Securing Healthcare Data in IoMT Using Hybrid Cryptosystem and Decentralized Storage Based Blockchain with IPFS

Soufian El Airaj [1], Salma Bendaoud [1], Fatima Amounas [1], Mourade Azrour [1,*], Mohamed Badiy [1], Abdullah M. Alnajim [2], Abdulatif Alabdulatif [3], and Sheroz Khan [4]

[1] IMIA Laboratory, MSIA Team, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, Morocco
[2] Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia
[3] Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia
[4] Department of Electrical Engineering, College of Engineering and Information Technology, Onaizah Colleges, Onaizah, Saudi Arabia
Email: s.elairaj@edu.umi.ac.ma (S.E.A.); salma.bendaoud2@gmail.com (S.B.); f.amounas@umi.ac.ma (F.A.); mo.azrour@umi.ac.ma (M.A.); m.badiy@edu.umi.ac.ma (M.B.); najim@qu.edu.sa (A.M.A.); ab.alabdulatif@qu.edu.sa (A.A.); cnar32.sheroz@gmail.com (S.K.)
*Corresponding author

***Abstract*—The rapid advancement of IoT has greatly revolutionized the healthcare sector, giving rise to the Internet of Medical Things (IoMT). While IoMT has significantly enhanced healthcare services by incorporating smart and intelligent sensor devices into hospital settings, it also introduces critical challenges related to security and privacy. As more devices connect to the IoMT, the need for robust security and privacy protection grows, particularly due to the sensitive nature of medical data. Medical information contains extensive personal details, making it vulnerable to privacy breaches and complicating its sharing. So, it is crucial to establish a framework that ensures the secure and efficient exchange and storage of vast amounts of medical data. Current approaches mainly support image-level sharing and rely on standard cryptographic algorithms. To overcome these limitations, this paper introduces a healthcare information security storage solution based on IPFS and Blockchain. This research enhances the security of decentralized storage by employing a hybrid crypto-compression scheme based on Wavelet Transform and Elliptic Curve Cryptography (ECC). This method utilizes first a joint compression and encryption strategy, ensuring secure encryption of medical data while preserving its privacy and confidentiality. The encrypted medical information is then stored on the InterPlanetary File System (IPFS), which provides a decentralized and secure storage solution. Instead of transmitting the medical data itself, only the Content Identifier (CID) generated by IPFS is sent over a public channel. This solution integrates IPFS technology to reduce the blockchain's storage burden. The finding confirms the feasibility of the proposed approach, ensuring both the secure storage and integrity of medical information while effectively addressing security challenges in IPFS. By combining these concepts, the approach aims to establish a secure, reliable, and confidential ecosystem tailored for the evolving landscape of healthcare data management in IoMT environments.**

***Keywords*—Internet of Medical Things (IoMT), Elliptic Curve Cryptography (ECC), cryptography, compression, blockchain, InterPlanetary File System (IPFS), healthcare**

I. Introduction

Nowadays, the Internet of Medical Things (IoMT) is revolutionizing healthcare through remote monitoring, improved patient care, and more efficient healthcare operations. This technology has opened up significant opportunities for innovation in healthcare. It has become a key subject of discussion in the field of research and its practical applications. While IoT generally refers to a network of devices that collect and exchange data, IoMT applies this technology to healthcare, integrating medical devices and systems for remote patient monitoring, real-time health tracking, and personalized care, as shown in Fig. 1. In the healthcare sector, large volumes of data, including patient information and medical images, are produced, stored, shared, and accessed daily across different hospitals. The healthcare industry's primary need is to quickly and efficiently diagnose patients using data collected and obtained from various healthcare systems. However, healthcare data is often unstructured, noisy, and disorganized, requiring significant processing power for accurate analysis and actionable insights. Additionally, healthcare data is critical for decision-making, making it an attractive target for cybercriminals [1].

With the growing number of devices connected to the IoMT, the need for robust security and privacy measures becomes even more critical, requiring enhanced mechanisms to safeguard patient privacy [2]. Various

Manuscript received February 17, 2025; revised March 21, 2025; accepted April 7, 2025; published August 26, 2025.

methods are utilized for capturing medical images. The most commonly employed techniques among them are Ultrasonography (US), Computed Tomography (CT) scans, X-rays, Positron Emission Tomography (PET), and Magnetic Resonance Imaging (MRI), as shown in Fig. 2.

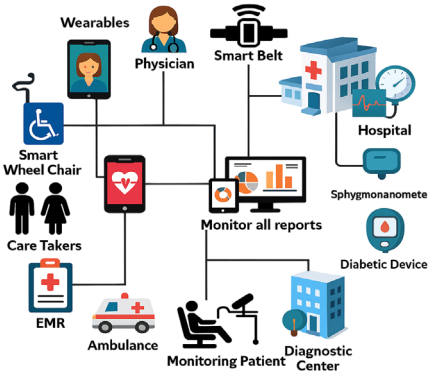


Fig. 1. Internet of medical things.

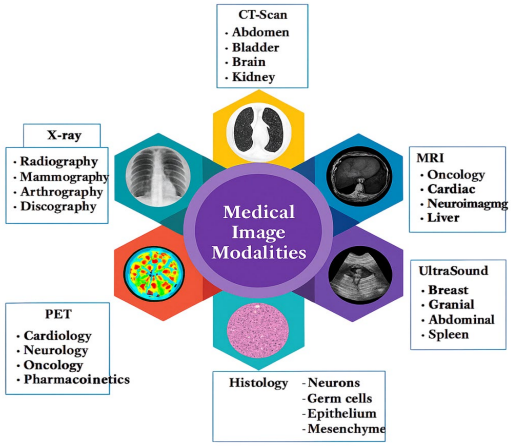


Fig. 2. Medical imaging modalities.

With advancements in digital healthcare technologies, medical images must be managed with great care, as they play a crucial role in diagnosing patients, particularly in the case of life-threatening conditions. The procedure for gathering and sending medical data, including medical images, has become a significant challenge related to security, privacy, and data integrity. Currently, IoMT devices, ranging from simple wearable sensors to advanced medical imaging systems, lack the computational power and security mechanisms required to protect against potential cyberattacks.

Secure transmission of medical images and information is a key requirement in healthcare systems. Encryption has proven to be a highly effective method for enhancing privacy in IoMT networks and ensuring that sensitive information remains protected from unauthorized access. However, traditional security solutions relying on centralized architectures encounter difficulties in adjusting to the dynamic, resource-limited, and extensively distributed characteristics of IoMT networks [3–6]. So, there is a pressing need to enhance existing security frameworks. Decentralized security mechanisms, such as blockchain-based frameworks, have emerged as promising alternatives to enhance the security and the efficiency in IoMT environments [7]. This technology is designed with robust security features, including cryptographic techniques, hash algorithms, and digital signatures [8–11]. However, it faces storage constraints that can limit its scalability. To overcome this challenge, InterPlanetary File System (IPFS) is adopted to provide a decentralized and efficient storage solution [12]. Furthermore, the integration of this hybrid encryption approach with decentralized technologies utilizing IPFS and blockchain will significantly transform the landscape of medical image analysis within the IoMT ecosystem.

Despite significant advancements in securing medical data in IoMT environments, existing solutions still face several challenges. Traditional approaches primarily focus on either encryption or compression separately, leading to inefficiencies in secure medical image storage and transmission. Additionally, many current security frameworks rely on centralized architectures, making them vulnerable to cyberattacks and scalability issues. While blockchain has emerged as a promising solution for decentralized security, its storage overhead limits practical implementation, especially for large medical datasets. Furthermore, most cryptographic mechanisms used in IoMT security are computationally intensive and unsuitable for resource-constrained IoMT devices. Existing research also lacks a comprehensive evaluation of security and performance, limiting the real-world applicability of proposed solutions. To address these gaps, this paper proposes a hybrid crypto-compression approach using Wavelet Transform and ECC, combined with decentralized storage through IPFS and blockchain, offering an efficient, scalable, and secure framework for medical data management in IoMT networks.

A. Research Contributions

The primary contributions of this paper are:

- To design a hybrid crypto-compression using the Advanced Encryption Standard (AES) algorithm and ECC mechanism along with a compression technique.
- To provide decentralized storage for medical images using IPFS and blockchain technology, enabling IoT devices to ensure security without centralizing data.
- To propose a distributed storage application that supports the storage of various medical images, where uploaded files are stored on IPFS and their hash values are recorded on the Ethereum blockchain.
- To conduct a series of experiments to validate the effectiveness of our framework through a security analysis and performance evaluation.

B. Outline of the Paper

The remaining sections are structured as follows: Section II reviews related work. Section III provides an overview of the preliminaries, including blockchain, IPFS, ECC, and Discrete Wavelet Transform (DWT). Section IV details the proposed methodology. Section V outlines the

simulation results, followed by the security analysis and performance evaluation. Lastly, Section VI concludes the paper with a summary.

II. Related Works

In the last few years, securing and managing medical data has become a critical focus in healthcare. The incorporation of advanced technologies, especially blockchain and IPFS, yields significant benefits for healthcare applications. The adoption of blockchain technology in the healthcare sector has a significant impact, owing to its decentralized structure, tamper-resistance, and transparency [13]. This technology profoundly impacts healthcare by enabling secure, decentralized storage and transparent sharing of medical images, fostering advancements in medical imaging management, and attracting global research interest. Many strategies have been introduced in this area to deal with security aspects of medical images, which are often computationally intensive. Researchers have introduced various frameworks that adopt emerging technologies like blockchain, the InterPlanetary File System (IPFS), Artificial Intelligence (AI), and advanced cryptographic methods to address challenges such as privacy, interoperability, and data integrity. However, there is still a need to address the limitations in terms of scalability, real-time data access, and seamless integration across diverse healthcare systems. This section provides an in-depth analysis of recent research on image cryptographic algorithms, focusing on both centralized and decentralized storage, and highlights the shortcomings of current studies. Table I summarizes the current cryptographic research in the literature with centralized and decentralized storage.

TABLE I. Recent Research Cited in the Literature Review on Encryption Approaches with Centralized and Decentralized Storage

Ref	Encryption Techniques	Blockchain	Data Storage	Smart contract	Distributed	Limitations
[14]	Chaotic encryption	+	IPFS	Yes	Yes	High computational complexity
[15]	Attribute-based encryption	+	IPFS	Yes	Yes	Key management complexity
[16]	ECC and AES encryption	+	IPFS	Yes	Yes	Computational overhead
[17]	Optimal Elliptic Curve Cryptography	-	Cloud system	No	No	Centralized control, security concerns
[18]	Cosine-transform encryption	-	Central server	No	No	Single point of failure
[19]	Extended zigzag encryption	-	Cloud system	No	No	Limited scalability
[20]	3D-chaotic permutation and diffusion	-	Central server	No	No	High storage overhead
[21]	Cryptography-based network and Deep Learning	-	Central server	No	No	High processing power requirement
[22]	an Ethereum blockchain and IPFS-based decentralized framework	+	IPFS	Yes	Yes	Smart contract vulnerabilities
[23]	Java-enabled GPG (GNU Privacy Guard) encryption	+	IPFS	Yes	Yes	Performance bottlenecks
Prop. Alg.	Hybrid Crypto-compression (DWT + ECC + AES)	+	IPFS	Yes	Yes	Efficiency concerns with compression and encryption

Note: "-": Not applicable, "+": applicable

A. Centralized Storage

The use of cryptographic mechanisms in IoT has attracted significant interest and has been the focus of extensive research and discussion. Numerous studies have previously been conducted to secure medical images [24–26]. Most of these studies primarily emphasize cryptographic methods and rely on centralized storage solutions. For example, Elhoseny *et al.* [17] investigated the security of medical images in IoT by utilizing an innovative cryptographic model with optimization strategies. As the patient data are stored on hospital cloud servers, another framework is required for the secure transmission and effective storage. The authors introduced an additional framework to enhance the security of medical images by selecting the optimal key through a hybrid swarm optimization approach, which integrates grasshopper optimization and particle swarm optimization within elliptic curve cryptography. However, the paradigm does have serious drawbacks. The encrypted images may still display identifiable patterns due to insufficient imperceptibility, potentially compromising their confidentiality. Additionally, while the hybrid optimization technique improves security, it can increase computational overhead, making it less suitable for resource-constrained IoT devices. Furthermore, the framework might face challenges in handling large-scale IoT deployments with extensive medical data and numerous connected devices, as optimization algorithms can become computationally intensive with increasing problem size.

To address the limitations of traditional encryption methods in the healthcare sector, particularly related to data size and confidentiality issues, Khan *et al.* [18] introduced a lightweight IoT framework-based probabilistic image encryption technique, as well as a secure surveillance mechanism that uses the YOLOv3 algorithm to extract keyframes. Their framework is designed to protect healthcare data from unauthorized access while enabling secure surveillance in healthcare environments. The authors highlight an advanced method based on chaotic sequences and diffusion-confusion

operations to ensure data confidentiality during transmission and storage in the hospital's servers. However, this approach has certain limitations. The static key architecture might be vulnerable to advanced attacks, scalability in large IoT networks remains unverified, reliance on YOLOv3 could reduce adaptability to various data types, and energy efficiency on resource-constrained devices has not been comprehensively addressed.

One year later, Deepika *et al.* [19] carried out a study focused on improving healthcare diagnostics by leveraging the integration of IoT and cloud computing. Their work focused on improving healthcare diagnostics, specifically in brain tumor prediction, by securely collecting and transferring medical datasets to the cloud for computational analysis. To facilitate diagnosis, the authors proposed a Fuzzy Convolutional Neural Network (FCNN) algorithm designed to classify medical images into two categories: normal and abnormal. This classification provides a critical step in identifying the presence of brain tumors. Once the images are analyzed and classified, the results are efficiently communicated to doctors and healthcare providers through IoT, enabling timely intervention and further treatment planning. However, this approach has certain limitations, including its reliance on a specific dataset, its lack of testing on different medical diseases, and its untested scalability for big datasets, even though it performs better than current techniques.

After that, Sarosh *et al.* [20] address the shortcomings of current techniques in fending off known-plaintext and chosen-plaintext attacks by proposing a strong picture encryption approach for protecting IoT-driven e-healthcare systems. Their approach combines Deoxyribonucleic Acid (DNA) encryption with hybrid chaotic maps, including 3D chaotic maps and the Piecewise Linear Chaotic Map (PWLCM), to enhance the robustness and security of medical image encryption. The authors introduced advanced diffusion mechanisms, including crisscross diffusion and eXclusive OR (XOR) diffusion, which leverage a key image to enhance the encryption process's complexity. The technique calculates an adaptive image parameter, providing robust resistance against known-plaintext and chosen-plaintext attacks, thereby ensuring enhanced security. Furthermore, the method effectively counters statistical attacks by producing uniform histograms, even for medical images with uneven intensity distributions. Achieving an average entropy of 7.9971 and Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values of 99.5996 and 33.499, respectively, the approach demonstrates a high level of security. Experimental tests with medical images, such as COVID-19 X-rays, confirm its resilience against differential and statistical attacks. However, the encryption time (3.9 s for a 256×256 image) presents a limitation that requires optimization.

More recently, Nadhan *et al.* [21] investigated and developed a cryptography-based approach for securing medical images transmitted through the Internet of Things (IoT) healthcare networks. The authors used deep learning techniques to enhance the encryption and decryption processes for medical image security. Specifically, they employed a key learning network built on the ResNet-50 architecture to map different image representations, enabling encryption tailored to specific domains. For decryption, they utilized reconstructive networks to convert the encrypted images back to their original form (plaintext). Their approach is validated on publicly accessible datasets and incorporates an Return on Investment (ROI) framework to simplify data mining from local contexts. However, the method may need optimization for scalability in large-scale healthcare systems, and its applicability could be constrained by its dependence on particular network designs and datasets.

B. Decentralized Storage

Decentralized security mechanisms have emerged as a novel paradigm that enables autonomy across IoT networks without relying on central authorities. Several frameworks have been designed to improve the security of medical images through decentralized storage solutions [27–30]. For instance, Jabarulla *et al.* [22] introduced a decentralized management system based on IPFS and blockchain technology to enable secure and distributed storage and sharing of medical images. Their approach integrates the Patient-Centric Access Control Protocol with Smart Contracts (PCAC-SC), for enabling the patient to maintain control over their data. The authors tested a PCAC-SC prototype on an Ethereum test network to demonstrate the feasibility of their method. The results have proved the potential of this approach in securing the transmission of medical images in IoT environments. Sun *et al.* [15] introduced a blockchain-based framework to address the challenges of ensuring integrity and security in Electronic Medical Records (EMRs), enabling secure storage and access. The proposed solution combines Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with IPFS to efficiently manage access to the encrypted EMRs without compromising retrieval performance. Blockchain's immutable and traceable features were leveraged to log storage and search activities, ensuring data authenticity and traceability. Performance evaluations and simulations confirmed the scheme's practicality and efficiency. The authors also identified areas for improvement, such as improving access privileges for expired users and incorporating smart contracts to enhance data functionality. Following this, Sun *et al.* [16] introduced the Medical Record Data Storage and Sharing (MedRSS) framework, a blockchain-based solution leveraging Hyperledger Fabric and encryption technologies for secure medical record storage and sharing. The framework employs cryptography, including Elliptic Curve Cryptography (ECC) and Advanced Encryption Standards (AES), alongside IPFS for decentralized storage. MedRSS ensures tamper-proof medical records, with smart contracts automating access control. Experiments highlighted its superior accuracy, integrity, and access throughput compared to existing approaches. Future research aims to enhance transaction anonymity, address vulnerabilities in the Kafka consensus algorithm, and evaluate distributed performance in multi-machine environments.

More recently, Wang *et al.* [14] introduced a privacy-preserving mechanism for sharing medical images, employing a novel image partition security-sharing approach. This system utilizes chaotic encryption and fine-grained access control based on Attribute-Based Access Control (ABAC) models. Smart contracts automate access permissions, allowing images to be partitioned into public and private sections. The integration of a Cuckoo filter-based transaction retrieval method further enhances the efficiency of blockchain-based retrieval processes, offering a secure and effective solution for managing sensitive image data. Another study by Kumari *et al.* [23] introduced a patient-centered architecture known as HealthRec-Chain, which utilizes InterPlanetary File System (IPFS) and Ethereum smart contracts to securely store and share medical data. It guarantees excellent security and privacy while allowing patients to maintain complete control of their record through the use of Java-enabled GPG encryption. Through graphical analysis and tests, the suggested four-layered design is shown to exhibit benefits in throughput, latency, and scalability. A customized Ethereum dashboard is also included in HealthRec-Chain for performance tracking. Other blockchain systems, such as Hyperledger and Corda, will be investigated in future research, and their effectiveness in storing vast amounts of real-time healthcare data will be assessed. In this paper, we implement the lightweight hybrid cryptographic mechanism to boost the capabilities of blockchain and IPFS in the IoT ecosystem. The proposed approach starts by leveraging wavelet transform to efficiently compress medical data, significantly reducing storage needs while preserving critical information. The next step combines the ECC mechanism with the AES algorithm to provide lightweight yet highly secure encryption, ensuring data confidentiality. To further improve security, we integrate decentralized storage via IPFS and blockchain, with smart contracts playing a key role in enforcing access control and key management. Smart contracts ensure that only authorized users can decrypt data by verifying permissions before granting access to encrypted content. Instead of storing keys on-chain, our system stores key references off-chain, using the blockchain to record immutable hashes of the keys, ensuring transparency and preventing unauthorized access. This multi-layered security strategy adds protection at different levels, ensuring confidentiality, integrity, and access control for sensitive medical data.

III. Preliminaries

Recent progress in research and development within the field of IoT security is focused on creating a strong and reliable IoT framework.This section introduces key concepts relevant to the current research, including blockchain, IPFS, and ECC. IPFS plays a crucial role in managing medical images through decentralized storage, enabling efficient retrieval of large files like MRI scans, CT scans, and X-rays. When combined, blockchain and IPFS form a robust framework for securing and managing data in resource-constrained IoT environments. Blockchain ensures the secure sharing and storage of data, preventing unauthorized alterations and establishing trust in the system. ECC is another promising solution for IoT devices with limited resources due to its strong security, shorter key lengths, reduced computational demands, low memory usage, energy efficiency, and scalability.

A. Blockchain Technology

Blockchain is a decentralized and distributed database system maintained collectively by all nodes in the blockchain network. It consists of a sequence of data blocks generated through cryptographic methods, where each block represents a component of the blockchain. These blocks are systematically linked in chronological order, forming a continuous data chain. The connection between blocks in a blockchain is achieved through the hash value stored in the block header. This hash value serves as a unique identifier for each block, allowing it to be linked to its predecessor via the parent block's hash, also recorded in the header. This process creates a continuous chain of blocks, starting from the most recent and extending back to the genesis block. The resulting structure is a sequentially linked data chain, where each block is securely tied to its parent through cryptographic hashing. This design not only facilitates the creation of decentralized networks but also ensures robust tamper resistance, making it ideal for applications in data management and secure sharing. Moreover, the integration of advanced cryptographic techniques further enhances the overall security of the blockchain.

B. IPFS

InterPlanetary File System (IPFS) is a distributed file system that enables decentralized storage and retrieval of data, offering efficient and resilient management of large files such as medical images [31]. While its decentralized nature offers benefits such as eliminating the need for a central authority and improving resilience, it also introduces security and privacy challenges, particularly in sensitive applications like secure Patient Health Record (PHR) exchange. These challenges include ensuring data confidentiality, managing access control, and protecting against unauthorized access or exposure of sensitive information. Without robust security measures, such as encryption and access management, vulnerabilities in data handling could indeed arise.

Fig. 3 illustrates the seamless integration of blockchain and IPFS, where decentralized file storage is combined with secure and efficient metadata management. In this architecture, large files are stored in the IPFS network, which divides them into content-addressable chunks, assigns them unique cryptographic hashes, and distributes them across a peer-to-peer network. Instead of storing entire files on the blockchain, only the IPFS hash (CID) is recorded, ensuring immutability and verifiability without overloading the network. Smart contracts manage metadata and access control, allowing only authorized entities to retrieve and modify data. This integration enhances data security, privacy, and scalability, making it an efficient solution for decentralized applications.

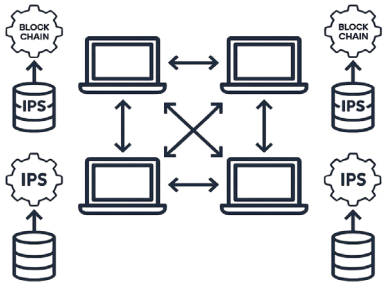


Fig. 3. Architecture of blockchain and IPFS.

C. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a promising approach for public key cryptography, leveraging the mathematical properties of elliptic curves defined over finite fields. It is an asymmetric cryptographic method that relies on the algebraic structure of elliptic curves over finite fields. Table II provides the comparative analysis of elliptic curves tailored for an IoMT environment [32]. In this research, we employed curve secp256k1, a widely adopted elliptic curve frequently used in various cryptographic contexts, including blockchain applications.

TABLE II. COMPARATIVE ANALYSIS OF ELLIPTIC CURVES OPTIMIZED FOR IOMT ENVIRONMENT

Criteria	Curve25519 $y^2 = x^3 + 486662x^2 + x$	secp256k1 $y^2 = x^3 + 7$	P-256 (secp256r1) $y^2 = x^3 - 3x + b$	Brainpool Curves $y^2 = x^3 + ax + b$	secp521r1 $y^2 = x^3 - 3x + by$
Energy efficiency	Very high: designed for limited devices	Average:Performant but less optimized	Good: effective but less suited for low resources	Average: not optimized for IoT	Weak: requires a lot of resources
Performance (speed)	Very fast	Fast	Good	Average	Slow
Security	Robust: better resistant to side-channel attacks	Robust: proven in Bitcoin	Robust: widely studied	Robust: designed for transparency	Very robust but excessive for IoTM
Resistance to attacks	Excellent (side-channel and timing attacks)	Good but inferior to Curve25519	Good	Good	Excellent
Interoperability	Excellent: supported in TLS (Transport Layer Security) 1.3, Signal	Good: especially in blockchains	Very good: widely used	Average: limited adoption	Weak: rarely used
Simplicity of implementation	Simple and reliable	Complex: requires careful management	Average: requires precautions	Average	Complex
Resource consumption	Weak	Average	Average	Average	High
Recommendation for IoMT	Recommended: best combination of security and performance	Usable but less optimized	Adapted but less efficient	Not recommended: limited adoption	Not recommended: too resource-intensive
Decentralized storage with IPFS	Optimal: very effective for secure health data exchanges	Effective: useful in the blockchain context, but more resource-intensive	Good: functional but more expensive in terms of storage	Less optimal: not ideal for use in a low-power IoMT environment	Inappropriate: too complex for an IoT environment with IPFS

1) Definition

The elliptic curve is defined over a finite field F_p by the following equation:

$$E = (\Omega) \cup (x, y) \in F_P \times F_P \,/$$
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

where $a_i \in F_p$, and Ω called the point at infinity.

For cryptographic propose, it is sufficient to limit to non-singular elliptic curve defined by the equation of the form:

$$y^2 = x^3 + ax + b \bmod p \qquad (2)$$

2) Rules for addition on elliptic curve

Let $E: y^2 = x^3 + ax + b$ be an elliptic curve and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E, where $P_1 \neq P_2$.

The addition of two points, P_1 and P_2, results in a point R that must also lie on the same elliptic curve E.

$$R = P_1 + P_2 = (x_3, y_3)$$

where,

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ and } y_3 = -(\lambda + a_1)$$
$$x_3 - t - a_3$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & if\ P_1 \neq P_2 \\ \frac{3x_1^2 + 2a_1x_1 + a_4 - a_1y_1}{2y_1 - a_1x_1 + a_3}, & if\ P_1 = P_2 \end{cases}$$

And,

$$t = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & if\ P_1 \neq P_2 \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & if\ P_1 = P_2 \end{cases}$$

3) Elliptic curve discrete logarithm problem

Elliptic Curve Cryptography is a public-key cryptosystem built upon the algebraic properties of elliptic curves over finite fields. Its security is based on the assumption that solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) is computationally infeasible. The ECDLP involves finding an integer k, given a rational point P on an elliptic curve E and another point $Q = k[P]$. The strength of elliptic curve cryptosystems lies in the difficulty of solving this problem,

making it a reliable foundation for secure cryptographic applications.

ECC is one of the most suitable technologies for IoT devices with constrained resources, providing strong security through shorter keys, low computational overhead, minimal memory usage, energy efficiency, and scalability [33, 34].

In this work, the secp256k1 elliptic curve is defined over a finite field F_p by the following equation:

$$y^2 = x^3 + 7$$

D. Discrete Wavelet Transform (DWT)

The primary goals of joint compression-encryption schemes are: (i) achieving an effective compression ratio to optimize storage space, and (ii) enhancing security to ensure the secure transmission of medical images over IoMT networks. The first goal can be accomplished by employing the Discrete Wavelet Transform (DWT) in the compression process. DWT is a mathematical method used in signal processing and image compression. It transforms a signal from the time domain to the frequency domain, enabling multi-resolution analysis [35]. By breaking down the signal into wavelet components, larger wavelets capture the broader features, while smaller wavelets focus on finer details. This method is commonly used in image compression due to its ability to represent image data both efficiently and effectively. As a result, DWT can achieve high compression ratios while maintaining image quality, making it a valuable tool in various image compression applications.

Alongside the conventional DWT approach, the Haar Wavelet Transform, a specific type of Discrete Wavelet Transform (DWT), is one of the most widely used wavelet techniques for image compression. It operates by decomposing an image into approximation and detail coefficients. The approximation coefficients represent the coarse features, while the detail coefficients capture finer details of the image.Haar wavelets use rectangular wavelets with step-like functions, which make them computationally efficient and easy to implement. This method is particularly effective for compression due to its ability to retain essential image characteristics with minimal data, achieving significant reductions in file size. Despite their simplicity, Haar wavelets perform well in preserving image quality, making them suitable for applications where fast and efficient compression is required, such as medical imaging in IoMT networks.

IV. Methodology

This paper presents an IoT-based healthcare system that employs a multilayer approach to ensure the secure transmission of medical images. The first layer, referred to as the crypto-compression layer, combines encryption and compression techniques, to secure the medical images in IoMT. The second layer enhances security by leveraging the robust features of Blockchain and IPFS, where IPFS provides decentralized and tamper-proof file storage, while blockchain ensures an additional layer of security, immutability, and transparency.

For this purpose, our system involves four key entities: the patient, blockchain, InterPlanetary File System (IPFS), and the doctor. Medical data generated by the system is securely encrypted and stored in the IPFS, preserving its privacy and integrity. The hash of the medical images, along with the hash address provided by the IPFS, is then recorded on the blockchain. The main processes of the proposed method, illustrated in Fig. 4, involve three phases. During the initial phase, the hybrid cryptographic approach combining the AES encryption and ECC key generation is performed. During the subsequent phase, the encrypted images are stored in the IPFS. In the third and final phase, Blockchain is adopted to obtain the required encrypted data. This model aims to tackle the challenges of securing and managing medical images within the IoMT. It integrates three main modules: crypto-compression, IPFS storage, and blockchain. This combined approach ensures efficient storage, robust security, and data integrity while maintaining high fidelity.

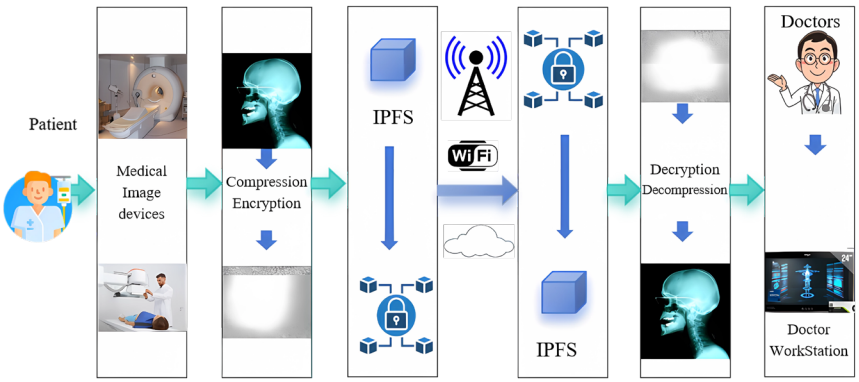


Fig. 4. Proposed IoMT framework.

A. Crypto-Compression Module

Image compression and encryption are combined in the first phase of the proposed method. First, two-dimensional Discrete Wavelet Transform (DWT) is performed, based on the Haar wavelet, so as to compress most of the effective components of the medical image. DWT separates the image into sub-bands: LL (Low-Low), LH

(Low-High), HL (High-Low), HH (High-High), holding important information in the LL sub-band, which decreases the storage cost while keeping a high fidelity. The Advanced Encryption Standard (AES) algorithm encrypts the LL sub-band from the generation. AES encryption, using a secret key derived from Curve secp256k1, provides robust cryptographic security. By leveraging Curve secp256k1, the implementation ensures both high-speed performance and resilience against modern cryptographic attacks. The key generation step further will make the encryption process stronger and also secure the sensitive medical data from external attacks.

The output of this phase is a compressed and encrypted medical image ready for secure storage and sharing.

This phase involves the following steps:

1. Input Image Preprocessing:

Read the input medical image I (grayscale or RGB (Red Green Blue).

2. Discrete Wavelet Transform (DWT):

A 2D DWT (Two-Dimensional Discrete Wavelet Transform) using the Haar wavelet is applied to the grayscale image. This operation decomposes the image into four sub-bands: LL, LH, HL, and HH. The LL sub-band, which contains the most significant information, is retained for compression.

$$[\mathrm{LL}, \mathrm{LH}, \mathrm{HL}, \mathrm{HH}] = \mathrm{DWT2(I)}$$

3. Key Generation Using Curve secp256k1:

Step three of the algorithm uses Curve secp256k1, an elliptic curve that allows the generation of a secure encryption key. Common with elliptic curves, Curve secp256k was designed specifically to minimize sizes and computation time while maximizing the security of both key exchange and cryptographic functions. It not only offers strong resistance to cryptographic attacks but is also highly efficient, making it suitable for IoMT settings.

$$K = \mathrm{GenerationKey(secp256k1)}$$

Steps in Key Generation:

i. Parameter Initialization: Curve secp256k1 operates in a prime field defined by $p = 2^{256} - 2^{32} - 977$. This prime ensures a large key space and minimizes the risk of collisions.

ii. Private Key Generation: A random 256-bit integer d is generated as the private key. This ensures randomness and uniqueness for each encryption operation.

iii. Public Key Calculation: Using the Curve secp256k1 scalar multiplication formula $K = dG$, where G is the base point on the curve, the public key K is derived.

iv. Key Derivation: For this encryption method, a shared symmetric key is derived by combining the private key and the corresponding public key through a key exchange protocol shown in Fig. 5. This shared key serves as the encryption key K_{AB} for the AES algorithm.

4. Encryption with AES:

The retained LL sub-band is encrypted using the AES algorithm, which includes a series of substitutions, permutations, and XOR operations based on the key K. The encryption step enshures data security while maintaining the compressed format of the image.

$$\mathrm{LL_{encrypt}} = \mathrm{AES\_Encrypt(LL, K)}$$

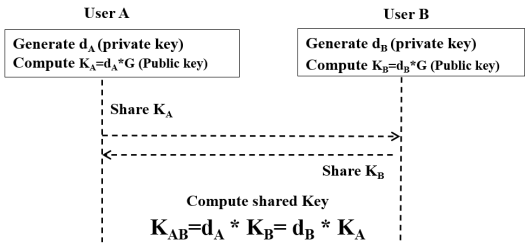


Fig. 5. Key generation and exchange process.

B. IPFS Storage Module

Phase 2 is decentralized storage of the encrypted $\mathrm{LL_{encrypt}}$ sub-band with the InterPlanetary File System (IPFS). IPFS saves the image as an object with two parts: a data part and links. Each object can store data of up to 256 KB, so larger images are broken into many objects, all linking to each other to be in sequence.

IPFS assigns a singular cryptographic hash to any file uploaded to the system using a SHA-256 hashing algorithm once the crypto-compressed image is up on IPFS. With this content-addressing mechanism, the data becomes immutable, and the data is never stored multiple times with identical content. In IPFS this file structure is represented using Merkle Directed Acyclic Graphs (DAGs). The hash value of an object, once changed, will also change, thus maintaining the integrity of the medical images stored. The generated hash, noted as $\mathrm{H_{IPFS}}$, acts as a unique identifier and is later used for retrieval without relying on traditional location-based addressing.

C. Blockchain Module

The third and last phase embraces the integration of blockchain to manage access control and transparency in medical image usage. A cryptographic hash is generated in the IPFS module and stored directly in the blockchain ledger as part of a transaction.

Every transaction stores additional information like:

- IPFS Hash ($\mathrm{H_{IPFS}}$): a unique identifier for the encrypted image.
- Public Key ($\mathrm{K_{public}}$): for verifying and requesting decryption.
- Access Metadata: information such as timestamps, owner ID, and permissions.

Ethereum technology is used with smart contracts used to enforce access control policy. Smart contracts are responsible for confirming transactions according to predetermined rules, like checking for the recipient's identity or the necessary access credentials. After verification, the transaction gets added to the blockchain, creating an immutable record of the image storage and retrieval process. The hash of the previous block is stored in each block, thus creating a secure and immutable chain. By leveraging IPFS for off-chain storage, the blockchain

ledger remains lightweight and efficient, focusing on metadata storage rather than the full image file.

D. Workflow of the Proposed Approach

Fig. 6 illustrates the activity diagram of the proposed approach. The process starts with the hospital personnel or authorized users uploading the medical image in the system. The crypto-compression module compresses the image before applying encryption. Then the crypto-compressed image is uploaded to IPFS, which generates a hash (SHA-256) of the binary data, divides the binary into objects if needed, and caches the resulting blob. Next, this hash gets written back to the blockchain as a transaction, ensuring access control. The authorized user must retrieve the image from the blockchain ledger associated with the transaction (obtaining the IPFS hash), then download it from IPFS and decrypt it through its AES key generated through Curve secp256k1. This decentralized and secure approach ensures efficiency, robust security, and high fidelity, making it suitable for sensitive medical applications in IoMT.

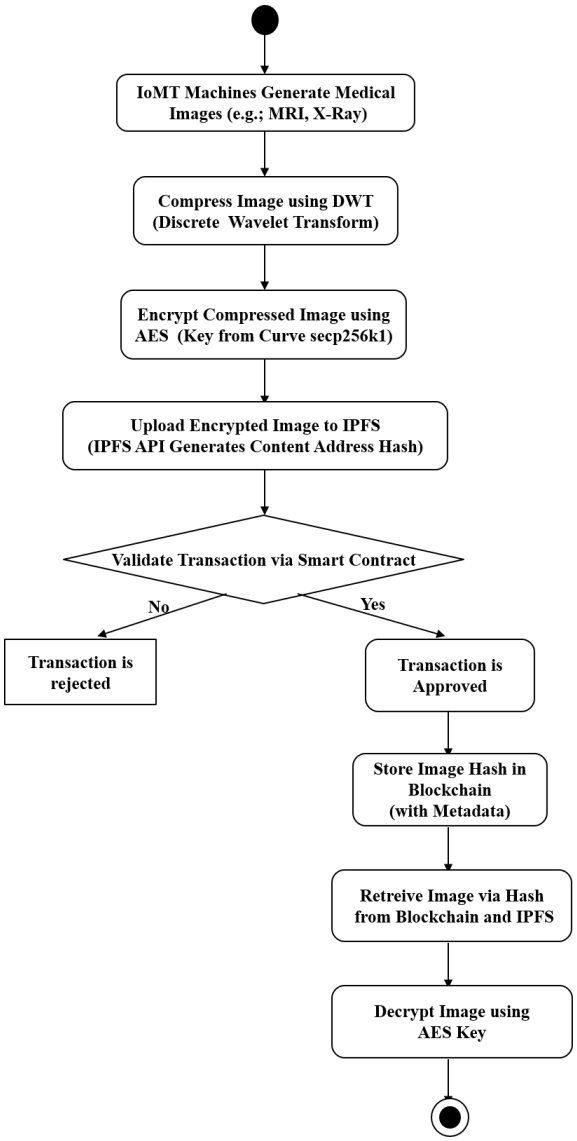


Fig. 6. Activity diagram of the proposed approach.

V. Simulation

This section provides an in-depth simulation analysis carried out to verify the effectiveness of the proposed model. A series of simulations were performed on a diverse set of medical images to confirm that our method is resilient to known attacks. The medical images used in this study included histology slides, CT scans, fused images, MRI, PET, ultrasound, and X-ray scans acquired from IoMT devices, which are available at: https://radiopaedia.org/search?scope=cases&sort=date_of_publication

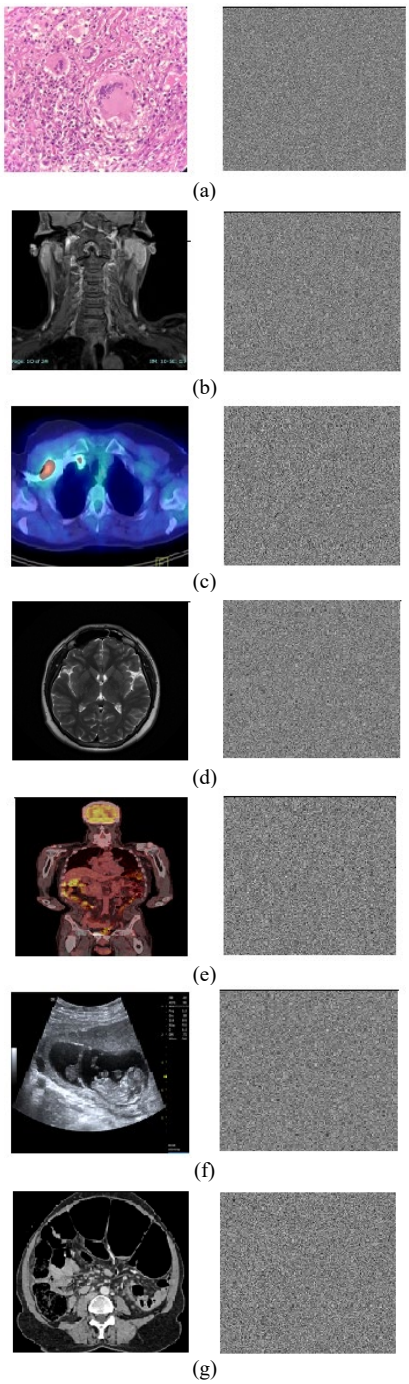


Fig. 7. Simulation results of plain and encrypted images.

Upon applying the algorithm to a set of 7 medical images, we found that the encrypted images appeared entirely scrambled, as depicted in Fig. 7.

The output shows that this process of compression and encryption scrambled the pixel information of the original images and made the visual content unrecognizable. Assessment of security performance confirms the effectiveness of the proposed method, ensuring that the encrypted images do not contain any identifiable information.

A. Security Analysis

The efficacy of the proposed security method is assessed through histogram, correlation, and entropy analyses.

1) Histogram analysis

The histogram of the original image illustrates the statistical distribution of each pixel's values, and it serves as a key criterion for evaluating the security performance of an image encryption method. In the case of the plain image, this distribution is typically irregular and dispersed due to the large amount of information contained in the image. In contrast, the pixel value distribution in encrypted images should exhibit a more uniform pattern, making it difficult for attackers to deduce the grayscale distribution by analyzing the histogram of the encrypted images. As shown in Fig. 8, the histograms of the various ciphertext images are highly uniform. This indicates that no statistical information about the plaintext can be derived from the ciphertext's histogram. This highlights the ability of the proposed image compression-encryption algorithm to effectively resist statistical analysis attacks.

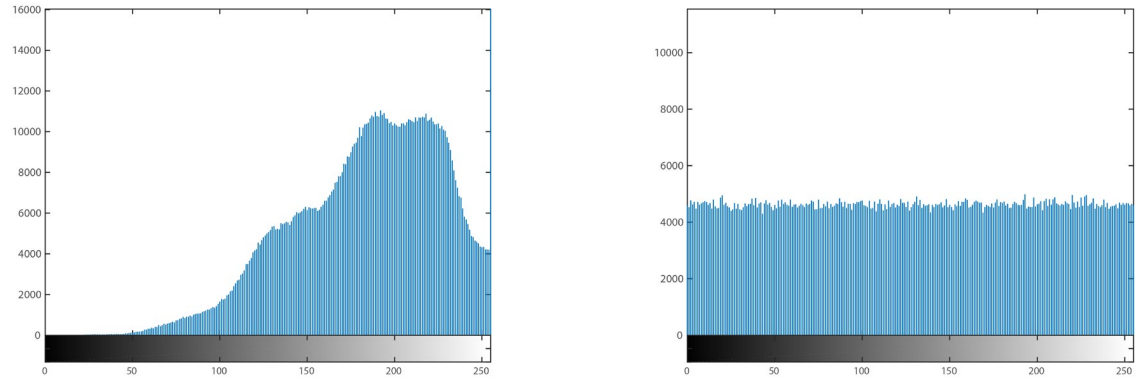
2) Pixel correlation analysis

The correlation between adjacent pixels can provide insights into the original image. In the unencrypted image, there are often strongly correlated pixels, but the encryption process effectively disrupts this correlation. The correlation coefficient ρ_{xy} is defined as follows:

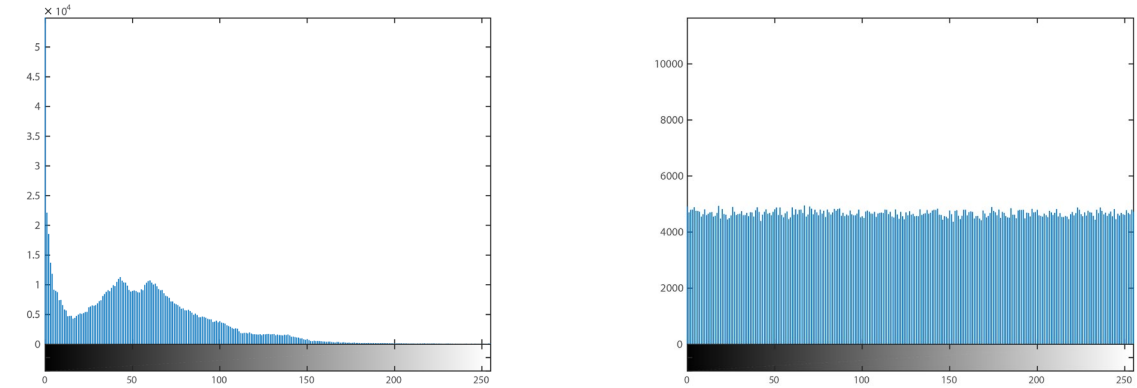
$$\rho_{xy} = \frac{E((x-E(x))(y-E(y)))}{D(x)D(y)}$$

Here, $E(x)$ and $D(x)$ the mean and variance of x, respectively, with the same applying to $E(y)$ and $D(y)$. The value of ρ_{xy} ranges from 0 to 1, where a value closer to 1 indicates a stronger correlation.

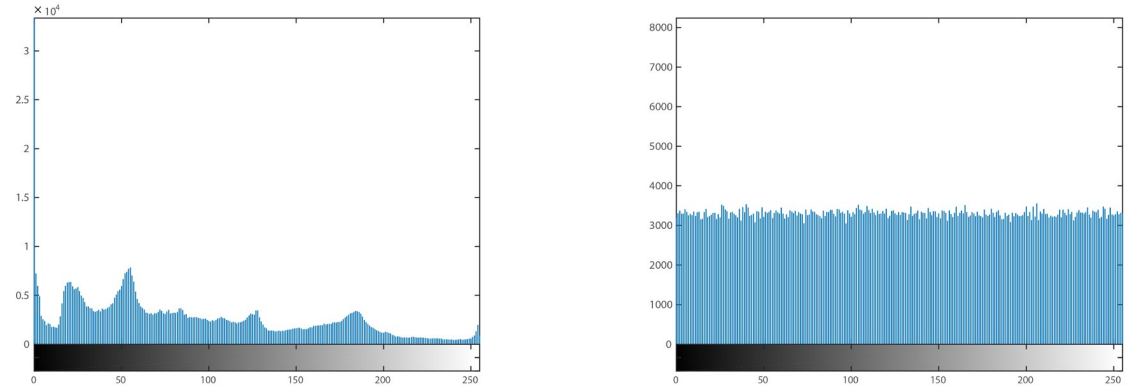
We computed the correlation coefficients for adjacent pixels in the horizontal, vertical, and diagonal directions for both the original and encrypted images. The results presented in Table III show a significant difference between the plain and cipher images.



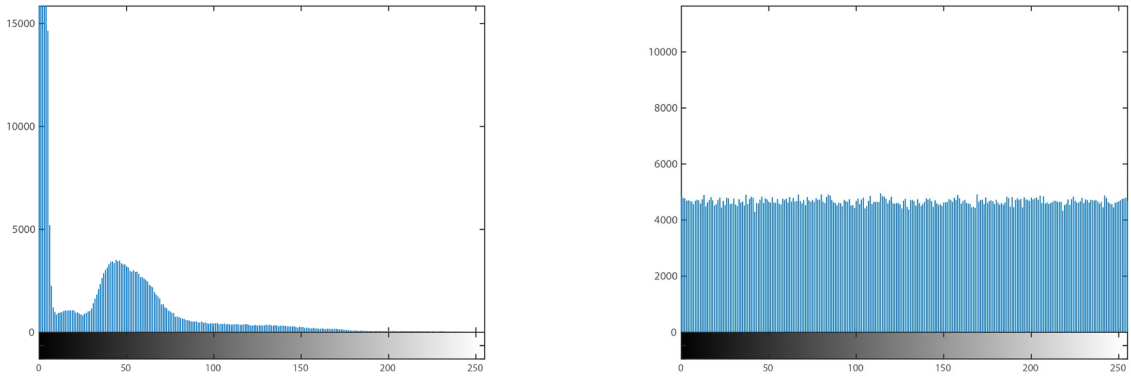
(a)



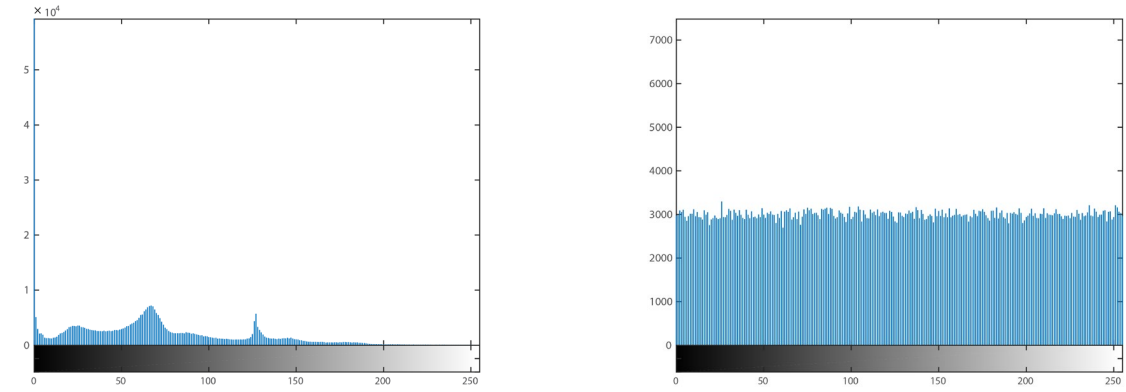
(b)


× 10^4
3
2.5
2
1.5
1
0.5
0
0 50 100 150 200 250
8000
7000
6000
5000
4000
3000
2000
1000
0
0 50 100 150 200 250

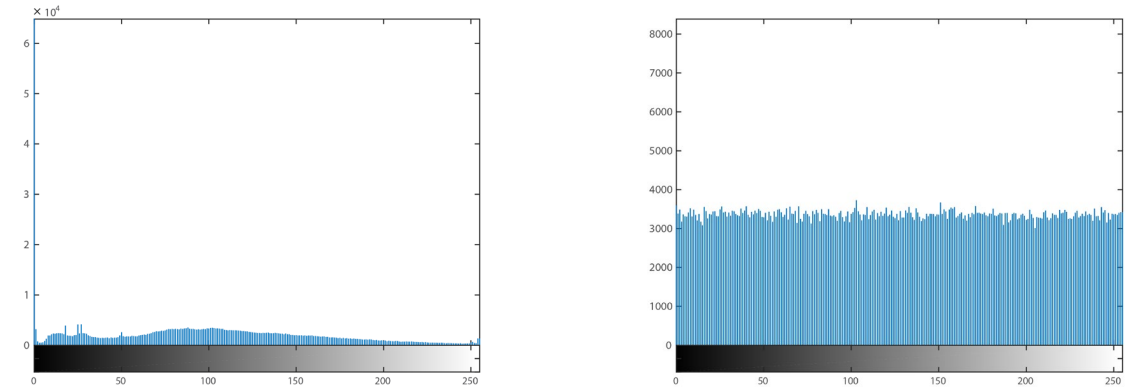
(c)


15000
10000
5000
0
0 50 100 150 200 250
10000
8000
6000
4000
2000
0
0 50 100 150 200 250

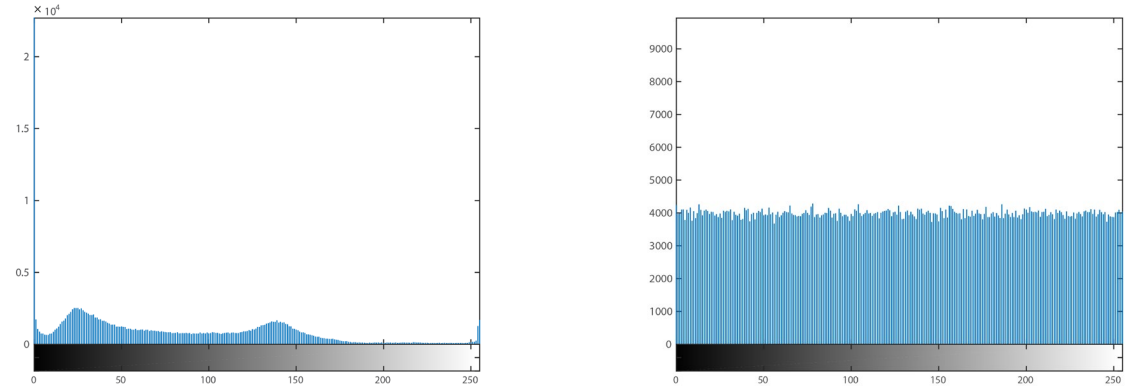
(d)


× 10^4
5
4
3
2
1
0
0 50 100 150 200 250
7000
6000
5000
4000
3000
2000
1000
0
0 50 100 150 200 250

(e)


× 10^4
6
5
4
3
2
1
0
0 50 100 150 200 250
8000
7000
6000
5000
4000
3000
2000
1000
0
0 50 100 150 200 250

(f)

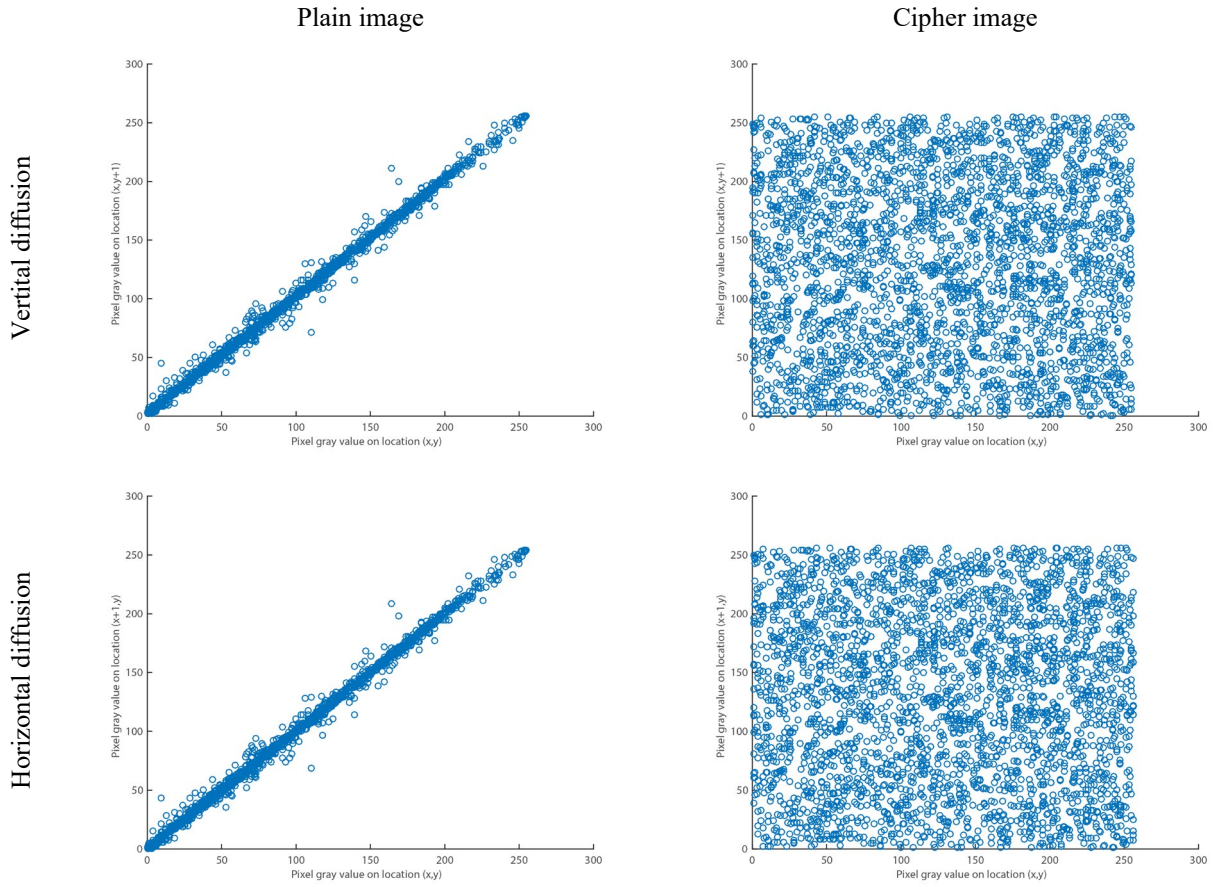


(g)

Fig. 8. Histogram of the original image and encrypted respectively.

TABLE III. CORRELATION OF TWO ADJACENT PIXEL OF IMAGES

Image obtained from IoMT device	Plain image			Cipher image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
histology	0.9527	0.9248	0.9629	9.5402×10^{-4}	-2.3026×10^{-4}	−0.1040
CTscan	0.9888	0.9798	0.9901	0.0012	-4.7537×10^{-4}	-3.6656×10^{-4}
fused images	0.9980	0.9965	0.9975	2.5771×10^{-4}	9.6641×10^{-4}	−0.0153
MRI	0.9833	0.9738	0.9890	6.9497×10^{-4}	-6.3211×10^{-4}	−0.0023
PET	0.9778	0.9717	0.9909	-3.5581×10^{-4}	-2.4495×10^{-4}	−0.0015
Ultrasound	0.9881	0.9733	0.9818	-6.6710×10^{-5}	−0.0013	0.0029
Xray	0.9871	0.9758	0.9871	9.8559×10^{-4}	0.0013	0.0186



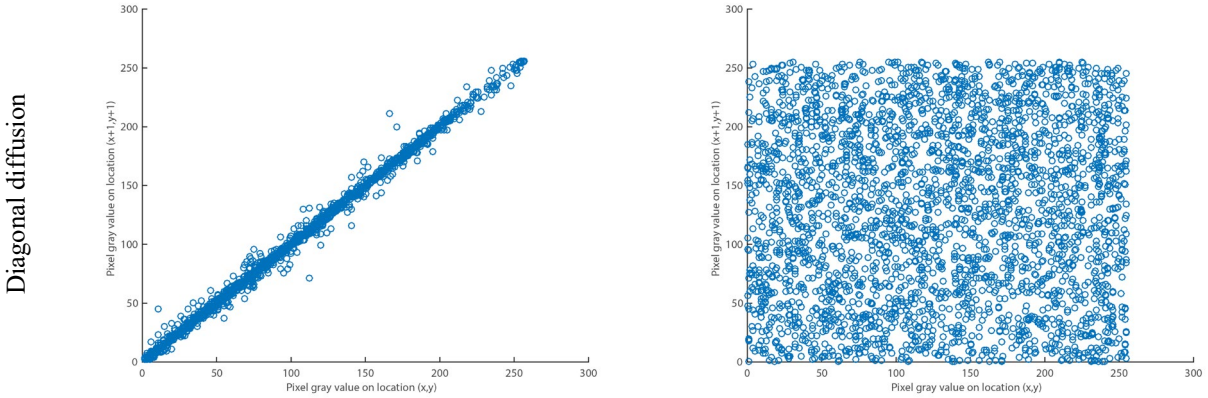


Fig. 9. Correlation of the original and its cipher image (image c).

We additionally plotted the correlation distributions of adjacent pixels for Plain Image c and its corresponding cipher text image across horizontal, vertical, and diagonal directions as shown in Fig. 9. The normalized cross-correlation for the original image c and its encrypted counterpart is shown in Fig. 10. The normalized cross-correlation plot for the plain image displays high values, suggesting a strong similarity between adjacent pixel values. Instead, the plot of the image after the cipher has very small numbers indicating that neighboring pixels are very dissimilar, or equivalently, the pixels of the image have very little to no similarity with adjacent pixels. The absence of similarity here validates the algorithm's effectiveness. Key sensitivity analysis.

To evaluate the robustness of cryptographic algorithms, especially their resistance to differential attacks, crucial indicators like NPCR (Number of Pixels Change Rate) and UACI (Unified Average Change Intensity) are used. These measures are critical in the context of image encryption as they define the sensitivity of the algorithm to slight changes in the plaintext image, an important element required to be effective in terms of security. Besides using NPCR and UACI, PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index Measure) are also significant metrics to measure the security and quality of the encrypted images. PSNR expresses the similarity of pixels between original images and their decrypted images, with higher numbers resulting in estimated higher quality images. In contrast, SSIM measures perceptual similarity between images based on the luminance, contrast, and structural content, providing more relevant assessments regarding image fidelity from the human perspective. The use of SSIM to assess perceptual similarity based on luminance, contrast, and structural content serves as a thorough evaluation of an encryption algorithm's ability to maintain both security and visual quality [36]. Table IV shows the results of encryption quality assessment through NPCR, UACI, PSNR, and SSIM.

TABLE IV. EVALUATION OF THE SENSITIVITY OF THE KEY USING DIFFERENT METRICS

Image	NPCR	UACI	PSNR	SSIM
histology	0.9961	0.3309	8.0980	0.0083
CTscan	0.9961	0.3934	6.4364	0.0049
fused images	0.9963	0.3746	7.6861	0.0051
MRI	0.9961	0.4259	5.8534	0.0035
PET	0.9961	0.4127	5.9175	0.0046
Ultrasound	0.9959	0.4016	6.2674	0.0048
Xray	0.9962	0.4041	6.2346	0.0047

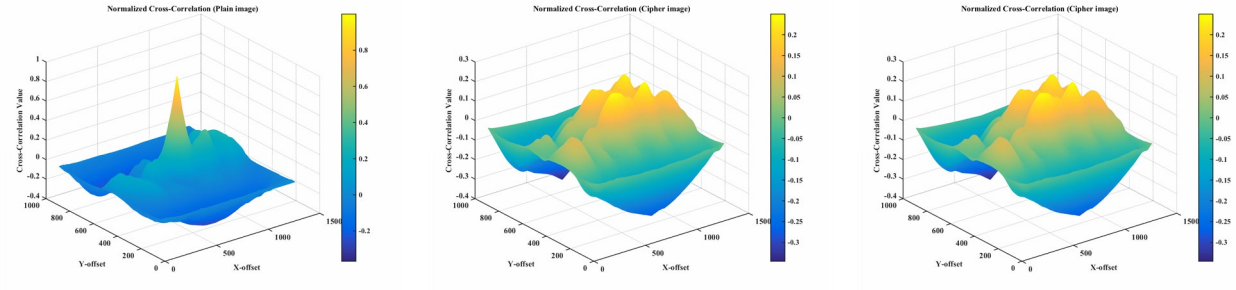


Fig. 10. Normalized cross-correlation of image c.

3) Information entropy analysis

Entropy is used here as a measure of disorder or randomness in the distribution of pixel intensities in an image cipher. Large values of entropy indicate better security on the part of image encryption. With an entropy value nearing the ideal value of 8, the proposed approach remains highly resistant to brute-force attacks. After encryption, the randomness and security of the image show a notable increase compared to the original image, as evidenced by the entropy values in Table V. The entropy

values of the plain images are between 4.90 and 7.02, indicating the possibility of predictability and susceptibility to the attack. On the other hand, cipher images have entropy values extremely near to the maximum ideal value of 8 (specifically, between 7.99 and 7.9996), which provides strong evidence for the conclusion that the encryption operation resulted in a sufficiently randomized and disrupted pixel distribution. Cipher images have entropy values close to the ideal maximum of 8 (between 7.99 and 7.9996), showing that encryption effectively randomizes and disrupts pixel distribution. This high entropy in the encrypted images suggests strong resistance to statistical and brute-force attacks, highlighting the effectiveness of the encryption algorithm in enhancing image security.

TABLE V. ENTROPY OF PLAIN AND CIPHER IMAGES

Image	Plain image	Cipher image
histology	7.0212	7.9995
CTscan	5.8661	7.9996
fused images	6.8154	7.9995
MRI	5.3728	7.9996
PET	4.9026	7.9993
Ultrasound	5.0090	7.9993
Xray	5.2818	7.9995

B. *Performance Analysis*

To evaluate the performance of the proposed approach, we performed the test across three phases: the crypto-compression layer, storage in IPFS, and blockchain integration. The evaluation was carried out on three file sizes (50 MB, 100 MB, and 500 MB) in order to provide a complete performance analysis on different data volumes. The tests were conducted on two CPU platforms: an Intel i5 processor and an Intel i7 processor. The systems run on Linux (Ubuntu 20.04 LTS), providing a stable and high-performance platform for the execution of algorithms.

1) Phase 1: Crypto-compression layer

The crypto-compression layer first applies compression to further reduce image size, followed by AES encryption alongside ECC key generation. The efficiency of their transmission and the security of the data rely on the performance of this phase. The joint operation of AES and ECC is needed to ensure data confidentiality with the minimum processing time. The execution times for AES+ ECC (without compression) on the i5 and i7 processors are shown in Table VI.

TABLE VI. HYBRID APPROACH WITHOUT COMPRESSION

Image Size (MB)	Time on i5 (s)	Time on i7 (s)
50	0.104	0.074
100	0.208	0.149
500	1.358	0.872

Fig. 11 shows the total execution times of AES and ECC without compression for different image sizes on i5 and i7 processors. The visual representation effectively highlights the benefits provided by the hybrid cryptographic strategy.

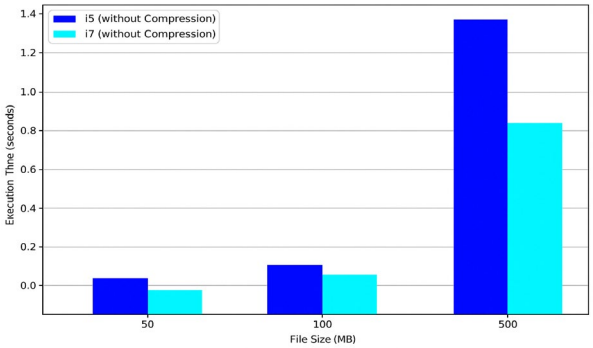


Fig. 11. Execution time of the hybrid approach without compression for different file sizes.

The simultaneous execution of encryption and compression operations ensures data security while optimizing overall processing time. Table VII displays the execution times for the hybrid approach (with compression) on the i5 and i7 processors.

TABLE VII. HYBRID APPROACH WITH COMPRESSION

Image Size (MB)	Time on i5 (s)	Time on i7 (s)
50	0.083	0.064
100	0.179	0.122
500	1.244	0.763

Fig. 12 provides a comprehensive evaluation of the performance of the hybrid approach with compression, considering different image sizes and CPU platforms. These findings emphasize the potential of joint encryption and compression for efficient and secure image encryption.

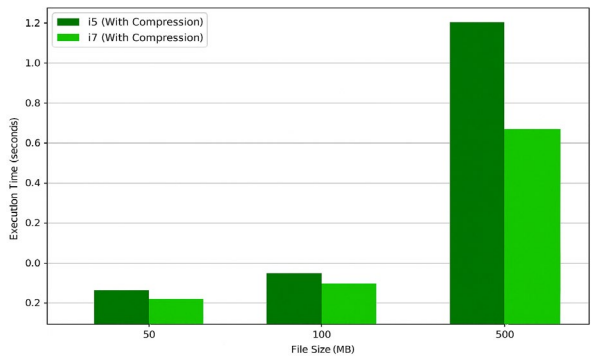


Fig. 12. Execution time of the hybrid approach with compression.

2) Phase 2: Storage in IPFS

Encrypted images were uploaded to IPFS after compression and encryption. It is a decentralized technology that lets files be stored and shared securely with a unique content identifier. These findings reveal that downloading takes progressively longer as the files get larger. Linearity of this nature is a boon, as it implies predictable performance, which helps with resource planning in a scalable system. Further optimizations could be imagined to decrease latency times, especially with faster IPFS gateways or with a better geographic distribution of the nodes in the network. That indicates reasonable scalability, although it is a needed property

when you are faced with the problem of very large data, such as medical images. As illustrated in Table VIII, the evaluation of IPFS was conducted in three phases, including uploading images, querying CIDs, and discovering images via CIDs.

TABLE VIII. STORAGE PERFORMANCE IN IPFS

Image Size (MB)	Upload Time (to IPFS)	CID Retrieval Time	Access Time (via CID)
50	0.420	0.205	0.412
100	0.720	0.315	0.715
500	2.320	1.215	2.310

As illustrated in the table, the upload times increase linearly with the image size, suggesting that IPFS can handle large data sets. CIDs ensure that files are accessible and can be fetched safely and quickly, and without a single point of failure present in IPFS's decentralized structure, storage systems for medical data will not be able to deliver the kind of high degree of reliability and resilience that are core requirements of such systems.

3) Phase 3: Blockchain integration

Blockchain has been included as an extra layer of security to ensure that the files kept in IPFS are secure as well as can be traced back. It provides a read-only way to log information related to files like modifications, exchanges, and authorizations in an immutable manner. We measured the performance of the blockchain over three basic operations: 1) Creating a block: This step stores the details of the files uploaded to IPFS in a new block, which ensures the immutability of data and reliable monitoring of medical files. For instance, this operation might be employed to store diagnostic images in an immutable history. 2) Hash Verification: This part of the operation verifies that the files are intact via their digital fingerprints. They have to detect any unauthorized attempt to modify the files so that it helps in keeping the medical records unaltered. 3) Transaction Completion: Records the source for the files and the particulars of these transfers or authorizations. This step is crucial for the secure sharing of data between healthcare professionals, making it possible to document each interaction and respect confidentiality standards. Table IX offers a comprehensive summary of the performance of these operations.

We also used the blockchain as the final layer of security to ensure the integrity and immutability of encrypted medical images stored in IPFS. The decentralized and immutable characteristics of blockchain help prevent unauthorized changes or deletions of medical data. The results highlight significant efficiency improvements in blockchain operations, reducing processing time by over 50%. The use of blockchain provides secure track and trace along with transparency, addressing the key challenges related to sensitive health data management. So, by integrating IPFS and the blockchain, we can build a strong, secure infrastructure for storing and sharing important data. These technologies also demonstrate their usefulness in decentralized identity management systems, where security and transparency are paramount. This makes them ideal for high-security applications like electronic medical record management.

TABLE IX. PERFORMANCE OF BLOCKCHAIN OPERATIONS

Operation	Time on i5 (s)	Time on i7 (s)	Added Security Features
Record Creation (Block)	0.315	0.129	Tamper-proof record of IPFS storage
Hash Verification	0.118	0.048	Immutable tracking of image modifications
Transaction Finalization	0.512	0.205	Ensures provenance and secure sharing

VI. CONCLUSION

IoMT security is a rapidly evolving field, with researchers devoting significant focus to medical images due to their sensitivity and crucial role in medical diagnoses and treatment. Medical images are a key component of the data infrastructure in any healthcare system. However, storage of these images in a centralized system, such as a cloud can expose a potential situation at which a security attack can happen. In today's distributed healthcare landscape, there is a focus on decentralized architectures that leverage blockchain technology and IPFS. We introduced an effective solution for securing healthcare data in IoMT by integrating decentralized storage through IPFS with the secure, transparent, and immutable features of blockchain technology. The key findings of this research include the model's ability to significantly enhance the security of medical data before being stored on IPFS, utilizing a hybrid cryptographic approach alongside a compression technique for optimal protection. Overall, the framework introduced in this research makes the integration of these technologies a robust and efficient solution, particularly useful in applications like the IoMT to secure sensitive healthcare data. In our future work, we aim to enhance this approach by incorporating advanced privacy-preserving techniques, such as homomorphic encryption, to facilitate secure data sharing among authorized stakeholders while ensuring patient confidentiality. To address the efficiency limitations of the proposed approach, future work will focus on optimizing DWT compression, parallelizing encryption processes, and implementing adaptive security levels to balance performance and security in the hybrid crypto-compression framework. Additionally, we plan to assess the model's scalability using large-scale healthcare datasets and explore its integration with federated learning frameworks. This will enable decentralized, privacy-preserving machine learning on medical records distributed across multiple institutions. Future research may also refine the proposed solution to improve its adaptability to emerging IoT security challenges, ensuring resilience against evolving threats.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Soufian El Airaj, Fatima Amounas, and Salma Bendaoud conducted the research and authored the paper; Mourade Azrour revised the final paper; Mohamed Badiy, Abdullah M. Alnajim, and Abdulatif Alabdulatif assisted

in implementing the hybrid cryptosystem and integrating with the blockchain-IPFS framework; Sheroz Khan provided the interpretation of the results; all authors reviewed and approved the final version of the paper.

FUNDING

This research is funded by the Deanship of Graduate Studies and Scientific Research at Qassim University (QU-APC-2025).

REFERENCES

[1] B. Kelly *et al.*, "Cybersecurity in Healthcare," in *Trends of Artificial Intelligence and Big Data for E-Health*, Cham: Springer International Publishing, 2023, pp. 213–231.

[2] A. Ghubaish *et al.*, "Recent advances in the Internet-of-Medical-Things (IoMT) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, Dec. 2020.

[3] M. M. Elamir, W. I. Al-Atabany, and M. S. Mabrouk, "Hybrid image encryption scheme for secure e-health systems," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 10, no. 1, 35, May 2021.

[4] Y. Wu *et al.*, "Medical image encryption by content-aware DNA computing for secure healthcare," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 2089–2098, July 2022.

[5] A. Odeh and A. A. Taleb, "A multi-faceted encryption strategy for securing patient information in medical imaging," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 14, no. 4, pp. 164–176, Dec. 2023.

[6] W. El-Shafai *et al.*, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 9007–9035, Mar. 2021.

[7] V. Pavithra and C. Jeyamala, "A survey on the techniques of medical image encryption," in *Proc. 2018 IEEE International Conf. on Computational Intelligence and Computing Research (ICCIC)*, 2018, pp. 1–8.

[8] C. Gilbert and M. A. Gilbert, "Cryptographic foundations and cybersecurity implications of blockchain technology," *Global Scientific Journals*, vol. 12, no. 11, pp. 464–487, Nov. 2024.

[9] M. Banerjee, J. Lee, and K. W. R. Choo, "A blockchain future for internet of things security: A position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018.

[10] P. Sharma *et al.*, "Blockchain-based IoT architecture to secure healthcare system using identity-based encryption," *Expert Systems*, vol. 39, no. 10, e12915, Dec. 2022.

[11] S. Almarri and A. Aljughaiman, "Blockchain technology for IoT security and trust: A comprehensive SLR," *Sustainability*, vol. 16, no. 23, 10177, Nov. 2024.

[12] R. K. Mishra, R. K. Yadav, and P. Nath, "Integration of blockchain and IPFS: Healthcare data management & sharing for IoT Environment," *Multimedia Tools and Applications*, vol. 84, pp. 27229–27250, September 2024.

[13] A. A. Jolfaei *et al.*, "A survey on blockchain-based IoMT systems: Towards scalability," *IEEE Access*, vol. 9, pp. 148948–148975, Oct. 2021.

[14] N. Wang *et al.*, "An image partition security-sharing mechanism based on blockchain and chaotic encryption," *PLOS One*, vol. 19, no. 7, e0307686, July 2024.

[15] J. Sun *et al.*, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, vol. 8, pp. 59389–59401, Mar. 2020.

[16] Z. Sun *et al.*, "MedRSS: A blockchain-based scheme for secure storage and sharing of medical records," *Computers & Industrial Engineering*, vol. 183, 109521, Sep. 2023.

[17] M. Elhoseny *et al.*, "Hybrid optimization with cryptography encryption for medical image security in internet of things," *Neural Computing and Applications*, vol. 32, pp. 10979–10993, Oct. 2018.

[18] J. Khan *et al.*, "SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption," *IEEE Access*, vol. 8, pp. 15747–15767, Jan. 2020.

[19] J. Deepika, C. Rajan, and T. Senthil, "Security and privacy of cloud and IoT-based medical image diagnosis using fuzzy convolutional neural network," *Computational Intelligence and Neuroscience*, vol. 2021, 6615411, Mar. 2021.

[20] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 7253–7270, Jan. 2022.

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

[22] M. Y. Jabarulla and H. N. Lee, "Blockchain-based distributed patient-centric image management system," *Applied Sciences*, vol. 11, no. 1, 196, Dec. 2020.

[23] D. Kumari *et al.*, "Healthrec-chain: Patient-centric blockchain enabled IPFS for privacy-preserving scalable health data," *Computer Networks*, vol. 241, 110223, Mar. 2024.

[24] M. K. Hasan *et al.*, "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731–47742, Feb. 2021.

[25] R. Anandkumar *et al.*, "Securing e-health application of cloud computing using hyperchaotic image encryption framework," *Computers and Electrical Engineering*, vol. 100, 107860, May 2022.

[26] Y. Ma *et al.*, "Privacy-preserving TPE-based JPEG image retrieval in cloud-assisted internet of things," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 4842–4856, Aug. 2023.

[27] S. D. Ashwini, A. P. Patil, and S. K. Shetty, "Moving towards blockchain-based solution for ensuring secure storage of medical images," in *Proc. 2021 IEEE 18th India Council International Conf. (INDICON)*, 2021, pp. 1–5.

[28] Z. Sun *et al.*, "A blockchain-based secure storage scheme for medical information," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, 40, April 2022.

[29] F. N. S. Vanin *et al.*, "A blockchain-based end-to-end data protection model for personal health records sharing: A fully homomorphic encryption approach," *Sensors*, vol. 23, no. 1, 14, Dec. 2022.

[30] S. A. H. Mohsan *et al.*, "Decentralized patient-centric report and medical image management system based on blockchain technology and the inter-planetary file system," *International Journal of Environmental Research and Public Health*, vol. 19, no. 22, 14641, Nov. 2022.

[31] C. Sekar, V. R. Falmari, and M. Brindha, "Secure IoT-enabled sharing of digital medical records: An integrated approach with reversible data hiding, symmetric cryptosystem, and IPFS," *Internet of Things*, vol. 24, 100958, Dec. 2023.

[32] A. Houria, B. M. Abdelkader, and G. Abderezzak, "A comparison between the secp256r1 and the koblitz secp256k1 bitcoin curves," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 3, pp. 910–918, Mar. 2019.

[33] I. Muhtadi-Alamsyah and Y. B. W. Tama, "Implementation of elliptic curve25519 in cryptography," *Theorizing STEM Education in the 21st Century*, 189, 2020.

[34] Z. Vahdati *et al.*, "Comparison of ECC and RSA algorithms in IoT devices," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 16, pp. 4293–4308, Aug. 2019.

[35] N. H. Hussein and M. A. Ali, "Medical image compression and encryption using adaptive arithmetic coding, quantization technique, and RSA in DWT domain," *Iraqi Journal of Science*, vol. 63, no. 5, pp. 2279–2296, May 2022.

[36] T. Shah, T. U. Haq, and G. Farooq, "Improved serpent algorithm: Design to RGB image encryption implementation," *IEEE Access*, vol. 8, pp. 52609–52621, Mar. 2020.