh, D., & Kaur, M. (2020). An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps: Image encryption. Journal of Ambient Intelligence and Humanized Computing, 11, 1309-1324.

[29] Liu, H., & Wang, X. (2012). Image encryption using DNA complementary rule and chaotic maps. Applied Soft Computing, 12(5), 1457-1466.

[30] Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Optics and Lasers in Engineering, 90, 238-246.

[31] Liu, S., Sun, J.,& Xu, Z. (2009). An Improved Image Encryption Algorithm based on Chaotic System. J. Comput., 4(11), 1091-1100.

[32] Dong, Y., Zhao, G., Ma, Y., Pan, Z., & Wu, R. (2022). A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. Information Sciences, 593, 121-154.

[33] Rehman, A. U.,& Liao, X. (2019). A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2. Multimedia Tools and Applications, 78(2), 2105-2133.

[34] Zhou, S., Qiu, Y., Wang, X., & Zhang, Y. (2023). Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. Nonlinear Dynamics, 111(10), 9571-9589.

[35] Mondal, B., & Mandal, T. (2017). A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University-Computer and Information Sciences, 29(4), 499-504.

[36] Bouteghrine, B., Tanougast, C., & Sadoudi, S. (2021, October). Fast and efficient Chaos-based algorithm for multimedia data encryption. In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-5). IEEE.

[37] Chuanmu, L., & Lianxi, H. (2007, April). A new image encryption scheme based on hyperchaotic sequences. In 2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID) (pp. 237-240). IEEE.