IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 15, Issue 3, March 2025, ||Series -1|| PP 19-24

Hybrid Chaotic System-Based Encryption and Decryption for Medical Images Using Logistic and Improved Logistic Maps

Mallidi Rishika kumari[1], Barthu Likhitha[2], Surla Jyothi[3], Panthadi Charan Sri Sai[4], Dr. M.Raghunath[5]

[1,2,3,4] *B.Tech Scholars, Department of ECE,*

[5]*Professor, Department of ECE, Aditya College of Engineering and Technology, Surampalem, Kakinada, AP, India.*

ABSTRACT

Since the medical images frequently contain sensitive patient data, the growing digitization of healthcare has raised serious concerns about medical image security. In order to provide strong protection, this study suggests a revolutionary two-stage encryption method for medical photos that combines the Lorenz Algorithm with an Improved Logistic Chaotic Map. Steganography is also used to embed the encrypted image in a cover file, which hides the data and adds an additional layer of security.The technology fixes vulnerabilities that arise when medical images are sent and stored across unprotected networks or cloud services. Preprocessing methods guarantee effective encryption without sacrificing image quality. This strategy seeks to adhere to stringent patient data privacy laws, enhance health informatics security, and protect medical data. The suggested approach shows great promise for effectively protecting huge, high-resolution medical photographs, which qualifies it for use in practical healthcare settings.

Keywords: Lorenz Algorithm, Steganography, Chaotic Systems, Medical Image Encryption, Patient Data Privacy, Health Informatics Security, and Encryption.

I. INTRODUCTION

The management and transmission of medical data, especially medical images, has changed dramatically as a result of the quick development of digital healthcare systems. Sensitive patient data in these images, which are essential for diagnosis and treatment, must be kept private and safe. However, the growing dependence on digital platforms has made such data vulnerable to serious security threats, such as cyberattacks and illegal access.The intricacy and scale of medical images can make traditional encryption techniques inadequate, particularly when sent over unprotected networks or kept in susceptible cloud systems. This calls for the creation of sophisticated encryption methods that offer strong security without sacrificing usability.A viable approach to encryption is provided by chaotic systems, which are characterized by their unexpected behavior and sensitivity to initial conditions. Steganography also provides a way to hide data by embedding encrypted images into unsuspecting files, thereby enhancing security. This project presents a two-stage encryption framework that combines chaos maps and encryption techniques with steganography to ensure privacy and integrity of medical images in medical applications.

sector remains a prime target for cyberattacks. It provides an alternative to traditional encryption methods like AES, which may not be optimized for handling large, complex image files, making it particularly suitable for institutions managing vast volumes of data. By incorporating chaotic logistic maps, the project advances cryptographic techniques, creating more adaptive and resilient encryption methods that could extend beyond healthcare. Furthermore, the project plays a vital role in protecting patient privacy, maintaining trust in digital healthcare systems by securing sensitive medical data. Through steganography, it adds an extra layer of security, making it highly relevant for confidential medical communications where interception risks are significant.

II. OBJECTIVES

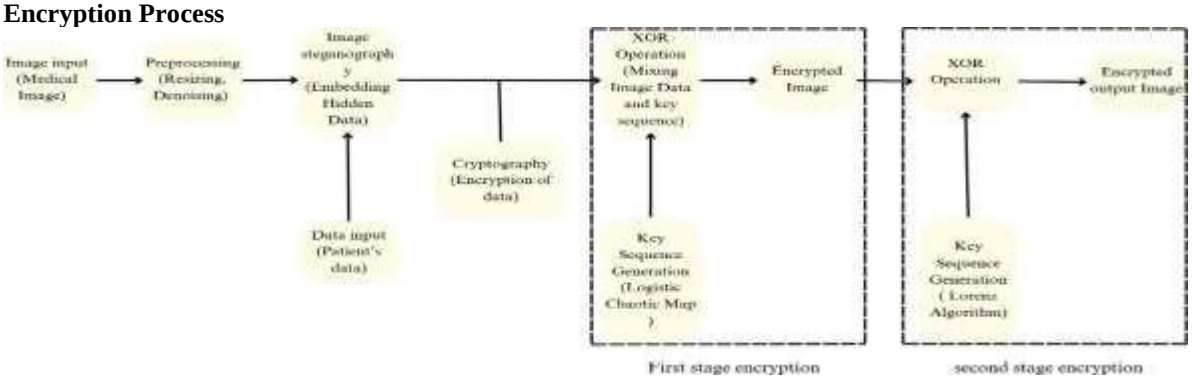
The objective of this project is to develop a robust medical image encryption algorithm based on chaotic logistic mapping, cryptography, and steganography to ensure the secure storage and transmission of sensitive medical data such as MRI, CT scans, and X-rays. By leveraging the unpredictability and non-linearity of chaotic logistic mapping, the algorithm aims to generate highly secure encryption keys, enhancing resistance to cryptographic attacks. The project also integrates steganography to embed encrypted medical images into carrier media, ensuring inconspicuous and secure transmission while maintaining minimal distortions in the carrier files.

A key focus is on preserving the quality of medical images after decryption, ensuring diagnostic accuracy and compliance with privacy regulations such as HIPAA and GDPR. The algorithm will be designed for high efficiency and scalability to handle diverse medical datasets and real-time applications. Rigorous testing and validation will be conducted to evaluate its resistance to common attacks, performance metrics like PSNR and SSIM, and comparative efficiency against existing methods. Additionally, the project aims to facilitate secure telemedicine applications, ensuring reliable data sharing over insecure networks, while also providing a user-friendly interface for healthcare professionals. Through this work, the project contributes to advancing research at the intersection of chaos theory, cryptography, and steganography, addressing critical needs in medical image security.

III. METHODOLOGY

The methodology for securing medical data through visual cryptography and chaotic mapping involves a systematic encryption and decryption process that ensures confidentiality, integrity, and robustness of sensitive medical images and patient information. Below is a detailed explanation of the **encryption** and **decryption processes**, tailored into a project paper format.

Encryption Process



The encryption process is a multi-stage procedure designed to transform sensitive medical images into secure, encrypted forms while embedding patient information. The process includes the following key steps:

1. Image Input (Medical Image)

The encryption process begins with the acquisition of a raw medical image (e.g., MRI, CT scan, or X-ray). Medical images contain sensitive information about patients, such as diagnostic details, which necessitates their protection during storage and transmission. This raw input serves as the foundation for subsequent encryption.

2. Preprocessing (Resizing and Denoising)

In this step, the medical image undergoes preprocessing to prepare it for encryption.

- **Resizing:** The image is resized to a standard dimension to ensure compatibility across diverse systems.
- **Denoising:** Noise and artifacts present in the raw image are removed using filtering techniques to enhance clarity and improve encryption efficiency.

By refining the image, preprocessing ensures the image quality is optimal for embedding patient data and applying encryption algorithms.

3. Data Input (Patient's Data)

To establish a secure link between the medical image and the corresponding patient's information, the patient's data (e.g., name, age, diagnosis, or ID number) is introduced.

This step is crucial in healthcare systems, as embedding patient data directly within the image ensures the integrity and association of the data with its corresponding medical image.

4. Image Steganography (Embedding Hidden Data)

Steganographic techniques are employed to embed the patient's data into the medical image.

- The process securely hides the data within the pixel values of the image in a non-intrusive manner.
- This layer of steganography ensures that the hidden information remains invisible to unauthorized users, thus providing additional security during transmission.

5. Cryptography (Encryption of Data)

At this stage, the medical image is converted into an unreadable cipher form.

- The pixel values of the image are encrypted, ensuring that unauthorized access to the data is thwarted.
- This process provides the first layer of protection by obscuring the image into a secure format.

6. Key Sequence Generation (Logistic Chaotic Map)

A **Logistic Chaotic Map**, a type of chaotic system, is used to generate a key sequence.

- **Chaotic maps** are highly sensitive to initial conditions and capable of producing pseudo-random sequences that are both highly complex and unpredictable.
- This key sequence serves as a critical component for the XOR-based encryption operation.

The use of chaotic systems ensures that the encryption keys are secure, dynamic, and difficult to reproduce.

7. XOR Operation (Mixing Image Data and Key Sequence)

The key sequence generated by the Logistic Chaotic Map is combined with the image data using the **XOR operation**.

- The XOR operation introduces non-linear mixing of pixel values with the chaotic key sequence.
- This step scrambles the image data, ensuring that the original image cannot be reconstructed without the correct key.

The output of this stage is an **encrypted image**, representing the first layer of encryption.

8. Key Sequence Generation (Lorenz Algorithm)

A second key sequence is generated using the **Lorenz Algorithm**, another chaotic system with high sensitivity to initial conditions.

- The Lorenz Algorithm introduces an additional layer of unpredictability, making the encryption more robust and resilient to attacks.

This step enhances security by creating a second, independent key sequence.

9. XOR Operation (Second Stage Encryption)

The first-stage encrypted image undergoes another XOR operation using the key sequence from the Lorenz Algorithm.

- The second XOR operation adds another layer of security, ensuring that even if the first layer of encryption is compromised, the image remains secure.

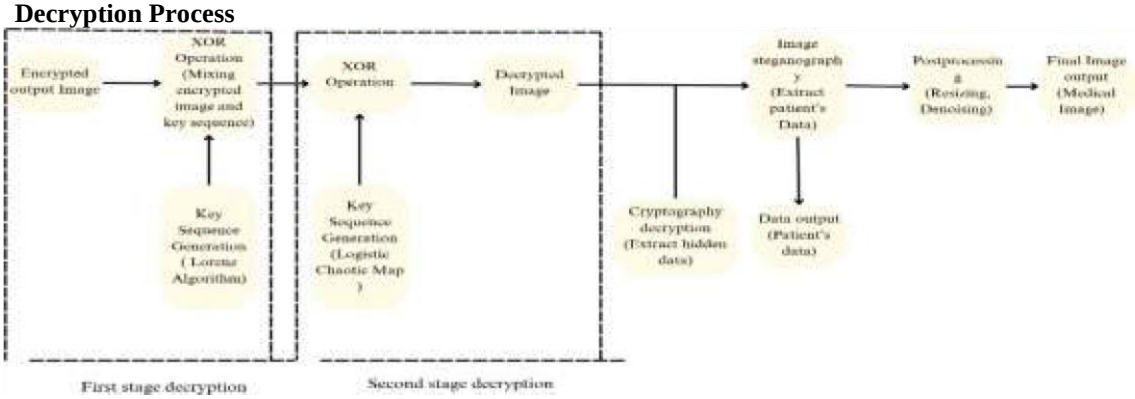
The final output of this stage is the **fully encrypted medical image**, which is ready for secure storage or transmission.

10. Encrypted Output Image

The result of the encryption process is a highly secure, encrypted medical image with embedded patient data.

- This output ensures that sensitive medical information is safeguarded from unauthorized access while maintaining its integrity and association with patient data.

Decryption Process



The decryption process reverses the encryption to retrieve the original medical image and patient data. It follows a similar multi-stage approach to ensure security and accuracy:

1. Encrypted Output Image (Input)

The encrypted medical image obtained from the encryption process is used as the input for decryption.

2. First Stage Decryption

Key Sequence Generation (Lorenz Algorithm):

- The Lorenz Algorithm is applied to regenerate the key sequence used in the second XOR operation during encryption.

XOR Operation:

- The regenerated key sequence is used to perform an XOR operation on the encrypted image.

- This operation removes the second layer of encryption, producing the first-stage encrypted image.

3. Second Stage Decryption

Key Sequence Generation (Logistic Chaotic Map):

- The Logistic Chaotic Map is utilized to regenerate the key sequence used in the first XOR operation.

XOR Operation:

- The first-stage encrypted image undergoes an XOR operation with the regenerated key sequence, reversing the first layer of encryption.
- This step retrieves the original medical image with the embedded patient data.

4. Image Steganography Decryption

The hidden patient data embedded during the steganography step in the encryption process is extracted.

- Specialized steganographic algorithms are used to recover the data securely without affecting the quality of the medical image.

5. Post Processing

The retrieved medical image undergoes postprocessing to restore it to its original state.

- **Denoising:** Any noise introduced during the encryption and decryption process is removed to enhance clarity.
- **Resizing:** The image is resized back to its original dimensions for compatibility with medical imaging systems.

6. Output

The final output includes:

1. The original medical image, free of encryption or distortion.
2. The extracted patient data, accurately linked to the medical image.

This ensures the complete and secure retrieval of sensitive medical information, maintaining its integrity and confidentiality throughout the process.

By employing two layers of chaotic encryption (Logistic Chaotic Map and Lorenz Algorithm), along with steganography and postprocessing, this methodology ensures a highly secure and efficient system for protecting sensitive medical images and patient data.

IV. SOFTWARE REQUIREMENT

This project utilizes Anaconda, a powerful open-source distribution of Python and R, to manage the project's environment and dependencies. Anaconda provides a convenient way to install and manage various Python packages required for the research.Key libraries utilized in this project include:

NumPy : For numerical computations and array manipulations essential for image processing and cryptographic operations.

OpenCV : A powerful library for image reading, writing, and processing, facilitating image loading and manipulation for encryption and decryption.

ChaoticPy : For implementing and analyzing chaotic systems. Cryptography : For Cryptographic operation.

Stegano : For steganography techniques and image embedding.

Jupyter Notebook serves as the primary development environment, offering an interactive and flexible interface for coding, experimentation, and visualization. It allows for the creation of organized and reproducible research notebooks.The combination of Anaconda and Jupyter Notebook provides a comprehensive and efficient environment for the development and testing of this medical image encryption algorithm.

V. RESULT

The encryption process was implemented using an improved logistic chaotic map to generate a pseudo-random sequence for pixel permutation and substitution.

Fig.1: Original Image

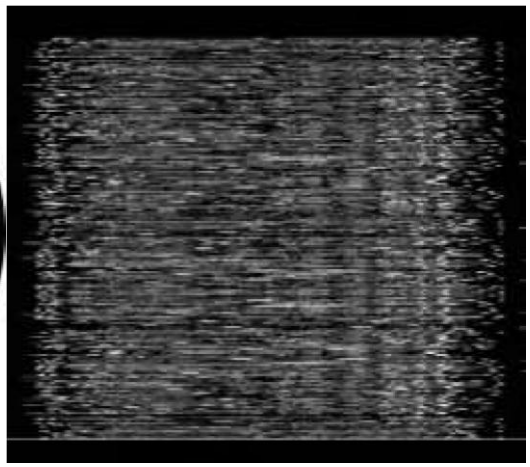


Fig.2: Encrypted Image using Logistics

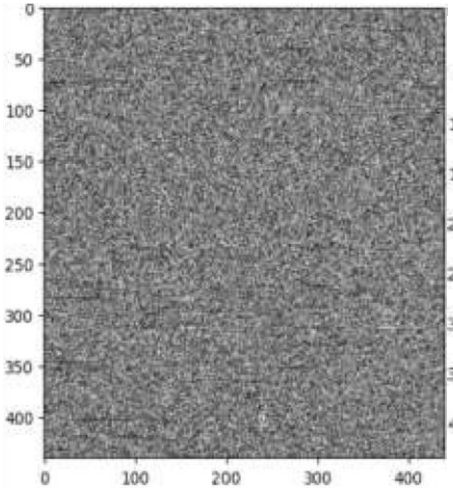


Fig.3: Encrypted Image using Lorenz

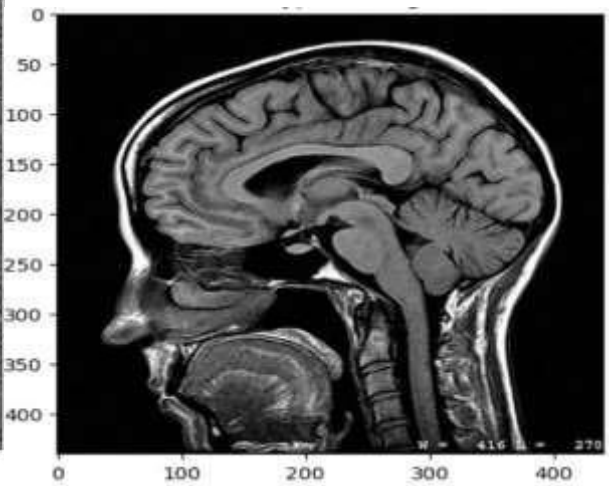


Fig.4: Decrypted Image

Fig.1 shows the original medical image before any encryption, which serves as the base for the encryption process. Fig.2 illustrates the image after encryption using the Logistic Chaotic Map, highlighting the transformed data with a high level of randomness for enhanced security. Fig.3 presents the image after further encryption using the Lorenz Algorithm, providing an additional layer of protection. Finally, Fig.4 demonstrates the decrypted image, which has been restored to its original form through the combined use of the Logistic Chaotic Map and Lorenz Algorithm, ensuring that the process does not degrade the image quality significantly.

VI. CONCLUSION

In this project, we developed a robust Medical Image Encryption Algorithm combining Improved Logistic Chaotic Mapping, Cryptography, and Steganography to enhance the security and privacy of medical images. The Improved Logistic Chaotic Map generates pseudorandom sequences, strengthening encryption by adding complexity and making the data resistant to attacks. The Steganography component embeds the encrypted data within the image itself, preserving the original image quality and allowing for the secure transmission or storage of sensitive information without perceptible distortion. This hybrid approach successfully addresses the challenges of maintaining security without compromising image integrity, making it highly suitable for real-world healthcare applications that require compliance with privacy laws. Future improvements could focus on optimizing the algorithm for faster processing and expanding its applicability to other types of medical imaging.

REFERENCE

[1] Huang-Guo, Z. Weipeng, C. Lisha and L. Ermin, "Medical Image Encryption Algorithm Based on Improved Logistic Chaotic System and 3D Space," 2023 IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2023

[2] M. Harshitha, C. Rupa, K. P. Sai, A. Pravallika and V. K. Sowmya, "Secure Medical Data Using Symmetric Cipher Based Chaotic Logistic Mapping," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021

[3] J. Xu, C. Zhao and J. Mou, "A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation," in IEEE Access, vol. 8, pp. 145995-146005, 2020

[4] P. A, U. R, J. N and P. S, "Securing Medical Images using Encryption and LSB Steganography," 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2022

[5] Liu Zhaoyong, Dai Anding, Li Kang et al., "Color image encryption algorithm based on compound chaotic system and Matlab implementation", Journal of Hunan City University (Natural Science Edition), vol. 27, no. 3, pp. 49-53, 2018.