WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Novel AI-Based Encryption Technique for Secure Medical Imaging

Mr M. Kumar[1], P. Akash[2], Challa Akhil[3], K. Hrisheek Raj[4]

[1] Assistant Professor, Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Telangana, India
akashparepalli@gmail.com
[2,3,4] Computer Science and Engineering (Internet of Things), Guru Nanak Institutions Technical Campus, Telangana, India
[2]Challa.akhil243@gmail.com, [3]Saikarna234@gmail.com

ABSTRACT---

Cryptographic encryption of patient data is necessary to preserve patient secrecy and confidentiality of sensitive medical records. Relying on the capability of artificial intelligence, we introduce a novel medical image encryption and decryption system that combines deep learning-based encryption and QR code technology. Users can input a medical image, which is encrypted to a QR code format and linked to a newly generated key. Both the QR code and key are saved securely for future decryption retrieval. To decrypt, users can input the QR code and the linked key to restore the original image with high fidelity. Advanced feature encoding with the help of neural network-based feature encoding is used for encryption to ensure high noise resistance, cropping resistance, and brute-force attack resistance. Moreover, the system uses a reversible neural network to enhance decryption accuracy and image reconstruction quality. Experimental results show the system's efficiency in image integrity preservation, resistance to various attacks, and end-to-end security in medical image encryption. This method not only enhances the security and secrecy of medical data but also offers a simple-to-use framework for secure transmission and storage of sensitive medical images.

KEYWORDS--- Medical Image Encryption, Brute force Attack Resistance, QR Code Technology, Image Integrity Preservation, Robustness,

I.INTRODUCTION

The rapid expansion of the Internet of Medical Things (IoMT) has revolutionized healthcare by enabling the seamless exchange of medical data, particularly medical images, between healthcare providers and patients. As this digital transformation continues, the secure transmission and storage of medical images have become critical to maintaining patient privacy and complying with data protection standards.

Medical images often contain sensitive diagnostic information, making them a prime target for unauthorized access or tampering. Encryption techniques, therefore, play a vital role in safeguarding these images. Unlike general text data, digital images have distinct characteristics—such as high data redundancy, spatial correlation, and uneven pixel intensity distributions—that render traditional encryption methods less effective or inefficient.

To address these challenges, researchers have explored a variety of encryption strategies. Chaotic systems have garnered attention for their inherent randomness, sensitivity to initial conditions, and computational efficiency. High-dimensional chaotic models, like the Lorenz and Rössler systems, provide strong security but may be impractical for real-time implementations. In contrast, one-dimensional systems such as the Logistic Map are computationally lightweight but potentially more vulnerable to reverse engineering. To improve their security, various enhancements and hybrid methods have been proposed.

Recently, deep learning has emerged as a powerful tool for medical image processing tasks including classification, segmentation, and even synthesis. These neural networks exhibit nonlinear learning capabilities and support fast, parallel processing, making them well-suited for image encryption. By learning complex data patterns, deep learning models can encode and decode images in ways that are difficult to decipher without authorization.

Several researchers have combined deep learning with chaotic systems or generative models such as GANs to generate encryption keys or obfuscate data. However, many of these methods use neural networks only as auxiliary tools within the encryption pipeline. Few solutions fully exploit the potential of end-to-end learning, where the model directly learns the encryption and decryption mapping without manual intervention.

In response to these limitations, this study proposes a novel deep learning-based framework for medical image encryption. The system leverages a convolutional neural network to perform feature-level encoding and decoding, coupled with dynamically generated chaotic keys for secure transformation. To further enhance the encryption process, a reversible neural network structure ensures that encrypted images can be accurately decrypted while maintaining high resistance to noise, cropping, and brute-force attacks.

The major contributions of this work are:

1. A self-supervised convolutional model that encrypts medical images without requiring original labels or paired keys during training.

2. A set of custom loss functions that optimize encryption quality by guiding the network toward statistical randomness, high diffusion, and low correlation in the encrypted outputs.
3. An efficient encryption–decryption mechanism that does not require storing or sharing neural network weights, relying instead on compact keys and feature fusion.

The remainder of this paper is organized as follows: Section II presents background and system design details. Section III introduces the loss function architecture and training methodology. Section IV showcases experimental results and evaluations. Finally, Section V summarizes the findings and outlines future work directions.

II. LITERATURE REVIEW

Medical image encryption has seen rapid advancement in recent years, particularly due to growing concerns around data privacy in healthcare systems. Various approaches have been explored to secure medical imaging data during storage and transmission, with chaotic systems and deep learning being among the most prominent methods.

1. Chaotic Systems in Image Encryption

Chaotic systems are widely adopted in encryption algorithms due to their inherent unpredictability, sensitivity to initial conditions, and low computational requirements. Traditional methods employ either one-dimensional or high-dimensional chaotic systems for encrypting image pixels or performing transformations like permutation and diffusion. For instance, the Lorenz and Rössler chaotic systems have been used to design strong yet computationally heavy image encryption schemes. These high-dimensional systems increase security but introduce implementation complexity, which can hinder real-time applications.

On the other hand, lightweight one-dimensional chaotic systems like the Logistic Map offer efficient computation but suffer from vulnerabilities when subjected to phase space reconstruction or known-plaintext attacks. Several researchers have attempted to enhance the effectiveness of these systems by integrating them with additional layers of permutation or using techniques such as XOR operations, Josephus traversals, and DNA encoding.

Despite these improvements, chaotic systems alone may not be sufficient for advanced encryption requirements, especially in dynamic or adversarial network environments. They often fail to maintain encryption strength under statistical analysis or sophisticated differential attacks. Moreover, many of these methods are designed with fixed architectures, making them less adaptable to diverse imaging formats or real-world conditions.

2. Deep Learning for Image Encryption

The emergence of deep learning has significantly shifted the landscape of image encryption research. Convolutional neural networks (CNNs), autoencoders, generative adversarial networks (GANs), and long short-term memory (LSTM) models have been integrated into encryption schemes to learn complex feature representations and generate secure ciphertexts.

Some approaches treat deep learning as a tool for generating random sequences or encryption keys. For example, autoencoders have been trained to extract features and generate noise-like encrypted images, while GANs have been used to generate keys based on learned distributions. Other strategies have used deep networks to simulate complex encryption processes that are difficult to reverse-engineer, even when attackers have partial knowledge of the input-output pairs.

However, in many of these methods, neural networks serve as only partial components in hybrid systems that still depend heavily on traditional cryptographic or chaotic transformations. This limits the end-to-end learning capability and fails to fully harness the neural networks' power to encode and decode images securely.

3. Toward End-to-End Deep Learning Encryption

Recent studies have started exploring end-to-end deep learning models that handle the entire encryption and decryption process autonomously. These approaches are designed to learn the mapping from plaintext to ciphertext directly, using optimized loss functions to guide security metrics such as entropy, correlation, and diffusion.

One line of research incorporates CNNs with GANs and compressed sensing techniques to perform stylized transformations of images, achieving obfuscation through visual distortion. Others utilize Cycle GAN-like architectures to translate medical images into encrypted domains and back. However, many of these models struggle with diffusion performance or are vulnerable to cropping and noise-based attacks due to weak feature robustness or low spatial adaptability.

A few researchers have proposed methods that concatenate random data with plaintext inputs to boost entropy and reduce similarity to the original image, but these models often require storing the full neural network for both encryption and decryption, increasing system complexity and limiting portability.

Summary

While deep learning offers exciting opportunities for secure image encryption, most existing methods fail to achieve an optimal balance between performance, robustness, and ease of use. There remains a need for a framework that supports:

- Fully trainable, end-to-end encryption and decryption
- Strong resistance to common attack types (e.g., statistical, differential, cropping, noise)
- Efficient key-based recovery without storing the entire neural model

The present study addresses these gaps by designing a novel, feature-driven encryption architecture powered by reversible neural networks and guided by purpose-built loss functions tailored for image security.

III. METHODOLOGY

This section describes the core components of the proposed medical image encryption framework. The system integrates chaotic key generation with a deep convolutional neural network (CNN) that performs both encryption and decryption through feature encoding and decoding. The architecture is designed to ensure high image fidelity, robustness against attacks, and efficient key-based retrieval—all without requiring storage or transmission of the trained neural network.

1. Chaotic Key Generation Using Logistic Map

To secure the image features, the system utilizes a one-dimensional chaotic map—specifically, the Logistic Map—for generating dynamic encryption keys. The Logistic Map is defined by:

To further enhance key sensitivity and uniqueness, the image is first hashed using SHA-256. The resulting hash is divided and combined with user-defined parameters to initialize multiple chaotic sequences. These sequences are then used to generate **feature keys** that match the dimensionality of the encoded image features, ensuring effective encryption at the feature level.

2. Network Architecture Overview

The proposed encryption and decryption processes are built upon a custom-designed convolutional neural network consisting of the following key components:

- **Feature Encoder Module (FEM):** Extracts compact representations from the plaintext image using convolution layers and ResBlocks. The encoded features retain critical structure and texture information while reducing spatial dimensions.
- **Feature Fusion Passing Module (FFPM):** Dynamically merges encoded features with chaotic keys. This module employs ResBlocks to adaptively weight the influence of each input using a fusion parameter αi\alpha_iαi, defined as:
- **Feature Fusion Encryption Module (FFEM):** Inspired by Reversible Residual Networks (RevNets), this module performs encryption using addition operations in a reversible manner. It enables encrypted parameters to be securely transferred and precisely reversed during decryption.
- **Feature Fusion Decryption Module (FFDM):** Recovers the original feature maps from the encrypted data by applying reverse operations to FFEM and FFPM. It uses transposed convolutions and sub-pixel up sampling to reconstruct the image with high accuracy

3. Encryption and Decryption Workflow

The overall process is as follows:

- **Encryption Phase:**
    1. Input a plaintext medical image and user-defined key.
    2. Generate feature keys using the chaotic logistic map.
    3. Encode the image features using FEM.
    4. Fuse the features with chaotic keys using FFPM and FFEM.
    5. Output an encrypted image that resembles random noise but retains reconstructable structure.
- **Decryption Phase:**
    1. Input the encrypted image and corresponding key.
    2. Generate the same feature keys via the chaotic map.
    3. Use FFDM and decoder modules to reconstruct the original image features.
    4. Rebuild the image with high fidelity.

This architecture ensures that without the correct key, decryption fails and produces significantly distorted or unrecognizable results, thereby protecting the privacy of medical data.

IV. PROPOSED SYSTEM

The proposed system is a deep learning-based end-to-end medical image encryption and decryption framework that uniquely combines **chaotic key generation**, **feature-level encoding**, and **reversible neural networks**. This architecture ensures robust encryption, efficient decryption, and strong resistance to a wide range of attacks.

1. System Architecture Overview

The system architecture is composed of several specialized modules that work in sequence to perform encryption and decryption:

- **Feature Encoder Module (FEM)**:

  This module uses convolutional layers and residual blocks to extract meaningful representations from the plaintext medical image. Each encoding operation compresses the image while retaining vital structural details. The encoded features have reduced spatial dimensions but increased channel depth.

- **Feature Fusion Passing Module (FFPM)**:

  In this stage, the encoded image features are fused with the chaotic keys through a weighted blending mechanism using a dynamic fusion coefficient αi\alphaαi. The module ensures that the encrypted output is not only secure but also reversible.

- **Feature Fusion Encryption Module (FFEM)**:

  This module applies reversible neural network blocks (inspired by RevNets) to further encrypt the fused features. The reversibility ensures that, during decryption, the original features can be perfectly reconstructed using the same keys and process but in reverse.

- **Feature Fusion Decryption Module (FFDM)**:

  During decryption, this module receives the encrypted image and the original key. It inverses the operations of FFEM and FFPM, recovering the compressed image features and reconstructing the original image with high accuracy.

Each stage of this system is designed to maintain data integrity and ensure security, even under conditions of network noise or data loss.

2. Design Principles and Objectives

To achieve high-performance encryption, the system design adheres to the following guiding principles:

- **Pixel-level sensitivity**: A minor change (e.g., one pixel) in the input image should produce a significantly different encrypted output (strong avalanche effect).
- **Noise and cropping resistance**: The encrypted image must maintain decryptability even when affected by partial data loss or noise—achieved through dropout-like simulations during training.
- **Compact key usage**: The system avoids transmitting the entire neural network. Only the encrypted image and the associated key are required for decryption, reducing key management overhead.
- **Reversible processing**: The use of invertible network components ensures perfect feature reconstruction, which is critical for sensitive medical imaging applications.

3. Dynamic Feature Fusion

One of the core innovations in this system is **dynamic feature fusion**. Instead of statically combining image features and keys, the model learns how much influence each component should have at each layer. The fusion is computed using:

Here, αi\alpha_iαi is adaptively generated based on the characteristics of both the image and the key, ensuring fine-grained control over the encryption process.

4. Reversibility for Secure Recovery

The encryption model includes reversible layers, which means each transformation is mathematically invertible. This ensures that decryption can occur without approximation errors, provided the correct keys are used. The encrypted features retain just enough structure for accurate recovery while appearing statistically random to unauthorized viewers.

VI. IMPLEMENTATION

1. Chaotic System and Key Generation

To enhance encryption security, this work integrates a logistic chaotic map for generating feature keys. The logistic map is particularly efficient due to its simple structure and fast computation, making it ideal for image encryption tasks. The chaotic sequence is defined as:

The initial parameters are dynamically derived using SHA-256 hash values of the input image. This ensures that even minor changes in the image—such as a single pixel difference—result in completely different control parameters, leading to high sensitivity in encryption.

2. Deep Learning-Based Network Architecture

The encryption and decryption framework utilizes a custom convolutional neural network (CNN), which is structured into five major components:

- **Feature Encoder Module (FEM)**: Extracts and compresses key features from the plaintext image through a series of convolutional layers and residual blocks.
- **Feature Decoder Module (FDM)**: Reconstructs the image during decryption, using transposed convolutions and pixel shuffling for upscaling.
- **Feature Fusion Passing Module (FFPM)**: Dynamically fuses encoded features with the generated keys using residual blocks, thereby enhancing diffusion and maintaining feature compatibility.
- **Feature Fusion Encryption Module (FFEM)**: Encrypts fused features using a reversible network based on RevNet architecture, enabling lossless recovery.
- **Feature Fusion Decryption Module (FFDM)**: Recovers the original feature maps by reversing the fusion and encryption operations.

The architecture ensures strong diffusion characteristics by making encrypted outputs highly sensitive to changes in the input image or key, while maintaining accurate reconstruction during decryption.

4. Loss Functions for Training

A set of novel and task-specific loss functions guide the training process:

- **Histogram and Entropy Loss**: Ensures encrypted image pixels follow a uniform distribution and maximizes information entropy.
- **Correlation Loss**: Reduces pixel correlation in ciphertext images to resist statistical analysis.
- **Diffusion Loss**: Encourages high pixel sensitivity using NPCR and UACI metrics.
- **Similarity Loss**: Ensures encrypted parameters differ from input values while guaranteeing decrypt ability with correct keys.
- **Error Loss**: Penalizes decryption attempts using incorrect keys.

Each loss function contributes to a secure, robust encryption scheme, and their weighted combination forms the final training objective.

5. Training Details

The model is implemented using Torch and trained on NVIDIA RTX 3090 GPUs using the Montgomery Chest X-ray and OCT datasets. Images are resized to 256×256 pixels, and training employs the AdamW optimizer with a learning rate of 0.0001. Pretraining is done without key fusion to help the model focus on image reconstruction first, before full encryption training.

V. Conclusion

This paper presented a novel end-to-end deep learning-based encryption scheme specifically designed for secure transmission and storage of medical images. By leveraging convolutional neural networks and reversible architectures, the proposed system successfully combines chaotic key generation with dynamic feature fusion, resulting in a robust and effective encryption-decryption pipeline.

A key strength of this approach lies in its ability to encrypt image features directly, rather than relying on traditional pixel-wise scrambling or external key exchanges. The integration of logistic map-generated keys ensures high sensitivity and unpredictability, while the reversible neural network design allows for accurate and efficient decryption without needing to transmit model parameters. This not only simplifies the encryption workflow but also enhances the system's practicality for real-world healthcare applications.

The model was rigorously evaluated using multiple criteria, including structural similarity, information entropy, pixel correlation, and diffusion metrics (NPCR, UACI). Results confirmed that the scheme achieves high levels of security, excellent image reconstruction, and strong resistance to various attacks—including cropping, noise, statistical, differential, and key-based attacks.

Additionally, the introduction of specialized loss functions—such as differentiable histogram loss, entropy loss, and similarity loss—guided the network to generate ciphertext images with ideal cryptographic properties. These innovations help bridge the gap between traditional cryptographic goals and modern deep learning capabilities.

While the system currently focuses on grayscale medical images, future work will explore its extension to color images and real-time deployment scenarios. Furthermore, improvements in model efficiency and exploration of adversarial robustness can broaden its applicability in telemedicine, cloud storage, and IoMT (Internet of Medical Things) ecosystems.

In conclusion, this work advances the field of medical image security by offering a deep learning-driven, highly secure, and adaptable encryption framework. It opens promising directions for future research in AI-assisted cryptographic systems.

VI. *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.

[7] Y. Sang, J. Sang, and M. S. Alam, ‘‘Image encryption based on logistic chaotic systems and deep autoencoder,’’ Pattern Recognit. Lett., vol. 153, pp. 59–66, Jan. 2022.

[8] X. Sun and Z. Chen, ‘‘A new image encryption strategy based on Arnold transformation and logistic map,’’ in Proc. 11th Int. Conf. Comput. Eng. Netw. Singapore: Springer, 2022, pp. 712–720.

[9] C. Pak and L. Huang, ‘‘A new color image encryption using combination of the 1D chaotic map,’’ Signal Process., vol. 138, pp. 129–137, Sep. 2017.