A Robust Chaos-Based Technique for Medical Image Encryption

Mrs. KANNIKA LAKSHMI D G [1], DIMPAL K L [2], INISHA K[3], MITHUN N [4], VEDALAKSHMI T P[5]

[1] *Assistant. Professor, Dept. of Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[2] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[3] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[4] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*
[5] *Information Science & Engineering, Rajeev Institute of Technology, Hassan*

Abstract - A method called A Robust Chaos-Based Technique for Medical Image Encryption was created to improve the security of medical image storage and transmission. Because they include private patient information, medical photos are susceptible to illegal access. In order to safeguard pictures like MRIs, CT scans, and X-rays, this project uses chaos-based encryption algorithms. By generating encryption keys using the Henon chaotic map, the system ensures great security through unpredictability and randomness. To improve anonymity, image preprocessing methods like pixel substitution and permutation are used. Histogram analysis, correlation analysis, and entropy computations are used to assess the security performance of the encrypted images. An effective way to protect medical data in contemporary healthcare systems, this approach combines the ideas of cryptography and chaos theory to provide strong protection against unwanted access.

Keywords: Histogram analysis, security, diagnostics, encrypted images, medical images, Henon Chaotic Map, and cryptosystem.

1. INTRODUCTION

In today's healthcare system, medical imaging is essential for both diagnosing and treating a wide range of illnesses. To avoid unwanted access and data breaches, these photographs' sensitive nature necessitates strong security measures. The speed and security requirements of real-time healthcare applications are frequently not met by traditional encryption approaches. In order to improve medical image security and guarantee confidentiality and integrity in healthcare systems, this study proposes a chaos-based encryption technique.

Grade I: Encrypting medical images is essential for safeguarding patient privacy in telemedicine and hospital settings. Unauthorized access to medical imaging, including CT, MRI, and X-rays, can result in ethical issues, data tampering, and privacy violations. Despite their effectiveness, traditional encryption methods can impede operations and add computational overhead. Using the unpredictability and randomization of chaotic maps, chaos-based encryption offers a safe and effective way to protect medical images.

Grade II: The suggested encryption method applies pixel-level changes to medical images and generates safe keys using the Henon chaotic map.To guarantee image confidentiality, the encryption procedure uses key-based transformations, substitution, and permutation. Histogram analysis, correlation testing, and entropy computations are used this to assess performance. The chaos-based approach provides a greater level of security while preserving computing efficiency when compare to conventional encryption techniques.

Grade III:By guaranteeing safe picture transmission and storage, chaos-based security approaches go beyond encryption and aid in healthcare decision-making. Encrypted photos can be safely shared between medical experts in cloud-based systems without worrying about unwanted access. By facilitating remote diagnosis and treatment, this improves telemedicine applications. Because chaotic maps are unpredictable, it is also challenging for attackers to recreate the original images without the encryption keys.

Grade IV: Accessibility and cost-effectiveness are increased when chaos-based encryption is combined with medical technology. Cloud-based solutions can safely store encrypted medical pictures, lowering storage vulnerabilities. Patients can safely communicate medical data with healthcare professionals by using automated encryption mechanisms in mobile healthcare applications. Secure digital recordings also make legal paperwork and insurance claims easier, guaranteeing openness in medical procedures.

Using chaos-based encryption in medical imaging is crucial for maintaining security, privacy, and effectiveness as healthcare technology advances. Combining sophisticated cryptographic concepts with the Henon chaotic map improves encryption robustness without sacrificing computing viability. Medical image security will be further strengthened by future developments, such as AI-driven encryption methods and secure telemedicine platforms, which will increase the dependability and accessibility of healthcare systems.

2. LITERATURE REVIEW

A literature review is an essential step in the software development process since it provides valuable insights and improvements for existing methods. This section highlights the key studies that have impacted the planned work on medical picture encryption utilizing chaos-based approaches.

For picture encryption, Patidar and Kaur (2023) suggested a brand-new conservative chaos-driven dynamic DNA coding method. Their method dynamically encoded and decrypted each pixel using pseudorandom sequences produced by a conservative chaotic standard map. With an entropy value of 7.9956, their results showed great security, making it ideal for safe image encryption.

In 2023, Dhanakshinamoorty Vignesh and Banerjee presented a fractional sine chaotic map for watermarking and image encryption. This method improved the encryption strength by displaying complex behavior and great non-linearity. The suggested technique, which used chaotic map-based modifications, proved particularly helpful in protecting digital assets, including medical photographs.

Kumar and Jain (2022) combined RSA encryption with a hyper-chaotic system and resilient zero-watermarking to propose an enhanced security method for e-healthcare photos. In order to strengthen security against cyberattacks, their research concentrated on encrypting private medical data by combining chaos theory with conventional cryptography techniques.

Saqlain and Iqbal (2022) used bit-level circular shifts and Henon chaotic maps to create an image encryption technique. Their method proved to be effective in producing highly randomized encrypted images, which makes it impervious to statistical attacks. But in order to maximize encryption security, their work also made clear the necessity for additional advancements in histogram consistency.

An image encryption technique based on compressive sensing and chaotic systems was proposed by Chai and Zheng (2018). Their study concentrated on combining chaotic key generation with wavelet transform (DWT) operations, which produced high entropy (7.9992) and low correlation between neighboring pixels, making it a practical option for safe medical image encryption.

Alghamdi and Munir (2022) combined random substitution and chaotic maps to create a lightweight picture encryption technique. Their approach guaranteed a high degree of randomness in the encrypted images by using logistic maps and XOR techniques. The experimental findings showed that the strategy maintained a modest computational overhead while greatly enhancing security.

3. SYSTEM DESIGN

Existing system:

Traditional encryption methods like Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest–Shamir–Adleman (RSA) are typically used in the current system to protect the confidentiality and privacy of medical images, including ultrasound, MRI, CT scans, and X-rays. These conventional encryption methods are unreliable when dealing with large photographs and high-dimensional data, but they provide only a limited level of protection for medical images. Additionally, these methods usually have trouble with processing speed, computing complexity, and protection against various cryptographic attacks.

Furthermore, most medical photos are stored in cloud databases or shared across multiple healthcare systems, making them extremely vulnerable to alteration, data breaches, and unauthorized access. Traditional encryption techniques' absence of dynamic security features increases the risk of endangering patient confidentiality and image fidelity.

Additionally, these techniques do not employ any chaotic-based encryption algorithms, which might significantly enhance the complexity and unpredictability of the encryption process. Because the current method lacks trustworthy encryption methods created specifically for medical images, it is unable to ensure high levels of security and confidentiality.
As a result, there is an increasing need for an efficient encryption technique that can handle high security, process large volumes of medical images, and ensure image integrity while being transmitted or stored. This flaw in the existing strategy highlights the need for a chaos-based encryption technique that can secure medical images by offering improved security, lower computational costs, and increased resistance to cryptographic attacks.

Proposed system:

Reliable storage and transmission are essential for digital images used in military, medical, and multimedia imaging systems. Image security is the most crucial concern as mobile phones, the internet, and multimedia technologies become more prevalent in society.Our objective is to provide a secure way for photo encryption and decryption using the Advanced Encryption Standard (AES) algorithm. The AES algorithm is used by many commonplace technologies, including smart cards, cell phones, automated teller machines, and WWW servers. When an input image is encrypted using AES, it becomes a cipher image that can be decoded with a shared private key to expose the original image. The cipher image is made in an entirely different format so that it cannot recognize the original image. Once decrypted, it ought to be in its original state.

4. METHODOLOGY

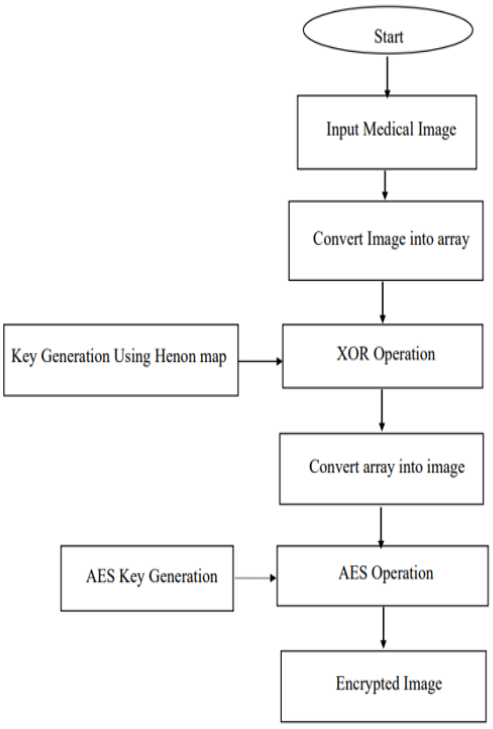

Figure 1: Encryption process

The Advanced Encryption Standard (AES) in conjunction with the flowchart is a strong chaos-based method for protecting medical pictures. A medical picture, such as an MRI, CT scan, or X-ray, is first fed into the procedure and subsequently transformed into an array. This conversion enables mathematical operations to be carried out on the image by converting its pixel values into numerical data. The Henon map, a chaotic map renowned for its unpredictability and sensitivity to beginning circumstances, is used to create a key in order to guarantee high-level security. This key is essential for increasing the encryption strength since it makes the picture encryption process more random.

After the key is created, the picture array and the key undergo an XOR (Exclusive-OR) operation, which produces a jumbled and unidentifiable image. As the initial security measure, this process makes it challenging for unauthorized users to decipher the picture.

To go on to the next stage of encryption, the jumbled array is subsequently transformed back into an image format. An AES key is created and used in the Advanced Encryption Standard (AES) process to further bolster security. The modified picture is next subjected to the AES encryption technique, which further encrypts the already-jumbled image.

The encrypted picture, the process's end product, is extremely safe and unintelligible without the matching decryption keys. By combining the resilience of the AES algorithm with the unpredictability of the chaos-based Henon map, this dual-layer encryption technique makes sure that the medical picture is kept private and safe from manipulation, illegal access, and data breaches.

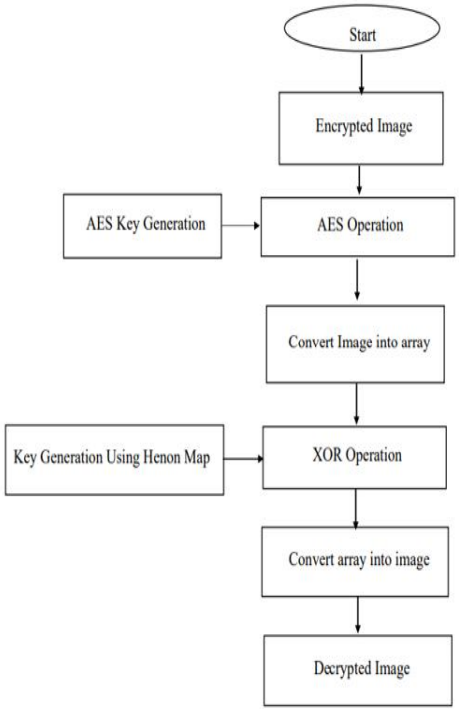

Figure 2 : Decryption process

The process of decrypting a medical picture that was previously encrypted using the Advanced Encryption Standard (AES) in conjunction with a strong chaos-based approach is depicted in the flowchart. To obtain the original medical image, the method begins with an encrypted image as input that must be decoded. In order to decode the picture, the AES operation first generates an AES key using the same technique as in the encryption procedure. For additional processing, the encrypted data from the AES operation is transformed into an array of pixel values. The Henon map—the same chaotic key used during the encryption phase—is utilized to construct a key that guarantees full decryption. The encrypted picture, which is the exact same as the original medical image, is produced by converting the array back into an image following the XOR operation. The security and integrity of the medical picture are preserved by this dual-layer decryption method that uses AES and Henon map-based XOR operation to securely decode the image without causing data loss or unauthorized access.

5. CONCLUSIONS

A strong medical image encryption system that can be included into cloud-based internet-of-health (IoHS) systems is part of the planned project effort. Chaoticmaps, which exhibit powerful and efficient chaotic behaviors, unpredictability, and extraordinary key sensitivity, are also introduced. An efficient permutation-substitution framework with good confusion and diffusion features serves as the foundation for an encryption system designed to increase encryption quality and performance. Tests utilizing different test medical pictures demonstrate the benefits of the suggested approach. Histogram analysis, key sensitivity analysis, correlation of adjacent pixels analysis, and randomness (entropy) tests are also performed in the proposed work. The results are compared with those of other state-of-the-art publications, and the results indicate that the proposed work performs better in all of the above mentioned analysis.

6. FUTURE DIRECTIONS

In future improvements we can create a chaotic cryptosystem with improved speed and security features for colour photos and videos in the future. Large photos can have their encryption and decryption execution times sped up. After decryption, the image quality for post-processing can be enhanced. It is possible to implement encryption and decryption for huge and varied format pictures (such as.jpj,.png,.jpeg, etc.)

REFERENCES

[1] A Novel Conservative Chaos Driven Dynamic DNA Coding For Image Encryption," by Vinod Patidar and Gurpreet Kaur, Dynamic Systems, vol. 8,1100839,2023.

[2] "A Novel Fractional Sine Chaotic Map And Its Application To Image Encryption And Watermarking" is presented by Dhanakshinamoorty Vignesh and Santo Banerjee in Mathematical Sciences, vol. 13, 6556, 2023.

[3] In the Department of Electrical and Computer Science Engineering, vol. 10, 1071, 2022, Sourab Kumar and Jaishree Jain present "Improved Security Of E-Healthcare Images Using Hybridized Robust Zero-Watermarking And Hyper-Chaotic System Along With RSA."

[4] "Henon Chaotic Map Based Image Encryption Scheme Using Bit-level Circular Shift" is presented by Syed Saqlain and Zeshan Iqbal in the Department of Computer Science Engineering, volume 100, 1992-8645, 2022.

[5] "An image encryption algorithm based on chaotic system and compressive sensing," presented by Xiuli Chai and Xiaoyu Zheng, Department of Electrical and Computer Science Engineering, 2018.

[6] "A Lightweight Image Encryption Algorithm Based On Chaotic Map And Random Substitution" by Yousef Alghamdi and Arslan

Munir, vol. 24, 1344, 2022.

[7] "A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map" is presented by M. Essaid and A. Saaidi in the Department of Mathematics and Computer Science, volume 57, 3670, 2018.

[8] "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution" is presented by Jameel Arif and Baraq Ghaleb in the Department of Computer Science, volume 10, 12966–12982,2022.

[9] "Image encryption scheme based on mixed chaotic Bernoulli measurement, matrix block compressive sensing" is presented by Qun Ding and Chen Yang in the Department of Electronic Engineering, vol. 24(2), 273, 2022.

[10] "Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption" is presented by Mohamed Gabr and Wassim Alexan