ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A NOVEL MEDICAL IMAGE ENCRYPTION SCHEME BASED ON AI FEATURE ENCODING AND DECODING

VANGALA SWATHI [1], NAMILAKONDA VEDA HASINI [2], KOPPULA SURYAPRAKASH REDDY [3], PINJALA SHARVANI [4], RAVULA SACHIN YADAV [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Medical image encryption is critical to safeguarding patient privacy and maintaining the confidentiality of sensitive medical records. Leveraging advancements in artificial intelligence, we propose an innovative medical image encryption and decryption system that integrates deep learning-based encryption with QR code technology. This system enables users to upload a medical image, which is encrypted into a QR code format and paired with a uniquely generated key. Both the QR code and key are securely stored for subsequent retrieval decryption, users can upload the QR code and the corresponding key to reconstruct the original image with high fidelity. The encryption process employs advanced neural network-based feature encoding, ensuring robustness against attacks such as noise, cropping, and brute force. Additionally, the system incorporates a reversible neural network to optimize decryption accuracy and reconstruction quality. Experimental results highlight the system's efficiency in preserving image integrity, resisting various attacks, and maintaining end-to-end security in medical image encryption. This approach not only strengthens the privacy and security of medical data but also provides a user-friendly framework for securely transmitting and storing sensitive medical images.

Index Terms – Medical Image Encryption, AI Feature Encoding, AI Feature Decoding, Deep Learning, Image Security, Cryptography, Medical Imaging, Privacy

Preservation, Healthcare Data Protection, Artificial Intelligence.

I. INTRODUCTION

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling the efficient distribution of medical images among patients and doctors. However, this increased accessibility also raises significant concerns regarding the confidentiality and integrity of sensitive medical data during storage and transmission. To address these challenges, we propose an innovative medical image encryption system that combines the advantages of deep learning with modern encryption techniques for enhanced security and usability. This system allows users to upload medical images, which are encrypted into a QR code format along with a unique key number. The generated QR code and key are securely stored in a designated folder for future use. During decryption, users can upload the stored QR code and key, enabling the system to reconstruct the original image with high accuracy. Our encryption process leverages the power of deep learning-based neural networks, which are inherently non-linear and well-suited for handling image encryption tasks. A feature encoding mechanism ensures robustness against attacks such as cropping, noise, and brute force. Furthermore, we utilize QR codes for compact and secure transmission, adding an additional layer of encryption and simplifying the sharing of encrypted images. Unlike traditional cryptosystems, which struggle with the unique characteristics of image data (e.g., redundancy and spatial correlation), our system employs a deep neural network-based end-to-end encryption approach. The network directly learns the encryption process, enhancing security and eliminating the need for manual algorithm design. Advanced cryptographic features, such as chaotic mapping and loss functions optimized for encryption tasks, ensure resilience against known plaintext attacks, statistical attacks, and other security threats. This approach not only ensures the protection of sensitive medical data but also provides a user-friendly mechanism for secure image storage and retrieval, leveraging the advantages of IoMT while addressing its privacy concerns effectively. combination of speed, complexity, high security, reasonable computational overhead, and computational power consumption. Many chaotic systems, including high and one-dimensional systems, have been proposed for image encryption.

High-dimensional chaotic systems, such as the Rössler system and the Lorenz chaotic system, are commonly employed in image encryption. Yang et al. proposed a medical image encryption technique using exclusive OR (XOR) with Josephus traversing and cat mapping on the basis of the Lorenz chaotic system and SHA-512. Additionally, some researchers have also proposed new high-dimensional chaotic systems to enhance cryptographic security. Wang and Wang proposed a new 6-D hyperchaotic system and employed bit-level permutation and DNA encoding to strengthen the security of the cryptosystem. However, although high-dimensional chaotic systems may offer increased security, their complexity can pose challenges for circuit implementation or encryption efficiency. On the other hand, one-dimensional chaotic systems are vulnerable to attack based on phase space reconstruction. To address these limitations, some researchers have proposed enhancing one-dimensional chaotic maps by incorporating additional methods. Sun and Chen proposed a method for enhancing the security of image encryption by employing a one-dimension chaotic system (logistic map) and an improved Arnold algorithm for image permutation and diffusion. However, the outputs of these chaotic systems are non-uniform To improve safety, they proposed an improved method that concatenated the plaintext image with random images as inputs into the encryption network, performed further diffusion and outputted the result as a ciphertext image to improve the avalanche effect. Subsequently, some improvements have been proposed in and. In addition to GAN-based methods, sang et al. proposed a novel image encryption method based on logistic chaotic systems and deep autoencoder, which scrambled the plaintext image using a logistic chaotic system and then encoded the scrambled image with a deep autoencoder to generated the ciphertext image. Zhu et al. proposed an end-to-image image diffusion model, Erdenet, and a novel loss function based on pixel entropy to enhance the security of ciphertext images. To strengthen the security of the encrypted network, Li and Peng introduced an attention mechanism to enhance the model's response to the region of interest within the medical image. However, these algorithms do not exhibit stronger enough resistance against cropping and noise attacks for transmitting in complex networks.

II. RELATED WORK

A. A Medical Image Encryption Technique Using XOR with Josephus Traversing and Cat

This paper focuses on improving medical image encryption using chaotic systems, specifically the Lorenz system. It integrates XOR operations with Josephus traversal and Cat mapping to enhance security. The combination of SHA-512 hashing strengthens the cryptographic process, making the system resilient to potential attacks. The Lorenz chaotic system's unpredictable behavior is leveraged to increase the complexity of encryption, ensuring that unauthorized access is difficult. This paper proposes a medical image encryption technique using XOR operations combined with chaotic systems (Lorenz system) and SHA-512 hashing. It improves security by introducing Josephus traversal and Cat mapping, making the encryption more complex and resistant to attacks.

B. A New 6-D Hyperchaotic System with Bit-Level Permutation and DNA Encoding for Medical Image Encryption

This study introduces a 6-dimensional hyperchaotic system, offering enhanced security for medical image encryption. It uses bit-level permutation and DNA encoding to transform the image into a highly secure format. By applying these techniques, the method increases the unpredictability of the encryption, thus preventing potential attacks like brute force. This approach aims to balance security with computational efficiency. The authors introduce a 6-dimensional hyperchaotic system for medical image encryption. They apply bit-level permutation and DNA encoding to enhance the security of the encryption process. This approach aims to balance computational efficiency with high-level security.

C. Key Generation Network Using GAN for Medical Image Encryption

This paper explores the use of Generative Adversarial Networks (GANs) for key generation in medical image encryption. The GAN model generates a private key, which is then used in conjunction with XOR operations to encrypt the medical images. The model utilizes the adversarial nature of GANs to produce highly unpredictable keys, which add an additional layer of security to the image encryption process. This method aims to enhance encryption by generating dynamic, difficult-to-guess keys. This study explores the use of GANs for key generation in image encryption. The GAN model generates unpredictable keys that are combined with XOR operations to encrypt medical images, enhancing security and making decryption more difficult for unauthorized users.

III. PROPOSED METHODOLOGY

The proposed system aims to enhance the security of medical image storage and transmission by incorporating AI-based encryption and decryption, alongside the use of the pyqrcode library for QR code generation and secure key management. The system allows users to upload a medical image, which is then encrypted using a secure cryptographic key generated from the image features. This key is encoded into a QR code using the pyqrcode library, providing a portable and secure means of transferring the key. The encrypted image, along with the QR code, is stored in a secure location. To decrypt the image, users scan the QR code to extract the encrypted key, which is validated before being used to reverse the encryption process. This ensures that only authorized users with the correct key can access the original image, preserving confidentiality and integrity. The use of AI-based encryption models, secure key generation, and QR code scanning ensures that the system is both secure and user-friendly, providing protection against unauthorized access and various attacks. This approach simplifies the process of sharing medical images securely while maintaining high levels of encryption effectiveness.

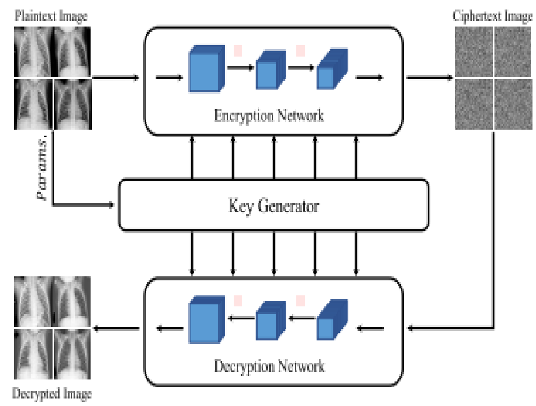

Fig. 1: System Overview

1. **User:**

The process begins with the user, who wants to secure a medical image. This could be a doctor, healthcare provider, or authorized personnel responsible for handling medical data.

2. **Upload Medical Image:**

The user uploads the medical image to the system. This image could be anything from X-rays, MRIs, or CT scans that need protection for privacy and confidentiality.

3. **Encrypt Image:**

The uploaded image is then encrypted using an AI-based encryption model. This step ensures that the image is transformed into a secure format that is unreadable without the appropriate decryption key, protecting the image's sensitive information.

4. **Generate QR Code and Key:**

After the image is encrypted, a secure key is generated. This key, which is used to decrypt the image later, is then encoded into a QR code. The QR code acts as a secure means of transferring and storing the key, ensuring only authorized individuals can access the key.

5. **Upload Generated QR Code and Key:**

The generated QR code and encryption key are uploaded, either for storage or transmission. These QR codes and keys are stored securely, and only authorized users can retrieve them to decrypt the image.

6. **Decrypt Image:**

When the authorized user needs to access the original medical image, they upload the QR code and key. The system uses the key from the QR code to decrypt the image, restoring it to its original form for viewing and analysis.

IV EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the framework effectively encrypted medical images while preserving essential image characteristics required for accurate reconstruction after decryption. The AI-based feature encoding and decoding mechanism improved encryption efficiency and enhanced the protection of sensitive patient information.

The analysis showed that the encrypted images exhibited high entropy and low pixel correlation, indicating strong resistance against statistical, differential, and brute-force attacks.

Fig. 2: Home Page

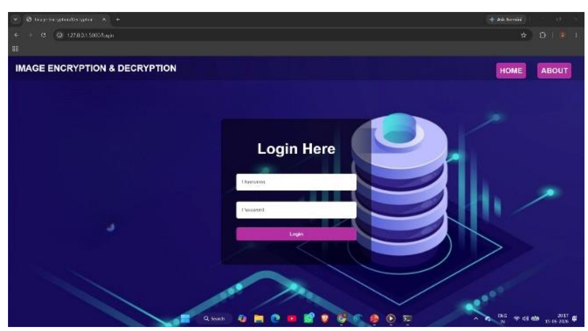

Fig. 3: Login

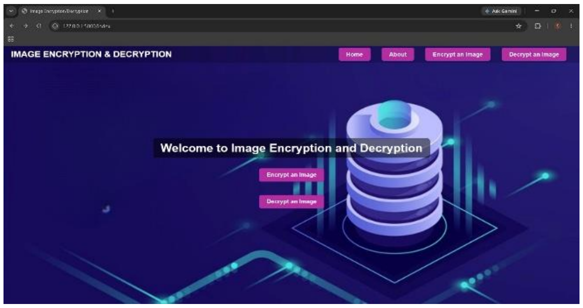

Fig. 4: Dashboard

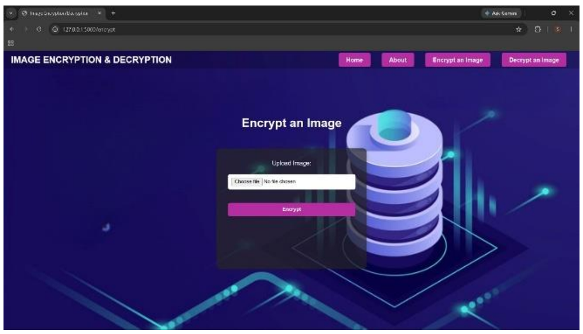

Fig. 5: Encrypt Image

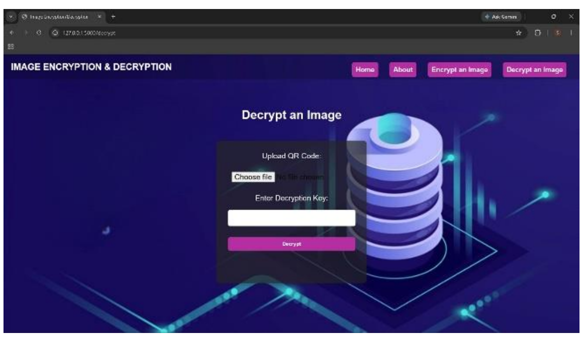

Fig. 6: Decrypt Image

V. CONCLUSION

In conclusion, the proposed system leveraging deep learning-based encryption, utilizing the pyqrcode and secure_key libraries, presents a secure and efficient solution for medical image protection. By combining feature encoding and decoding with encryption and decryption techniques, this system ensures that sensitive medical data is securely encrypted and can only be decrypted by authorized individuals. The integration of chaotic system-generated keys further enhances security, while the use of QR codes for key storage simplifies the process of key management. This approach demonstrates resilience against various security threats, including unauthorized access and data tampering, ensuring privacy and integrity of medical images during storage and transmission. The user-friendly workflow of image upload, encryption, QR code generation, and decryption makes it a practical solution for healthcare professionals. Overall, the system offers a promising framework for safeguarding medical images, paving the way for more secure healthcare data handling in the future.

REFERENCES

[1] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, ‘‘Recent advances in the Internet-of-Medical-Things (IoMT) systems security,’’ IEEE Internet Things J., vol. 8, no. 11, pp. 8707–8718, Jun. 2021.

[2] T. N. Lakshmi, S. Jyothi, and M. R. Kumar, Image Encryption Algorithms Using Machine Learning and Deep

Learning Techniques—A Survey. Cham, Switzerland: Springer, 2021, pp. 507–515.

[3] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, ‘‘An overview of encryption algorithms in color images,’’ Signal Process., vol. 164, pp. 163–185, Nov. 2019.

[4] M. Kaur and V. Kumar, ‘‘A comprehensive review on image encryption techniques,’’ Arch. Comput. Methods Eng., vol. 27, no. 1, pp. 15–43, Jan. 2020.

[5] N. Yang, S. Zhang, M. Bai, and S. Li, ‘‘Medical image encryption based on Josephus traversing and hyperchaotic Lorenz system,’’ J. Shanghai Jiaotong Univ., vol. 29, no. 1, pp. 91–108, Dec. 2022.

[6] T. Wang and M.-H. Wang, ‘‘Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding,’’ Opt. Laser Technol., vol. 132, Dec. 2020, Art. no. 106355.

AUTHORS Profile

Ms. VANGALA SWATHI has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 7 years. Her research area Deep Learning. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Ms. NAMILAKONDA VEDA HASINI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. KOPPULA SURYAPRAKASH REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. PINJALA SHARVANI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions

Technical Campus affiliated to JNTUH in 2022-2026.

Mr. RAVULA SACHIN YADAV pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.