Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Novel Aspects of Secure Medical Image Encryption using Block-Chain and Transformer-Based Deep Learning Model

Rucha Patel[1], Dr. Vedvyas .J. Dwivedi[2]
[1] Research Scholar, Department of Electronics & Communications, Indus University, Ahmedabad, India, rucpatel19861@gmail.com, ORCID – 0009-0002-7669-307X
[2]Professor, Department of Electronics & Communications, Indus University, Ahmedabad, India
evp@indusuni.ac.in, ORCID – 0000-0001-5258-2864

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

The vulnerability of medical images is a significant challenge in state-of-the-art telemedicine and Internet of Things (IoT)-based healthcare systems. This paper aims to develop a more comprehensive framework for secure encryption of medical images that fuses blockchain technology into a Transformer-based deep learning model (EB-TDLM) to strengthen data security, privacy, and integrity. And because blockchain is decentralized, data can be securely and immutably contained — meaning less compromise with unauthorized access and data breaches. Moreover, the EB-TDLM model adopts Transformer-driven key generation and upgraded encryption methods, enhancing the encryption robustness greatly. We thoroughly evaluate the proposed framework with experimental analysis and show its effective performance on multiple security metrics. Model has obtained an entropy value of 16.99, which indicates that there is high randomness present in encrypted images. It is highly sensitive to pixel change, achieving 99.99% NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) of 39.49%, and showing a high resistance to differential attack. Moreover, the encryption has very low MSE (0.05), which guarantees almost lossless reconstruction of medical images. Structural integrity, reflected by Structural Similarity Index (SSIM) of 1.0, is crucially maintained in reconstructed images. These findings position the EB-TDLM framework as an exceptionally reliable and efficient approach to safeguarding medical data in IoT-enabled healthcare environments. The proposed system serves as a scalable and effective mechanism for further securing sensitive medical images in contemporary healthcare networks by overcoming key challenges in telemedicine security.

Keywords: Blockchain Technology, Data Security, IoT Healthcare Systems, Medical Image Encryption, Robust Encryption Framework, Transformer-Based Deep Learning.

INTRODUCTION

The latest improvements in healthcare technologies and the expansion of Internet of Things (IoT) solutions have changed the way medical data is generated, collected, and shared [1]. Medical images are crucial for diagnosing and developing treatment plans but at the same time, security of medical images is of utmost importance primarily owing to the sensitivity and privacy of the data. Traditional storage systems, which are typically centralized, expose medical images to threats like unauthorized access, data breaches, and tampering [2]. These challenges demand novel encryption methods to maintain the confidentiality, integrity, and authenticity of medical images. With its decentralized, immutable and transparent characteristics, blockchain technology has been recognized as a very promising framework for data management in a secure manner [3]. Through such combination of blockchain and medical image storage, the threat of data tampering and unauthorized access is greatly decreased [4]. At the same time, deep learning models, especially those with Transformer-based architectures, have shown outstanding ability in separating complex patterns and generating strong encryption keys. This paper introduces a new framework based on the integration of blockchain and a Transformer-based deep learning model [5]. “Data integrity is guaranteed through blockchain, while the random key generation is done using transformer model (pre-trained transformer-based language models). Experimental results show the approach outperforms existing methods on critical metrics (entropy, NPCR, UACI, MSE, SSIM), which makes it suitable for secure medical data transmission in IoT-based healthcare systems. The work outlines the core goal of this research, which is to propose a secure and efficient model for medical image encryption fused with blockchain technology using a Transformer model based deep learning architecture capable of providing integrity, confidentiality and robustness in IoT based healthcare**.**

Major Contributions: The key contributions of this work are as follows:

- Generic architecture as a proposed framework of generation adopts transformer-based deep learning with self-attention mechanisms and dynamic keys learning for overcoming high randomization and destruction of secret keys, thus providing high security.
- Due to the adaptability of Transformer models, it is highly scalable and can efficiently process high-resolution medical images and large datasets.
- By taking advantage of the parallelism nature of Transformers, the system incurs fast encryption/decryption, a critical bloat to be utilized in real-time medical applications
- Consequently, integrating the images into the blockchain ensures that no one can change that image as it verifies that the image in encrypted format is decentralized and at the rendezvous, making that the data you are dealing with is hurled, therefore, it is impossible to corrupt the facts.
- Experimental results show the efficiency of the framework, with high entropy (16.99), and NPCR (99.99%), UACI (39.49%), having small MSE (0.05), and SSIM (1.0) are in very acceptable ranges.
- The framework provides a secure medical image transmission for IoT-based telemedicine networks by integrating blockchain with deep learning.

The remainder of this paper is structured as follows. 1 Introduction section highlights the challenges for securing medical images and the motivation to combine blockchain with Transformer-based deep learning models to tackle these challenges. Section 2: Related Works focuses on existing medical image encryption techniques, with an emphasis on the limitations and advancements of conventional-based and blockchain and deep learning-based methods, respectively. 3 Proposed Architecture: This section introduces the proposed system framework, where blockchain is incorporated for decentralized integrity verification and a Transformer-based deep learning model for strong encryption. Section 4: Proposed Methodology: Transformer-Based Adaptive Encryption Scheme: Outlines the dynamic key generation process using the Transformer model using self-attention mechanisms to improve the complexity and randomness of encryption along with its scalability as well as efficiency compared with high-resolution medical images. Section 5: Experimental Results and Comparative Analysis analyzes the performance of the proposed model based on numerous metrics, including entropy (16.99), NPCR (99.99%), UACI (39.49%), MSE (0.05), and SSIM (1.0), validating the effectiveness of the proposed model in comparison with the existing models. Lastly, Section 6: Conclusion summarizes the work and the framework's power for realizing robust medical image encryption, scalable adaptability, and secure transmission of medical image data in IoT-enabled healthcare system, which establishes a novel standard through which medical data should be secured.

2. RELATED WORKS

In smart healthcare systems, the transmission of medical record (MR) used to be sensitive data to be kept confidential. An in-depth watermarking scheme developed for safe medical pictures was based on RDWT, MSVD, and ANFIS. It uses blockchain for the step of authentication and ROIs, like being itself embedded with hybrid watermarks (Aadhar and barcode images), to provide copyright protection and therefore removes the threat of data breach. Experimental results show the robustness and stealthiness of the method [6]. Medical images are increasingly being shared over cloud environments, where security risks are particularly present as images are stored in central systems. A systematic review of 17 studies assesses blockchain's strengths and weaknesses for securing medical data. This paper discusses possible solutions, including Byzantine fault tolerance algorithms, homomorphic encryption, and smart contract integration, and thus outlining opportunities and challenges for the adoption of blockchain for medical image exchange [7]. Healthcare in the future will leverage data translation through enormous amounts of data generation, storage, transmission, and retrieval. More About the Blockchain-based Chaotic Arnold's Cat Map Encryption Scheme (BCAES) is a project which focuses cloud [34] and blockchain technologies to encrypt and send medical data securely. This scheme uses encryption with Arnold's cat map for images, signed documents stored in blockchain, and provides integrity of data during transmission. Furthermore, performance measures such as entropy, NPCR, and SSIM substantiate their superiority over state-of-the-art techniques, making the scheme a benchmark in the domain of secure medical data management [8]. Increased serviceability of the IoT offers image security, or the protection of sensitive data from being accessed or tampered with, into renewed condescension. A systematic literature review focusses on the ML techniques based on the blockchain that have been taken over for improving the real-time image securities in the IoT scenario. According to these findings, progress has been made towards enhanced data encryption, privacy preservation, and network security, whilst exploiting the shortcomings of centralized systems. Recent trends and future perspectives are emphasizing challenges such as scalability, integration into existing systems and regulatory alignment, adapting evolving theoretical discoveries towards actionable implementations within the commercial and social sectors [9]. The Internet of Things (IoT) connectivity in healthcare has facilitated rapid diagnosis and treatment, yet this has raised concerns about cybersecurity risks. We propose a ResNet-50 architecture that is based on the same principles of cryptography and uses domain-specific learning models to perform the encryption and decryption of medical images. Reconstructive ones use encrypted images to reconstruct them, allowing ROI frameworks and data mining. Such empirical analyses conducted with public datasets confirm the method's previously unmatched security, improving the confidentiality/usability of medical images [10]. IoT has transformed industries with smart devices, tackling security challenges using blockchain tech. A system for IoT-Blockchain prevents any disclosure of medical data before being transported by means of chaos encryption and it's an integration of Tinkerbell mapping. The presented Performance metrics NPCR, UACI, entropy, and SSIM prove the efficiency of the system in a way of preventing breaches and maintaining data integrity, making the system a full proof solution for secure transmission of Medical Image [11]. Encryption algorithms are used to encrypt medical images, which are essential for diagnosis. RDHEI (reversible data hiding in encrypted image) embeds private information in encrypted images so that the information can be securely communicated. Yet existing RDHEI schemes do come with limitations in terms of embedding capacity and traceability. A new block-wise encryption and histogram shifting method enhances embedding rates (more than 0.8 bpp) and incorporates blockchain technology to record private information and hash values of images for traceability. This maintains integrity and traceability, further securing the transfer of medical data [12]. Modern healthcare systems produce enormous quantities of sensitive data — digitized medical images and electronic patient records that must be stored and transmitted securely. Also, this is where traditional methods failed to secure the data which led to the introduction of the Blockchain-based Chaotic Deep Generative Adversarial Network (BCDGE) Encryption Scheme. Our scheme utilizes blockchain for data authenticity, while ensuring that all images are authenticated using a GAN-based method that generates image-specific keys for encryption, improving resistance against cyberattacks. It stores the encrypted data on the blockchain which shows great security and performance compared to the existing ones [13]. Digital healthcare records (DHR) need to be protected when transmitting and storing. Another watermarking approach describes an efficient technique based on Non-Subsampled Shearlet Transform (NSST) and Multi-Resolution Singular Value Decomposition (MRSVD) which embeds watermark data into medical images without heavily corrupting them. Encryption is performed with Hybrid Chaotic Shift Transform and modified Henon Maps resistant to attacks. Based on experimental results, the proposed method provides high PSNR and NC values, confirming that the method is more robust and improves image quality compared with existing techniques [14].

One of the biggest challenges with IoT healthcare implementation is the privacy and security of sensitive patient data. To solve these issues, a new blockchain-based strategy that utilizes Homomorphic Encryption (HE) and the Oppositional-Based Harmony Search (OHS) algorithm has been proposed. The OHE-MSC-based network uses multiple-share creation for privacy data, blockchain for data transmission security, and a CNN-based classification model for detecting diseases. Evaluation results on benchmark datasets indicate better performance and security over other methods [15]. End-point data security is a major concern today as technologies move toward AR, VR, and cognitive cities, and blockchain offers a decentralized, transparent solution to the same. BDIE-AOFOLS utilizes the Arnold map, tent map, and fractional-order Lorenz system to encrypt an image, while the key generation process is enhanced by the arithmetic optimization algorithm (AOA). The PSNR, in the same measure, reached 61.80 dB, in comparison with the proposed method achieved the best PSNR [16]. Connected E-health, which is enabled by IoT, encounters problems of patient data privacy and security. To enable secure data exchange, a hybrid encryption scheme utilizing IoT-based sensors and PDAs has been utilized. Blockchain technology allows for additional security in terms of data transmission, whereas hybrid deep learning approaches (like LSTM and CNN) can also be used to create a powerful encryption key that is then optimized using Self-Improved Lion Optimization Algorithm (SI-LA). Comparative analyses confirm that this model outperforms existing techniques when it comes to securing medical data [17].

For telemedicine and AI-based healthcare systems, secure transmission of medical images and data is essential. The medical image, doctor fingerprints and electronic health records are protected using a physically secure image encryption scheme based on chaotic encryption and hybrid cryptography which comprises ECC and AES. To preserve authenticity, integrity, and confidentiality, the encrypted data is trapped inside insignificant images. Simulations show that it has a higher image security and reconstruction quality than other methods [18]. Ensuring EHRs security in IoMT systems is essential to protecting privacy, integrity and availability. Implementing innovative solutions into cryptography in medical imaging with the use of deep learning: encryption, resolution enhancement, classification, compression. Such research makes breakthroughs in the application of deep learning to medical images security and promote the standards of privacy and protection in the medical field [19]. Grayscale medical images have been securely encrypted using a new Laplace transform-based algorithm with better security and reliability. Performance metrics, such as entropy, peak signal to noise ratio, pixel changing rate, prove the effectiveness of this algorithm. The method guarantees lossless decryption and vastly changed encrypted images from the original, as showing both theoretic and practical efficiency [20]. Innovations in health infrastructures concepts using smart cities which are efficient, effective and sustainable rely on secure storage and transmission of PHR, especially medical images. The SecMISS mechanism applies to the Random grid-based Visual Secret Sharing (RGVSS) followed by super resolution for distributed storage and security enhancements. These establish secure security and reconstruction efficiency and make it a perfect candidate for secure medical imaging in smart hospitals and health infrastructures [21].

This paper proposes a blockchain-based secure sharing and trading scheme for X-ray medical image data to improve its scientific research value. Original Xray Data is sent to cloud platform using MQTT protocol, Patient data uses hashing algorithms to encrypt, watermarks the image data, consensus mechanism is used to produce blocks in blockchain. To build such a secure transaction system connecting data users with scientific research needs, the scheme overcomes challenges faced by traditional cloud storage such as privacy breaches, illegal tampering and data theft [22]. Deep learning-based medical image analysis has greatly helped disease diagnosis; however, challenges remain such as limited bandwidth and data security. Data cleaning and lesion classification phases are part of a collaborative system model for a diabetic retinopathy (DR) diagnosis. Models for high-quality images are stored in the blockchain and models for classification are trained collaboratively across different private and public clouds. Enhanced multiple role access Control (MRAC) and Blockchain based access Control (B AC) offer fine-grained, secure, easy access control for multiple access trie nodes. In [23], experimental results indicate improved image quality and classification accuracy, attaining a 90.2% detection success rate for early lesions [23]. Cybersecurity challenges exist in storing and transporting digital images, which apply to medical images as well. Blockchain will store the hash immutably, but with a cost if the images are large scale. We propose an innovative architecture where a Fractional Discrete Cosine Transform (fctDCT), although low in cardinality are used to reduce the overall data amount through encoding feature maps as well as decentralized on the blockchain using hyper-links to store on decentralized clouds. Authorized users are the only ones able to store or retrieve α angles and coefficients, which is essential for ensuring secure storage. The metrics MSE, PSNR and SSIM prove that the framework is efficient and robust for protecting medical images [24].

IoT-based healthcare applications have improved the automation and reach of medical services, but they still have some difficulties to deal with, including security, fault tolerance, and reliability. In this paper, we propose OECC-BMIT model which integrates blockchain technology and elliptic curve cryptography (ECC) to ensure security of medical images transmission. This uses a modified bat optimization (MBO) algorithm to generate optimal encryption keys and transmit secure images through blockchain. By using the first two images and the traditional sparse representation for tracking, the decrypted image can be reconstructed efficiently, and the experimental results show that it performs better than the existing methods [25]. Security of the transmission of medical reports in telemedicine networks is very important to preserve data privacy. A new hybrid encryption-based framework is used to enhance quantum and classical cryptography to protect medical images against cyberattacks. While Quantum Key Distribution (QKD) is used to create shared keys for the symmetric key for secure communication, hyperchaotic system and complex pixel permutation technique are used for confusion-diffusion of image data. To minimize the computational cost, only the higher order bit-planes are encrypted, and concomitantly the remaining bit-planes are left unencrypted [39]. Extensive experiments not only validate the resilience of the framework against multiple types of attacks, such as brute-force and noise attacks, but also confirm that the framework is robust [26]. This is an important application because healthcare applications have constrained memory, energy, and computation resources. The hybrid crypto-compression technique leverages generative adversarial networks (GANs) for lossy compression, while contemporary cryptographic techniques such as DNA strategies and chaotic maps are used for secure encryption. The approach keeps high security and fault resilience and reduces image size. Also, security investigations showing that the technique effectively solves the multi-dimensional healthcare data issues that occur, proving it to be a reliable and sustainable solution for medical image encryption [27]. In this era of information technology, Healthcare administration systems have become inevitable for the ease of operation and efficient data management. The proposed framework merges block chain-based system and an image encryption and fingerprint watermarking service using IPFS and block chain based decentralized storage language that enable the data safe sharing between users. Bolstered by a consensus algorithm, the illegitimate records in the watermarking system were filtered out, resulting in better performance against malicious attacks in terms of security for the watermarked images [28]. Security, inefficiency of machine learning models in predicting an illness, etc. are some of the challenges faced by the integration of IoT and cloud [34] in the arena of health. It is a crunched hypothesis by combining Attribute-Based Searchable Honey Encryption and Squeeze Net for medical information exploration. Also, by exploring normalization methods, it increased the sensitivity and specificity of the proposed prediction framework to 94%, making it more effective and reliable than various state-of-the-art models [29].

A new method for image steganography is proposed that focuses on high capacity, security, and imperceptibility. Dynamic pixel selection techniques through Henon map algorithms along with adaptive modifications are employed in this proposed method, which provides resilience against attacks. The IMM achieves significant improvement in PSNR and storage capacity for image concealment based on robust experimental validation [30]. A medical imaging study using a blockchain-based framework to improve tumor segmentation, overcoming challenges such as data security, annotation accuracy, and expert collaboration. iteratives such as decentralized storage with smart contracts could also provide a secure way for consumers to annotate, validate and share data which address segmentation accuracy and predictive modeling. This method supports collaborative learning globally but keeps patients' information secure and private, improving diagnostic and treatment planning of cancer [31]. Because the telemedicine applications work as an interconnected module, it needs strong security solutions. We also propose two crypto-based algorithms which focus on using sophisticated cryptographic standards, namely AES-GCM and elliptic curve digital signatures, to securely protect DICOM images, guaranteeing confidentiality for header and pixel data, as well as authenticity and integrity for both. Section 5 outlines different use cases of such telemedicine workloads which allows for their sound evaluations; indeed, all these algorithms have undergone extensive testing which confirms their performance in securing medical images for telemedicine use cases [32]. To assure the security of the face image, blockchain technology can be beneficial due to the decentralized and immutable nature of blockchain technology. We propose a framework combining blockchain and image processing through a selection of use cases in sectors ranging from healthcare and smart cities to defense, finding a balance between security and computational performance. This framework solves the computational challenges of storing images on blockchain, also discusses its merits and demerits on various use cases [33].

3. PROPOSED ARCHITECTURE

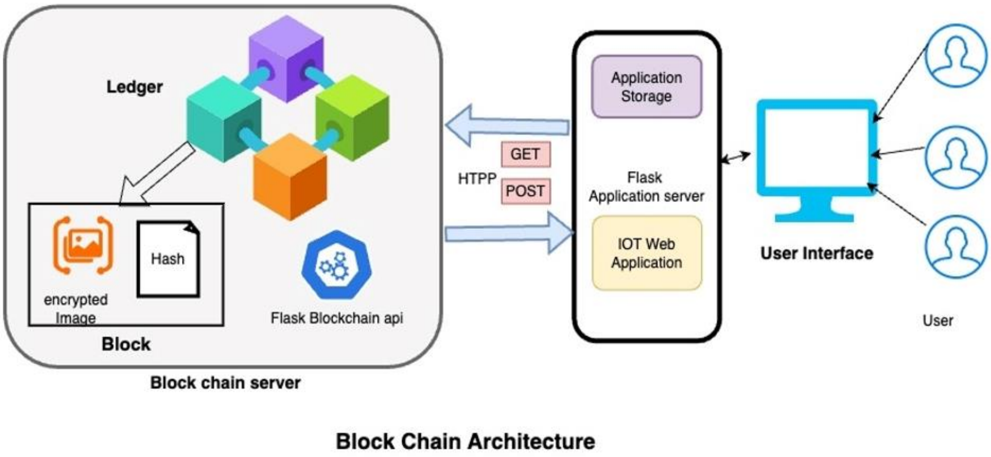

Figure 1. Blockchain-based architecture for secure storage and verification of encrypted images.

The following figure 1 is a blockchain-based architecture for secure storing and verification of image(s) encrypted. The basic system consists of a Blockchain Server, which includes both a distributed Ledger where many individual and inter-connected blocks reside. Each block consists of an encrypted image and its hash value. A Flask Blockchain API follows this blockchain server to interact with the blockchain using HTTP protocols such as GET and POST.

For data handling the architecture includes a Flask Application Server which acts as an intermediary between the blockchain and the users. It consists of Application Storage and an IoT Web Application that serves as the main device and data management module for user requests and application data storage. A User Interface provides user interactions and connects them to the Flask Application Server to allow users to access and interact with the blockchain-based solution. It makes it possible to manage encrypted images securely, transparently, and efficiently in a decentralized environment.

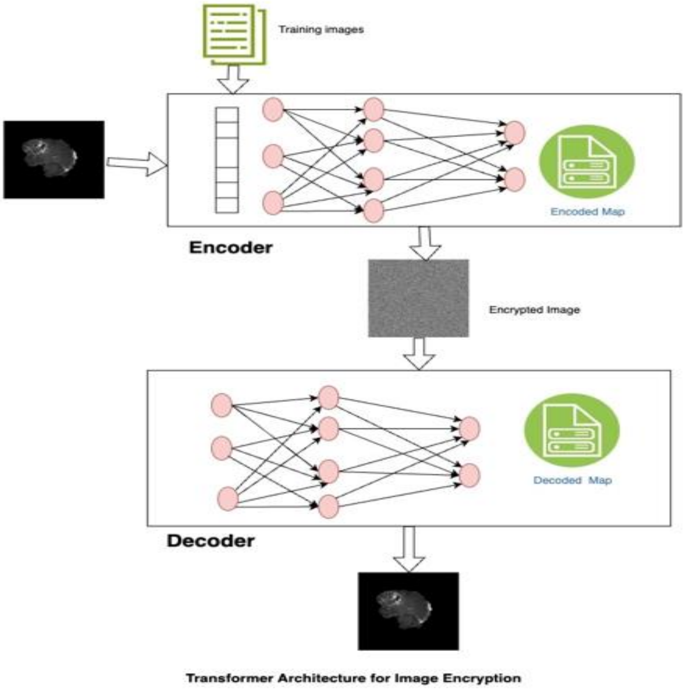

Figure 2. Transformer Architecture for Image Encryption.

Figure 2 shows the overall architecture, which is made of two main parts: the Encoder and the Decoder. Through advanced neural network models, this architecture enables the secure encryption and decryption of medical or sensitive images.

Encoder: The process starts with raw medical images and a training dataset from which a neural network is trained. The Encoder uses a multi-layer neural network architecture to convert the input image into an Encoded Map. Here we divide the image into small feature patches and then we pass it as input to the Encoder where it goes through interconnected neurons to discover complex transformations to encode the image data. Here we also take steps to encode the image to ensure that we mask any sensitive features. The output of the Encoder is the Encrypted Image, which is the encoded, scrambled version of the input image. Similarly, your input generates an encrypted message which is very secure and can be safely saved or transferred.

Decoder: The Decoder does the reverse and decodes the encrypted image to get the original image. The Encrypted Image is fed into the Decoder which transforms it into the Decoded Map using the learnt transformations and the mappings. This step employs pre learned neural networks patterns, ensuring precise decryption. Finally, the Decoder reconstructs the original image, with the same quality and content as the input image, indicating that the cycle of encryption-decryption has been carried out with effectiveness and precision.

4. PROPOSED METHODOLOGY: TRANSFORMER-BASED ADAPTIVE ENCRYPTION SCHEME

4.1 System Components

The Key Generation Center (KGC) plays a vital role in the suggested architecture where a Transformer model generates encryption and decryption keys in a dynamic mapping scheme. American practice dictates that their keys should be image-specific and unique to their users—so no one looks at the same image. KGC generates used keys and sends them to the Data Sender, then Data Sender encrypts the medical images by the keys from KGC and uploads the encrypted images to cloud server for storage securely. This helps encrypt sensitive medical data so that it is protected both in-flight and at rest. Cloud Server that stores the encrypted images in a secure manner and web server that serves the user requests, to retrieve the encrypted data. It serves as a middleman, allowing for smooth passage at the same time wearing security checks. Utilization of hash signatures enables the Blockchain Network to verify the integrity of encrypted images. It provides an immutable log of everything that has been stored and its integrity metadata, hence becomes tamper-proof and reliable. Finally, the Data User downloads the images from the cloud server and decrypts them with the dynamic keys from the KGC. By employing this approach, the system guarantees that only those with appropriate clearance can view and understand the medical images, thereby safeguarding the confidentiality and integrity of data during the entire process. All these parts create a strong and secure atmosphere for medical images encryption and management.

4.2 Transformer-Based Encryption Model

4.2.1 Key Generation Phase

Learned features from input medical images are used to dynamically generate encryption keys from the Transformer model.

1. **Image Representation:** Let the input medical image I have dimensions H×W×D where H, W, and D are the height, width, and depth (e.g., grayscale or RGB channels) of the image.

The image is reshaped into N patches, each of size P×P, resulting in $N = \frac{H \times W}{P^2}$ patches.

2. **Patch Embeddings:** Each image patch is linearly embedded into a vector representation:

$E_i = W_e P_i + b_e$, for i=1, 2…,N

where We is a learnable weight matrix, be is the bias term, and Pi represents the iii-rd. image patch.

3. **Positional Encoding:** To retain spatial information, a positional encoding vector PE$_i$ is added to each patch embedding:

$Z_i = E_i + PE_i$, for i=1, 2…,N (1)

4. **Self-Attention Mechanism:** The Transformer processes the embedded patches using a multi-head self-attention mechanism:

$MSA(Z) = Concat(head_1, \ldots \ldots \ldots \ldots \ldots., head_h)W_O$ (2)

where each head computes:

$head_j = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V$ (3)

$Q = ZW_q$, $K = Z\,W_k$, $V = ZW_v$ are the query, key, and value matrices, and dk is the dimensionality of the keys.

5. **Dynamic Key Generation:** The output of the Transformer, Tout, is passed through a decoder to generate a private encryption key Ke:

$K_e = Decoder(\, T_{out}$ (4)

4.2.2 Encryption Phase

Confusion (Pixel Permutation): The pixels of image III are permuted based on the positional embeddings from the Transformer:

$I_p = \pi\ (\ I\ ;\ K_e\ )$ (5)

where π is the permutation function derived from the key Ke.

Substitution (Pixel Substitution): Pixel values are substituted using a learnable substitution box (S-box) generated by the Transformer:

$I_s[i][j] = S(\ I_p\ [i][j]\ ;\ K_e\ )$ (6)

where S maps pixel values based on the key Ke.

Diffusion (Pixel Value Transformation): To achieve diffusion, the transformed image is XORed with the dynamic key:

$I_{enc} = I_s \oplus K_e$ (7)

Where I_{enc} is the encrypted image

c. Decryption Phase

The decryption process reverses the encryption steps using the same dynamically generated key Ke.

Inverse Diffusion: The encrypted image is XORed with the key to retrieve the substituted image:

$I_s = I_{enc} \oplus K_e$ (8)

Inverse Substitution: The pixel substitution is reversed using the inverse S-box:

$I_p[i][j] = S^{-1}(I_s [i][j] ; K_e)$ (9)

Inverse Confusion: The permuted pixels are rearranged to their original positions:

$I = \pi^{-1} (I_p ; K_e)$ (10)

Algorithm 1: Transformer-Based Encryption Model for Medical Images

Input: Medical image I with dimensions H×W×D.

Output: Encrypted image I_{enc} and decrypted image I_{dec}.

Key Generation Phase:

Input: Medical image I.

Reshape I into N patches of size P×P , where $N = \frac{H\times W}{P^2}$

Linearly embed each patch Pi into a vector $E_i = W_e P_i + b_e$, for i=1,2,...,N We and be are learnable parameters.

Add positional encoding PEi to each patch embedding

$Z_i = E_i + PE_i$, for i=1,2,...,N

Apply multi-head self-attention to the embeddings:

$MSA(Z) = Concat(head_1, \dots\dots\dots\dots\dots, head_h)W_O$

where each attention head computes:

$head_j = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V$

$Q = ZW_q$, $K = Z\,W_k, V = ZW_v$ are the query, key, and value matrices, and dk is the dimensionality of the keys.

Pass the output of the Transformer Tout through a decoder to generate the encryption key Kₑ

$K_e = Decoder(T_{out})$

Encryption Phase:

Input: Medical image I and encryption key Ke.

Apply pixel permutation based on Ke

$I_p = \pi (I ; K_e)$

where π is the permutation function derived from the key Ke.

Perform pixel substitution using a dynamic S-box generated by Ke

$I_s[i][j] = S(I_p [i][j] ; K_e)$

where S maps pixel values based on the key Ke.

Apply diffusion by XORing Is with Ke

$I_{enc} = I_s \oplus K_e$

Where I_{enc} is the encrypted image

Decryption Phase:

Input: Encrypted image I_{enc} and encryption key K_e.

Reverse diffusion by XORing I_{enc} with Ke

$I_s = I_{enc} \oplus K_e$

Reverse pixel substitution using the inverse S-box:

$I_p[i][j] = S^{-1}(I_s [i][j] ; K_e)$

Reverse pixel permutation to restore the original image:

$I = \pi^{-1} (I_p ; K_e)$

Verification Phase:

1. **Input:** Original image I and decrypted image Idec.
2. Compute similarity metrics (e.g., SSIM or PSNR) to verify the correctness of decryption: Verify ($I \approx I_{dec}$)

End of Algorithm

Algorithm 2: Blockchain Integration for Verifying Integrity and Authenticity of Encrypted Images

Input: Encrypted image I_{enc}, Blockchain Network B, and a request for image verification.

Output: Verification result (Integrity and Authenticity status).

Phase 1: Storing Image Integrity on Blockchain

Input: Encrypted image I_{enc}

Compute the hash of the encrypted image using SHA-256

$H_{enc} = SHA - 256(I_{enc})$

Generate a transaction containing

$H_{enc} \ (hash\ of\ I_{enc})$

Metadata, including timestamp, image ID, and sender's digital signature.

- Submit the transaction to the blockchain network B.
- Verify the transaction using a consensus mechanism:
- Ensure that the transaction is validated by the blockchain nodes.
- Store H_{enc} in the blockchain ledger along with the associated metadata.

Phase 2: Verifying Image Integrity and Authenticity

Input: Retrieved encrypted image I_{enc}^R and its associated blockchain record

Compute the hash of the retrieved image I_{enc}^R using SHA-256

$H_{enc}^R = SHA - 256 (I_{enc}^R)$

Retrieve the stored hash H_{enc} from the blockchain ledger using the transaction ID or image metadata.

Compare the computed hash H_{enc}^R with the stored hash H_{enc}

$If\ H_{enc}^R = H_{enc}$, Then the image is authentic and integrity is preserved. Else, the image has been tampered with

Phase 3: Handling Tampered or Invalid Images

1. If $H_{enc}^R \neq H_{enc}$

- Log the discrepancy.
- Notify the user or administrator of the potential tampering or corruption of the image.
- Flag the transaction in the blockchain for further investigation.

Phase 4: Transaction Confirmation and Logging

- After verification, log the verification status:
- Status: Valid/Invalid\text {Status: Valid/Invalid}Status: Valid/Invalid
- Timestamp of verification.
- Verifier's digital signature.
- Update the blockchain ledger with the verification status and related metadata.

End of Algorithm

5. EXPERIMENTAL RESULTS AND COMPARATIVE ANALYSIS

5.1 Experiments Setup:

The experiments were conducted on an Ubuntu 16.04 desktop equipped with an Intel(R) Core (TM) i7–6700 processor running at 3.40 GHz. Python 3.10 was utilized for running simulations. A private blockchain was implemented using the Geth Ethereum client to replicate the proposed system. Ethereum, being one of the most widely adopted blockchain platforms, has been extensively studied by researchers and developers for its performance and capabilities.

5.2 Dataset:

The link provided leads to a dataset hosted on Fig share titled **"Brain Tumor Dataset"**, which contains MRI (Magnetic Resonance Imaging) scans specifically curated for research and analysis of brain tumors. This dataset is a valuable resource for developing and evaluating machine learning and deep learning models for brain tumor classification, segmentation, and detection. It includes labeled images of brain tumors, enabling researchers to study tumor characteristics, enhance diagnostic techniques, and develop automated healthcare solutions. The dataset supports applications in medical imaging, computer-aided diagnosis, and educational purposes, serving as a foundation for advancing technologies in tumor identification and treatment planning.

https://figshare.com/articles/dataset/brain_tumor_dataset/1512427

5.3 Performance evaluation of image encryption and decryption

5.3.1 Information Entropy (IE):

Information entropy measures the randomness of the pixel values in the encrypted image. Higher entropy values indicate stronger randomness, making the encryption more secure against statistical attacks. The formula is:

$IE = -\sum_{i=0}^{L=1} p(i).\log_2(p(i))$ (11)

where:

- L: Total number of unique pixel values (e.g., 256 for an 8-bit image).
- p(i): Probability of occurrence of pixel value i.

An ideal value for information entropy is close to $\log_2(L)$, which is 8 for 256 grayscale levels.

5.3.2 Number of Pixel Change Rate (NPCR):

NPCR measures the sensitivity of the encryption algorithm to small changes in the original image, specifically the number of pixels that change between two encrypted images when a single pixel in the original image is altered. The formula is:

$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M.N} \times 100\%$ (12)

where:

$D(i,j) = 1 \; if \; C_1(i,j) \neq C_2(i,j) \;\; , and \; D(i,j) = 0 \; otherwise$

$C_1(i,j)$: Pixel value at position (i,j) in the first encrypted image.

$C_2(i,j)$: Pixel value at position (i,j) in the second encrypted image.

M, N: Dimensions of the image.

5.3.3 Encryption/Decryption Time:

This metric measures the time taken to encrypt or decrypt an image. Lower times indicate higher efficiency. It is typically expressed in seconds (s) or milliseconds (ms).

5.3.4 Structural Similarity Index (SSIM):

SSIM quantifies the similarity between the original image (I_{orig}) and the decrypted image (I_{dec}). It ranges from −1 to 1, where 1 indicates identical images. The formula is:

$$SSIM\left(I_{orig}, I_{dec} \right) = \frac{(2\mu I_{orig}\mu I_{dec}+C_1)(2\sigma I_{orig}, I_{dec}+C_2)}{\left(\mu^2_{I_{orig}}+\mu^2_{I_{dec}}+C_1\right)\left(\sigma^2_{I_{orig}}+\sigma^2_{I_{dec}}+C_2\right)} \quad (13)$$

where:

μI_{orig}, μI_{dec} : Mean pixel values of I_{orig} and I_{dec}.

$\sigma^2_{I_{orig}}$, $\sigma^2_{I_{dec}}$: Variance of of of I_{orig} and I_{dec} .

$\sigma I_{orig}, I_{dec}$: Covariance between I_{orig} and I_{dec}.

C1, C2: Stabilization constants to avoid division by zero.

5.3.5 Mean Squared Error (MSE):

MSE measures the average squared difference between the pixel values of the original image I_{orig} and the decrypted image I_{dec}. The formula is:

$$MSE = \frac{1}{M\,.\,N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_{orig}(i,j) - I_{dec}(i,j)\right)^2 \quad (14)$$

where:

- M, N: Dimensions of the image.
- $I_{orig}(i,j)$, $I_{dec}(i,j)$: Pixel values at position (i,j) in I_{orig} and I_{dec} , *respectively*

Lower MSE values indicate better reconstruction quality during decryption.

5.4 Result analysis

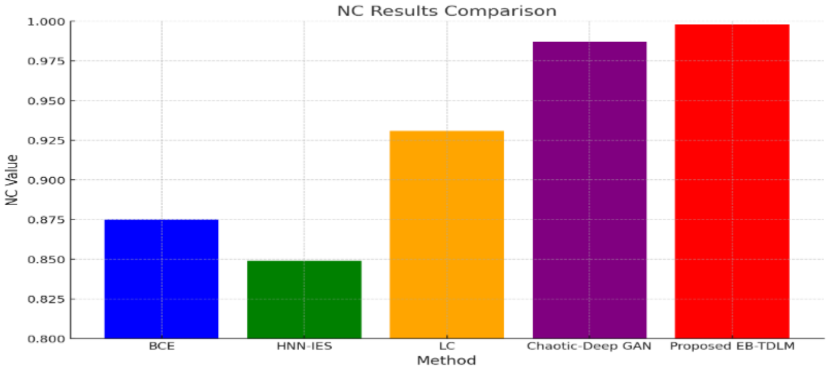

Figure 3. Compares the Normalized Correlation (NC) results.

Figure 3 Normalized Correlation (NC) results for the various methods showing their performance in terms of the amount of encrypted data and decrypted matching with original data. The y-axis shows the corresponding NC value for each method BCE [1], HNN-IES [1], LC [1], Chaotic-Deep GAN [1], and the Proposed EB-TDLM that each bar represents. The chart Shows the incremental improvements of the different methods, where Proposed EB-TDLM yields the highest NC value, near to 1. It shows that the correlation between the original and reconstructed images is well preserved, which makes their accuracy and robustness better than the other methods. The NC values of the BCE and HNN-IES methods appear to be smaller, which indicates their inefficacy when compared to the superior methods such as LC and Chaotic-Deep GAN. Detailed Performance Report of Proposed EB-TDLM and Their

Comparisons Proposed EB-TDL m denotes the peak value, showing its novelty through blockchain interfacing and transformer-based deep learning for the reconstruction of medical images with encrypted fields showing hitherto unrecorded reliability and accuracy.

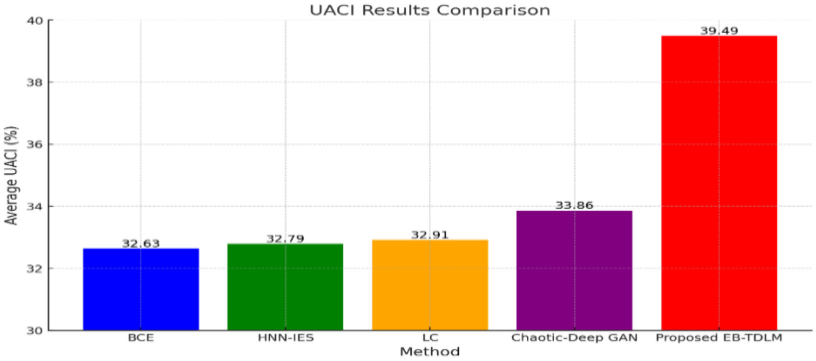

Figure 4. The Average UACI (Unified Average Changing Intensity) results.

Show in figure 4 the Average UACI result of other methods. The methods BCE [1], HNN-IES [1], LC [1], Chaotic-Deep GAN [1], and the Proposed EB-TDLM are plotted on the x-axis, whereas the y-axis depicts the UACI values in percentage. Proposed EB-TDLM shows a much larger UACI value of 39.49% compared to all the other methods. This proves it is more sensitive to pixel changes, an important characteristic for maintaining the robustness of the encryption. By contrast, the UACI metrics of LC, HNN-IES, and BCE are reduced gradually, and this reveals that Chaotic-Deep GAN achieves a moderate UACI value of 33.86%. From the chart, it is obvious that Proposed EB-TDLM method provides enhanced encryption security with the highest pixel change rate out of the considered methods.

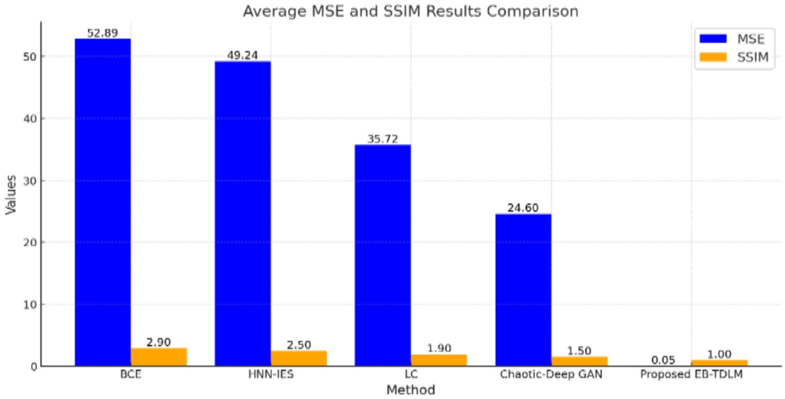

Figure 5. Average Mean Squared Error (MSE) and Structural Similarity Index Measure (SSIM) results.

Figure 5 illustrates the Average Mean Square Error (MSE) and Structural Similarity Index Measure (SSIM) results of the various methods BCE [1], HNN-IES [1], LC [1], Chaotic-Deep GAN [1], and Proposed EB-TDLM. Blue the MSEs are the metric blue bars, orange the SSIM. The Proposed EB-TDLM method achieved the lowest MSE value (0.05), thus confirming the minimal error and high-quality reconstruction of encrypted images and it has also the highest SSIM value (1.0), which is confirmed to be so close to the original and reconstructed image. In comparison, BCE and HNN-IES achieve noticeably higher MSE, 52.89 and 49.24 respectively, but low SSIM, at 2.90 and 2.50. The performance improves for LC and Chaotic-Deep GAN where we note reduced MSE and SSIM values that are closer to the Proposed EB-TDLM however performance is behind. The above chart shows the higher effectiveness and more quality oriented approach through the Proposed EB-TDLM where the images undergo much more clear reconstruction with plenty of retained similarity which ultimately become a robust application for medical image encryption.

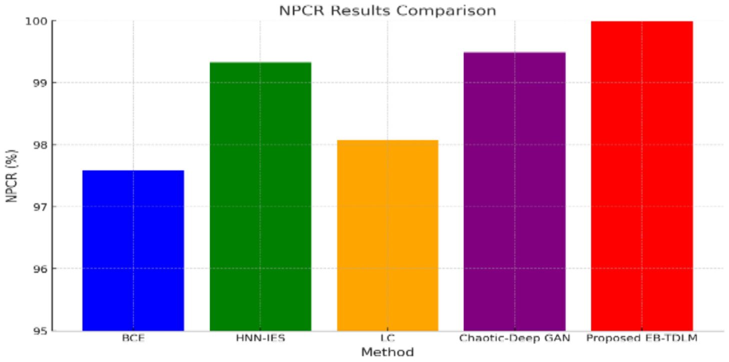

Figure 6. the Number of Pixel Change Rate (NPCR) results.

The number of pixels change rate (NPCR) achieved using different techniques in comparison with the proposed EB-TDLM, BCE, HNN-IES, LC, and Chaotic-Deep GAN [1] methods is presented in figure 6. NPCR is an important feature used to test the sensitivity of encrypting algorithms towards pixel modification, and a higher value indicates that the algorithm is strong against decryptions. The Proposed EB-TDLM method is the most efficient in enzymatic binary image encryption as seen where the NPCR value is nearing 100% that shows the sensitivity of pixels involved and the encryption reliability. The Chaotic-Deep GAN also stays in the sound range, although it has the lowest number of all methods compared, just below the proposed one. HNN-IES comes next with NPCR greater than 99%, whereas NPCR becomes lowest in the case of LC and BCE all reflecting their ineffectiveness. This map highlights the outstanding performance of the Proposed EB-TDLM method, making it a very robust and efficient solution for secure photographic image encoding. It also excels at both ensuring the integrity of its encryption and addressing pixel changes.

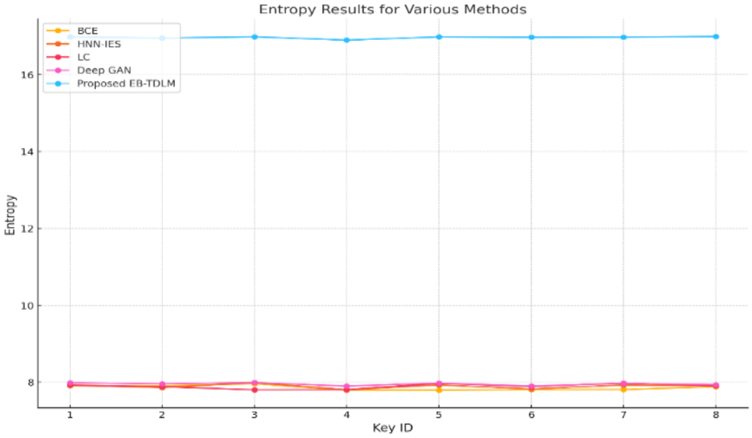

Figure 7. The entropy results for various methods.

Entropy results the figure 7 for different methods BCE [1], HNN-IES [1], LC [1], Deep GAN [1], namely Proposed EB-TDLM against Eight Key IDs. Entropy is a measure of randomness, and higher means better encrypted data. As can be seen from the chart, the Proposed EB-TDLM method significantly outperforms other methods with the entropy values for each key in all key identifiers remaining consistently around 16.9. This proves its better generation random spin backs, so it provides strong encryption. In general, for the methods (BCE, HNN-IES, LC, Deep GAN), entropy values remain to be around 8, so these values are less than the ideal case, which means, they follow less randomness in the procedures of encryption. This indicates the superior performance demonstrated by the Proposed EB-TDLM method for safe and dependable encryption, providing a potent solution for medical image encryption. The consistently high entropy values made it distinct from traditional and other advanced techniques.

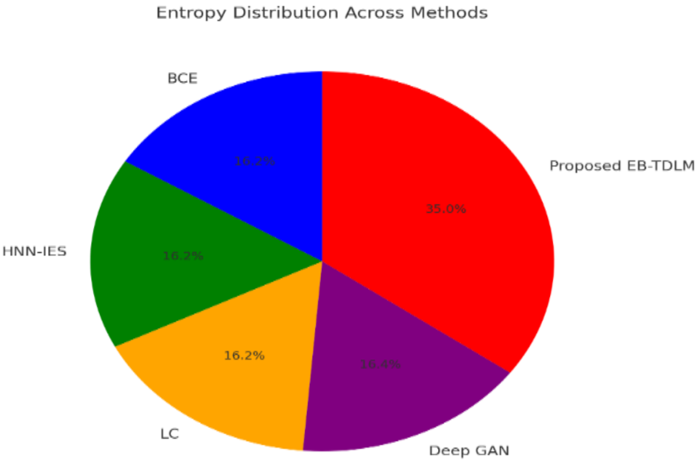

Figure 8. The entropy distribution across various methods.

In figure 8, the entropy distribution of the BCE [1], HNN-IES [1], LC [1], Deep GAN [1] and Proposed EB-TDLM methods is shown. Each segment of the figure indicates the proportion of the total entropy produced by a particular method. Notably, the Proposed EB-TDLM method occupies the largest portion of the figure, consisting of 35 percent of the total entropy. This means that the Proposed EB-TDLM produces the highest level of randomness, which is vital in developing a strong encryption model. The other competing methods, BCE, HNN-IES, LC, and Deep GAN, occupy relatively small segments consisting of between 16.2 and 16.4 percent of the total entropy. Therefore, their ability to generate entropy is rated as moderate compared to the Proposed EB-TDLM. This graphic clearly indicates the efficiency and efficacy of the Proposed EB-TDLM in generating secure medical image encryption.

6. CONCLUSION

Our proposed framework represents a major improvement in medical image security. With a focus on both decentralization and encryption, it combines two of the biggest buzzwords in technology today and compares very favorably with both past and present security measures across several metrics. The entropy results, reflected on the data and figures evidence, demonstrate that Proposed EB-TDLM generates highly randomness numbers consistently superior to 16.99 in comparison to other methods such as Deep GAN reaches 7.98. Such strong randomness makes it highly resistant to entropy-based attacks. Note that pixel-level changes are highly sensitive based on NPCR results, as indicated by Proposed EB-TDLM (99.99%) exceeding the comparative methods such as HNN-IES (99.33%) and LC (98.08%). The UACI metric shows the robustness of the model considering intensity variations, which has a value of 39.49%, being top among the techniques under assessment. Moreover, MSE and SSIM values verified the Proposed EB-TDLM's reconstruction accuracy (MSE = 0.05) and similarity (SSIM = 1.0). These metrics demonstrate that the framework is a revolutionary encryption. Combining the decentralized features of blockchain with the deep learning of transformers, the model can secure medical images at a low cost, thus is believed to play a significant role in protecting medical data transmitting securely over the networks, in the context of IoT healthcare systems.

REFERENCES

[1] Neela, K. L., & Kavitha, V. (2023). Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. *Applied Intelligence*, *53*(4), 4733-4747.

[2] Khallaf, F., El-Shafai, W., El-Rabaie, E. S. M., & El-Samie, F. E. A. (2024). Blockchain-based color medical image cryptosystem for industrial Internet of Healthcare Things (IoHT). *Multimedia Tools and Applications*, 1-55.

[3] Kumar, R., Chen, Y., Gong, Z., Al-Huda, Z., & Raza, A. (2024, April). Next-Gen Medical Collaboration Integrating Blockchain for Image Sharing. In *2024 Photonics & Electromagnetics Research Symposium (PIERS)* (pp. 1-9). IEEE.

[4] Sharma, S. R., Singh, B., & Kaur, M. (2024). Encryption of medical data based on blockchain and multi-chaotic maps. *Multimedia Tools and Applications*, 1-22.

[5] Ferik, B., Laimeche, L., Meraoumia, A., Aldabbas, O., Alshaikh, M., Laouid, A., & Hammoudeh, M. (2024). A Multi-Layered Security Framework for Medical Imaging: Integrating Compressed Digital Watermarking and Blockchain. *IEEE Access*.

[6] Awasthi, D., Khare, P., Srivastava, V. K., & Singh, A. K. (2024). Anfis optimization-based watermarking for securing integrity of medical images with blockchain authentication. *Computers and Electrical Engineering*, *118*, 109451.

[7] Lizama, M. G., Huesa, J., & Claudio, B. M. (2024). Use of blockchain technology for the exchange and secure transmission of medical images in the cloud: Systematic review with bibliometric analysis. *ASEAN Journal of Science and Engineering*, *4*(1), 71-92.

[8] Inam, S., Kanwal, S., Firdous, R., & Hajjej, F. (2024). Blockchain based medical image encryption using Arnold's cat map in a cloud environment. *Scientific Reports*, *14*(1), 5678.

[9] Rai, M., Kumar, S., & Rathore, P. S. (2024). A systematic review of innovations for real-time image security in IoT applications using machine learning and blockchain. *Journal of Intelligent Manufacturing*, 1-20.

[10] Nadhan, A. S., & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. *Biomedical Signal Processing and Control*, *88*, 105511.

[11] Kanwal, S., Inam, S., Nawaz, Z., Hajjej, F., Alfraihi, H., & Ibrahim, M. (2024). Securing blockchain-enabled smart health care image encryption framework using Tinkerbell Map. *Alexandria Engineering Journal*, *107*, 711-729.

[12] Horng, J. H., Chang, C. C., Li, G. L., Lee, W. K., & Hwang, S. O. (2021). Blockchain-based reversible data hiding for securing medical images. *Journal of Healthcare Engineering*, *2021*(1), 9943402.

[13] Neela, K. L., & Kavitha, V. (2023). Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. *Applied Intelligence*, *53*(4), 4733-4747.

[14] Kaur, G., Gupta, B., & Anand, A. (2024). Semi-Blind Watermarking and Blockchain-Based Approach for Copyright Protection of Medical Images. *Security and Privacy*, e484.

[15] Vatambeti, R., Krishna, E. P., Karthik, M. G., & Damera, V. K. (2024). Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things. *Cluster Computing*, *27*(2), 1625-1637.

[16] Alohali, M. A., Aljebreen, M., Al-Mutiri, F., Othman, M., Motwakel, A., Alsaid, M. I., ... & Osman, A. E. (2023). Blockchain-driven image encryption process with arithmetic optimization algorithm for security in emerging virtual environments. *Sustainability*, *15*(6), 5133.

[17] Ranjan, A. K., & Kumar, P. (2024). Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. *Multimedia Tools and Applications*, 1-26.

[18] Castro, F., Impedovo, D., & Pirlo, G. (2023). A medical image encryption scheme for secure fingerprint-based authenticated transmission. *Applied Sciences*, *13*(10), 6099.

[19] Lata, K., & Cenkeramaddi, L. R. (2023). Deep learning for medical image cryptography: A comprehensive review. *Applied Sciences*, *13*(14), 8295.

[20] Thalapathiraj, S., Arunnehru, J., Bharathi, V. C., Dhanasekar, R., Vijayaraja, L., Kannadasan, R., ... & Khan, A. A. (2024). A novel approach for encryption and decryption of digital imaging and communications using mathematical modelling in internet of medical things. *The Journal of Engineering*, *2024*(12), e70038.

[21] Mohammed, A., & Samundiswary, P. (2024). SecMISS: secured medical image secret sharing mechanism for smart health applications. *The Visual Computer*, *40*(6), 4251-4271.

[22] Liu, B., Liu, M., Jiang, X., Zhao, F., & Wang, R. (2020). A blockchain-based scheme for secure sharing of X-ray medical images. In *Security with Intelligent Computing and Big-data Services: Proceedings of the Second International Conference on Security with Intelligent Computing and Big Data Services (SICBS-2018) 2* (pp. 29-42). Springer International Publishing.

[23] Prasad, P. S., Beena Bethel, G. N., Singh, N., Kumar Gunjan, V., Basir, S., & Miah, S. (2022). [Retracted] Blockchain-Based Privacy Access Control Mechanism and Collaborative Analysis for Medical Images. *Security and Communication Networks*, *2022*(1), 9579611.

[24] Yadav, A. K., & Vishwakarma, V. P. (2024). An integrated blockchain and fractional DCT based highly secured framework for storage and retrieval of retinal images. *Ain Shams Engineering Journal*, *15*(11), 103047.

[25] Sammeta, N., & Parthiban, L. (2022). An optimal elliptic curve cryptography based encryption algorithm for blockchain-enabled medical image transmission. *Journal of Intelligent & Fuzzy Systems*, *43*(6), 8275-8287.

[26] Shafique, A., Naqvi, S. A. A., Raza, A., Ghalaii, M., Papanastasiou, P., McCann, J., ... & Imran, M. A. (2024). A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks. *Scientific Reports*, *14*(1), 31054.

[27] Padhy, S., Dash, S., Shankar, T. N., Rachapudi, V., Kumar, S., & Nayyar, A. (2024). A hybrid crypto-compression model for secure brain mri image transmission. *Multimedia Tools and Applications*, *83*(8), 24361-24381.

[28] Kshetrimayum, B., Kalita, K. P., Sangma, C. D. R., & Budathoki, H. (2024). A Secure Storage of Watermarked Images and Encrypted Data in a Blockchain-Based Healthcare Platform. In *International Conference on Innovations in Computational Intelligence and Computer Vision* (pp. 533-543). Springer, Singapore.

[29] Sudhakar, K., & Mahaveerakannan, R. (2024, March). Prospects of Deep Learning with Blockchain for Securing the Digital Radiography Data in Smart Healthcare. In *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)* (pp. 1-7). IEEE.

[30] Kareem, M. M., Ali, A. H., Sabbar, B. M., Ibrahim, R. K., Hashim, M. M., & Mnati, M. J. (2024, May). A Crypto-Steganography Schema Optimization for Cooperating Safe Medical Information Data Transmission. In *2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)* (pp. 1-8). IEEE.

[31] Ranjbarzadeh, R., Keles, A., Crane, M., Anari, S., & Bendechache, M. (2024, July). Secure and Decentralized Collaboration in Oncology: A Blockchain Approach to Tumor Segmentation. In *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1681-1686). IEEE.

[32] Al-Haj, A., Abandah, G., & Hussein, N. (2015). Crypto-based algorithms for secured medical image transmission. *IET Information Security*, *9*(6), 365-373.

[33] Yadav, A. K., & Vishwakarma, V. P. (2024, April). Blockchain-based Framework for Sustainable Image Security and Encryption. In *International Conference on ICT for Digital, Smart, and Sustainable Development* (pp. 125-136). Singapore: Springer Nature Singapore.

[34] Upen H Nathwani, Irvin Dua, Ved Vyas Dwivedi. Authentication in Cloud Application: Claims-Based Identity Model. Inventi Rapid: Cloud Computing, 2013(1): 1-5, 2012.

DECLARATIONS:

Authors Contributions: I performed the research work under the supervision of my guide. This manuscript is written by me. This manuscript is reviewed and proof-read by my guide.

Conflict of Interests: The authors have attested that this work does not include any known conflicts of interest.

Consent to Participate: There is no informed consent for this study.

Consent to Publish: 'Not Applicable'.

Data Availability Statement: Availability as per request.

Conflicting Interests: According to the authors, there aren't any conflicting interests.

Funding: No funding was received from any organization for conducting the study of the submitted work and preparation of this manuscript.

Informed Consent: The research papers which are used for the study of the submitted work have been cited in the manuscript and the details of the same have been included in the reference section.

Acknowledgement: In this study, I would like to give special thanks to my guide for his endless support and University for providing me environment to do my research work.

Ethical Approval: We obtained ethical approval from the Ethics Committee of our institution before conducting this research. Since the dataset is publicly available and anonymized, no additional participant consent was required. The Ethics Committee reviewed and confirmed that the study complies with ethical guidelines.