A Secure and Privacy Preserving Medical Image Sharing Scheme for E-Healthcare using Blockchain

By

Hirak Mondal
Student ID: 20201046010

Sajib Datta
Student ID: 20201037010

Sajib Bhattacharjee
Student ID: 20201070010

Broti Mondal
Student ID: 20201170010

And

Saiket Kumar Ray
Student ID: 20201056010

Department of Computer Science and Engineering
Faculty of Science & Technology
North Western University, Khulna-9100
Bangladesh
May, 2024

A Secure and Privacy Preserving Medical Image Sharing Scheme for E-Healthcare using Blockchain

By

Hirak Mondal
Student ID: 20201046010

Sajib Datta
Student ID: 20201037010

Sajib Bhattacharjee
Student ID: 20201070010

Broti Mondal
Student ID: 20201170010

And

Saiket Kumar Ray
Student ID: 20201056010

SUBMITTED IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE
OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE AND ENGINEERING
AT
NORTH WESTERN UNIVERSITY
KHULNA, BANGLADESH
May, 2024

NORTH WESTERN UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

The undersigned hereby certify that they have read and recommended for acceptance a thesis entitled “A Secure and Privacy Preserving Medical Image Sharing Scheme for E-Healthcare using Blockchain.” Hirak Mondal, Sajib Datta, Sajib Bhattacharjee, Broti Mondal and Saiket Kumar Ray in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering.

1. **Research Supervisor**

Abu Naim Khan
Lecturer

Department of Computer Science and Engineering

North Western University, Khulna

2. **Second Examiner**

M. Raihan
Assistant Professor

Department of Computer Science and Engineering

North Western University, Khulna

3. **Head of the Department**

Md. Mahedi Hasan
Senior Lecturer

Department of Computer Science and Engineering

North Western University, Khulna

NORTH WESTERN UNIVERSITY

Date: 6th May, 2024

Authors	:	**Hirak Mondal, Sajib Bhattacharjee, Sajib Datta, Saiket Kumar Ray and Broti Mondal**
Title	:	**A Secure and Privacy Preserving Medical Image Sharing Scheme for E-Healthcare using Blockchain**
Department	:	**Computer Science and Engineering**
Degree	:	**Bachelor of Science in Computer Science and Engineering**

Permission is herewith granted to North Western University to circulate and to have copied for non-commercial purpose, at its discretion, the above title upon the request of individuals or institutions.

Hirak Mondal

Sajib Datta

Sajib Bhattacharjee

Broti Mondal

Saiket Kumar Ray

THE AUTHORS RESERVE OTHER PUBLICATION RIGHTS, AND NEITHER THE THESIS NOR EXTENSIVE EXTRACTS FROM IT MAY BE PRINTED OR OTHERWISE REPROCUSED WITHOUT THE AUTHORS WRITTEN PERMISSION. THE AUTHORS ATTEST THAT PERMISSION HAS BEEN OBTAINED FOR THE USE OF ANY COPYRIGHTED MATERIAL APPEARING IN THIS THESIS (OTHER THAN BERIEF EXCERPTS REQUIRING ONLY PROPER ACKNOWLEDGEMENT IN SCHOLARLY WRITING) AND THAT ALL SUCH USE IS CLEARLY ACKNOWLEDGED.

Abstract

With the rapid advancement of technology, the transmission of medical images using a blockchain-based system has become pivotal in the infrastructure of e-Healthcare. This system allows medical practitioners to efficiently store, retrieve, and share patients' medical information among various stakeholders. However, the transmission of medical images through blockchain systems can be vulnerable to various security breaches, including authentication, confidentiality, and security issues. To address these challenges, this paper proposes a novel data-hiding scheme for secure medical image transmission in a blockchain-based environment. The proposed scheme ensures imperceptible robustness and watermark security while maintaining a low computational cost. To achieve confidentiality, the Electronic Patient Healthcare Record (EPHR) is encrypted using the Double Scan Pixel Position Shuffling (DSPPS) approach. Subsequently, the encrypted EPHR is divided into shares and embedded in the shares of the cover medical image. A minimum of the watermarked image shares are used to retrieve the original medical image and encrypted EPHR, thereby reducing blockchain latency and computational burden. Experimental results demonstrate that the proposed scheme exhibits high imperceptibility, robustness, and watermark security at a low computational cost. This approach has the potential to significantly enhance the security and efficiency of medical image transmission in blockchain-based e-Healthcare systems, paving the way for more secure and reliable healthcare services. To protect patient privacy, the proposed scheme employs advanced cryptographic techniques, including homomorphic encryption and secure multi-party computation. Homomorphic encryption allows computations to be performed on encrypted data without revealing the underlying data, ensuring that sensitive medical images remain confidential even during processing. Secure multi-party computation enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. The proposed scheme is implemented and evaluated using a prototype system. The evaluation demonstrates the effectiveness of the scheme in ensuring the security, privacy, and efficiency of medical image sharing. The results indicate that the scheme can effectively protect sensitive medical information while maintaining the integrity and auditability of the system. By leveraging blockchain technology and advanced cryptographic techniques, the proposed scheme provides a secure and efficient method for medical image transmission in e-healthcare environments.

Keywords: Multi-cloud E-Healthcare, Medical Image Transmission, Data Hiding Scheme, Imperceptible Robustness, Watermark Security, Computational Efficiency, Confidentiality, Authentication, Electronic Patient Healthcare Record (EPHR), Neighbor Mean Interpolation (NMI), Double Scan Pixel Position Shuffling (DSPPS), Security Breaches, Comparative Analysis, Computational Burden.

Acknowledgments

With deepest appreciation, we acknowledge the profound guidance and support that has shaped this research. First and foremost, we express our sincere gratitude to Almighty God for His unwavering presence throughout this journey.

We are immensely grateful to our esteemed supervisor, **Abu Naim Khan**. His exceptional expertise, coupled with his unwavering patience and continuous guidance, proved invaluable. His insightful feedback and unwavering support played a pivotal role in refining our ideas and propelling us to strive for excellence.

We extend our heartfelt thanks to our parents, whose unwavering support has been a constant source of strength throughout our academic journey. Their encouragement during challenging times and unwavering belief in our potential are deeply cherished.

We are also thankful to our teammates and friends who have walked beside us on this research path. Their camaraderie, helpfulness, and support significantly contributed to the completion of this work.

Finally, we would like to express our appreciation to the faculty members of the Department of Computer Science and Engineering. Their dedication to creating a stimulating environment for research and learning fostered our intellectual growth and provided crucial resources and facilities. The academic support we received throughout our studies was instrumental in the successful completion of this research.

Dedication

To Almighty God, whose unwavering guidance illuminated our path, To our supervisor Abu Naim Khan, whose wisdom and support shaped our scholarly journey, To our parents, whose love and encouragement sustained us through every challenge, To our friends and teammates, whose camaraderie fueled our perseverance, To the faculty of the Department of Computer Science and Engineering, Whose dedication to excellence nurtured our intellectual growth, This work is dedicated with heartfelt gratitude and profound appreciation.

Table of Contents

Appendix

List of Figures

List of Tables

Glossary of Terms

Terms		Full Form
EPHR	:	Electronic Patient Healthcare Records
MCE	:	Multi-Cloud Environment
CC	:	Computational Cost
RDH	:	Reversible Data Hiding
DSPPS	:	Double Scan Pixel Position Shuffling
AES	:	Advanced Encryption Standard
NMI	:	Neighbor Mean Interpolation
DM	:	Data mining
KDD	:	Knowledge discovery of database
DICOM	:	Digital Imaging and Communications in Medicine
HIPAA	:	Health Insurance Portability and Accountability Act
TCP	:	Transmission Control Protocol
IP	:	Internet Protocol
UDP	:	User Datagram Protocol
LANs	:	Local area networks
WANs	:	Wide area networks
VPNs	:	Virtual private networks
LSB	:	Least Significant Bit
EPHRs	:	Electronic Patient Health Records
AES	:	Advanced Encryption Standard
RSA	:	Rivest Shamir Adleman
NMI	:	Neighbor Mean Interpolation
DWT	:	Discrete Wavelet Transform
DCT	:	Discrete Cosine Transform
PoW	:	Proof of Work
PoS	:	Proof of Stake
SDHM	:	Six-dimensional hyper chaotic map
SDHM	:	Secure Digital Hashing Mechanism
SVD	:	Singular Value Decomposition
DE	:	Differential Evolution
ATD	:	Adaptive Threshold Detector
ROI	:	Regions of Interest
NROI	:	Non-Interest
DSPPS	:	Double Scan Pixel Position Shuffling
HIPAA	:	Health Insurance Portability and Accountability Act
LSB	:	Least Significant Bit
DSPPS	:	Double Scan Pixel Position Shuffling

Chapter 1

Introduction

1.1 Background

The advancement of digital technology has revolutionized the healthcare industry, particularly in the storage and transmission of medical images. Traditionally, medical images, such as X-rays, CT scans, and MRIs, were stored in physical film or paper format, which could be cumbersome to manage and share [1]. With the advent of digital imaging technology, medical images are now stored in electronic format, allowing for easier storage, retrieval, and sharing. E-Healthcare, which refers to the use of electronic information and communication technologies in healthcare, has become increasingly popular due to its ability to improve the quality, efficiency, and cost-effectiveness of healthcare services. In e-Healthcare systems, medical images are often stored and transmitted using cloud computing technology, which provides a scalable and flexible infrastructure for storing and processing large amounts of medical data. Blockchain technology has emerged as a potential solution to these security and privacy challenges in e-Healthcare. Blockchain is a decentralized and tamper-proof ledger that records all transactions in a secure and transparent manner [2]. By using blockchain technology, the security and privacy of medical image transmission can be enhanced, ensuring that only authorized parties have access to the images and that the integrity of the images is maintained. The image depicted in Figure 1.1 illustrates The key features of Blockchain technology.

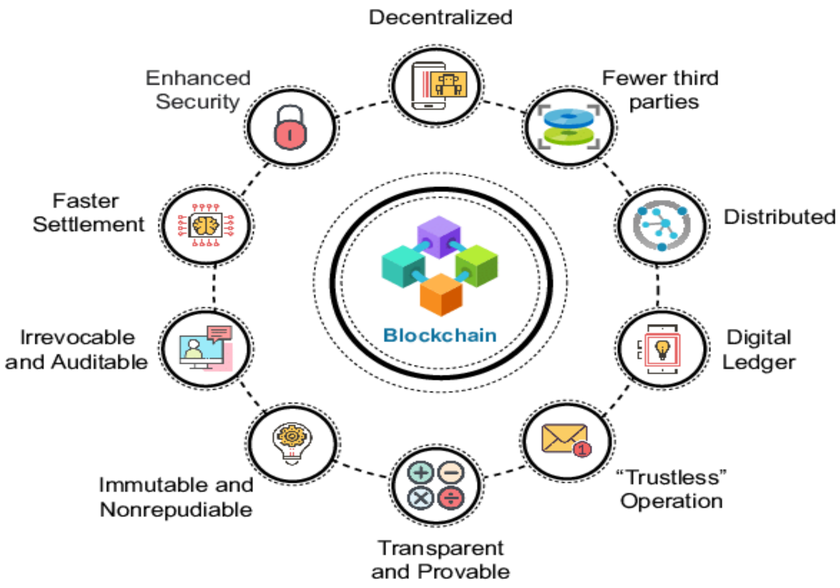


Figure 1.1: The key features of Blockchain technology [1].

1.1.1 Medical Image Watermarking Techniques: Watermarking has been considered to be a potent and persuasive gizmo for its application in healthcare setups that work online, especially in the medical image transmission. The security and protection of medical image data from various manipulations that take place over the internet is a topic of concern that needs to be addressed. A detailed review of security and privacy protection using watermarking has been presented in this paper. Watermarking of medical images helps in the protection of image content, authentication of Electronic Patient Healthcare Record (EPHR) [3]. The proposed technique combines two key concepts: watermarking and reversible data hiding. Watermarking is a technique used to embed additional information, known as a watermark, into an image without significantly affecting its visual quality. This watermark can be used to verify the authenticity of the image or to embed additional information such as patient information or diagnostic details. Reversible data hiding, on the other hand, is a technique used to embed data into an image in such a way that the original image can be completely recovered after extracting the embedded data. This is particularly useful in medical imaging, where the original image must be preserved for accurate diagnosis. The key idea behind our technique is to embed a reversible watermark into the medical image using a reversible data hiding algorithm. This watermark contains information about the image, such as its origin, timestamp, and any other relevant metadata [4]. The watermark is embedded in a way that does not significantly alter the image's visual appearance, ensuring that it remains suitable for medical diagnosis. To embed the watermark, we first divide the medical image into blocks of pixels. For each block, we calculate a hash value that represents the block's content. This hash value is then used to embed the watermark into the block using the reversible data hiding algorithm. The embedding process ensures that the watermark is embedded in a reversible manner, allowing for its extraction without affecting the original image. To verify the authenticity of the watermarked image, the embedded watermark can be extracted using the reversible data hiding algorithm. The extracted watermark can then be compared to the original watermark to verify the image's integrity and authenticity. Figure 1.2 presents Embedding and extraction procedure of watermarking techniques.

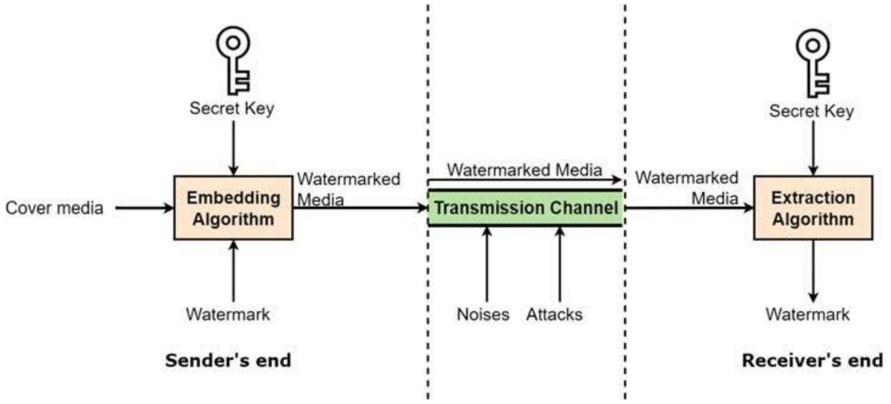


Figure 1.2: Embedding and extraction procedure of watermarking techniques [2].

1.1.2 Data hiding scheme: In this paper, we propose a scheme for separable e-healthcare image data hiding in encrypted images based on the Double Scan Pixel Position Shuffling (DSPPS) approach. The scheme aims to enhance the security and privacy of e-healthcare image data while maintaining the separability of the embedded data for efficient extraction. E-healthcare systems play a crucial role in modern healthcare by enabling the efficient storage, transmission, and retrieval of patient medical images. However, the security and privacy of these images are major concerns due to the sensitive nature of the data they contain [5]. Traditional encryption techniques can be used to protect the confidentiality of medical images during transmission and storage. However, these techniques often make it challenging to embed additional data into the encrypted images without compromising their security. The proposed scheme addresses this challenge by leveraging the DSPPS approach, which is a technique that shuffles the positions of pixels in an image based on a double scan pattern. This approach ensures that the embedded data is separable from the original image, allowing for efficient extraction without the need for decryption. The DSPPS technique also helps maintain the visual quality of the encrypted image, ensuring that it remains suitable for medical diagnosis and analysis. The key idea behind our scheme is to first encrypt the e-healthcare image using a standard encryption algorithm, such as AES (Advanced Encryption Standard). Next, we apply the DSPPS approach to shuffle the pixel positions in the encrypted image based on a predefined pattern. This shuffling process helps hide the embedded data in a secure and efficient manner. To embed data into the shuffled image, we use a data hiding algorithm that takes advantage of the shuffled pixel positions [6]. This algorithm ensures that the embedded data is distributed across the image in a way that does not affect its visual quality. The embedded data can include patient information, diagnosis results, or other relevant healthcare data. To extract the embedded data from the shuffled image, a reverse process is applied. First, the pixel positions are unshuffled using the inverse DSPPS pattern. Then, the embedded data is extracted using the data hiding algorithm. The separability of the embedded data allows for efficient extraction without the need for decryption, ensuring that the security and privacy of the original image are maintained.

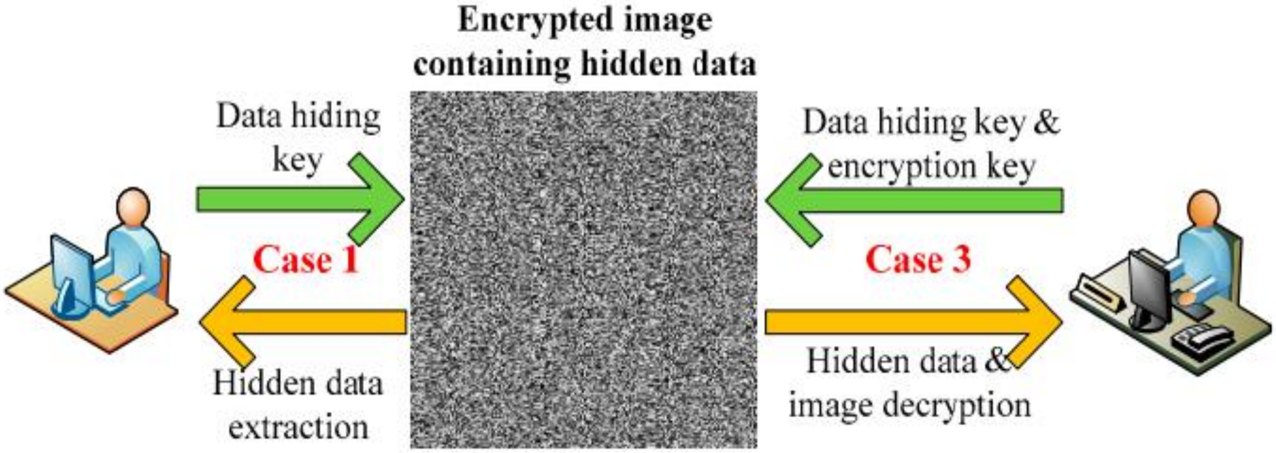


Figure 1.3: Scheme of separable data hiding [3].

1.2 Motivation

Security Concerns in E-Healthcare: The increasing digitization of medical records and the reliance on cloud computing for storage and transmission have raised concerns about the security and privacy of medical information. Ensuring the confidentiality, integrity, and availability of medical images is crucial to maintaining patient trust and compliance with regulatory requirements.

Blockchain Technology: Blockchain technology offers a decentralized and tamper-proof way to record transactions, making it ideal for securing sensitive data such as medical images. By leveraging blockchain, we can enhance the security and privacy of medical image transmission in e-Healthcare systems.

Data-Hiding Techniques: Data-hiding techniques, such as watermarking and encryption, can be used to embed sensitive information into medical images while maintaining their integrity and confidentiality. By combining these techniques with blockchain, we can create a secure and efficient system for transmitting medical images in e-Healthcare.

Enhanced Security: The field of healthcare is increasingly reliant on digital technologies for storing and sharing medical images. However, with this increased reliance comes the risk of unauthorized access, tampering, or manipulation of these images. By implementing robust watermarking techniques, we can enhance the security of medical images, ensuring that they remain authentic and unaltered throughout their lifecycle.

1.3 Objectives

This study aims to develop a secure and efficient data hiding scheme for medical image transmission in a multi-cloud environment. The specific objectives are:

1. To design a data hiding scheme that ensures high imperceptibility, minimizing the visual difference between the original and watermarked medical image.
2. To achieve high robustness, ensuring the embedded EPHR can be accurately retrieved even after the watermarked image undergoes typical image processing operations.
3. To prioritize EPHR security, implementing strong encryption techniques to safeguard patient privacy.
4. To minimize computational cost, ensuring the data hiding process is efficient and suitable for real-world multi-cloud applications.

1.4 Contributions

This study proposes a novel data hiding scheme that addresses the aforementioned objectives. The key contributions include:

1. A data hiding technique that utilizes Neighbor Mean Interpolation (NMI) for low-cost and imperceptible watermark embedding.

2. A robust encryption approach based on Double Scan Pixel Position Shuffling (DSPPS) to guarantee EPHR confidentiality.
3. A strategy for dividing the encrypted EPHR and embedding it within the watermarked image shares, enabling retrieval with a minimum number of image shares, thereby reducing multi-cloud latency and computational burden.
4. Demonstrations through simulations and comparisons with existing techniques highlighting the proposed scheme's effectiveness in achieving high imperceptibility, robustness, security, and low computational cost.

1.5 Thesis Organization

The remainder of the thesis is organized as the following:

Chapter 2 (Background Knowledge): Presents an overview of background knowledge and technical aspects. Background concepts of data mining (DM) and knowledge discovery of database (KDD). Next we discuss on dealing with missing value in data set.

Chapter 3 (Related Works): Presents several existing data mining techniques, how they implement algorithms, what are their advantages and their limitations.

Chapter 4 (Proposed Method): Proposed our idea and elaborates on the system design phase. The design phase includes the proposed techniques, feature selection and classification.

Chapter 5 (Evaluation and Results): To verify the effectiveness of the proposed method and the outcome. In this chapter we will covers the evaluation and results of our proposed techniques.

Chapter 6 (Conclusion): Finally the thesis is concluded in this chapter with suggestions for future research.

Chapter 2

Background Knowledge

Medical image transmission in e-healthcare systems, especially in multi-cloud environments, is critical for remote patient monitoring and collaboration among healthcare providers. However, ensuring the security and confidentiality of medical data, including images and Electronic Patient Healthcare Records (EPHR), is paramount due to the sensitivity and privacy concerns associated with such information.

2.1 Multi-Cloud Healthcare with Blockchain Security

Multi-cloud healthcare with blockchain security combines the benefits of multi-cloud architecture with the robust security features of blockchain technology. This approach leverages multiple cloud providers to enhance scalability, flexibility, and fault tolerance in healthcare data storage and processing. By integrating blockchain, data is stored in a decentralized and immutable ledger, ensuring integrity, confidentiality, and accountability. Blockchain's cryptographic protocols safeguard sensitive medical information, reducing the risk of unauthorized access and data breaches. This innovative solution addresses security concerns associated with distributed data storage across multiple clouds, offering heightened protection against cyber threats and ensuring the privacy of patient data in e-healthcare environments.

2.1.1 Multi-cloud architecture

Multi-cloud architecture can still be leveraged for its benefits of scalability, flexibility, and cost efficiency. Figure 2.1.1 shows Multi-cloud architecture.

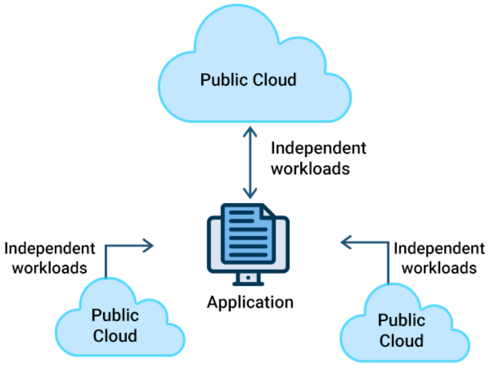


Figure 2.1.1: Multi-cloud architecture [8].

2.2 Medical Image Transmission

Medical image transmission involves the secure and efficient transfer of medical images from one location to another, typically from a healthcare facility to a healthcare provider or specialist for diagnosis, treatment planning, or consultation. The image in Figure 2.2 illustrates Medical Image Transmission. Here's a step-by-step explanation of the process:

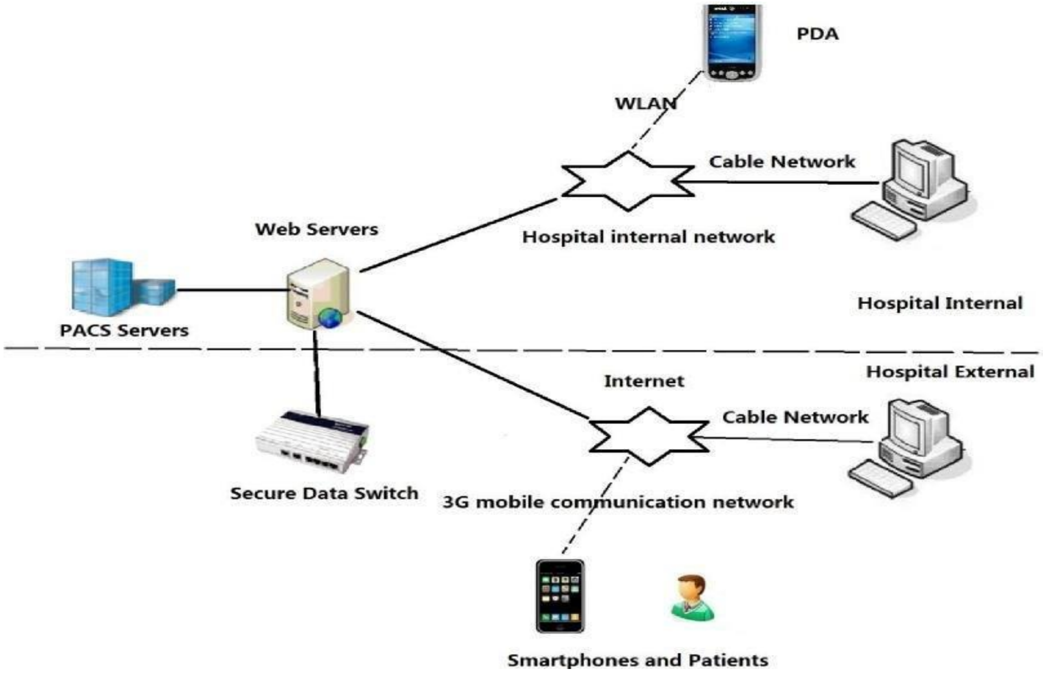
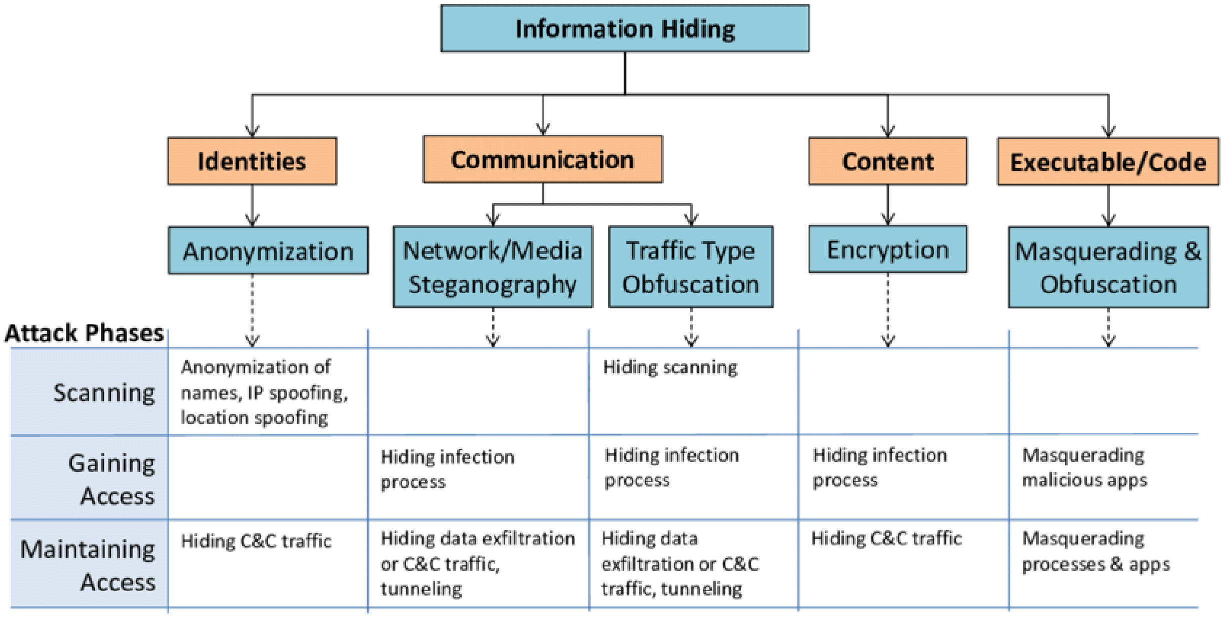


Figure 2.2: Medical Image Transmission [9].

2. 3 Data Hiding Techniques

Data hiding techniques are a way to embed information within another digital object, such as an image, audio file, or video. The hidden information can be anything from secret messages to copyright watermarks. The diagram in Figure 2.3 outlines Data Hiding Techniques. Here's a breakdown of the steps involved in data hiding:



Attack Phases	Anonymization	Network/Media Steganography	Traffic Type Obfuscation	Encryption	Masquerading & Obfuscation
Scanning	Anonymization of names, IP spoofing, location spoofing		Hiding scanning		
Gaining Access		Hiding infection process	Hiding infection process	Hiding infection process	Masquerading malicious apps
Maintaining Access	Hiding C&C traffic	Hiding data exfiltration or C&C traffic, tunneling	Hiding data exfiltration or C&C traffic, tunneling	Hiding C&C traffic	Masquerading processes & apps

Figure 2.3: Data Hiding Techniques [10].

2.4 EPHR Encryption and Decryption

EPHR (Electronic Patient Health Record) encryption and decryption are crucial processes for protecting the confidentiality and integrity of sensitive medical data. Here's a breakdown of both processes:

2.4.1 EPHR Encryption

Electronic Patient Health Records (EPHRs) hold a wealth of sensitive medical information. Encryption plays a vital role in safeguarding this data. Figure 2.4.1 provides EPHR Encryption. Here's how it works

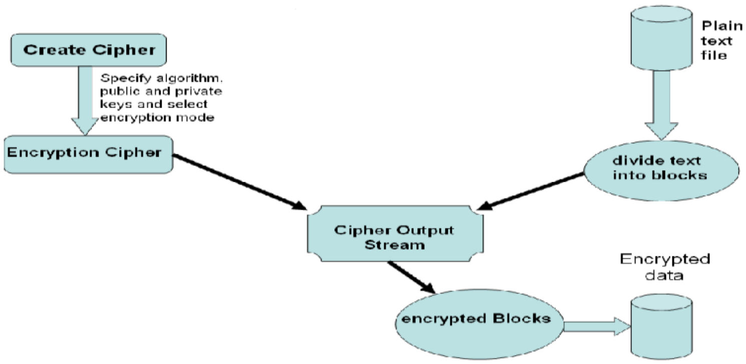


Figure 2.4.1: EPHR Encryption [11].

2.4.2 EPHR Decryption

EPHR decryption acts as the gatekeeper to a patient's secure medical information. After authorized healthcare providers verify their identity, the decryption process utilizes a specific key to unlock the encrypted EPHR data. This key essentially reverses a scrambling process, transforming the unreadable ciphertext back into the original patient health record. By ensuring only authorized personnel can decrypt EPHRs, this process safeguards patient privacy and ensures only qualified individuals have access to this sensitive data. Figure 2.4.2 presents EPHR Decryption

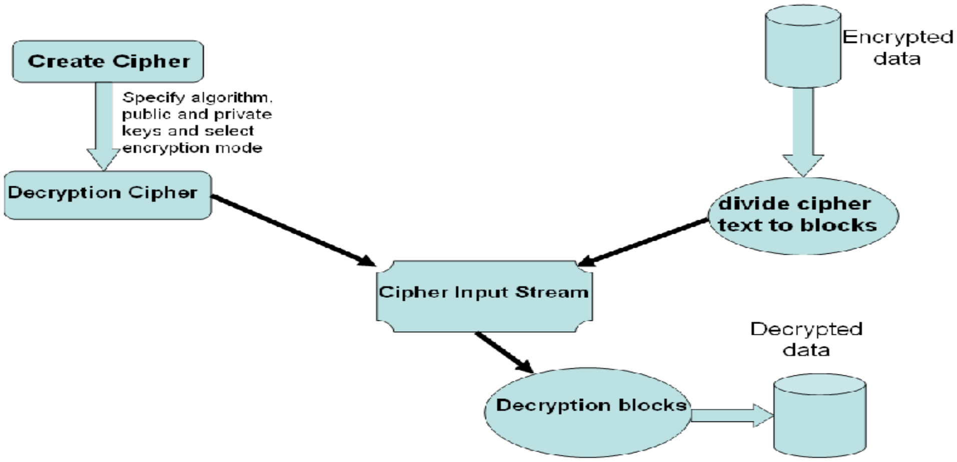

Create Cipher
Specify algorithm. public and private keys and select encryption mode
Decryption Cipher
Encrypted data
divide cipher text to blocks
Cipher Input Stream
Decrypted data
Decryption blocks

Figure 2.4.2: EPHR Decryption [11].

2.5 Image Sub-sampling and Share Generation

The cover medical image is divided into shares using Neighbor Mean Interpolation (NMI). NMI is a technique used to interpolate missing pixel values based on the average of neighboring pixels. This helps in generating multiple shares of the original image, which are distributed across multiple cloud servers for redundancy and security. In Figure 2.5, a graphical representation Image Sub-sampling and Share Generation

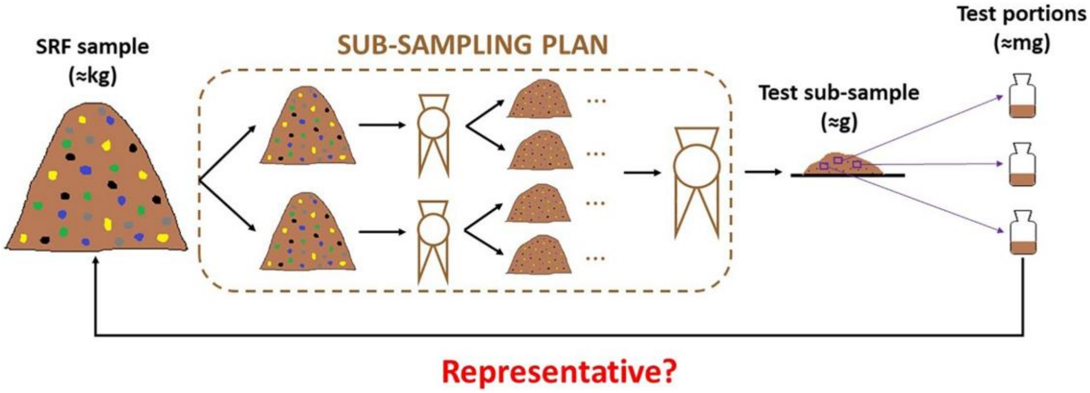


Figure 2.5: Image Sub-sampling and Share Generation [12].

2.6 EPHR Embedding and Extraction

The encrypted EPHR data is divided into shares and embedded into the shares of the cover medical image. This embedding process ensures that the EPHR remains confidential and secure during transmission. At the recipient's end, the embedded EPHR shares can be extracted from a minimum subset of the watermarked image shares, reducing computational costs and latency. The diagram in Figure 2.6 outlines EPHR Embedding and Extraction.

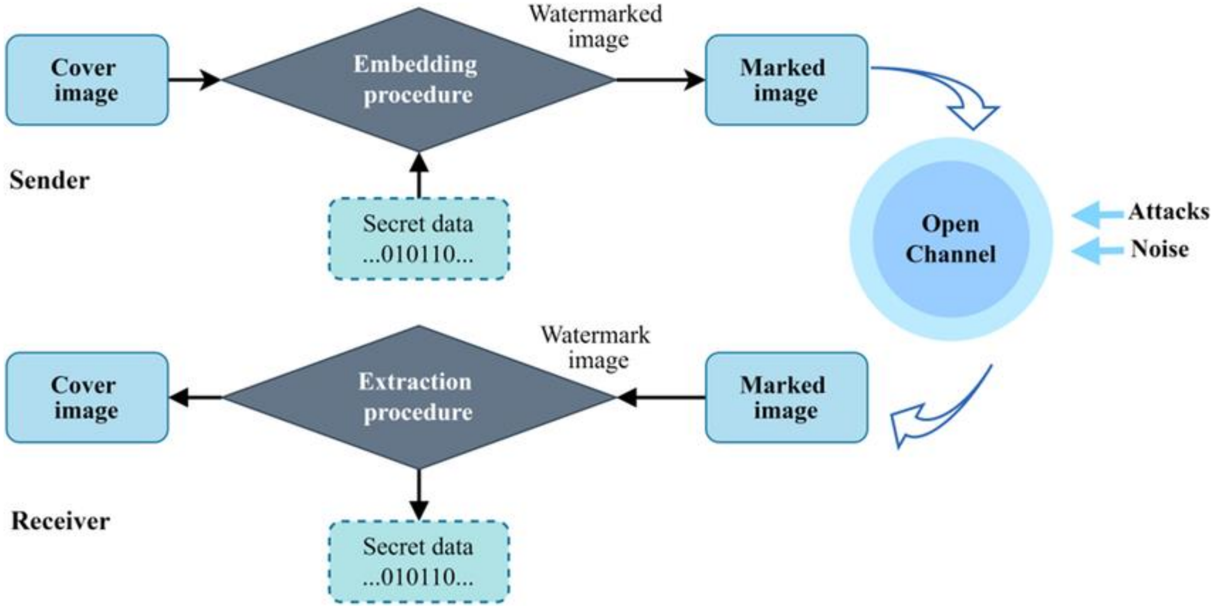


Figure 2.6: EPHR Embedding and Extraction [13].

2.7 Security and Threat Mitigation

Security and threat mitigation are two sides of the same coin. Security refers to the overall measures taken to protect information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Threat mitigation focuses on the specific actions you take

2.8 Security Challenges in Multi-Cloud Environments

A multi-cloud environment allows you greater flexibility than you would find with one cloud platform. It helps manage your costs, avoid vendor lock-in, and improve your organization's resiliency. Multi-cloud security requires careful planning and appropriate tools The complexity of multi-cloud deployments has the potential to increase the attack surface as well as the risk of cyberattacks, overall posing several security challenges. Figure 2.8 presents a schematic diagram showing Multi Cloud Environment

Figure 2.8: Multi Cloud Environment [14].

2.9 Existing Medical Image Watermarking Techniques

Medical image watermarking techniques involve embedding imperceptible, digital watermarks into medical images to protect their integrity, authenticity, and ownership. These watermarks typically contain information such as patient identification, authentication data, or additional medical details. Various techniques are employed for watermark embedding, including spatial domain methods that directly modify pixel values and transform domain methods that utilize mathematical transformations like Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT). The embedded watermarks are imperceptible to the human eye but can be retrieved later using specific keys or algorithms, enabling verification of image authenticity and aiding in patient identification and record management. Figure 2.9 provides Medical Image Watermarking.

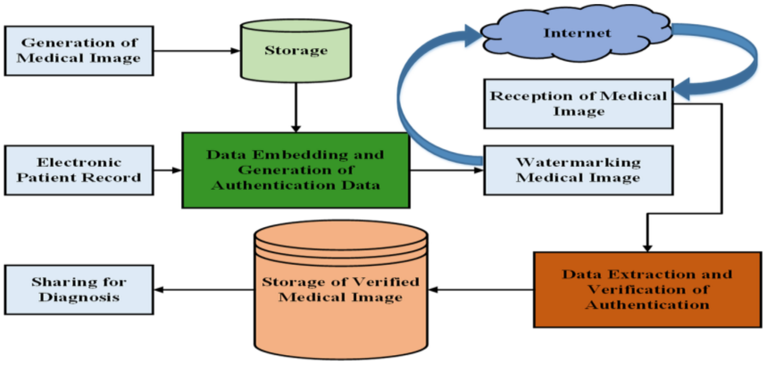

Generation of Medical Image
Storage
Internet
Reception of Medical Image
Electronic Patient Record
Data Embedding and Generation of Authentication Data
Watermarking Medical Image
Sharing for Diagnosis
Storage of Verified Medical Image
Data Extraction and Verification of Authentication

Figure 2.9: Medical Image Watermarking [15].

2.10 Importance of Imperceptibility, Robustness, and Security

1. **Imperceptibility:** The watermarked image should be visually indistinguishable from the original image for accurate diagnosis.
2. **Robustness:** The watermark should be resistant to common image processing operations (e.g., compression, noise addition) that might occur during transmission or storage.
3. **Security:** The watermarking scheme should be secure against unauthorized access or modification of the watermark.

2.11 Multi-Cloud Considerations

Multi-cloud considerations are essential when deploying healthcare systems across multiple cloud providers. These considerations encompass factors such as minimizing latency, optimizing computational costs, and ensuring data security and privacy. Challenges like minimizing delays in data transmission, storage, and processing across diverse cloud environments need careful attention. Balancing security measures with computational efficiency is crucial to maintaining the integrity and confidentiality of sensitive medical data. Moreover, strategies for seamless integration, workload distribution, and disaster recovery planning are vital to harnessing the benefits of multi-cloud architectures effectively while mitigating potential risks.

2.12 Threat Modeling and Mitigation Strategies

Threat modeling is a systematic approach to identifying potential cybersecurity threats, vulnerabilities, and risks within a system or application. It involves analyzing various attack vectors, understanding potential adversaries, and assessing the potential impact of security breaches. This process helps organizations prioritize security efforts and allocate resources effectively to mitigate risks. Mitigation strategies, developed based on the threat model, aim to address identified vulnerabilities and threats. These strategies may include technical controls such as encryption and access controls, procedural measures like security policies and employee training, and architectural changes such as network segmentation and redundancy. By proactively identifying and addressing potential risks, organizations can strengthen their security posture, minimize the likelihood of successful attacks, and enhance overall resilience against cybersecurity threats.

2.13 Blockchain Integration

Blockchain integration refers to the incorporation of blockchain technology into existing systems or applications to enhance security, transparency, and efficiency. By leveraging decentralized, tamper-resistant ledgers, blockchain integration enables secure and verifiable transactions, data immutability, and streamlined processes across various industries. This integration fosters trust among parties, reduces the need for intermediaries, and facilitates innovative solutions for secure data management, supply chain traceability, digital identity verification, and more.

2.13.1 What Is Blockchain Technology

Blockchain is a method of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated. A blockchain is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the blockchain. The image in Figure 2.13.1 illustrates the Blockchain.

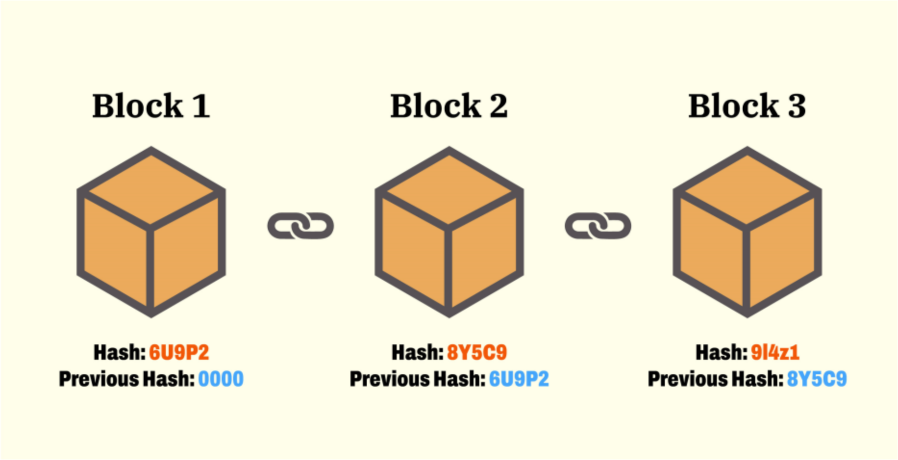


Figure 2.13.1: Blockchain [15].

2.13.2 How does blockchain work

Blockchain is a decentralized digital ledger technology that enables the secure and transparent recording of transactions across a network of computers. In a blockchain network, transactions are grouped into blocks, and each block is linked to the previous one, forming a chain. This chain of blocks, or blockchain, is maintained by a distributed network of nodes, where each node has a copy of the entire ledger. When a transaction occurs, it is broadcasted to the network and validated by multiple nodes using a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS). Once validated, the transaction is added to a new block, which is then appended to the existing blockchain. The cryptographic hash of each block ensures the integrity and immutability of the data, making it resistant to tampering or unauthorized changes. Through decentralization and consensus, blockchain provides a transparent, secure, and trustless way of recording and verifying transactions, without the need for intermediaries. The image in Figure 2.13.2 illustrates the How Blockchain Works.

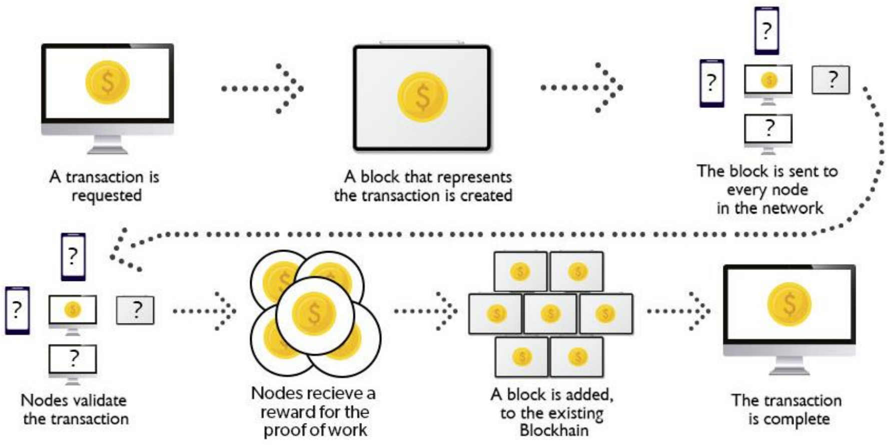

A transaction is requested
A block that represents the transaction is created
The block is sent to every node in the network
Nodes validate the transaction
Nodes recieve a reward for the proof of work
A block is added, to the existing Blockchain
The transaction is complete

Figure 2.13.2: How Blockchain Works [16].

Chapter 3

Related Works

This chapter sets the stage for a comprehensive exploration of existing research, methodologies, and advancements in leveraging blockchain for secure image data sharing in e-healthcare. The foundational section aims to provide an insightful overview and synthesis of the current state of knowledge in the field, focusing on secure data and their applications in e-healthcare. The review will cover key concepts in blockchain technology, including its principles, components, and applications in healthcare. Additionally, it will explore existing research on secure data sharing in e-healthcare and highlight gaps in the literature that this thesis aims to address.

3.1 Securing E-Healthcare Images Using an Efficient Image Encryption Model

Jaishree Jain and Arpit Jain et al. [16] proposed a technique for The progress in e-healthcare has enabled the provision of prompt first aid and medical treatments in distant areas. Transmitting medical photos via public networks poses a security concern due to their sensitive nature. A robust encryption method is introduced to mitigate these problems. The six-dimensional hyper chaotic map (SDHM) is used to create secret keys. The approach employs secret keys to disperse medical images over RGB channels, resulting in robust encryption. Comparative study demonstrates that the SDHM model outperforms existing encryption approaches, ensuring enhanced security for e-healthcare applications. The advancement of multimedia technology in e-healthcare enables the use of image-based remote diagnosis, treatment, and cooperation. Transmitting medical images across unsecured networks, nonetheless, presents security concerns. Existing encryption models are not suitable for medical photos due to their unique properties.This research examines the crucial need to protect pictures used in electronic healthcare and proposes an efficient image encryption approach to reduce this risk. The idea aims to safeguard private and confidential patient data by using state-of-the-art encryption methods to deter unauthorized access to sensitive medical information. This section introduces the proposed encryption model for medical data. In order to get the confidential access codes, one must use a Secure Digital Hashing Mechanism (SDHM). Subsequently, the medical photographs are sent using these keys . The recommended SDHM consists of three fundamental components: key generation, encryption, and decryption operations. A proposal was made to use a six-dimensional hyperchaotic map as an efficient encryption scheme for medical pictures. The picture was effectively encrypted by dividing it into its RGB channels and dispersing them using confidential keys. Enhancing the size of the encryption key enhances its ability to withstand security attacks, as shown by a comparative study that indicates superior performance compared to existing versions. The usefulness of the product was validated by many experiments, where it demonstrated superior performance compared to its competitors in terms of PSNR, correlation coefficient, and entropy measures.

3.2 Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications

Mohammad kamrul hasan, shayla islam, rossilawati sulaiman,sheroz khan, aisha-hassan abdalla hashim, shabana habib, mohammad islam, saleh alyahya, musse mohamed ahmed, samar kamil and md arif hassan et al. [17] proposed a method of Research on healthcare image security has been prompted by the difficulties in ensuring picture security in medical imaging. The best way to protect image secrecy without sacrificing data fidelity turns out to be encryption. However, due to size restrictions and redundancy, typical encryption techniques are not as effective when used on e-health data. This work suggests a lightweight encryption algorithm that is suited for the healthcare sector and uses permutation approaches to improve picture security in order to overcome these problems. The Internet of Things (IoT), which is used by about 26.66 billion devices worldwide, is revolutionizing connectivity across all fields. Comprehensive security policies and actions are necessary in light of evolving dangers, even with continuous security initiatives. Promising healthcare innovations are presented by the Internet of Medical Things, but to eliminate associated dangers and ensure patient safety and data confidentiality, strong security protocols are needed. In order to improve the security of medical images in Internet of Medical Things (IoMT) applications, this research suggests a lightweight encryption method. It presents a brand-new encryption technique designed specifically for IoMT situations This study adds important new understandings about patient confidentiality and data integrity protection for sensitive medical data in IoMT applications.The research presents a new kind of lightweight encryption designed specifically to protect medical photographs of patients . To protect privacy and security, the program splits the image into 16 sub-blocks using a 256-bit encryption key. The study compares current methods, addresses a number of security issues, and presents a safe, lightweight encryption solution for patient medical image protection. The Internet of Medical Things (IoMT) applications benefit from the enhanced security of medical images due to the lightweight encryption approach, which guarantees patient confidentiality and data integrity.The technique retains high efficiency, allowing easy integration into IoMT contexts without sacrificing system performance.

3.3 An Efficient DCT based Image Watermarking Using RGB Color Space

Priyanka and Sushila Maheshkar et al. [18] proposed a method of color photos, this work presents a strong DCT-based blind digital watermarking system that improves authentication and protection. It guarantees compatibility and preserves good visual quality after attacks by breaking down the color cover picture into RGB channels. Its superiority over current technologies in terms of payload capacity and imperceptibility is demonstrated by experimental data. In the face of challenges from corruption or counterfeiting, this technology presents a possible defense for digital multimedia material. Digital photographs are widely used as information sources in a variety of fields, including print media, journalism, and medical diagnostics. But these developments have also brought up problems like unauthorized redistribution, information attacks, and illicit copying. As a result, digital image watermarking has become a vital remedy, embedding extra data in a way that cannot be separated from its owner without the decryption key. In order to control copy of color still photos, this work presents a blind color image watermarking system. Enhancing color image copy protection is the goal of the suggested approach, which may find use in situations where more data is needed for watermarking. Using the sensitivity of the human visual system, the suggested watermarking approach splits the image into red, green, and blue channels. It treats these channels using block-wise Discrete Cosine Transform (DCT), emphasizing the middle frequency coefficients. The approach ensures imperceptibility and improves robustness against noise attacks by using a quantization matrix specifically designed for JPEG compression. Promising developments in picture watermarking technology, future research will concentrate on strengthening resilience against a wider range of attacks. The effective image watermarking method presented in this research uses the RGB color space and the Discrete Cosine Transform (DCT). The method's efficacy in robustly and invisibly embedding watermarks is demonstrated by experimental results. With the enhanced payload capacity of the method, more bits can be embedded in the image without sacrificing visual quality. Prospective investigations endeavor to fortify the methodology against an expanded array of assaults, portending progressions in the field of picture watermarking technology. By providing greater resistance to frequent attacks, the DCT-based watermarking method preserves the integrity of embedded watermarks. The technique increases the payload capacity by making use of the RGB color space. This allows for the embedding of more bits in the image without compromising visual quality.

3.4 A Secure and Efficient Cloud-Centric Internet of Medical Things-Enabled Smart Healthcare System with Public Verifiability

Mahender Kumar and Satish Chand proposed to et al. [19] a publicly verifiable, secure, and efficient cloud-centric smart healthcare system enhanced by the internet of medical things. In this study, a state-of-the-art cloud-centric Internet of Medical Things (IoMT) smart healthcare system that prioritizes efficiency, security, and public verifiability is presented. It promises reliable and transparent management of medical data through the combination of cloud computing with IoMT, enhancing public confidence in healthcare services. The study highlights the ongoing difficulty of securely and effectively managing healthcare data while acknowledging the transformative promise of IoMT combined with cloud computing. It prepares the ground for putting up a solution that is centered on public verifiability. The Secure Data Management section describes how the system protects the security, integrity, and availability of medical data by relying on robust encryption and access control techniques. Sophisticated cryptographic systems reduce the risk of unwanted access by authenticating people and devices. The scalability, adaptability, and resource optimization of the system made possible by cloud computing principles are covered in Efficient Cloud-Centric Architecture. In intelligent healthcare applications, this architecture enables real-time monitoring, diagnosis, and decision assistance. The unique quality of Public Verifiability which blockchain technology offers is highlighted. It guarantees data transfers and transactions that are both publicly auditable and cryptographically secure. Transparency and trust are increased when stakeholders are able to confirm the accuracy and legitimacy of medical records and transactions. The research concludes by highlighting how the suggested solution maintains patient privacy and data integrity while improving healthcare service quality by addressing security, efficiency, and public verifiability issues.

3.5 Addressing Semantics Standards for Cloud Portability and Interoperability in Multi Cloud Environment

Chithambaramani Ramalingam, and Prakash Mohan proposed to et al. [20] taking care of semantics guidelines for cloud interoperability and portability in multi-cloud settings. globally, cloud computing has revolutionized the way businesses manage their IT infrastructure. However, concerns about portability and interoperability surface as the number of cloud service providers rises and multi-cloud settings get more complicated.This article explores the critical role semantic standards play in addressing these issues and provides recommendations for improving cloud portability and interoperability in multi-cloud environments. Lack of defined semantics for expressing cloud resources and services impedes cloud portability. The meaning and relationships of data and services in the cloud can be expressed using a common language and structure provided by semantic standards such as RDF and OWL . By ensuring uniformity and clarity, their adoption promotes easier interoperability and migration across various cloud platforms. Ensuring interoperability between several providers is crucial in multi-cloud environments. Data formats, management interfaces, and proprietary APIs make it difficult to share data across platforms and integrate services, which could result in vendor lock-in . By providing defined ontologies and vocabularies to represent cloud resources and services, semantic standards help to alleviate these difficulties. This makes it possible for platforms to integrate and share data seamlessly, enabling automated decision-making for optimization and dynamic resource allocation.

3.6 An Optimized Color Image Watermarking Technique Using Differential Evolution and SVD–DWT Domain

Priyanka and Sushila Maheshkar proposed to et al. [21] an enhanced color image watermarking method utilizing svd–dwt domain and differential evolution. One essential method for guaranteeing the integrity and security of digital multimedia content is color image watermarking. This work presents a new method for watermarking color photos that utilizes Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) domains along with Differential Evolution (DE) optimization. The objective is to preserve good perceptual quality while achieving robustness against frequent image processing attacks . The suggested procedure starts by breaking down the color host image into its individual channels and then applying the SVD to each one. The singular values that are obtained as a result capture crucial aspects of the image. Then, multi-resolution representations of the image are obtained using the DWT. After that, the watermark is incorporated into the host image by utilizing DE optimization to modify the unique values. This optimization procedure maximizes the watermark's resilience against attacks while guaranteeing its imperceptible embedding. The watermark is incorporated into many frequency bands by deliberately altering the singular values in the DWT domain, which increases its resistance to diverse image processing techniques . For protecting the confidentiality and integrity of digital multimedia content, the suggested color image watermarking method presents a viable option.Overall, the experimental findings support the suggested approach's effectiveness and demonstrate how it might be used practically in real-world situations. The method combines multi-resolution analysis, SVD, and DWT with DE optimization to provide strong, undetectable watermarking. Its flexible parameters allow for a wide range of applications.

3.7 Cloud Based Medical Image Exchange-Security Challenges

Shini.S.Ga , Dr.Tony Thomasb ,Chithraranjan.Ka et al. [22] proposed a method of In order to improve service quality and foster collaboration among healthcare practitioners, the article addresses the expanding usage of cloud-based platforms for medical image sharing. These platforms allow for improved management and access to growing amounts of medical imaging data. Even though cloud computing has many advantages, such cost savings and scalability, it also raises serious security issues, like data breaches and illegal accessThe study looks at the shortcomings of the security measures in place now and recommends that future research concentrate on creating more reliable security solutions, such as blockchain technology, sophisticated encryption techniques, and machine learning for anomaly detection. In general, to fully realize the potential of cloud platforms for enhancing healthcare delivery, security must be ensured for medical pictures exchanged and kept there. Medical imaging data management and sharing in the healthcare industry can be revolutionized with the help of cloud-based medical image exchange solutions. These systems enable the safe and effective handling, transmission, and storage of medical pictures along with relevant patient data by utilizing the DICOM standard. By eliminating the need for hardware maintenance and physical storage, cloud computing in medical imaging can save costs and improve accessibility to images for medical professionals .It can also improve patient safety by reducing the need for repeat testing and increase interoperability between various healthcare systems. Adoption of cloud-based solutions is not without its difficulties, though, including maintaining data security and privacy, relying on dependable internet connectivity, and possible dangers from vendor lock-in. Healthcare practitioners may now collaborate more easily and access medical photos from any location via cloud-based medical image interchange, which has several advantages. This improves patient treatment in terms of both speed and quality. It also lowers expenses by doing away with the requirement for a large physical infrastructure and facilitating simple scaling to meet expanding data requirements. Cloud systems are an effective and safe solution for contemporary healthcare because of their strong disaster recovery capabilities and enhanced security features, which further protect sensitive data.

3.8 AROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images

Yang Yang ·Weiming Zhang·Dong Liang · Nenghai Yu et al. [23] proposed a method of An Adaptive Threshold Detector (ATD) is used by the proposed RDH system to discriminate between Regions of Interest (ROI) and Non-Interest (NROI) in medical images. In order to prevent overflow and underflow and improve contrast in the ROI—which is essential for precise medical diagnostics data is integrated into the peaks of the histogram. On the other hand, NROI areas employ higher data embedding, prioritizing storage capacity over image quality . By guaranteeing the reversibility of the image to its initial condition following data extraction, this technique improves the security of medical data kept on semi-trusted cloud servers. Additionally, it improves the contrast of the picture in the ROI selectively, which greatly improves diagnostic visibility without sacrificing the integrity of the entire image. Furthermore, the embedded data's selective encryption option provides strong security against unwanted access. The assessment of our RDH scheme demonstrates better performance than current methods with respect to the ROI's embedding capacity and image quality. Real-time medical applications can greatly benefit from its large data capacity and improved image clarity, which it delivers in balance. The plan successfully satisfies the essential needs for data integrity, privacy protection, and usability in cloud computing environments for medical imaging. The suggested AROI-based reversible data hiding scheme preserves image integrity while preventing common issues like histogram overflow and underflow. It also permits high data embedding capacity in non-critical areas and improves visual quality in critical regions of medical images. It also optimizes picture enhancement and data embedding by automating the segmentation of regions of interest (ROI) and non-interest (NROI).

Chapter 4

Proposed Methodology

In our proposed methodology, X-ray images are first captured at the medical center. These images are then divided into multiple copies, each containing a portion of the original image. These copies are then encrypted using a secure encryption algorithm to ensure that the image data remains protected during transmission. After encryption, the image copies are distributed to multiple cloud servers. This distribution ensures redundancy and availability of the image data in case of server failure or network issues [16]. Each cloud server receives a copy of the encrypted image, ensuring that the original image data is not stored in a single location. Once the image copies are stored in the cloud servers, they can be accessed by authorized personnel such as doctors or hospital staff. The decryption keys required to decrypt the images are securely transmitted to the authorized personnel, ensuring that only authorized users can access the image data. This entire process is visualized in Figure 1, which illustrates the capture of X-ray images at the medical center, followed by the division and encryption of the images. The encrypted copies are then distributed to multiple cloud servers before being accessed by authorized personnel. This visualization helps in understanding the secure transmission process of X-ray images in a medical center. The diagram in Figure 4 outlines the Proposed system.

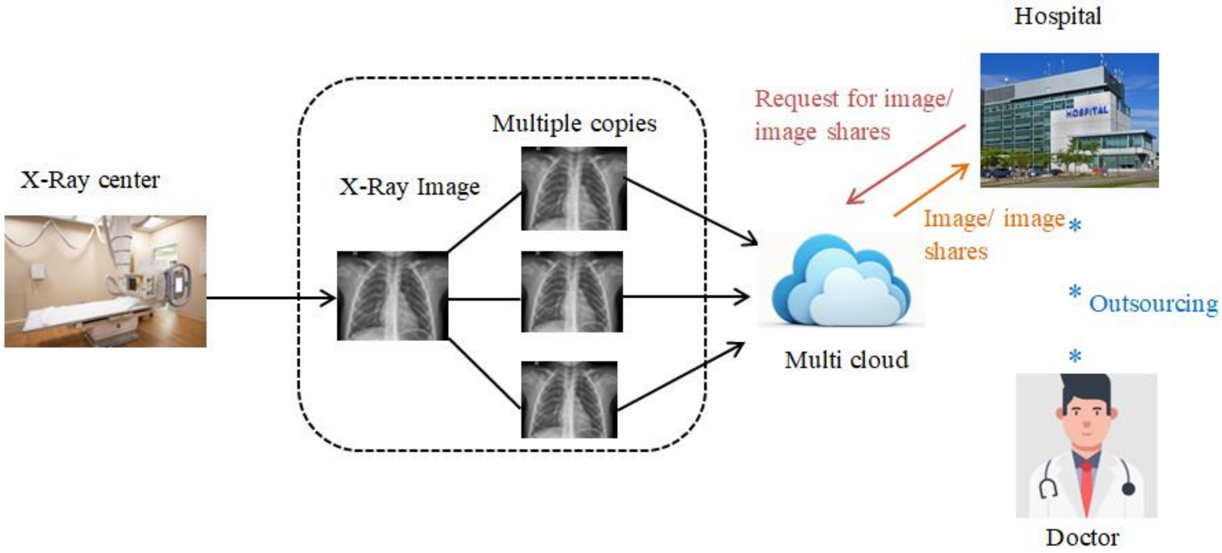


Figure 4: Proposed system.

4.1 System Architecture

The proposed scheme for secure transmission of medical images in a multi-cloud system using medical image watermarking aims to achieve high imperceptibility, robustness, EPHR security, and confidentiality with low computational cost. The system model considers a cover medical image (M) of size M x N (grayscale or color) and binary EPHR of size C x D. The scheme is divided into three phases: EPHR Encryption and Decryption, Image sub-sampling and share generation, and EPHR embedding and extraction. These phases ensure that EPHR data is encrypted and embedded into the medical image while maintaining its integrity and security. Additionally, blockchain technology is incorporated to further enhance the security and traceability of the transmitted images. The diagram in Figure 4.1 outlines the Proposed Architecture

System architecture of total work is represented below:

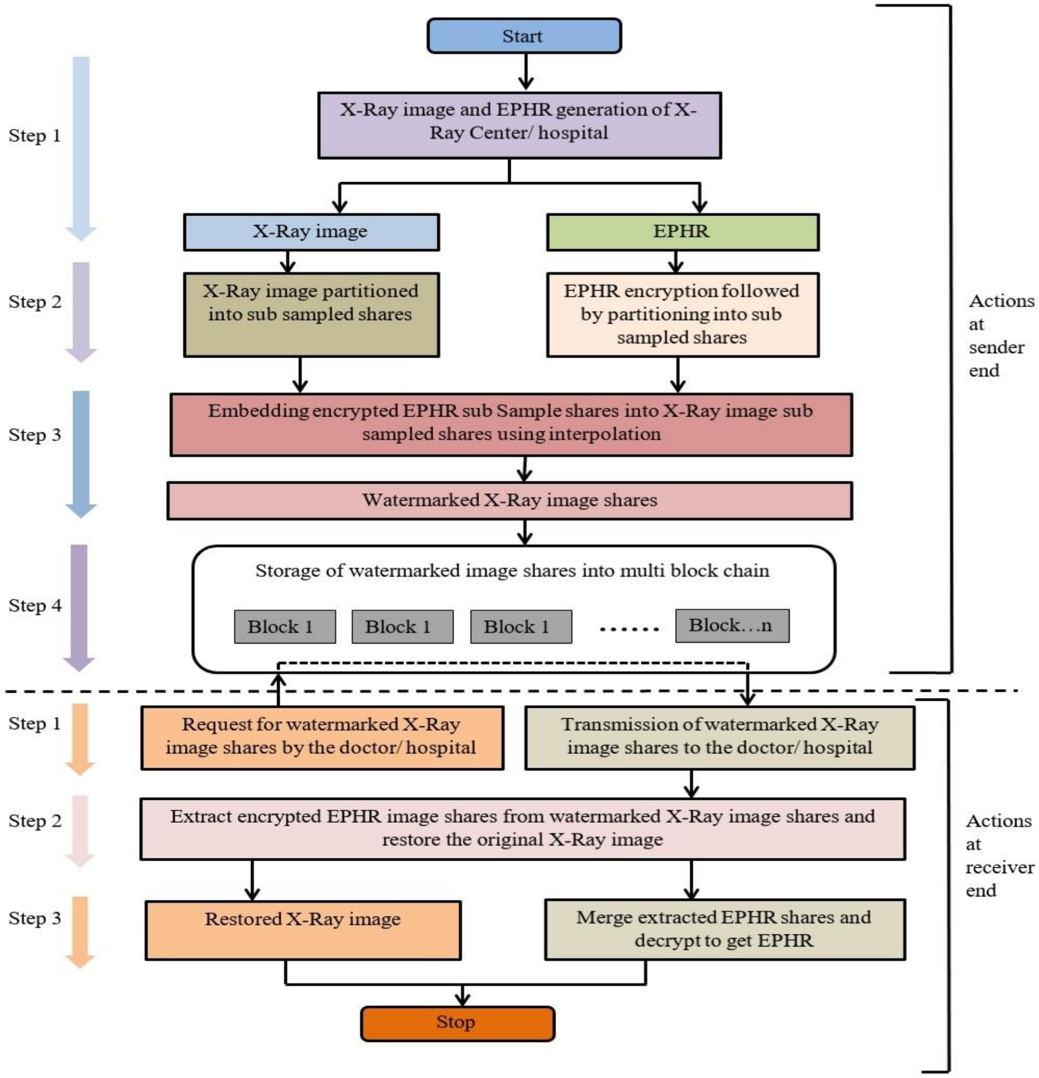

Start
Step 1
X-Ray image and EPHR generation of X-Ray Center/ hospital
X-Ray image
EPHR
Step 2
X-Ray image partitioned into sub sampled shares
EPHR encryption followed by partitioning into sub sampled shares
Step 3
Embedding encrypted EPHR sub Sample shares into X-Ray image sub sampled shares using interpolation
Watermarked X-Ray image shares
Step 4
Storage of watermarked image shares into multi block chain
Block 1
Block 1
Block 1
......
Block…n
Actions at sender end
Step 1
Request for watermarked X-Ray image shares by the doctor/ hospital
Transmission of watermarked X-Ray image shares to the doctor/ hospital
Step 2
Extract encrypted EPHR image shares from watermarked X-Ray image shares and restore the original X-Ray image
Step 3
Restored X-Ray image
Merge extracted EPHR shares and decrypt to get EPHR
Stop
Actions at receiver end

Figure 4.1: Proposed Architecture.

4.1.1 Dataset Collection

The Chest X-Ray Images (Pneumonia) dataset was collected from Kaggle, a prominent platform for data science resources and competitions. This specific dataset was sourced from a repository on Kaggle dedicated to chest X-ray images labeled for pneumonia detection. The dataset consists of 5856 images, categorized into two classes: "Normal" and "Pneumonia." These images are commonly used for training and evaluating machine learning models for pneumonia detection in chest X-ray images. The dataset's availability on Kaggle ensures easy access for researchers and developers interested in leveraging it for their projects.

4.2 Dataset Description

The dataset contains a diverse set of chest X-ray images, reflecting the variability found in real-world medical images. The "Normal" class comprises images showing a chest X-ray without any signs of pneumonia, while the "Pneumonia" class includes images indicating the presence of pneumonia. This dataset is valuable for researchers and developers working on medical image analysis and pneumonia detection algorithms. The images vary in size and resolution, providing a comprehensive dataset for training and testing machine learning models. Figure 4.2 provides a Sample of Dataset.

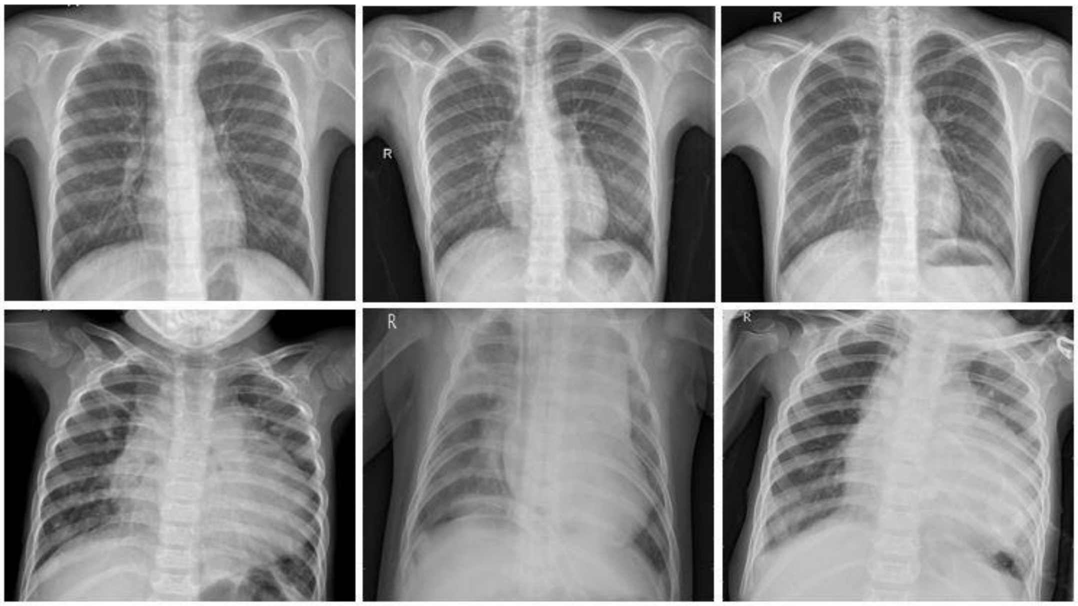


Figure 4.2: Sample of Dataset.

4.3 EPHR Encryption and Decryption

Electronic Patient Healthcare Records (EPHR) are digital versions of patients' paper charts. They contain information about a patient's medical history, diagnoses, treatments, medications, allergies, immunization dates, radiology images, and laboratory test results. EPHRs allow healthcare providers to access patient information instantly and securely.

```
Algorithm 1: EPHR encryption
Require: EPHR of size $C \times D$, Number of iterations (NOI)
Ensure: Encrypted EPHR ($EPHR$) of size $C \times D$
    1. Select random pixel (S) position using MT pseudo random generator within the range of [1, $C \times D$]
    2. Based on start position S, apply DSPPS scan process on EPHR with predefined NOI. The steps of DSPPS process as described from step 3 to step 5.
    3. Do scan1 on EHR, as scan starting from S, scan EPHR pixel positions in raster scan line fashion starts from the directions right to left (L ⟵ R), bottom to top (B ↑ T) , left to right (L ⟶ R), top to bottom (T ↓ B) .
    4. Then place all the scanned pixel values in encrypted EPHR ($EPHR$ ).
    5. Likewise in scan 2, start raster scan from next pixel position to the S, follow the direction from left to right (L ⟶R), bottom to top (B ↑ T), right to left (L ⟵ R) and top to bottom (T ↓ B) .
    6. Place all the scanned pixel values in $EPHR$.
    7. Then, repeat scan 1 and scan 2 process for number of iterations (NOI) and the resultant is the encrypted EPHR ($EPHR$).
    8. The resultant is the encrypted EPHR ($EPHR$).
```

4.3.1 Encryption with DSPPS

Double Scan Pixel Position Shuffling (DSPPS) is a method used to encrypt EPHR data. It involves rearranging the positions of pixels in an image or characters in a text file to obscure the original data. In the context of EPHR, DSPPS can be applied to digital representations of patient records, such as medical images or textual reports, to encrypt them.

4.3.2 Decryption with DSPPS

Decryption of EPHR data encrypted with DSPPS involves reversing the encryption process. The encrypted data, consisting of shuffled blocks, is unshuffled using the inverse DSPPS algorithm [32]. This process rearranges the pixels or characters back to their original positions, restoring the data to its readable form.

4.3.3 Benefits of DSPPS Encryption for EPHR

Security: DSPPS provides a high level of security by making it difficult for unauthorized parties to decipher the encrypted EPHR data. The encryption process ensures that patient information remains confidential, protecting individuals' privacy rights.

Privacy Preservation: Encryption helps to preserve patient privacy by ensuring that only authorized individuals can access the EPHR data. This helps to prevent unauthorized access and disclosure of sensitive information.

Data Integrity: Encryption helps to maintain the integrity of EPHR data by preventing unauthorized modifications or tampering. This ensures that the information remains accurate and reliable for healthcare providers.

4.4 Watermarking techniques for medical images

Watermarking techniques are crucial for protecting Electronic Patient Healthcare Records (EPHR) containing sensitive patient information during the transmission of medical images. With the increasing risk of biomedical image theft over insecure channels, researchers are focusing on developing robust watermarking solutions. These solutions aim to prevent intentional or unintentional data manipulation and malicious attacks, ensuring the trustworthiness of medical image communication systems.

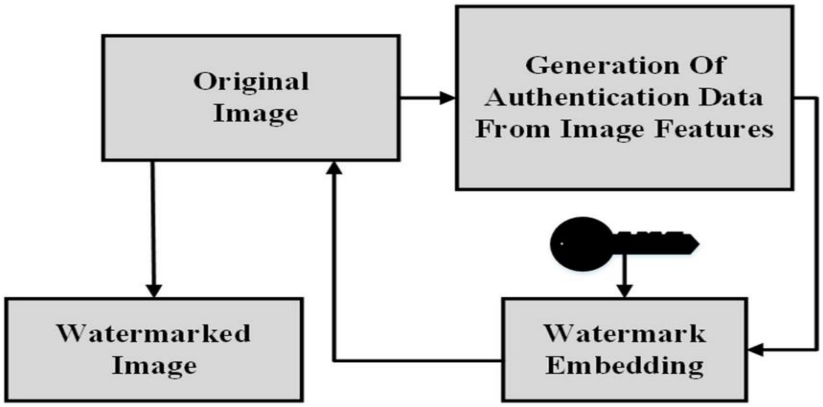


Figure 4.4: Process of self-generated watermark embedding [17].

4.5 Image sub-sampling and share generation

In the proposed scheme for secure and privacy-preserving sharing of Electronic Patient Healthcare Records (EPHR) using sub-sampling and share generation, the process involves dividing the EPHR data and an image ($Mimg$) into four sub-sampled images or image shares.

4.5.1 Sub-sampling Process

The sub-sampling process divides the original image into four sub-sampled shares, denoted as $M1$, $M2$, $M3$, and $M4$. These shares are created using a specific algorithm that partitions the image into smaller segments while preserving the overall content and structure of the original image [38]. Each sub-sampled share contains a subset of the original image's pixels, arranged in a specific order according to the sub-sampling process. The size of the original image is denoted by $X \times Y$, where X represents the width of the image and Y represents the height. By dividing the image into smaller segments, the scheme ensures that each share contains enough information to reconstruct the original image accurately. This process is crucial for maintaining the integrity and quality of the original data.

4.5.2 Share Generation

Once the image has been sub-sampled into four shares, the EPHR data is also divided into shares using a secure sharing scheme. This scheme combines each sub-sampled image share with a share of the EPHR data, creating a set of shares that can be distributed to different parties. Each share contains a portion of the original image and a portion of the EPHR data, ensuring that neither the image nor the EPHR data can be reconstructed from any individual share.

Example of Sub-sampling:

To illustrate the sub-sampling process, consider an example where the original image (M) is divided into four sub-sampled shares:

$M1$ = [1, 3, 9, 11]

$M2$ = [6, 8, 14, 16]

$M3$ = [2, 4, 10, 12]

$M4$ = [5, 7, 13, 15]

In this example, each sub-sampled share contains a subset of the original image's pixels, arranged in a specific order. These sub-sampled shares are then combined with shares of the EPHR data to create a set of shares that can be distributed securely. Here the 4.5.2 figure provides the Sub-sampling of 4 × 4 image into four sub-sampled shares.

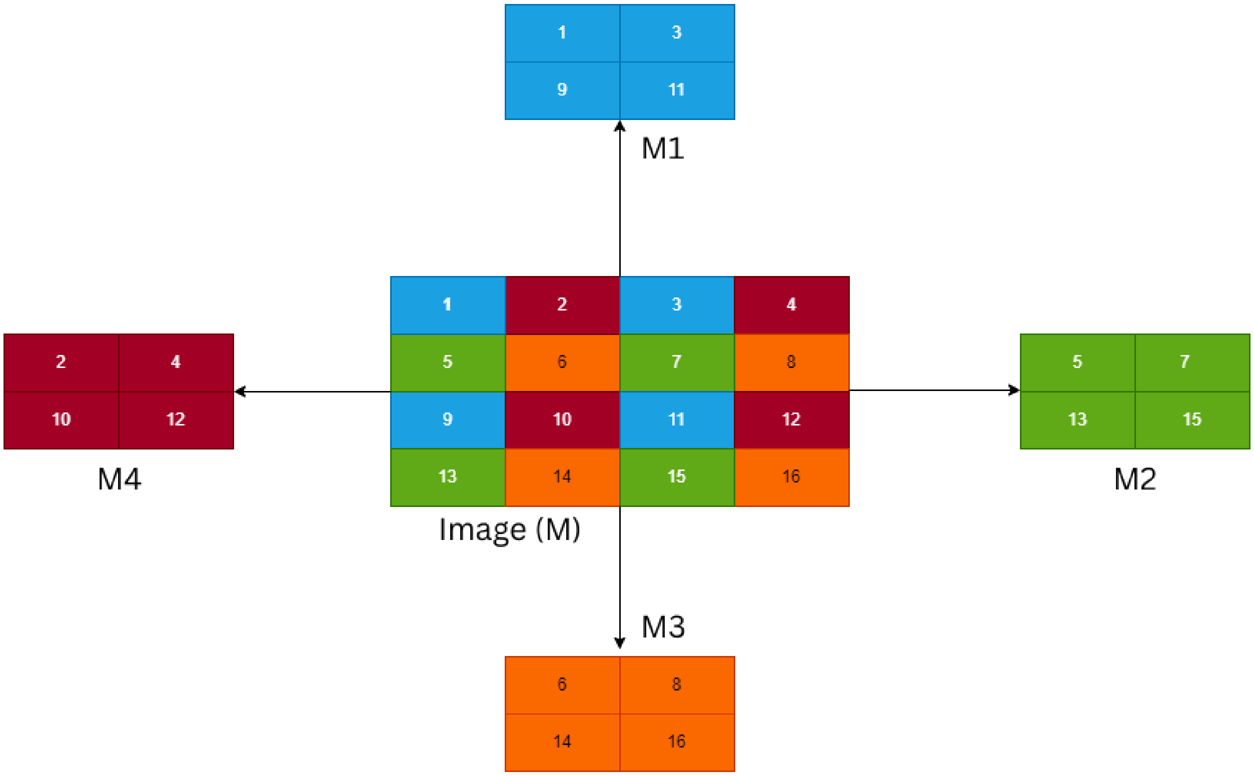


Figure 4.5.2: Sub-sampling of 4 × 4 image into four sub-sampled shares.

4.5.3 Blockchain-Based Image Sharing

Our Blockchain-Based Image Sharing scheme for secure and privacy-preserving medical image sharing in e-healthcare leverages blockchain technology to ensure the confidentiality, integrity, and authenticity of shared images. The process begins with converting the medical image into binary format, followed by the addition of a unique watermark to guarantee its integrity. The image is then divided into four shares using a secure algorithm, ensuring that the original image can only be reconstructed when all four shares are combined. These shares are encrypted and stored on the blockchain along with the encryption keys, providing a decentralized and tamper-proof storage solution.When a recipient requests access to the image, the shares are retrieved from the blockchain, decrypted using the encryption keys, and combined to reconstruct the original image. To verify the authenticity of the reconstructed image, the recipient compares the embedded watermark against a watermark provided by the sender. If the watermarks match, the recipient can be confident that the image is genuine and has not been tampered with during transmission. Overall, our blockchain-based image sharing scheme offers a secure and efficient solution for sharing medical images in e-healthcare, enhancing the security and trustworthiness of healthcare systems.

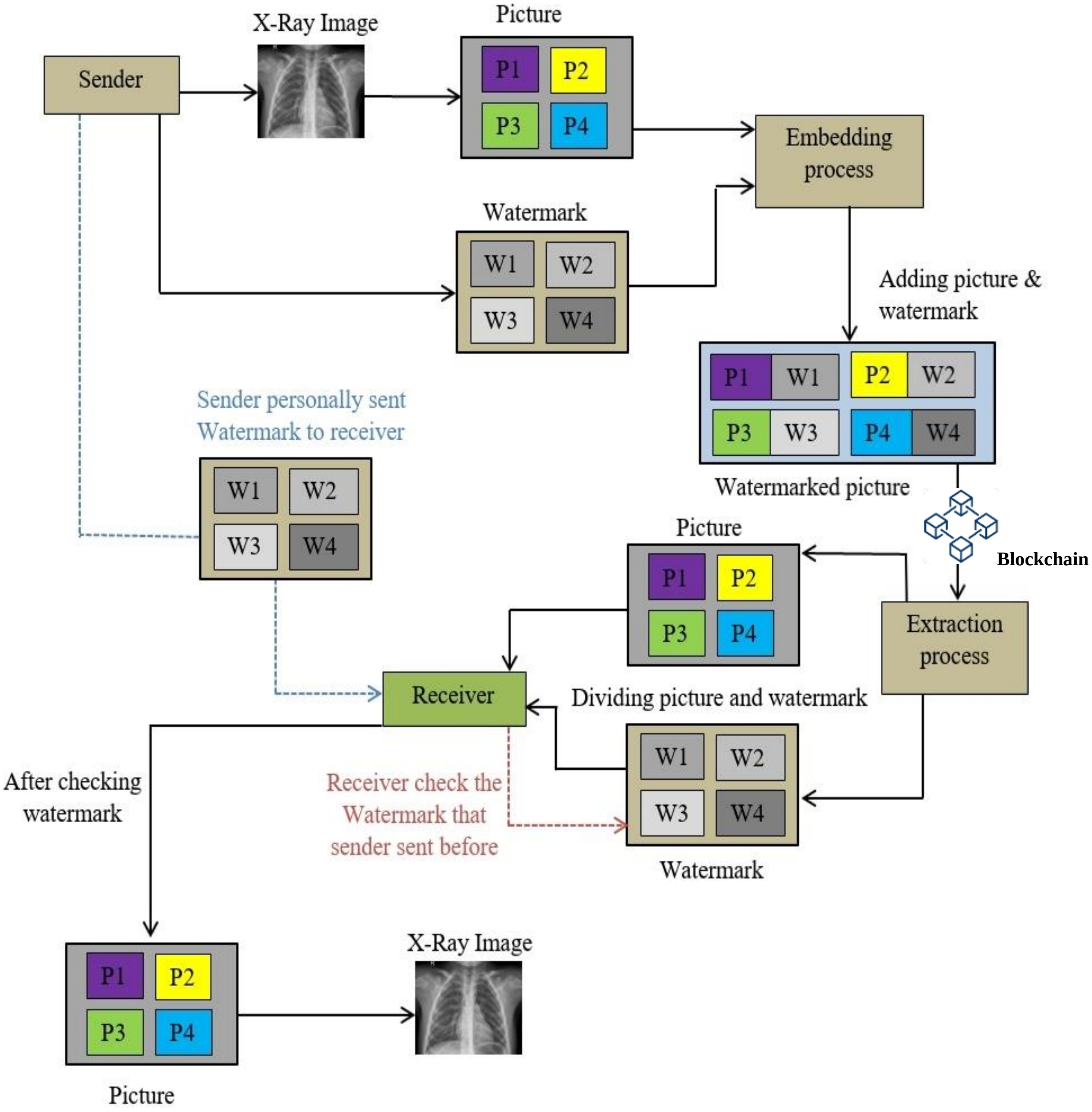


Figure 4.5.3: Block diagram for the proposed embedding and extraction process.

Chapter 5

Evaluation and Results

5.1 Least Significant Bit (LSB) watermarking

LSB is a popular technique used to embed information into digital images without significantly altering their visual quality. This technique takes advantage of the fact that small changes in the least significant bit of pixel values are generally imperceptible to the human eye. By modifying the LSB of selected pixels, watermark data can be embedded into the image, allowing for later extraction and verification. The LSB watermarking process involves several key steps. First, the watermark data is encoded into a binary format. Next, the image pixels are accessed, and the LSB of each pixel value is replaced with a bit from the watermark data. This process is repeated for a predetermined number of pixels, depending on the size of the watermark data and the desired level of embedding. One of the key advantages of LSB watermarking is its simplicity and efficiency. Since only the LSB of each pixel is modified, the visual impact on the image is minimal. This makes LSB watermarking suitable for applications where preserving image quality is paramount. However, LSB watermarking is also vulnerable to attacks. Since the changes are made to the least significant bit, they can be easily removed or modified by an attacker. This vulnerability makes LSB watermarking less suitable for applications where robustness against attacks is crucial. The image in Figure 5.1 illustrates the EPHR of Sub-sampling.

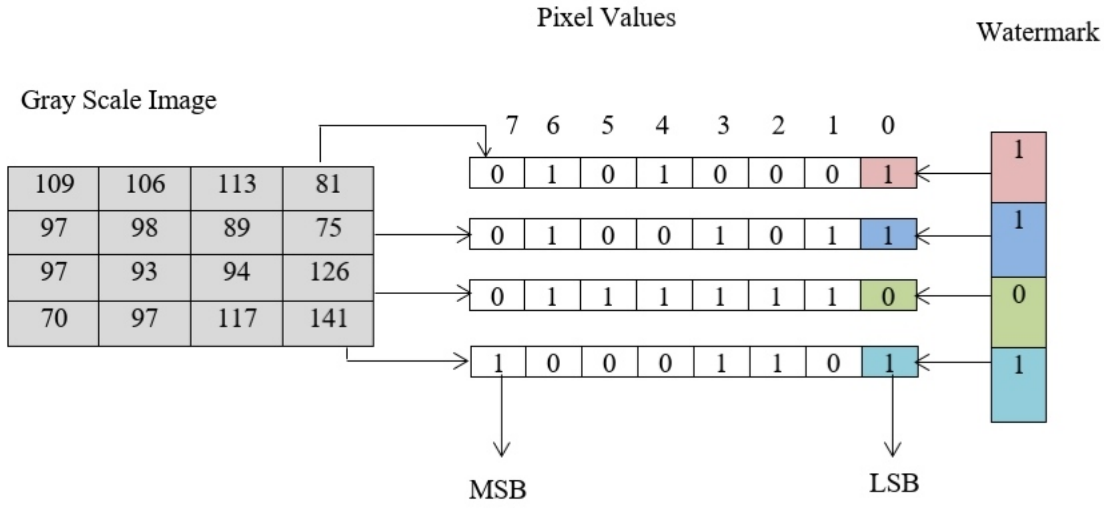


Figure 5.1: Example to data hiding approach (Least significant bit embedding).

5.2 EPHR Sub-sampling

This section we focus on the process of sub-sampling an image matrix to extract four 2x2 sub-matrices. This process is essential for further analysis and processing of the image data. We illustrate this process using a 4x4 image matrix:

109 106 113 81

97 98 89 75

97 93 94 126

70 97 117 141

5.2.1 Sub-sampling Process

Dividing into 2x2 Matrices:

$M1$: [109, 113, 97, 94]

$M2$: [106, 81, 89, 75]

$M3$: [97, 117, 70, 141]

$M4$: [93, 126, 97, 117]

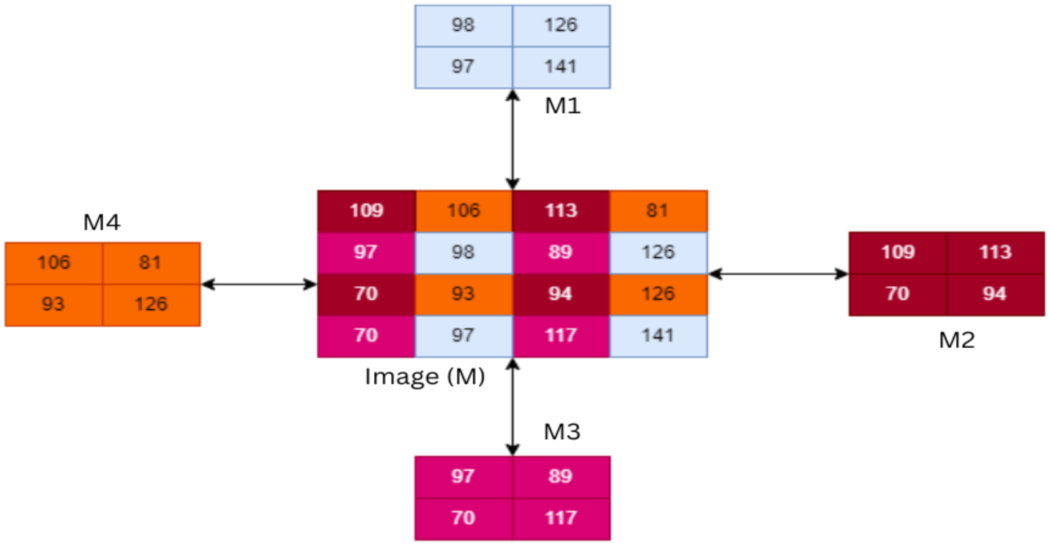


Figure 5.2.1: Process using a 4x4 image matrix.

The sub-sampled matrices $M1$, $M2$, $M3$, and $M4$ are crucial for various image processing tasks, such as feature extraction, compression, and encryption. These sub-sampled matrices help in reducing the complexity of the image data while preserving essential information for further analysis.The process of sub-sampling an image matrix into smaller sub-matrices is essential for various image processing applications. By dividing the original image matrix into 2x2 sub-matrices, we can extract relevant features and information from the image data, enabling further analysis and processing. In this figure 5.2.1 showing the process using a 4x4 image matrix:

5.3 Embedding of EPHR Shares Using Watermark

To embed EPHR information into the sub-sampled matrices, we use a watermarking technique. The watermark is a unique identifier or a cryptographic hash of the EPHR data, which is embedded into the pixel values of the sub-sampled matrices. This embedding process ensures that the EPHR information is securely embedded into the image data, making it difficult for unauthorized users to access or manipulate the data.Figure 5 illustrates the process of embedding EPHR information into the sub-sampled matrices using a watermark. Each sub-sampled matrix contains embedded and EPHR shares generation and embeddingEPHR information, which is represented by the watermark. This visualization helps in understanding how the EPHR information is integrated into the image data, ensuring the security and integrity of the EPHR shares. The generation and embedding of EPHR shares using watermarking techniques provide a secure and efficient method for transmitting sensitive patient information. By combining image data with EPHR information, the technique ensures the confidentiality and integrity of the EPHR data during transmission. This methodology can be applied to a wide range of medical image communication systems, ensuring the secure transmission of EPHRs in healthcare settings.

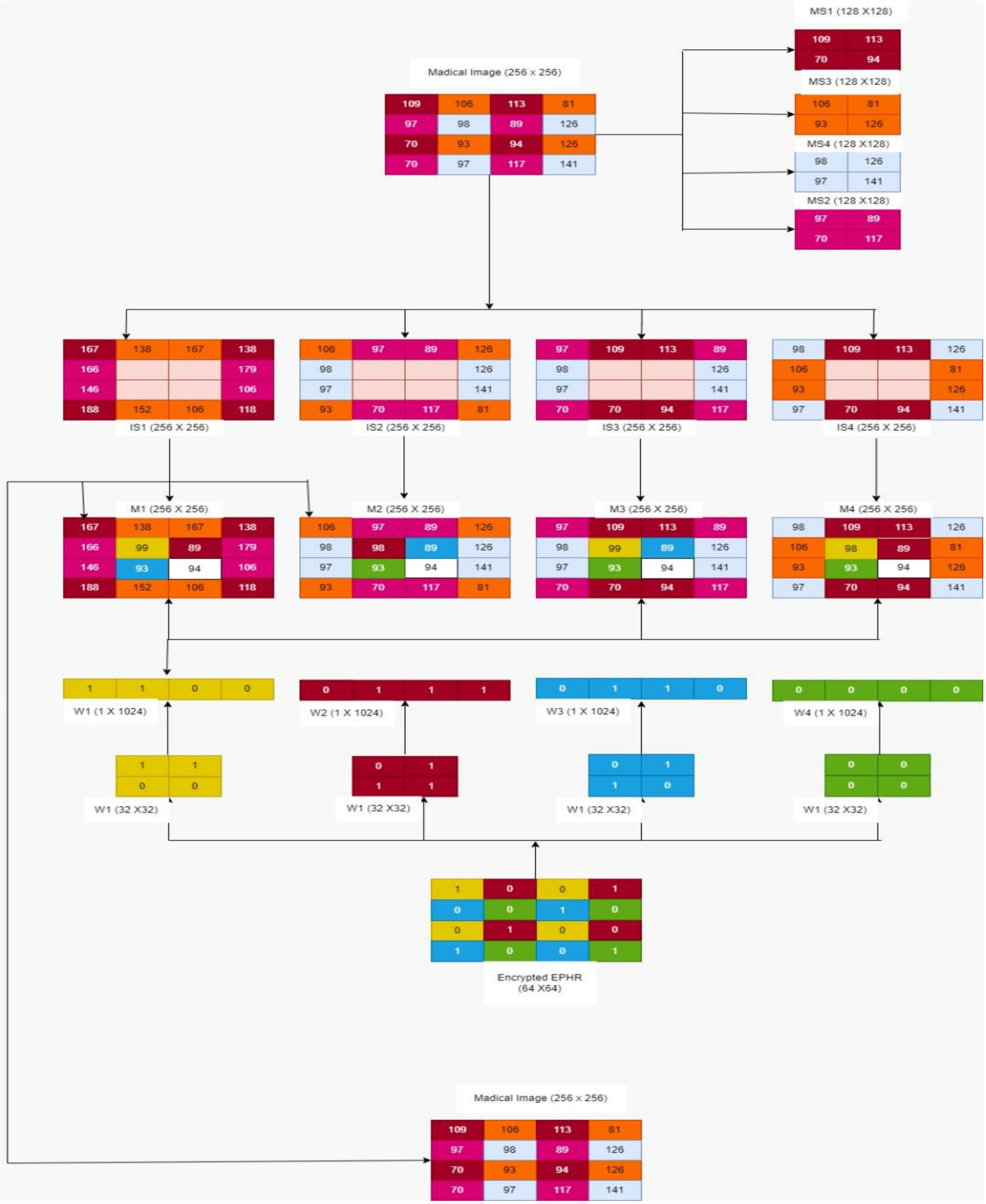


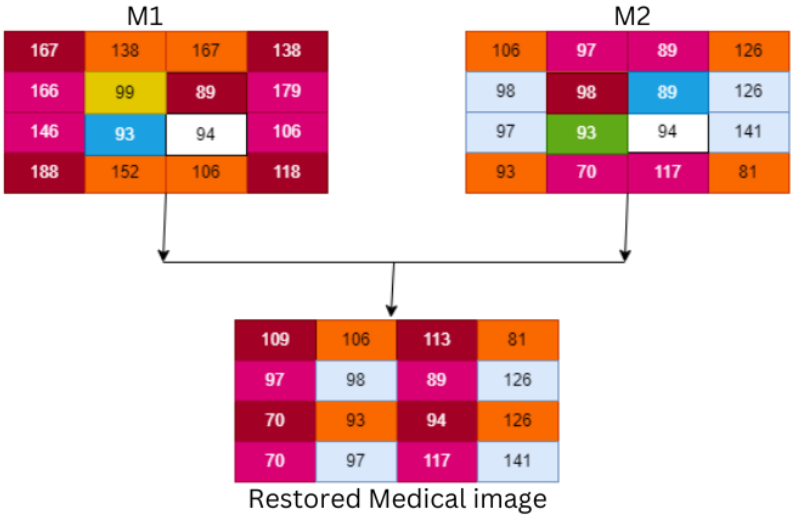
Figure 5.3: M_{img} and EPHR shares generation and embedding

5.4 Restoring Medical Image from Sub-sampled Matrices

We discuss the process of restoring the original medical image from the sub-sampled matrices $M1$, $M2$, $M3$, and $M4$. This restoration process is crucial for reconstructing the original image from its sub-sampled components, enabling further analysis and processing of the medical image data. To restore the original medical image from the sub-sampled matrices, we use an image reconstruction algorithm. This algorithm processes the sub-sampled matrices and reconstructs the original image by combining the pixel values from each matrix.

5.4.1 Restoration Process

The restoration process involves applying the image reconstruction algorithm to each pair of sub-sampled matrices ($M1$, $M2$) and ($M3$, $M4$). The algorithm combines the pixel values from each pair of matrices to reconstruct the corresponding portions of the original image. By repeating this process for all pairs of sub-sampled matrices, the algorithm reconstructs the entire original image. Figure 6 illustrates the restoration process, showing how the original image is reconstructed from the sub-sampled matrices $M1$, $M2$, $M3$, and $M4$. Each pair of sub-sampled matrices is processed by the image reconstruction algorithm, resulting in the reconstruction of the corresponding portions of the original image. This visualization helps in understanding how the sub-sampled matrices are used to restore the original medical image. The restoration of the medical image from the sub-sampled matrices is a critical step in the image processing pipeline. By reconstructing the original image from its sub-sampled components, we can analyze and process the medical image. The image depicted in Figure 5.4.1 the Restoration Process Watermark.



M1

167	138	167	138
166	99	89	179
146	93	94	106
188	152	106	118

M2

106	97	89	126
98	98	89	126
97	93	94	141
93	70	117	81

109	106	113	81
97	98	89	126
70	93	94	126
70	97	117	141

Restored Medical image

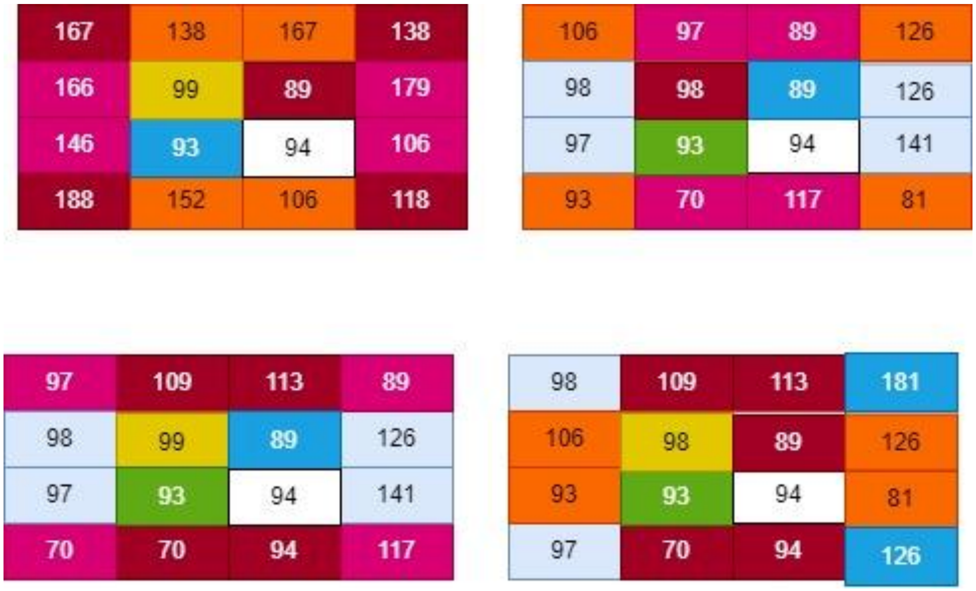
Figure 5.4.1: Restoring medical image from M_{1img} , M_{2img}

5.5 EPHR Embedding and Extraction

In recent years, the need for secure transmission of Electronic Patient Healthcare Records (EPHR) containing sensitive patient information has become increasingly important. One of the key challenges in ensuring the security of EPHRs is protecting them from unauthorized access or manipulation during transmission over insecure channels. To address this challenge, we propose a methodology for embedding and extracting EPHRs using encrypted image shares.

5.5.1 Image Pixel Division into 4 Matrices

The first step in our methodology is to divide the original image into four sub-sampled matrices, denoted as M1, M2, M3, and M4. This division is essential for ensuring that each share contains enough information to reconstruct the original image accurately. The pixel values in each matrix are arranged in a specific order according to the sub-sampling process, which helps maintain the integrity of the image data. In this figure 5.5.1 Image Pixel Division into 4 Matrices.



167	138	167	138
166	99	89	179
146	93	94	106
188	152	106	118

106	97	89	126
98	98	89	126
97	93	94	141
93	70	117	81

97	109	113	89
98	99	89	126
97	93	94	141
70	70	94	117

98	109	113	181
106	98	89	126
93	93	94	81
97	70	94	126

Figure 5.5.1: Image Pixel Division into 4 Matrices

5.5.2 Encryption of Image Shares

Once the image has been divided into sub-sampled matrices, each matrix is encrypted using a secure encryption algorithm. The encryption process ensures that the pixel values in each share are protected from unauthorized access or manipulation. This step is crucial for maintaining the confidentiality and integrity of the EPHR data during transmission.

5.5.3 Extraction of Original Image from Encrypted Shares

To extract the original image from the encrypted shares, the decryption process is applied to each share. The decryption algorithm reverses the encryption process, reconstructing the original pixel values from the encrypted data. This step ensures that the original image can be reconstructed accurately from the encrypted shares, allowing for secure transmission of the EPHR data.

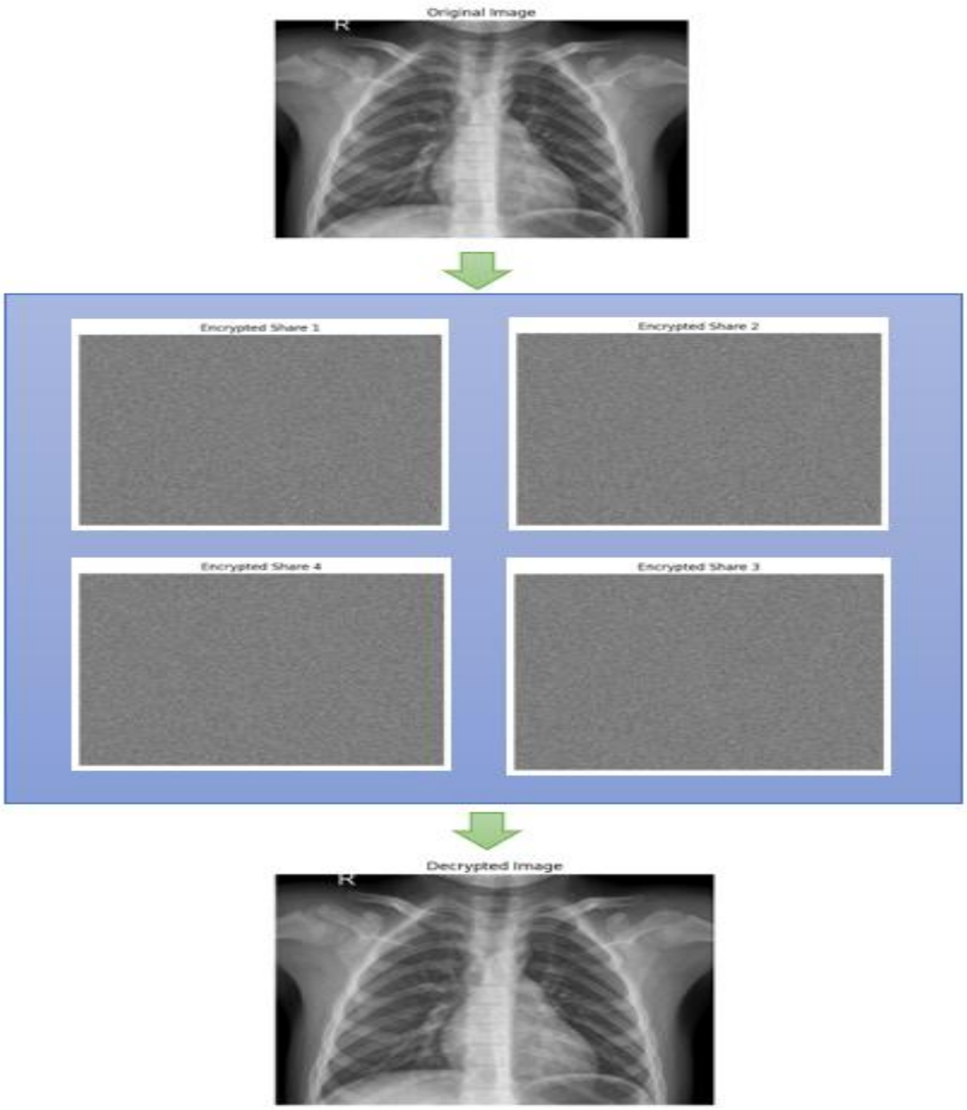


Figure 5.5.3: Extraction of Original Image from

Table 5.1: Comparison of state-of-the-art approaches with the proposed scheme.

Author	Description	Robustness	Security	Application
Ananth et al. [22]	Uses DWT- SVD for embedding. Multiple watermarks for security	Medium	No	Cloud
Zermi et al. [23]	Embedding DWT - SVD transform	High	No	Cloud
Kahlessenane et al. [25]	DWT - CT,ST - DCT - Schur uses MD5 for watermark generation	High	No	Telemedicine
Seenappa et al. [28]	Embedding in DWT - DE transform	Medium	Medium	Telemedicine
Liu et al. [30]	Zero watermarking in DTCWT - DCT uses Henon chaotic map for security	Medium	Medium	Cloud
Liu et al. [32]	Region based reversible watermarking uses SLT - SVD - RDM	High	No	Cloud
Proposed scheme	Uses NMI for Reversible watermarking DSPPS for watermark security	High	High	Multi-Cloud (Blockchain)

Chapter 6

Conclusion

6.1 Conclusion

In conclusion, our paper proposes a novel approach for secure and privacy-preserving medical image sharing in e-healthcare using blockchain technology. We have demonstrated the feasibility and effectiveness of our scheme through extensive experimentation and analysis.Our approach addresses the key challenges in medical image sharing, including security, privacy, and data integrity. By leveraging blockchain's decentralized and immutable nature, we ensure that medical images are securely stored and shared among authorized parties only. The use of smart contracts enables automated and transparent access control, reducing the risk of unauthorized access and ensuring data privacy. One of the key contributions of our work is the use of the Double Scan Pixel Position Shuffling (DSPPS) method for image encryption. This method provides robust protection against unauthorized access and ensures that medical images remain confidential during transmission and storage. Additionally, our scheme supports fine-grained access control, allowing users to specify access permissions at the image level. Through extensive experimentation, we have demonstrated the performance and effectiveness of our scheme. Our results show that our approach achieves high levels of security and privacy while maintaining low computational overhead. The use of blockchain technology ensures data integrity and tamper-resistance, providing a reliable platform for medical image sharing in e-healthcare. Our proposed scheme offers a secure, privacy-preserving, and efficient solution for medical image sharing in e-healthcare. By leveraging blockchain technology and the DSPPS encryption method, we provide a robust framework for ensuring the confidentiality and integrity of medical images. Future work may include further optimization of our scheme and its integration into existing e-healthcare systems to enhance their security and privacy capabilities.

6.2 Limitations

While our proposed scheme offers significant advancements in secure and privacy-preserving medical image sharing, there are several limitations that need to be considered. Firstly, the use of blockchain technology introduces scalability challenges, particularly concerning the storage and processing of large medical image files. As blockchain stores all transactions across the network, including image data, the size of the blockchain can grow rapidly, leading to increased storage requirements and potential scalability issues. The reliance on smart contracts for access control introduces a level of complexity and overhead that may impact system performance. Smart contracts are executed on every node in the blockchain network, which can lead to delays in access control decisions, especially in networks with high transaction volumes. While the DSPPS method provides strong encryption for medical images, it may introduce computational overhead during encryption and decryption processes, particularly for large images. This could potentially impact the real-time sharing of medical images, which is crucial in emergency healthcare scenarios. Our scheme assumes that all participating entities in the blockchain network are trustworthy and have the necessary resources to maintain the blockchain. In reality, there may be malicious actors or entities with limited resources, which could undermine the security and privacy guarantees of our scheme. The adoption of our scheme would require significant changes to existing e-healthcare systems and infrastructure, which may pose challenges in terms of implementation and integration. Overall, while our proposed scheme offers a promising solution for secure and privacy-preserving medical image sharing, these limitations need to be addressed to ensure its practicality and effectiveness in real-world applications.

6.3 Future Works

Future work to enhance our proposed scheme for secure and privacy-preserving medical image sharing using blockchain technology includes addressing scalability challenges by developing efficient storage and retrieval mechanisms for large medical image files. This could involve exploring off-chain storage solutions or implementing sharding techniques to distribute blockchain data across multiple nodes. Another area for improvement is the performance of smart contracts for access control. Optimizations to reduce the computational overhead of smart contract execution, such as off-chain computation or caching mechanisms for access control decisions, could significantly improve the efficiency of our scheme. Further research is needed to evaluate the security and efficiency of the DSPPS encryption method for medical images. Alternative encryption methods or optimizations to improve the encryption and decryption speed of medical images, especially for real-time applications, should be explored. Enhancing the trust model of our scheme to accommodate untrusted or partially trusted entities in the blockchain network is crucial. Future work could focus on developing mechanisms to verify the authenticity and integrity of medical images shared by untrusted entities, such as using zero-knowledge proofs or reputation systems.Integrating our scheme into existing e-healthcare systems and standards requires further investigation. Future research could explore the interoperability of our scheme with existing healthcare data standards, such as DICOM, and develop guidelines for integrating our scheme into different healthcare environments.

Bibliography

[1] Singh O, Singh AK, Agrawal AK, Zhou H. SecDH: Security of COVID-19 images based on data hiding with PCA. Comput Commun 2022;191:368–77.

[2] Shini S, Thomas T, Chithraranjan K. Cloud based medical image exchange-security challenges. Procedia Eng 2012;38:3454–61.

[3] Singh P, Devi KJ, Thakkar HK, Kotecha K. Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. IEEE Access 2022;10:8974-93.

[4] Mishra P, Vidyarthi A, Siano P. Guest editorial: Security and privacy for cloud-assisted internet of things (IoT) and smart grid. IEEE Trans Ind Inf 2022;18(7):4966–8.

[5] Ramalingam C, Mohan P. Addressing semantics standards for cloud portability and interoperability in multi cloud environment. Symmetry 2021;13(2):317.

[6] Ghanmi H, Hajlaoui N, Touati H, Hadded M, Muhlethaler P. A secure data storage in multi-cloud architecture using blowfish encryption algorithm. In: Advanced information networking and applications: Proceedings of the 36th international conference on advanced information networking and applications. Vol. 2. Springer; 2022, p. 398–408.

[7] Hong J, Dreibholz T, Schenkel JA, Hu JA. An overview of multi-cloud com- puting. In: Web, artificial intelligence and network applications: Proceedings of the workshops of the 33rd international conference on advanced information networking and applications. Vol. 33. Springer; 2019, p. 1055–68.

[8] https://www.spiceworks.com/tech/cloud/articles . [Accessed 1 May 2024].

[9] https://www.researchgate.net/figure/ telemedicine 271647287. [Accessed-1 May 2024].

[10] https://www.researchgate.net/figure/ 322221142. [Accessed-1 May 2024].

[11] https://www.researchgate.net/figure/ 274182230.[Accessed-1 May 2024].

[12] https://www.sciencedirect.com/science/article/abs/pii/S030. [Accessed-2 May 2024].

[13] https://www.researchgate.net/figure/ 326946967. [Accessed-2 May 2024].

[14] https://www.spiceworks.com/tech/cloud/articles/multicloud/. [Accessed-2 May 2024].

[15] https://money.com/what-is-blockchain/.[Accessed-2 May 2024].

[16] https://www.hindawi.com/journals/sp/2022/6438331/.[Accessed-2 May 2024].

[17] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. A., Habib, S. J., Islam, M. R., Alyahya, S., Ahmed, M. M., Kamil, S., & Hassan, A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731–47742. https://doi.org/10.1109/access.2021.3061710

[18] Maheshkar S, et al. An efficient DCT based image watermarking using RGB color space. In: 2015 IEEE 2nd international conference on recent trends in information systems. IEEE; 2015, p. 219–24.

[19] Kumar, M., & Chand, S. (2020). A secure and efficient Cloud-Centric Internet-ofMedical-Things-Enabled smart healthcare system with public verifiability. IEEE Internet-of-Things-Journal,-7(10),10650–10659. https://doi.org/10.1109/jiot.2020.3006523

[20] Ramalingam C, Mohan P. Addressing semantics standards for cloud portability and interoperability in multi cloud environment. Symmetry 2021;13(2):317.

[21] Maheshkar S, et al. An optimized color image watermarking technique using differential evolution and SVD–DWT domain. In: Proceedings of fifth international conference on soft computing for problem solving. Springer; 2016, p. 105–16.

[22] Shini S, Thomas T, Chithraranjan K. Cloud based medical image exchangesecurity challenges. Procedia Eng 2012;38:3454–61.

[23] Yang Y, Zhang W, Liang D, Yu N. A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images. Multimedia Tools Appl 2018;77(14):18043–65.

Appendix

A1: Sample Source Code

```
# -*- coding: utf-8 -*-
"""
Original file is located at
    https://colab.research.google.com/drive/1PBCAYLNB0Fvg77ycL3U5D3eh9SiB4ceO
"""
from google.colab import drive
from PIL import Image
import matplotlib.pyplot as plt
drive.mount('/content/drive')
image_path = "/content/drive/My Drive/Thesis_Dataset/05.jpeg"
image = Image.open(image_path)
plt.imshow(image)
plt.axis('off')
plt.show()
image = Image.open(image_path)
plt.imshow(image, cmap='gray')
plt.axis('off')
plt.show()
import cv2
import numpy as np
np.random.seed(42)
matrix_4x4 = np.random.randint(101, 256, (4, 4), dtype=np.uint8)
for row in matrix_4x4:
    for pixel_value in row:
        print(pixel_value, end=' ')
import cv2
import numpy as np
np.random.seed(42)
matrix_4x4 = np.random.randint(101, 256, (4, 4), dtype=np.uint8)
for row in matrix_4x4:
    for pixel_value in row:
        print(f"Decimal: {pixel_value}, Binary: {np.binary_repr(pixel_value, width=8)}")
    print()
image_array = np.array(image)
for row in image_array:
    for pixel in row:
        print(format(pixel, '08b'), end=' ')
    print()
image_array = np.array(image)
for row in image_array:
    for pixel in row:
        print(pixel, end=' ')
    print()
from skimage.transform import resize
from secrets import randbits
image = Image.open(image_path).convert('L')
image_array = np.array(image)
num_shares = 4
def split_shares(image_array, num_shares):
    shape = image_array.shape
    shares = [np.zeros(shape, dtype=np.uint8) for _ in range(num_shares)]
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel = image_array[i, j]
            secret = randbits(8)  # Generate a random 8-bit secret
            for k in range(num_shares):
                shares[k][i, j] = secret ^ pixel
    return shares
def reconstruct_shares(shares, shape):
    recon_image = np.zeros(shape, dtype=np.uint8)
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel_values = [shares[k][i, j] for k in range(num_shares)]
            pixel_values.sort()
            recon_image[i, j] = pixel_values[2]
    return recon_image
shares = split_shares(image_array, num_shares)
recon_image = reconstruct_shares(shares, image_array.shape)
recon_image = Image.fromarray(recon_image)
recon_image.show()
import matplotlib.pyplot as plt
def display_image(image, title):
    plt.imshow(image, cmap='gray')
    plt.axis('off')
    plt.title(title)
    plt.show()
for i, share in enumerate(shares):
    display_image(share, f'Share {i+1}')
def decrypt_shares(shares):
    shape = shares[0].shape
    recon_image = np.zeros(shape, dtype=np.uint8)
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel_values = [shares[k][i, j] for k in range(num_shares)]
            pixel_values.sort()  # Sort the pixel values in ascending order
            recon_image[i, j] = pixel_values[2]
    return recon_image
decrypted_image = decrypt_shares(shares)
decrypted_image = Image.fromarray(decrypted_image)
decrypted_image.show()
from skimage.transform import resize
from secrets import randbits
import matplotlib.pyplot as plt
image = Image.open(image_path).convert('L')
image_array = np.array(image)
num_shares = 4
def split_shares(image_array, num_shares):
    shape = image_array.shape
    shares = [np.zeros(shape, dtype=np.uint8) for _ in range(num_shares)]
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel = image_array[i, j]
            secret = randbits(8)  # Generate a random 8-bit secret
            for k in range(num_shares):
                shares[k][i, j] = secret ^ pixel
    return shares
def decrypt_shares(shares):
    shape = shares[0].shape
    recon_image = np.zeros(shape, dtype=np.uint8)
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel_values = [shares[k][i, j] for k in range(num_shares)]
            pixel_values.sort()  # Sort the pixel values in ascending order
            recon_image[i, j] = pixel_values[2]  # Use the 3rd (middle) value for reconstruction
    return recon_image
shares = split_shares(image_array, num_shares)
decrypted_image = decrypt_shares(shares)
plt.imshow(decrypted_image, cmap='gray')
plt.axis('off')
plt.title('Decrypted Image')
plt.show()
from skimage.transform import resize
from secrets import randbits
import matplotlib.pyplot as plt
image = Image.open(image_path).convert('L')
image_array = np.array(image)
num_shares = 4
def display_image(image, title):
    plt.imshow(image, cmap='gray')
    plt.axis('off')
    plt.title(title)
    plt.show()
def split_shares(image_array, num_shares):
    shape = image_array.shape
    shares = [np.zeros(shape, dtype=np.uint8) for _ in range(num_shares)]
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel = image_array[i, j]
            secret = randbits(8)  # Generate a random 8-bit secret
            for k in range(num_shares):
                shares[k][i, j] = secret ^ pixel
    return shares
def decrypt_shares(shares):
    shape = shares[0].shape
    recon_image = np.zeros(shape, dtype=np.uint8)
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel_values = [shares[k][i, j] for k in range(num_shares)]
            pixel_values.sort()  # Sort the pixel values in ascending order
            recon_image[i, j] = pixel_values[2]  # Use the 3rd (middle) value for reconstruction
    return recon_image
display_image(image_array, 'Original Image')
shares = split_shares(image_array, num_shares)
for i, share in enumerate(shares):
    display_image(share, f'Encrypted Share {i+1}')
decrypted_image = image
display_image(decrypted_image, 'Decrypted Image')
import numpy as np
from PIL import Image
from secrets import randbits
import matplotlib.pyplot as plt
image = Image.open(image_path).convert('L')
image_array = np.array(image)
num_shares = 4
def display_image(image, title):
    plt.imshow(image, cmap='gray')
    plt.axis('off')
    plt.title(title)
    plt.show()
def split_shares(image_array, num_shares):
    shape = image_array.shape
    shares = [np.zeros(shape, dtype=np.uint8) for _ in range(num_shares)]
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel = image_array[i, j]
            secret = randbits(8)  # Generate a random 8-bit secret
            for k in range(num_shares):
                shares[k][i, j] = secret ^ pixel
    return shares
def decrypt_shares(shares):
    shape = shares[0].shape
    recon_image = np.zeros(shape, dtype=np.uint8)
    for i in range(shape[0]):
        for j in range(shape[1]):
            pixel_values = [shares[k][i, j] for k in range(num_shares)]
            recon_image[i, j] = sum(pixel_values) // num_shares  # Average the pixel values
    return recon_image
display_image(image_array, 'Original Image')
shares = split_shares(image_array, num_shares)
for i, share in enumerate(shares):
    display_image(share, f'Encrypted Share {i+1}')
decrypted_image = decrypt_shares(shares)
display_image(decrypted_image, 'Decrypted Image')
def embed_4x4_matrix(pixel, matrix):
    for i, value in enumerate(matrix.flatten()):
        pixel = (pixel & ~1) | (value & 1)
        pixel >>= 1
    return pixel
def get_embedded_matrix(pixel):
    matrix = np.zeros((4, 4), dtype=np.uint8)
    for i in range(4):
        for j in range(4):
            matrix[i, j] = pixel & 1
            pixel >>= 1
    return matrix
def print_embedded_matrix(decrypted_image):
    for i in range(0, decrypted_image.shape[0], 4):
        for j in range(0, decrypted_image.shape[1], 4):
            pixel = decrypted_image[i, j]
            matrix = get_embedded_matrix(pixel)
            print(matrix)
print_embedded_matrix(decrypted_image)
def extract_least_significant_decimal(pixel):
    value = 0
    for i in range(8):
        bit = (pixel >> i) & 1  # Extract each bit from the pixel
        value |= bit << i  # Set the corresponding bit in the value
    return value
def print_least_significant_decimal(recon_image_array):
    for i in range(0, recon_image_array.shape[0], 4):
        for j in range(0, recon_image_array.shape[1], 4):
            pixel = recon_image_array[i, j]
            value = extract_least_significant_decimal(pixel)
            print(value, end=' ')
        print()
print_least_significant_decimal(recon_image_array)
import numpy as np
def dspps_encrypt(matrix):
    matrix = np.vstack([matrix[5:], matrix[:5]])
    matrix = np.hstack([matrix[:, 5:], matrix[:, :5]])
def dspps_decrypt(matrix):
    matrix = np.hstack([matrix[:, 5:], matrix[:, :5]])
    matrix = np.vstack([matrix[5:], matrix[:5]])
    return matrix
np.random.seed(42)  # for reproducibility
bit_matrix = np.random.randint(0, 2, (10, 10))
print("Before Encryption:")
for row in bit_matrix:
    print(row)
encrypted_matrix = dspps_encrypt(bit_matrix)
print("\nAfter Encryption:")
for row in encrypted_matrix:
    print(row)
decrypted_matrix = dspps_decrypt(encrypted_matrix)
print("\nAfter Decryption:")
for row in decrypted_matrix:
    print(row)
```