People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University Echahid Cheikh Larbi Tebessi- Tebessa



Faculty of Exact Sciences and Natural and Life Sciences
Department of computer science/mathematics
Domiciliation laboratory: laboratory of mathematics, informatics and systems (LAMIS)

Thesis

Presented and Publicly Defended for Obtaining the Diploma of Doctorate in Third Cycle

By:
Brahim Ferik

Domain: mathematics and computer science **Stream:** computer science
Speciality: Networks and Security

Title

Medical Image Watermarking for Secure E-Health Application

Defended on: July 10, 2025

Before the jury composed of:

Full name	**Rank**	**University**	
Mr. Hakim Bendjenna	Pr	Univ. of Tebessa	President
Mr. Lakhdar Laimeche	Pr	Univ. of Tebessa	Supervisor
Mr. Abdallah Meraoumia	Pr	Univ. of Tebessa	Co- supervisor
Mr. Mohammad Charaf Eddine Meftah	Pr	Univ. of Eloued	Examiner
Mr. Issam Bendib	MCA	Univ. of Tebessa	Examiner
Mr. Abdelkader Laouid	Pr	Univ. of Eloued	Invited

Academic year: 2024/2025

Acknowledgments

First and foremost, I would like to express my deepest gratitude to God, who provided me with the strength and resilience to complete this endeavor.

I am immensely thankful to my PhD supervisor, Professor. Lakhdar Laimeche, whose unwavering support, valuable guidance, and profound insights have shaped my academic journey.

I also sincerely appreciate my friend and brother, Professor. Laouid Abdelkader, whose belief in my abilities and sage advice have been invaluable throughout these challenging years.

Additionally, I would like to thank the jury members for their time and effort in evaluating my thesis and for their constructive feedback.

Lastly, I am grateful to all those who have supported me personally and professionally in completing this PhD thesis.

Dedication

In the name of Allah, the Most Gracious, the Most Merciful

To my beloved parents, whose souls continue to guide and inspire me. May Allah have mercy upon them and grant them eternal peace. Your unconditional love and unwavering faith in me have been the foundation of my every success.

To my dear family, each of you holds a special place in my heart. To my brothers and sisters, your constant support and encouragement have strengthened and motivated me throughout this journey.

To my precious children, Sidra and Abdallah, who bring endless joy and purpose to my life. Your smiles and boundless curiosity have fueled my determination to persevere and succeed.

My cherished friends have supported me with kindness, understanding, and encouragement. Your belief in me and unwavering support have enriched this journey in countless ways.

Abstract

The rapid advancement of communication technologies creates significant challenges in protecting medical imaging data. Digital watermarking has emerged as a formidable solution, embedding inconspicuous yet traceable information into multimedia content to safeguard data security and authenticity, especially in healthcare. Unlike other methods, watermarking intrinsically links the information to the data, providing robust protection against tampering and unauthorized modifications.

In e-healthcare, the secure transfer of medical images is crucial for services such as telemedicine and teleradiology, as it improves diagnostic accuracy and protects patient data. This study introduces advanced blind watermarking methods based on biometric technology to ensure secure transmission while maintaining image integrity and authenticity. The proposed techniques are designed to balance the practical challenges of detection rates, watermark visibility, and overall robustness.

This work presents robust watermarking frameworks to enhance medical image management in e-healthcare systems, highlighting practical benefits and challenges. It integrates advanced security methods like encryption, blockchain, and compression algorithms, which will be tested in realistic scenarios to validate their effectiveness. By combining these innovative solutions, this research supports the creation of secure and efficient systems for electronic medical records.

This thesis introduces two advanced watermarking frameworks founded on biometric technology to ensure secure image transmission while preserving integrity. The first, a Multi-Layered Security Framework (MLSF), integrates compressed fingerprint watermarking with encryption and blockchain. The second approach, Improved DWT and ACM Watermarking (IDAW), combines palmprint features with chaotic transformations to enhance the watermark's resilience.

Experimental evaluations confirm the effectiveness of these contributions. The MLSF demonstrates exceptional imperceptibility, achieving a PSNR of 63.24 dB and an SSIM of 1.0. The IDAW framework proves highly robust against a range of attacks, including compression and noise, maintaining a PSNR of 53.95 dB and an SSIM of 0.99996. By integrating innovative security solutions, this research contributes to the development of secure and efficient systems for managing electronic medical records in the modern digital era.

Keywords: Medical Images, Digital watermark, Biometric, Teleradiology, Embedding, Extraction, Blockchain, Integrity.

Résumé

Tatouage numérique des images médicales pour des applications sécurisées en e-santé

L'avancement rapide des technologies de communication a engendré des défis importants pour la protection des données d'imagerie médicale. Le tatouage numérique s'est imposé comme une solution puissante, intégrant des informations discrètes mais traçables pour garantir la sécurité et l'authenticité des contenus, ce qui est essentiel dans le secteur de la santé. Contrairement à d'autres méthodes, le tatouage lie intrinsèquement l'information aux données, offrant une protection robuste contre les altérations.

En cybersanté, le transfert sécurisé des images médicales est fondamental pour la télémédecine et la téléradiologie, afin d'améliorer la précision du diagnostic et de protéger les données des patients. Cette étude introduit des méthodologies avancées de tatouage numérique aveugle basées sur la technologie biométrique pour assurer une transmission sécurisée tout en préservant l'intégrité et l'authenticité des images. Les approches proposées sont conçues pour équilibrer les défis pratiques des taux de détection, de la visibilité du tatouage et de la robustesse globale. Ce travail présente des cadres de tatouage robustes qui intègrent des méthodes de sécurité avancées telles que le chiffrement, les réseaux blockchain et la compression, qui seront testés dans des scénarios réalistes pour valider leur efficacité.

Cette thèse introduit deux cadres de tatouage avancés fondés sur la technologie biométrique. Le premier, un Cadre de Sécurité Multi-couches (MLSF), intègre le tatouage par empreintes digitales compressées avec le chiffrement et la blockchain. La seconde approche, le Tatouage Amélioré par DWT et ACM (IDAW), combine les caractéristiques des empreintes palmaires avec des transformations chaotiques pour renforcer la résilience du tatouage.

Les évaluations expérimentales confirment l'efficacité de ces contributions. Le MLSF démontre une imperceptibilité exceptionnelle, atteignant un PSNR de 63,24 dB et un SSIM de 1,0. Le cadre IDAW se révèle très robuste contre diverses attaques, y compris la compression et le bruit, maintenant un PSNR de 53,95 dB et un SSIM de 0,99996. En intégrant ces solutions innovantes, cette recherche contribue au développement de systèmes sécurisés et efficaces pour la gestion des dossiers médicaux électroniques à l'ère numérique.

Mots clés: Images médicales, Tatouage numérique, Biométrie, Téléradiologie, Intégration, Extraction, Blockchain, Intégrité.

الملخص

العلامة المائية للصور الطبية لتطبيقات الصحة الإلكترونية الآمنة

التقدم السريع في تقنيات الوسائط المتعددة والاتصالات أحدث تحديات كبيرة في حماية وصون بيانات الوسائط المتعددة، وخاصة في مجال التصوير الطبي. لقد برزت تقنية العلامة المائية الرقمية كحل قوي لهذه التحديات عن طريق تضمين معلومات تبقى غير ملحوظة ولكن يمكن تتبعها ضمن المحتوى المتعدد الوسائط. وتُعد هذه التقنية ضرورية لضمان أمان البيانات وأصالتها، مما يجعلها لا غنى عنها في القطاعات الحيوية، وبخاصة في مجال الرعاية الصحية. وعلى عكس التقنيات البديلة، ترتبط المعلومات المضمنة بالبيانات بشكل جوهري، مما يوفر مقاومة ضد التلاعب والتعديلات غير المصرح بها.

في مجال الرعاية الصحية الإلكترونية، يُعد النقل الآمن للصور الطبية أمرًا بالغ الأهمية لخدمات مثل الطب عن بعد والتصوير الشعاعي عن بعد، لأنه يحسن دقة التشخيص ويحمي بيانات المرضى. تقدم هذه الدراسة منهجيات متقدمة للعلامة المائية العمياء تعتمد على التكنولوجيا البيومترية لضمان النقل الآمن مع الحفاظ على سلامة الصور وأصالتها. وقد صُممت التقنيات المقترحة لتحقيق التوازن بين التحديات العملية المتمثلة في معدلات الكشف ووضوح العلامة المائية والمتانة الشاملة.

يقدم هذا العمل أطرًا قوية للعلامة المائية لتحسين إدارة الصور الطبية في أنظمة الرعاية الصحية الإلكترونية، مسلطًا الضوء على الفوائد العملية والتحديات. ويدمج أساليب أمان متقدمة مثل التشفير وشبكات البلوك تشين وخوارزميات الضغط، والتي سيتم اختبارها في سيناريوهات واقعية للتحقق من فعاليتها. من خلال الجمع بين هذه الحلول المبتكرة، يدعم هذا البحث إنشاء أنظمة آمنة وفعالة للسجلات الطبية الإلكترونية.

تؤكد التقييمات التجريبية فعالية هذه المساهمات. يُظهر إطار **MLSF** إخفاءً استثنائيًا، حيث حقق نسبة إشارة إلى ضوضاء قصوى (**PSNR**) تبلغ **63.24** ديسيبل ومؤشر تشابه هيكلي (**SSIM**) قدره **1.0** ويثبت إطار **IDAW** متانة عالية ضد مجموعة من الهجمات، بما في ذلك الضغط والضوضاء، محافظًا على **PSNR** يبلغ **53.95** ديسيبل و**SSIM** قدره **0.99996** من خلال دمج حلول أمنية مبتكرة، يساهم هذا البحث في تطوير أنظمة آمنة وفعالة لإدارة السجلات الطبية الإلكترونية في العصر الرقمي الحديث.

الكلمات المفتاحية :الصور الطبية، العلامة المائية الرقمية، البيومترية، التصوير الشعاعي عن بُعد، التضمين، الاستخراج، البلوك تشين، السلامة.

Contents

Acknowledgments i

Dedication ii

Abstract iii

Contents x

List of Figures xi

List of Tables xi

General Introduction 1

Objectives of the research 2
Core Principles of Security in E-Health 2
Principal contributions 4
Structure of the manuscript 6
List of publications 7

1 Background 9

1.1 Introduction 9
1.2 An Overview of Medical Image Security 9
1.2.1 Medical Imaging Modalities 10
1.2.2 Necessity of Security in E-Healthcare 10
1.2.3 Risks and Challenges 11
1.3 Watermarking in Medical Image Security 12
1.3.1 What is Digital Watermarking? 12
1.3.2 Applications of Watermarking in Medical Imaging 14
1.3.3 Challenges in Medical Image Watermarking 15
1.3.4 The Discrete Wavelet Transform 15

1.3.5 LSB-Based Watermark Embedding 17
1.3.6 Arnold Cat Map 19
1.4 Biometrics in Medical Image Security 20
1.4.1 Fingerprint-Based Watermarking 20
1.4.2 Palmprint-Based Watermarking 25
1.4.2.1 Gabor Filter 25
1.4.3 Other Biometric Modalities 26
1.5 Blockchain Technology in Medical Image Security 26
1.5.1 Key Features of Blockchain 27
1.5.2 Blockchain in Healthcare 28
1.5.3 Integration with Watermarking 29
1.6 Conclusion 29

2 Related Works **33**
2.1 Introduction 33
2.2 Review of Medical Image Watermarking Techniques 34
2.2.1 Non-Blind Watermarking 34
2.2.2 Blind Watermarking 36
2.2.3 Semi-Blind Watermarking 37
2.3 Compression and Encryption in E-Health Systems 38
2.3.1 The Role of Compression in Medical Image Security . . . 39
2.3.2 Encryption Techniques for E-Health Data Security 39
2.3.3 Integrating Compression and Encryption with Watermarking 40
2.4 Blockchain in Healthcare: Traceability and Immutability 41
2.4.1 Blockchain for Image Authentication and Copyright Protection 41
2.4.2 Blockchain for Medical Image Traceability and Verification 42
2.4.3 Combining Blockchain with Encryption and Compression . 43
2.4.4 Challenges and Future Directions 43
2.5 Synthesis and Comparative Analysis 44
2.6 Conclusion 47

3 The Proposed Contributions **49**
3.1 Introduction 49
3.2 Proposed Schemes 51
3.2.1 The Multi-Layered Security Framework Specifications . . . 51

3.2.1.1 Binary Matrix Compression with Integrity Verification . . . 51
3.2.1.2 Embedding Process . . . 55
3.2.1.3 Secure Storage of Watermarked Images with Blockchain and IPFS . . . 58
3.2.1.4 Extraction Process . . . 61
3.2.2 Improved DWT and ACM Watermarking Approach Specifications . . . 64
3.2.2.1 Embedding Process . . . 64
3.2.2.2 Extraction Process . . . 68
3.3 Implementation and Experimental Evaluation . . . 70
3.3.1 Implementation . . . 70
3.3.1.1 Dataset Description and Image Types . . . 71
3.3.1.2 Device Characteristics and Computational Environment . . . 75
3.3.2 Experimental Evaluation . . . 77
3.3.2.1 Quality and Robustness Evaluation Metrics . . . 77
3.3.3 Imperceptibility Measurements . . . 78
3.3.4 Robustness Measurements . . . 81
3.3.5 Computational Complexity and Practical Feasibility . . . 84
3.3.6 Comparative Study . . . 86
3.3.6.1 Imperceptibility . . . 86
3.3.6.2 Robustness . . . 88
3.4 Conclusion . . . 89

4 Case Studies of Watermarking in Healthcare 91
4.1 Introduction . . . 91
4.2 Real Applications of Watermarking in Healthcare . . . 92
4.3 Case Studies and Examples . . . 94
4.3.1 Christian Medical College (CMC), Vellore (India) . . . 94
4.3.2 National Technical University of Athens & Hippokratio Hospital (Greece) . . . 95
4.3.3 Ongoing Adoption in Research and Practice . . . 95
4.4 Key Applications and Benefits . . . 96
4.5 Discussion . . . 98

4.6 Future Trends and Innovations 98
4.7 Conclusion 99

Conclusion **100**

List of Figures

1.1 A Comparative Overview of Common Medical Imaging Modalities. 10
1.2 A Classification of Digital Image Watermarking Methods. 14
1.3 Two-Level Discrete Wavelet Decomposition. 17
1.4 2D Wavelet Decomposition: (a) Original Medical Image. (b) 2D-DWT at the First Level. (c) 2D-DWT at the Second Level. . . . 18
1.5 Replacement Diagram of LSB. 18
1.9 Advantages of Blockchain. 28
1.6 Applying ACM Iterations. 31
1.7 Visualization of BSIF-based Feature Extraction Pipeline. 32
1.8 The Extracted Features from the Palmprint Image using the Gabor Filter. 32

3.1 A Global Overview of the Blockchain-based Watermarking Process. 57
3.2 Blockchain and IPFS Integration Diagram to Store Watermarked Images. 61
3.3 The Extraction Steps of the Multi-Layered Security Framework. . 63
3.4 The Embedding Process of IDAW. 67
3.5 The Extraction Process of IDAW. 69
3.6 Samples of Used Human Brain MRI Image Dataset. 71
3.7 Illustrative Samples of The PolyU II Palmprint Database. 72
3.8 Gray-scale Medical Image Sample from The Pulmonary Fibrosis Progression Dataset. 72
3.9 Results of Utilizing Various Visibility Factors (t) to Embed Watermarks. 73
3.10 Performed BSIF Feature Extraction on Fingerprint Images. 75
3.11 Comparison between original and reduced matrix sizes in bits. . . 76

3.12 Watermark Embedding and Encryption Processes in Medical Images. 77
3.13 Different Sizes of Watermark. 80
3.14 Robustness Against JPEG and Image Processing Attacks. 82
3.15 Comparison of The Obtained PSNR and SSIM for JPEG Compression. 90

List of Tables

2.1 Summary of Existing Studies on Medical Image Watermarking . . 45
2.2 Summary of Existing Studies on Medical Image Watermarking (Continued) 46

3.1 Gaussian-like Filter and LoG Filter Comparisons. 74
3.2 Imperceptibility Results of the Multi-Layered Security Framework. 79
3.3 Performance Metrics of Watermark Compression and Embedding in Host Images. 79
3.4 Performance Metrics for Watermark Embedding. 81
3.5 Watermark Extraction Results. 81
3.6 Robustness measurement against different attacks. 83
3.7 Robustness Measures Against Different Attacks. 85
3.8 The Performance Comparative Study. 87
3.9 Watermarked Image Quality: PSNR, SSIM, and NCC Comparison. 87
3.10 PSNR and SSIM Values Comparison of the Extracted Watermarks. 88
3.11 Comparison of PSNR Values for Different Attacks. 88
3.12 Comparison of NCC Values for Different Attacks. 89

General Introduction

In the modern era, integrating technology in healthcare has led to remarkable advancements in disease diagnosis, treatment, and management. Medical imaging, a cornerstone of modern diagnostics, is crucial in delivering precise and reliable information to healthcare professionals. However, the increasing reliance on digital imaging has introduced new challenges, particularly in data security and privacy. Medical images often contain sensitive patient information, which, if compromised, can lead to severe ethical, legal, and financial repercussions. This underscores the necessity for robust mechanisms to ensure medical images' confidentiality, integrity, and authenticity. Among the various security measures, digital watermarking has emerged as a promising solution, offering the capability to embed imperceptible yet recoverable information within images. This thesis explores the application of digital watermarking techniques in secure e-health systems, aiming to enhance the security and reliability of medical imaging (1).

The rapid digitization of medical records and images has introduced vulnerabilities that malicious actors could exploit. Unauthorized access, tampering, and data breaches pose significant threats to patient confidentiality and the integrity of medical data. In addition, the rise of telemedicine and cloud-based storage solutions further amplifies these risks, as medical images are frequently transmitted over untrusted networks (2). While effective in protecting data during transmission, conventional encryption methods fail to ensure the integrity of images once they are decrypted. Consequently, there is a pressing need for a security mechanism that protects medical images from unauthorized access and provides a means of verifying their authenticity and integrity.

Objectives of the research

The primary objective of this thesis is to develop a comprehensive framework for securing medical images in e-health applications using advanced digital watermarking techniques. The proposed methods aim to:

1. Embed robust and imperceptible watermarks in medical images without compromising diagnostic quality (3).
2. Ensure the resilience of the watermarks against various attacks, including compression, noise, and geometric distortions.
3. Integrate the watermarking techniques with emerging technologies, such as blockchain, to create a decentralized and tamper-evident security framework.
4. Provide a scalable and adaptive solution seamlessly integrated into existing e-health infrastructures.

Core Principles of Security in E-Health

In e-health applications, the security of medical images is critical to ensuring healthcare services' safe and efficient delivery. Medical images such as X-rays, MRIs, and CT scans (4) are integral to diagnosis and treatment planning, making their protection from unauthorized access and tampering essential. This protection revolves around the foundational principles of data security: confidentiality, integrity, and availability (5). These principles are especially crucial in environments where medical data is stored, transmitted, and accessed digitally.

1. **Confidentiality**: Confidentiality ensures that sensitive information is accessible only to authorized individuals, safeguarding patient privacy and maintaining trust in healthcare systems. Confidentiality involves implementing secure authentication protocols and encryption methods to restrict access to authorized personnel for medical images. Measures such as access control systems and user authentication mechanisms ensure that healthcare

professionals, and only those with proper clearance, can retrieve and view medical images.

2. **Integrity**: Integrity guarantees that medical images remain unaltered and reliable from acquisition to their use in diagnosis and treatment. This security aspect is particularly significant in e-Health systems, where even minor alterations can lead to misdiagnosis or incorrect treatment plans. Integrity is maintained by employing hash functions and digital signatures that can verify the authenticity and originality of medical images. These techniques detect unauthorized modifications, ensuring that tampering attempts are identified and mitigated.

3. **Availability**: Availability ensures that medical images are accessible to authorized users when needed, supporting timely and effective healthcare delivery. In e-Health systems, this principle addresses the challenges of maintaining system uptime, even during cybersecurity incidents. Redundancy strategies, such as backup servers and distributed storage systems, are implemented to prevent downtime and ensure continuous access to medical data.

Practical Measures for Medical Image Security

- Access Control: Implementing robust authentication and authorization mechanisms to restrict access to imaging systems ensures that only verified healthcare professionals can retrieve and process medical images (6).

- Data Segmentation: Segregating medical image data from other network data minimizes the risk of cross-contamination and limits the impact of potential breaches (7).

- Encryption: The use of advanced encryption techniques during data storage and transmission adds a layer of protection, preventing unauthorized interceptation or leaks (8).

- Regular Audits: Regular security assessments of e-Health systems help identify vulnerabilities and implement timely updates to safeguard sensitive data.

- Resilience to Attacks: Designing systems to resist tampering, breaches, and cyberattacks ensures the continued reliability of medical image storage and transmission (9).

By addressing confidentiality, integrity, and availability through these measures, e-Health systems can provide a secure environment to manage and use medical images, fostering trust and reliability in digital healthcare solutions.

Principal contributions

The protection of medical images remains paramount, necessitating robust solutions to ensure their confidentiality, authenticity and integrity. This raises a pivotal question. What innovative watermarking techniques can be implemented to ensure robust protection and secure sharing of medical images in e-health systems? Our research addresses this question through a novel framework that integrates advanced watermarking and blockchain technologies to improve medical image security.

The challenge lies in developing innovative techniques that can robustly protect medical images without compromising their quality. This raises the question: What innovative watermarking techniques can be implemented to ensure robust protection and secure sharing of medical images in e-Health systems? Our research addresses this question by proposing a comprehensive framework that integrates advanced watermarking, encryption, and blockchain technologies to improve the security and reliability of medical images in e-health applications.

1. **Comprehensive Framework for Medical Image Security:** This research presents a meticulously designed framework that effectively integrates advanced watermarking, compression, encryption and blockchain technologies. The innovative framework ensures the secure integration of watermarks within medical images, thereby preserving exceptional image quality while proficiently protecting confidentiality and integrity across various e-Health applications. This addresses significant concerns about data security and patient privacy.

2. **Innovative Watermarking Techniques:** The framework incorporates sophisticated methodologies, including Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) techniques, to embed highly specialized biometric-based compressed watermarks into medical images. This careful methodology ensures imperceptibility, rendering the watermark virtually invisible to the naked eye while providing substantial robustness against potential alterations. Additionally, it maintains the integrity of sensitive patient data, thereby improving the reliability of electronic medical records.

3. **Decentralized and Secure Storage Mechanisms:** In response to the contemporary challenges associated with data storage within the healthcare sector, the framework integrates the InterPlanetary File System (IPFS) alongside Ethereum blockchain technology. This advanced decentralized solution enhances traceability and immutability and facilitates the secure sharing of encrypted watermarked images. Consequently, it addresses the numerous vulnerabilities typically linked to conventional centralized systems, thereby significantly improving the security of sensitive medical information.

4. **Resilience Against Security Threats:** The framework is designed to exhibit robust resilience against a diverse range of image-processing attacks, which may include compression, noise addition, and cropping factors that present considerable risks to the integrity of medical images. The strong protective measures embedded within the framework safeguard the integrity of watermarked medical images, ensuring their security against unauthorized modifications, particularly within sensitive e-Health settings where security breaches can have severe implications.

5. **Scalability and Practical Integration:** Tailored for real-world applications in the healthcare sector, the framework demonstrates scalability and full compatibility with existing healthcare infrastructures, such as electronic health records (EHRs) and telemedicine systems. It adeptly manages extensive datasets while rigorously adhering to healthcare privacy regulations, establishing itself as an efficient solution for secure medical image sharing within contemporary e-Health systems. Such adaptability is crucial for promoting innovation in healthcare delivery while ensuring safety and compliance in data management practices.

These noteworthy contributions collectively establish a coherent and robust solution to significantly enhance the security, integrity, and reliability of e-health applications. By advancing innovative medical image watermarking techniques, this research effectively addresses the multifaceted challenges healthcare providers face, ultimately facilitating the development of safer and more efficient electronic health solutions.

Thesis Structure

This manuscript is organized to methodically address the security concerns associated with medical images in e-Health. Chapter 1, establishes the foundational context, underscoring the essential functions of digital watermarking, compression, encryption, and blockchain in protecting sensitive medical information. Chapter 2 critically examines recent progress in watermarking techniques across spatial, frequency, and hybrid domains, emphasizing their effectiveness in ensuring data integrity, resistance to tampering, and copyright protection while highlighting existing vulnerabilities within e-health systems. Chapter 3, presents original contributions, including a Multi-Layered Security Framework (MLSF) that incorporates various protective mechanisms and the technical details of the Improved DWT and ACM Watermarking (IDAW) scheme designed for robust embedding and assesses the performance of the proposed methodologies, discusses their limitations, and highlights their capacity to bolster trust in e-health platforms. Lastly, Chapter 4, examines real-world applications and case studies of digital watermarking in healthcare, including reversible, adversarial, and adaptive techniques for securing medical images.

Collectively, these chapters provide a comprehensive examination of innovative approaches to enhance the security of medical imaging within digital healthcare environments.

List of publications

Journal papers:

1. A Multi-Layered Security Framework for Medical Imaging: Integrating Compressed Digital Watermarking and Blockchain, IEEE Access, 2024 (10).

   Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Omar Aldabbas, Muath AlShaikh, Abdelkader Laouid and Hammoudeh Mohammad.

2. An Efficient Semi-Blind Watermarking Technique Based on ACM and DWT for Mitigating Integrity Attacks, Arabian Journal for Science and Engineering (AJSE), 2025 (11).

   Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Muath AlShaikh, Khaled Chait and Hammoudeh Mohammad.

Conference papers:

1. A Blind Digital Watermarking Approach using Palmprint-Embedded Local Binary Patterns and Arnold Cat Map Transformations, The 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS2024), 2024 (12).

   Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Khaled Chait, and Muath AlShaikh.

2. An Adaptive Image Watermarking based on Bellman-Ford Algorithm, The 7th International Conference on Future Networks & Distributed Systems (ICFNDS2023), 2023 (13).

   Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Muath AlShaikh, and Khaled Chait.

3. A Medical Image Watermarking Technique based on Blockchain, The 1st International Conference on Smart Mobility and Logistics Ecosystems (SMiLE), September 2024, (accepted).

Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Muath AlShaikh and Khaled Chait.

4. A Decentralized GPS Positioning Consensus Based on Secure Image Watermarking for UAV Networks, The First International Conference on Innovative and Intelligent Information Technologies (IC3IT), December 2024, (14).

   Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Ahcene Bounceur, and Mostefa Kara.

Communications / National Conference papers:

1. A Smart Watermarking Medical Image Approach Based on Dual Authentication, The 1st National Conference on Artificial Intelligence and Information Technology (NCAIIT'24), December 2024, Relizane.

   Authors: Brahim Ferik, Lakhdar Laimeche.

2. Enhancing Security of Medical Images via Biometric Watermarking with Palmprint Feature Extraction, The Second National Conference on the Digital Health Revolution: Applications and Impacts of Artificial Intelligence, November 2024, Tebessa.

   Authors: Brahim Ferik, Lakhdar Laimeche.

3. A Dual Medical Image Authentication Approach: Siamese Networks with Standard Deviation-Based Watermarking, The Second National Conference on the Digital Health Revolution: Applications and Impacts of Artificial Intelligence, November 2024, Tebessa.

   Authors: Brahim Ferik, Lakhdar Laimeche.

4. An Efficient Image Watermarking Technique Based on Arnold Cat Map, National Conference on Artificial Intelligence (NCAI'23), December 2023, Tebessa.

   Authors: Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia.

Chapter 1

Background

1.1 Introduction

Medical image security is a critical concern in modern healthcare, necessitating robust solutions to ensure privacy, integrity, and accessibility (15). This chapter examines the key technologies that underpin our proposed approach. Digital watermarking embeds imperceptible identifiers into data to preserve authenticity and protect against tampering (16). Advanced data compression optimizes storage while maintaining quality, ensuring efficient resource usage. Encryption, utilizing robust algorithms, safeguards sensitive information from unauthorized access and ensures secure communication. Blockchain technology introduces transparency, integrity, and decentralized data management, enabling immutable records and secure metadata handling (17).

Additionally, distributed storage systems provide scalable and efficient solutions for securely managing large datasets. Together, these innovations address key challenges in medical imaging, providing a comprehensive and future-proof solution for secure healthcare data management.

1.2 An Overview of Medical Image Security

Medical images, including X-rays, magnetic resonance imaging (MRI), computed tomography (CT) scans and ultrasounds, examples of which are illustrated in Figure 1.1 (sourced from the MedPix database of the National Library of Medicine (18)),

are essential tools in modern healthcare (4). These diagnostic modalities provide non-invasive methods for visualizing the human body, offering critical insights into anatomical and physiological conditions. They enable accurate diagnosis, treatment planning, and disease monitoring, making them indispensable in clinical practice (19). The transition from analog to digital imaging has revolutionized the field, enabling efficient storage, retrieval, and analysis of medical data.



(a) X-ray (b) CT (c) US (d) MRI

Figure 1.1: A Comparative Overview of Common Medical Imaging Modalities.

1.2.1 Medical Imaging Modalities

Key imaging modalities underpinning modern diagnostics include MRI, CT, PET, ultrasound, and radiography. MRI relies on magnetic fields and radio waves to produce high-resolution images of soft tissues, while CT scans utilize X-rays to generate detailed cross-sectional views. PET imaging provides metabolic information by detecting radiotracers, and ultrasound employs high-frequency sound waves to visualize internal organs and soft tissues (20). The digitization of these modalities enhances their integration into e-healthcare systems, enabling seamless connectivity, remote access, and streamlined clinical workflows.

1.2.2 Necessity of Security in E-Healthcare

The digitization of medical imaging has significantly improved healthcare delivery while also presenting new challenges regarding the security and privacy of data. With the widespread adoption of electronic health records (EHRs), telemedicine platforms, and cloud storage solutions, the risk of data exposure has notably

increased. It is essential to protect the confidentiality and integrity of medical images to safeguard patient privacy, uphold trust in healthcare systems, and mitigate the potential misuse of sensitive information (21). Unauthorized access to these images can impact the accuracy of diagnoses and result in negative clinical outcomes. Moreover, altered or tampered images can pose threats to both patients and healthcare providers, underscoring the critical need for effective security measures. Ensuring the secure management of medical data is crucial in supporting the increasing reliance on digital technologies within contemporary healthcare.

1.2.3 Risks and Challenges

The security of medical imaging is confronted with substantial threats, particularly concerning the confidentiality and integrity of sensitive information. Cyberattacks that focus on undermining the confidentiality of medical images including unauthorized access, interception during data transmission, and breaches of information pose grave risks to patient privacy (22). Furthermore, manipulation and modification attacks intensify these issues by transforming medical images in ways that may result in erroneous clinical diagnoses or inappropriate medical treatments, thereby potentially jeopardizing patient health. Such attacks not only compromise the dependability of medical data but also erode trust in healthcare systems. Moreover, the challenge of ensuring confidentiality for patient data stored in conjunction with medical images continues to be paramount, as it necessitates the protection of both clinical and personal information from unauthorized breaches. Effectively addressing these risks is vital for preserving the integrity and security of digital healthcare infrastructures.

Achieving effective security for medical images necessitates a careful equilibrium between accessibility and safeguarding. Medical images must be easily accessible to support swift clinical decision-making; however, this accessibility must not jeopardize their privacy or integrity. To address these competing requirements, robust security frameworks that utilize encryption, digital watermarking, and decentralized storage solutions are vital. As digital medical images increase, establishing scalable, interoperable, and regulatory compliant security strategies becomes imperative. Such strategies are essential to the architecture of secure, patient-centered, and technologically advanced healthcare systems.

1.3 Watermarking in Medical Image Security

Watermarking plays a crucial role in safeguarding sensitive healthcare data against unauthorized disclosure and tampering. By seamlessly embedding identifying information, watermarking enhances traceability, ensures compliance with regulatory standards, and upholds the reliability of medical records. Consequently, it underpins trust across modern clinical workflows and processes.

1.3.1 What is Digital Watermarking?

Digital watermarking discreetly embeds hidden data into multimedia files such as images, audio, or video without noticeably altering their appearance or quality. Once in place, this embedded information can be extracted to confirm authenticity, protect copyrights, and discourage illicit sharing. Unlike overt logos or text, digital watermarks are usually imperceptible to viewers, yet they can remain intact through compression or file format changes. Recent studies highlight their vital role in high-stakes settings like healthcare and law enforcement, where data integrity must be assured (23). By combining cryptographic methods with signal processing, watermarking effectively encodes ownership details, detects tampering, and provides forensic evidence (24). As a result, it has become a cornerstone for maintaining security, reliability, and trustworthiness in today's digital environments.

Watermarking techniques can be broadly categorized into three domains, , as shown in Figure 1.2 (25):

1. **Spatial Domain Watermarking**: By embedding bits directly into pixel intensities or color values, spatial domain watermarking introduces only minor modifications, keeping inserted data nearly invisible (26). The Least Significant Bit (LSB) method modifies only the lowest-order bits of each pixel, preserving most of the original appearance. Because of its straightforward, efficient embedding, this approach is particularly suited for real-time or resource-constrained contexts (24). However, it can be vulnerable to compression, filtering, or geometric transformations, which disrupt or remove the

watermark (27). Despite these weaknesses, spatial domain watermarking remains widely favored when speed and simplicity take priority over robust resilience. In medical imaging, it enables rapid insertion of essential data, like patient or diagnostic details, directly into radiological images for efficient archiving and retrieval.

2. **Frequency Domain Watermarking**: Frequency domain watermarking embeds data into transformed versions of media, using approaches such as the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), or Discrete Wavelet Transform (DWT) (28). By altering selected frequency coefficients, it becomes more resilient to image operations like compression, filtering, or partial data loss. Compared with spatial methods, frequency-based techniques often exhibit higher durability, especially under heavy manipulation (29). Embedding in mid- or low-frequency bands further protects the watermark from common distortions and preserves imperceptibility. Although frequency transforms add computational overhead, studies since 2020 confirm their effectiveness in healthcare, media, and surveillance scenarios (30). Consequently, frequency domain watermarking remains the preferred option for robust and secure data embedding. This embedding balances invisibility with resilience across applications.

3. **Hybrid Domain Watermarking**: Hybrid domain watermarking combines spatial and frequency-based methods, leveraging their respective strengths (31). It involves partially transforming an image, modifying specific coefficients, and embedding additional bits directly into pixel values. This dual approach improves imperceptibility by altering low-frequency components while enhancing robustness through spatial redundancy. Such schemes are adaptable to various threats, making them ideal for applications like medical image protection and high-quality media distribution (32). Ultimately, hybrid techniques achieve a balance between computational efficiency, resilience, and visual quality preservation.

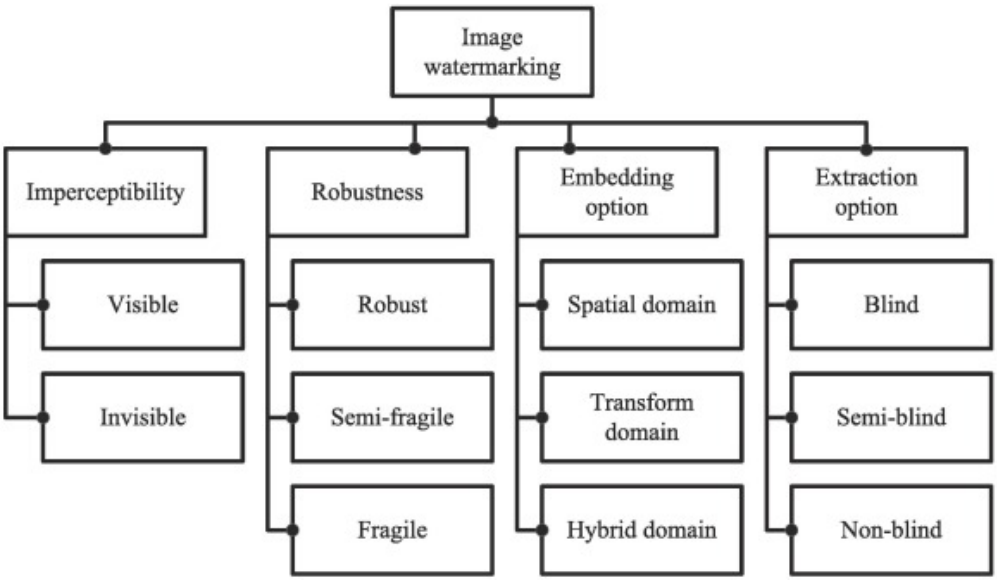


Figure 1.2: A Classification of Digital Image Watermarking Methods.

1.3.2 Applications of Watermarking in Medical Imaging

In medical imaging, watermarking serves as a dependable method to embed patient details, diagnostic codes, or timestamps into image data without affecting diagnostic quality (33). This ensures critical metadata remains permanently linked to the images, minimizing errors like mismatches or intentional alterations. Such capabilities are especially important in telemedicine, where images often move across various platforms and networks (34). Watermarking also enhances traceability, as embedded marks can identify instances of tampering, indicating when and where unauthorized changes occurred. As healthcare systems handle increasing amounts of digital medical data, watermarking provides an efficient and automated way to uphold the integrity, security, and reliability of medical images (35). This makes it a valuable tool for modern healthcare environments reliant on accurate and trustworthy imaging workflows.

1.3.3 Challenges in Medical Image Watermarking

Digital watermarking bolsters security and authenticity of medical data but faces various hurdles when integrated into healthcare imaging. First, to preserve diagnostic reliability, watermarks must remain imperceptible while resisting compression, noise, or other artifacts (36). Second, differing image dimensions, modalities, and color depths challenge universal watermarking solutions (32). Third, strict regulations demand robust encryption to safeguard patient privacy. Fourth, efficiency is critical in clinical settings that require rapid processing (37). Finally, typical operations such as cropping and scaling can degrade watermark integrity, spurring ongoing research into adaptive or hybrid methods for next-generation medical systems. Large data volumes require scalable solutions.

- **Imperceptibility vs. Robustness:** Achieving a balance between minimal distortion and resistance to attacks.
- **Diagnostic Quality Preservation:** Ensuring modifications do not compromise the diagnostic value of images.
- **Scalability:** Handling large datasets typical of healthcare environments efficiently.

1.3.4 The Discrete Wavelet Transform

The Discrete Wavelet Transform enables multi-resolution image analysis through spectral decomposition into hierarchical frequency subbands, mathematically formalized as:

$$X[n] = \sum_{k} \left(h[k] \cdot x[2n-k]\right) + \sum_{k} \left(g[k] \cdot x[2n-k]\right), \tag{1.1}$$

where $h[k]$ and $g[k]$ denote quadrature mirror filters for low-frequency (approximation) and high-frequency (detail) component extraction, respectively. This decomposition produces four directional subbands per level: LL (low-low), LH (low-high), HL (high-low), and HH (high-high), corresponding to spatial orientation selectivity horizontal, vertical, and diagonal edge representations (38; 39).

The subband derivation process employs cascaded filtering operations:

$$\begin{aligned}
\text{LL} &= \mathcal{L} \circ \mathcal{L}(I), \\
\text{LH} &= \mathcal{H} \circ \mathcal{L}(I), \\
\text{HL} &= \mathcal{L} \circ \mathcal{H}(I), \\
\text{HH} &= \mathcal{H} \circ \mathcal{H}(I),
\end{aligned}$$

where $\mathcal{L}$ and $\mathcal{H}$ represent low-pass and high-pass decomposition operators applied to host image I.

Multi-scale analysis is achieved through iterative decomposition of the approximation coefficients. As depicted in Figure 1.3, a second-level DWT further partitions the LL subband into:

$$\begin{aligned}
\text{LL2} &= \mathcal{L} \circ \mathcal{L}(\text{LL}), \\
\text{LH2} &= \mathcal{H} \circ \mathcal{L}(\text{LL}), \\
\text{HL2} &= \mathcal{L} \circ \mathcal{H}(\text{LL}), \\
\text{HH2} &= \mathcal{H} \circ \mathcal{H}(\text{LL}).
\end{aligned}$$

The LL2 subband, containing over 70% of the image's energy (40), is prioritized for watermark embedding due to its maximal energy concentration and inherent stability against signal processing perturbations. This strategic selection ensures watermark invisibility while preserving robustness against compression artifacts and noise interference critical for medical image authentication systems.

Mathematically, the second-level approximation coefficients are computed via:

$$LL2[n] = \sum_{k} \left(h_2[k] \cdot LL[2n-k]\right) + \sum_{k} \left(g_2[k] \cdot LL[2n-k]\right), \tag{1.2}$$

where $h_2[k]$ and $g_2[k]$ represent optimized second-stage filters for successive approximation refinement. This hierarchical decomposition facilitates strategic information embedding in perceptually optimized coefficients, achieving dual objectives of visual transparency and resistance to geometric/radiometric distortions (41; 42).

The 2-level DWT architecture (Figure 1.4) provides enhanced spectral isolation compared to single-level decomposition, enabling precise watermark placement in frequency bands least affected by common image processing operations. This multi-scale approach synergizes with human visual system characteristics, where

low-frequency components dominate perceptual recognition, thereby ensuring watermarked content maintains diagnostic fidelity in healthcare applications.

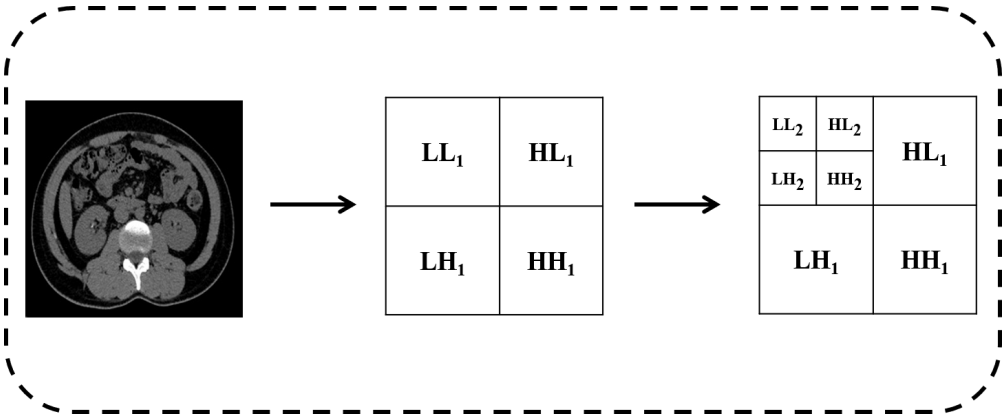


Figure 1.3: Two-Level Discrete Wavelet Decomposition.

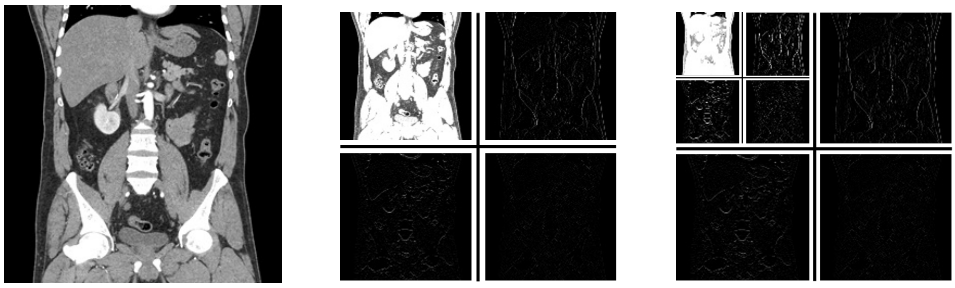
1.3.5 LSB-Based Watermark Embedding

The Least Significant Bit (LSB) modification technique encodes auxiliary data by manipulating the lowest-order bits of pixel intensity values. The embedding operation is formalized as:

$$I'(x, y) = I(x, y) \oplus \Delta(W(n)), \tag{1.3}$$

where $I'(x, y)$ denotes the watermarked pixel, $I(x, y)$ the host pixel intensity, $W(n)$ the n-th watermark bit, and $\oplus$ symbolizes the bitwise insertion operator. As illustrated in Figure 1.5, the Multi-Layered Security Framework implements this method within the Level-2 LL2 (Low-Low) subband of DWT, exploiting the spectral characteristics of approximation coefficients for stealthy data insertion (43).

This approach is particularly advantageous for compressed watermark payloads comprising binary feature vectors (44), as it optimizes embedding capacity while maintaining perceptual fidelity. The LL2 subband's energy concentration ensures watermark resilience against common signal processing operations, as high-frequency distortions predominantly affect detail coefficients. Strategic LSB modification in this spectral region achieves dual objectives:



(a) (b) (c)

Figure 1.4: 2D Wavelet Decomposition: (a) Original Medical Image. (b) 2D-DWT at the First Level. (c) 2D-DWT at the Second Level.

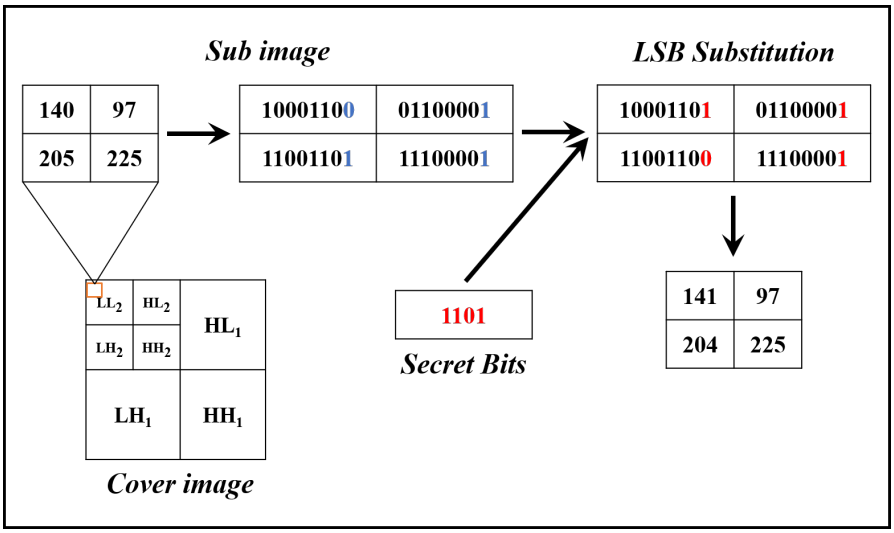


Figure 1.5: Replacement Diagram of LSB.

- Imperceptibility through minimal alterations to perceptually dominant low-frequency components.
- Robustness by leveraging the inherent stability of approximation coefficients against compression artifacts (45).

The framework's computational efficiency stems from direct bit-plane manipulation, avoiding complex transformations during embedding. Experimental validations confirm that LL2-LSB integration preserves diagnostic quality in medical images while enabling reliable watermark extraction critical for authentication in healthcare data systems.

1.3.6 Arnold Cat Map

The Arnold Cat Map (ACM) constitutes a discrete nonlinear transformation widely employed in cryptographic image processing applications. Mathematically, this bijective mapping operates over a two-dimensional discrete grid, commonly represented by the transformation matrix in Equation (1.4):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod n, \tag{1.4}$$

where (x, y) and (x', y') denote the original and transformed pixel coordinates, respectively, and n corresponds to the spatial dimensionality of the host image.

In image security frameworks, ACM induces pseudorandom pixel permutations through its ergodic properties, introducing nonlinear chaotic perturbations that enhance robustness against adversarial attacks such as statistical analysis and geometric distortions. For digital watermarking, ACM facilitates secure data embedding by iteratively scrambling the spatial distribution of both host image pixels and watermark signals. During embedding, the watermark, typically encoded as a binary payload, is diffusely integrated into the transformed image domain. Subsequent extraction leverages iterative inverse transformations to recover the embedded payload, ensuring fidelity even under compression or noise interference. This cryptographic dispersion mechanism renders ACM particularly effective for applications demanding tamper detection, copyright verification, and integrity assurance in secure multimedia distribution and digital authentication frameworks (46).

As illustrated in Figure 1.6, ACM exhibits deterministic periodicity, wherein repeated applications cyclically restore the image to its initial configuration. The periodicity is contingent upon the spatial dimensions of the host image: larger resolutions necessitate increased iterations to complete the cyclical permutation sequence. This intrinsic reversibility ensures lossless recovery of original content while maintaining cryptographic security through controlled iteration counts, thereby balancing computational efficiency with robust data protection (47; 12).

1.4 Biometrics in Medical Image Security

Biometrics relies on unique physical or behavioral traits such as fingerprints, irises, and facial features to verify an individual's identity. These characteristics are distinctive, stable over time, and challenging to forge, which makes them particularly useful for authentication in healthcare systems (48). Integrating biometrics makes patient data more secure and less vulnerable to unauthorized access. In e-health contexts, biometric solutions reduce administrative errors and streamline recordkeeping, ensuring that sensitive medical data is accessible only to the correct person (49). As telemedicine grows, the need for robust and reliable patient identification further highlights the importance of biometric-based security.

1.4.1 Fingerprint-Based Watermarking

Fingerprints are a popular biometric marker due to their uniqueness, permanence, and universality, making them ideal for bolstering medical image security (50). During **feature extraction**, distinct ridge patterns and minutiae are identified, often using techniques like Binary Statistical Image Features (BSIF) for high accuracy. Next, **compression** reduces the fingerprint's data size, preserving key details while minimizing storage demands and transmission overhead. Finally, in the **embedding process**, the compressed feature set is discreetly embedded into the medical image typically within the low-frequency LL sub-band if wavelet transforms are used or via LSB substitution in spatial approaches. This combination balances imperceptibility and robustness, ensuring the watermarked medical image retains its diagnostic quality and resists tampering or unauthorized modifications.

Binarized Statistical Image Features (BSIF)

The Binarized Statistical Image Features (BSIF) approach represents an advanced paradigm in fingerprint feature extraction, demonstrating significant improvements over conventional texture analysis methods including Local Binary Patterns (LBP) (51), Histograms of Oriented Gradients (HOG) (52), and Local Phase

Quantization (LPQ) (53; 54; 55). This methodology employs Independent Component Analysis (ICA) to learn a bank of statistically independent linear filters from natural image datasets. When applied to fingerprint images through convolutional operations, these optimized filters encode local textural patterns into compact binary representations that exhibit remarkable discriminative power (56). Empirical evaluations of various filter configurations revealed the Laplacian of Gaussian (LoG) operator (57) as particularly effective for fingerprint analysis due to its dual noise suppression and edge enhancement capability.

The LoG filter integrates Gaussian smoothing with second-order derivative computation, mathematically expressed as a two-stage process. First, a Gaussian kernel $G(x, y, \sigma)$, defined by:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}, \tag{1.5}$$

where σ governs the spatial extent of smoothing and attenuates high-frequency noise. Subsequently, the Laplacian operator is applied to this smoothed representation:

$$\nabla^2 G(x, y, \sigma) = \left(\frac{x^2 + y^2 - 2\sigma^2}{\sigma^4} \right) G(x, y, \sigma), \tag{1.6}$$

Amplifying regions of rapid intensity transition corresponding to ridge-valley structures in fingerprints. This synergistic combination enables precise localization of minutiae points while mitigating sensor noise artifacts (58).

BSIF transforms filter responses into binary codes through thresholding operations. For each pixel i, the binary feature b_i is determined by:

$$b_i = \begin{cases} 1 & \text{if } s_i > 0 \\ 0 & \text{otherwise,} \end{cases} \tag{1.7}$$

where $s_i = W_i \cdot x$ represents the inner product between the i-th learned filter W_i and the local image patch x. The complete feature extraction process is formalized as follows:

$$s_i = \sum_{u,v} W_i(u, v) \times X(u, v) = w_i^T x, \tag{1.8}$$

utilizes vectorized representations of filters (w_i) and image patches (x) for computational efficiency. Aggregating these binary codes into histogram-based descriptors yields illumination-invariant representations that preserve discriminative texture information under varying acquisition conditions (59).

This binary encoding paradigm offers three principal advantages:

- Compact feature dimensionality through bit-string representations.
- Enhanced robustness to non-linear intensity variations.
- Computational efficiency suitable for real-time applications.

When applied to fingerprint watermarking, BSIF-derived features generate compact yet highly distinctive templates that optimize embedding capacity while maintaining authentication accuracy (60). Figure 1.7 illustrates the transformation from original fingerprint images to BSIF-encoded representations, demonstrating the method's ability to preserve critical structural information.

The method's superiority stems from its data-driven filter optimization process, which adaptively captures salient fingerprint characteristics rather than relying on handcrafted feature detectors. This property makes BSIF particularly effective for contactless fingerprint recognition systems where pose variations and partial captures present significant challenges (60). By combining statistical learning with efficient binary encoding, BSIF establishes a robust framework for secure biometric watermarking that outperforms traditional techniques in both recognition accuracy and computational overhead.

Algorithm 1 BSIF feature extraction from fingerprint images.

Require: Input:

Fingerprint image W

Filter size s

Standard deviation σ

Threshold T_C

Ensure: Binary feature image W_BSIF

1: Load the fingerprint image $W(x, y)$ in grayscale

2: Apply Otsu's thresholding to $W(x, y)$ to obtain binary image $B(x, y)$:

$$B(x, y) = 1 \text{ if } I(x, y) \geq T$$

$$B(x, y) = 0 \text{ if } I(x, y) < T$$

3: Generate the $\text{LoG}(x, y)$ filter with size s and standard deviation σ

$$\text{LoG}(x, y) = \left(\frac{x^2 + y^2 - 2\sigma^2}{\sigma^4} \right) \exp\left(-\frac{x^2 + y^2}{2\sigma^2} \right)$$

4: Convolve the binary image $B(x, y)$ with the LoG filter $\text{LoG}(x, y)$ to obtain convolution result $C(x, y)$

$$C(x, y) = B(x, y) * \text{LoG}(x, y)$$

5: Threshold the BSIF feature responses using T_C to obtain binary feature image $W_BSIF(x, y)$:

$$W_BSIF(x, y) = 1 \text{ if } C(x, y) \geq T_C$$

$$W_BSIF(x, y) = 0 \text{ if } C(x, y) < T_C$$

6: Save and return the binary feature image $W_BSIF(x, y)$

Algorithm 1 details the operational workflow for deriving BSIF descriptors from fingerprint based watermark images. The visualization in Figure 1.7 demonstrates the feature encoding pipeline using an 8-bit binary string length and a 5×5 BSIF

convolution kernel. The transformation sequence comprises: (a) the source biometric capture (Figure 1.7a), (b) intermediate binary mapping through adaptive thresholding (Figure 1.7b), and (c) the finalized BSIF-encoded template emphasizing ridge-valley minutiae (Figure 1.7c). Feature extraction concentrates exclusively on the fingerprint's Region of Interest (ROI) to optimize computational resources and preserve discriminative patterns.

The dimensional efficiency of this approach is quantified through the compression metric:

$$\text{Dimensional Compression} = \left(1 - \frac{D_c}{D_o}\right) \times 100\% \tag{1.9}$$

Where:

- D_c: Compressed feature dimensionality
- D_o: Original image data dimensionality

Experimental implementation achieved a dimensional compression factor of 69.25%, as calculated in Equation (1.9). This substantial size reduction enables efficient watermark embedding while maintaining fidelity to the host image's structural integrity, a critical requirement. The compact BSIF representation is advantageous for MLSF architectures, where patient fingerprint watermarks require optimized storage before lossless compression protocols.

This methodology addresses two critical challenges in biometric watermarking:

- Minimizing payload size without compromising authentication features.
- Ensuring compatibility with healthcare data standards through perceptually lossless encoding.

The BSIF derived templates retain sufficient discriminative power for robust patient identification while reducing computational overhead in subsequent processing stages.

1.4.2 Palmprint-Based Watermarking

Palmprints offer another reliable biometric option, as they capture rich, intricate patterns of ridges and lines in the hand (12; 61). A key step involves **Gabor filtering**, highlighting essential textural features by emphasizing edges and ridges while reducing noise. After filtering, **binary conversion** translates these enhanced details into a more compact format suited for watermark embedding. Once transformed, palmprint data can be imperceptibly inserted into medical images using wavelet or spatial methods, ensuring minimal impact on visual integrity. This approach demonstrates notable **robustness** under common distortions such as compression or minor geometric transformations. By incorporating palmprint-based watermarks, e-health systems benefit from strong patient identification and reduced data manipulation or fraudulent alteration risk.

1.4.2.1 Gabor Filter

The Gabor filter, a complex linear filter in image processing, is extensively utilized for texture and spatial frequency analysis in computer vision applications. Its efficacy in biometric recognition systems, such as fingerprint and palmprint authentication, stems from its capacity to resolve fine structural details and extract discriminative features. The filter is mathematically defined by a sinusoidal plane wave modulated by a Gaussian envelope, expressed as:

$$G(x, y; \lambda, \theta, \psi, \sigma, \gamma) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right) \cos\left(2\pi \frac{x'}{\lambda} + \psi\right),$$

where x and y denote spatial coordinates; λ specifies the sinusoidal wavelength; θ governs orientation; ψ defines the phase offset; σ regulates the Gaussian envelope's scale; and γ adjusts ellipticity (62). Gabor filters function as orientation- and frequency-selective convolutional kernels in biometric applications. Convolution operations with these kernels decompose an image into localized texture components, effectively capturing ridge orientations, minutiae points in fingerprints, and palmar flexion creases in palmprints (63). This multi-scale, multi-directional analysis isolates salient features invariant to illumination variations, generating robust

representations for identification. Integrating Gabor-filtered features into biometric templates enhances matching accuracy by emphasizing unique topological characteristics, as illustrated in Figure 1.8. Consequently, Gabor-based methodologies significantly improve the reliability of automated recognition systems, establishing them as a cornerstone in advanced image processing architectures for security-critical applications.

1.4.3 Other Biometric Modalities

Beyond fingerprints and palmprints, various biometrics also enhance watermarked medical images. **Iris scans** rely on the complex patterns within a person's iris, offering high distinctiveness and resilience against aging (64; 65). Similarly, **facial recognition** uses unique facial contours and distances between landmarks to create a recognizable digital signature (66). Although these approaches may be more sensitive to lighting or pose variations, they provide valuable solutions in specific healthcare environments. Integrating multiple biometric modalities can further strengthen identification accuracy, accommodating diverse patient scenarios while upholding data security and authenticity.

1.5 Blockchain Technology in Medical Image Security

Blockchain is a decentralized ledger technology that records transactions across a network of nodes, ensuring data cannot be retroactively altered without changing subsequent blocks. Typically operating on a peer-to-peer architecture, it uses consensus mechanisms to verify each block, fostering trust without a central authority. Because every node maintains a copy of the ledger, single points of failure are eliminated, improving resilience and security (67). In healthcare contexts, blockchain's transparent and tamper-resistant structure provides an ideal platform for managing sensitive data, reducing operational inefficiencies, and enabling verifiable trust among critical stakeholders.

1.5.1 Key Features of Blockchain

Blockchain's core strengths lie in four interrelated features, as illustrated in Figure 1.9.

- **Decentralization** disperses control among multiple nodes rather than relying on a central authority, thereby mitigating single points of failure.
- **Immutability** ensures data blocks, once finalized, cannot be overwritten or deleted, preserving an unalterable audit trail (68; 69).
- **Transparency** arises because every node maintains its own copy of the ledger and can view transaction details, fostering accountability across the network.
- **Smart Contracts** automate predefined processes such as granting access rights or triggering events based on coded rules stored on the blockchain. By executing these programs when certain conditions are met, smart contracts facilitate trustless, self-enforcing agreements without centralized oversight (70).

Together, these attributes reinforce data integrity and verifiability, elevating blockchain's potential in applications such as secure medical imaging.

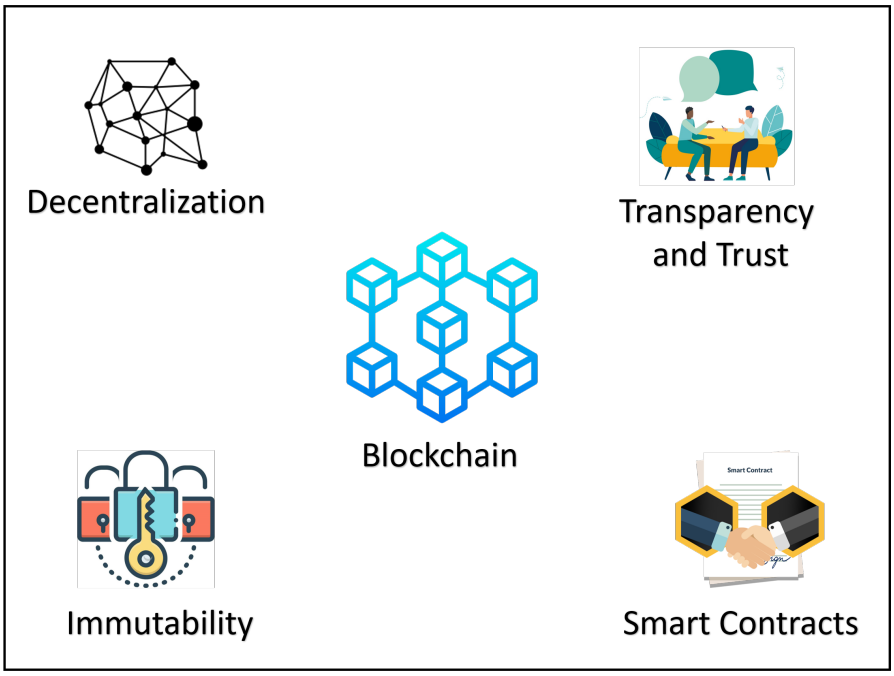


Figure 1.9: Advantages of Blockchain.

1.5.2 Blockchain in Healthcare

Blockchain technology rapidly reshapes how medical data is protected and shared across diverse healthcare systems. By decentralizing record management, it removes single points of failure and ensures a higher level of security. Each data transaction is validated by consensus mechanisms, preserving authenticity and privacy. This shift enables trustworthy collaboration among hospitals, insurers, and patients, improving coordination and integrity overall.

- **Secure Storage:** By encrypting and distributing patient records across multiple nodes, blockchain offers robust storage that prevents single-point vulnerabilities (30). Authorized users can retrieve data with decryption keys, while any unauthorized attempt to modify records fails consensus validation. This design ensures medical images and patient details remain safe from hacking, corruption, accidental loss, and unauthorized breaches.
- **Traceability:** Each medical image transaction is timestamped and cryptographically hashed, leaving an audit trail on the distributed ledger (71).

Any revision triggers a new entry, allowing healthcare providers to pinpoint the exact timing, source, and nature of changes for thorough accountability.

- **Interoperability:** Blockchain's uniform data format and distributed validation simplify exchanging patient records among hospitals, labs, and insurers. This shared ledger reduces fragmentation, harmonizes workflows, and promotes seamless collaboration across healthcare stakeholders.

1.5.3 Integration with Watermarking

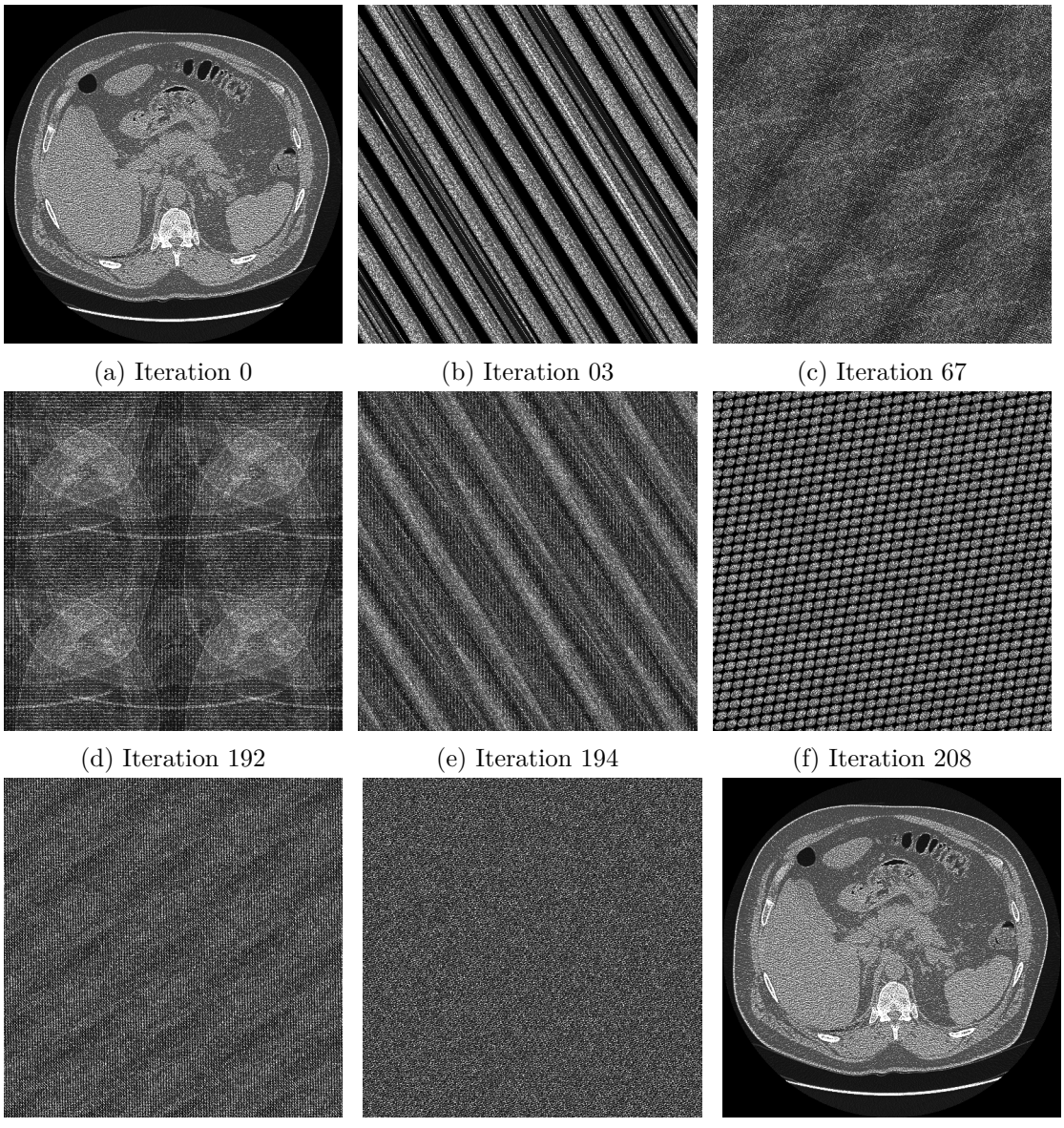
Combining blockchain with watermarking produces a more resilient framework for safeguarding medical images. Once a watermark is embedded into the image to verify ownership or authenticity, blockchain records the transaction details, establishing a tamper-proof timeline (72). Any subsequent alterations trigger updates on the ledger, immediately flagging suspicious changes. Meanwhile, blockchain's immutable properties protect critical metadata such as encryption keys or hashed fingerprints against tampering, thus preserving access control. Smart contracts can further automate restrictions by granting or revoking rights based on predefined rules (73). This synergy keeps medical images secure at every step, watermarking defends content integrity within the image itself, and blockchain reinforces transparency and traceability at the ledger level, ensuring compliance with strict healthcare data standards.

1.6 Conclusion

This chapter presents the core elements underpinning modern medical image security, emphasizing the synergistic roles of digital watermarking, compression, encryption, and blockchain technologies. Watermarking improves data integrity by embedding hidden identifiers that remain resistant to tampering. Compression techniques optimize storage and transmission without compromising diagnostic fidelity; encryption protects sensitive patient information against unauthorized access, preserving privacy within distributed healthcare infrastructures. The decentralized blockchain framework further strengthens immutability and traceability, offering a tamper-proof ledger for secure data transactions. These collective

innovations address critical vulnerabilities, promoting trust, accountability, and operational efficiency in e-health systems.

Subsequent chapters will expand on these foundational principles, introducing advanced solutions designed to meet emerging security challenges and guiding the development of a robust, patient-centric healthcare ecosystem.



(a) Iteration 0 (b) Iteration 03 (c) Iteration 67

(d) Iteration 192 (e) Iteration 194 (f) Iteration 208

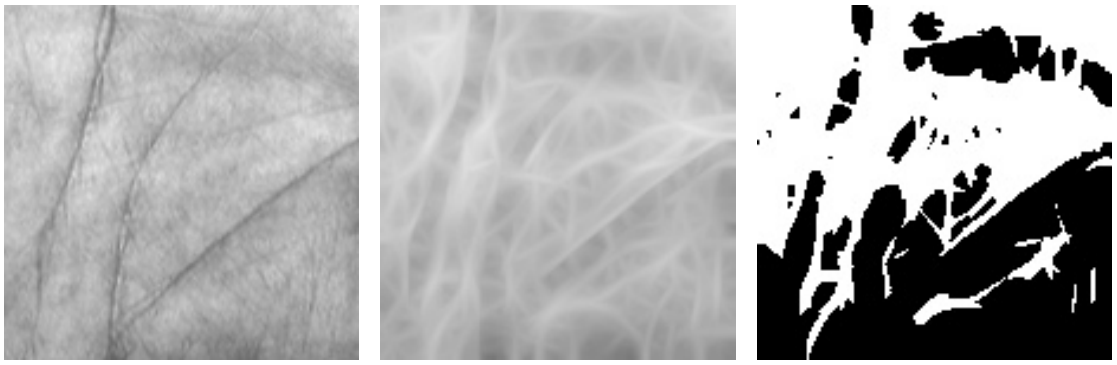
(g) Iteration 287 (h) Iteration 334 (i) Iteration 384

Figure 1.6: Applying ACM Iterations.



(a) Original Watermark (b) Binary Watermark (c) BSIF Watermark

Figure 1.7: Visualization of BSIF-based Feature Extraction Pipeline.



(a) Palmprint Image (b) Gabor Features Palmprint (c) Enhanced Binary Image

Figure 1.8: The Extracted Features from the Palmprint Image using the Gabor Filter.

Chapter 2

Related Works

This chapter comprehensively examines the latest studies focused on medical image watermarking aimed at securing e-Health applications. It delves into various methodologies based on spatial, frequency, and hybrid domains, emphasizing their roles in ensuring data integrity, resisting tampering, and safeguarding copyright. Through an analysis of contemporary advancements, this chapter situates the proposed frameworks within the broader context of the field and pinpoints areas requiring improved security in e-Health.

2.1 Introduction

In recent years, e-healthcare has evolved significantly, enabling real-time diagnostics, remote monitoring, and data-driven decision-making. Central to these advancements is the secure management of medical images, which is crucial for diagnosing and treating patients. The most common medical images are X-rays, MRIs, and CT scans; protecting them from unauthorized access and manipulation is paramount.

This chapter comprehensively reviews existing research on medical image security in e-healthcare applications, focusing on key elements such as watermarking techniques, compression and encryption methods, and blockchain-based approaches for traceability and immutability. Examining the strengths and limitations of these methods identifies the current gaps and sets the foundation for the solutions proposed in this thesis.

2.2 Review of Medical Image Watermarking Techniques

In securing medical images, watermarking techniques are essential to preserve the durability and authenticity of patient information while it is transferred or stored. This section thoroughly examines various watermarking methods designed to protect sensitive patient data. Our study assesses notable watermarking strategies for the process we propose. We discuss research proposals related to our contribution, focusing on their methodologies, findings, and potential limitations.

Our study analyzes representative watermarking approaches compared to the proposed method to provide a comprehensive evaluation. These techniques are categorized into spatial, frequency, and hybrid domains, and they are also categorized through another categorization based on watermarking approaches ranging from non-blind to blind and semi-blind schemes. We highlight the unique features of each category, offering a detailed analysis that underscores their strengths and weaknesses relative to our approach.

2.2.1 Non-Blind Watermarking

Non-blind watermarking schemes require the original host image during the extraction process. This requirement allows for precise watermark recovery and robust detection, However, it presents challenges related to the storage and retrieval of the original image. Several notable works have proposed innovative, non-blind watermarking strategies for medical images.

Ajib Susanto et al. (74) introduced a hybrid approach that integrates the Discrete Cosine Transform (DCT) and a two-level Haar Wavelet Transform (HWT). In this method, the host image is decomposed into its frequency subbands using two-level HWT, with emphasis placed on the LL2 subband where core image information is concentrated. This subband is partitioned into 4×4 blocks, and DCT is applied to each block. The watermark is embedded by modulating the DC coefficients with a scaling factor α, improving robustness and imperceptibility. Such a dual-transform technique optimizes the selection of the embedding domain. Similarly,

Pandey et al. (75) also explored color watermarking within the Y channel using a two-level Lifting Wavelet Transform (LWT) combined with Singular Value Decomposition (SVD) To enhance the embedding process further. These methods underscore the importance of aligning watermarking techniques with human visual perception to maintain the diagnostic quality of medical images. Further contributions include the work of Manasi Jana et al. (76), who proposed a self-embedding fragile watermarking scheme designed explicitly for tamper detection and recovery. Their method involves segmenting the original image into 4×4 blocks and generating watermarks from each pixel's six most significant bits (MSB) of each pixel. Blocks are classified based on pixel similarity: smooth regions use the mean as recovery data, whereas complex areas are processed using Absolute Moment Block Truncation Coding (AMBTC) to preserve vital image features. The recovery data are then embedded into the 2 LSB of the corresponding block, ensuring that any tampering can be detected and the original image can be recovered with minimal distortion.

Another significant contribution is the dual-image Reversible Data Hiding (RDH) technique that Lu et al. (77) presents. Their approach increases the embedding capacity by encoding secret data as two-digit base-9 numbers and embedding these into two cover images. Although this technique diverges from traditional watermarking schemes, its ability to reversibly embed a large amount of data without significant quality degradation makes it a noteworthy strategy for sensitive medical imagery. Laouamer et al. (78) proposed an innovative watermarking approach based on the Local Binary Pattern. LBP is employed to identify regions of interest within the host image, constructing a watermark that captures the essential texture features. By using linear interpolation for watermark embedding, the method ensures that the texture details of the medical image are preserved, which is a critical factor for maintaining diagnostic accuracy.

The principal advantage of non-blind watermarking is the enhanced robustness and minimal visual distortion achieved by leveraging the original host image. However, the need for the original image during extraction increases storage and logistical complexity, which can be a significant challenge in resource-constrained or real-time medical systems.

2.2.2 Blind Watermarking

Blind watermarking schemes overcome the limitations of non-blind methods by eliminating the need for the original host image during the extraction process. This feature simplifies storage requirements and can facilitate deployment in scenarios where the original image is not available. However, blind techniques must balance the trade-off between imperceptibility and robustness, as the absence of the original image can sometimes reduce the watermark's resilience to attacks.

Soleymani et al. (79) introduced a blind watermarking method that leverages the ACM for image scrambling. The ACM serves to randomize the host image, enhancing the security of the watermark embedding process. In this approach, watermark bits are embedded using weakly correlated pseudo-noise strings in the high-frequency coefficients generated by the Fast Discrete Curvelet Transform (FDCuT). The randomness introduced by the ACM and the use of a high-frequency domain Not only does it ensure a high level of imperceptibility, but it also adds a layer of protection against common signal processing attacks. Khaled Hebbache et al. (80) developed a blind watermarking system for medical imaging, utilizing image gradients and Discrete Wavelet Transform (DWT). Image gradients created a topological map to identify disruption-prone areas, while DWT ensured robustness and imperceptibility. The watermark was embedded in the DWT-decomposed image's low-low (LL) band, targeting 3×3 blocks selected by gradient data. Gradient direction and magnitude relationships were analyzed to identify relevant blocks, and their codes were combined with the watermark using XOR, embedding them into the blocks with LSB technique.

Kahlessenane et al. (38) developed another blind watermarking method specifically for CT scans. In their approach, the host image is decomposed using DWT, and the LL subband coefficients are reorganized using ZigZag scanning to maximize embedding capacity in areas less susceptible to visual distortion. Patient data as a hash is then embedded into these reorganized coefficients. In (81), the authors utilized a secure and blind watermarking algorithm based on Integer Wavelet Transform (IWT), LSB, and chaotic sequences (ILC) for high-capacity watermarking of grayscale images. Chaotic sequences ensured encryption and determined embedding locations. Due to its diagnostic sensitivity, the image was divided into the region of interest and non-interest, with no embedding in the ROI.

An integrity check record (ICR), derived from ROI features, detected tampering. Encrypted ICR data and patient information were embedded in middle-frequency IWT sub-bands, while the physician's signature was embedded in the robust LL3 sub-band for authentication.

Despite the advantages of blind watermarking, challenges persist. One significant drawback is that blind techniques may be more vulnerable to severe signal processing operations or attacks, as the absence of the original image during extraction can limit recovery precision. Additionally, the selection of embedding regions often determined by pseudo-random generators can sometimes lead to statistically detectable distortions, especially if the embedding occurs in uniform or "flat" regions of the host image.

2.2.3 Semi-Blind Watermarking

Semi-blind watermarking schemes seek to capture the best of both non-blind and blind approaches by reducing dependency on the original image while still incorporating some additional reference data to aid in watermark extraction. These schemes aim to improve both robustness and imperceptibility by carefully balancing the requirements of watermark embedding and extraction.

Kumar et al. (82) proposed a semi-blind technique that integrates multiple watermarking strategies. Their method employs edge detection and information entropy analysis to determine optimal embedding regions, ensuring that the watermark is placed in areas that are less sensitive to visual distortion. LWT is then used to decompose the image, and an alpha blending scheme is applied to embed the watermark into color images. To further secure the watermark, ACM is used to scramble the image prior to embedding. In another study, Jana et al. (83) introduced a semi-blind watermarking technique that employs image interpolation and bit reversal permutation to embed multiple secret messages into a cover image. The process begins with encrypting the hidden messages, which are then partitioned and embedded into a cover image generated by interpolating the original image. Notably, this method minimizes image distortion while achieving high embedding capacity. During extraction, the cover image is regenerated from the

watermarked image, allowing for the accurate recovery of the encrypted messages without requiring the original cover image.

Zear et al. (84) proposed another semi-blind approach that combines the LWT, DCT and SVD. The host image undergoes a 3-level LWT decomposition, after which the LH3 and LL3 subbands are transformed using DCT followed by SVD. MD5 hashing is applied before the transformation process, and Hamming coding is used to protect the textual watermark data to enhance security. Furthermore, some approaches exploit spatial domain techniques alongside chaotic maps. For instance, Munir et al. (85) introduced a semi-blind watermarking scheme for medical images that integrates Chaotic Map-based Arnold's Cat Map with a differential evolution (DE) method for data embedding.

Recent developments have also seen the emergence of deep learning-based watermarking methods. Although these approaches offer superior feature extraction and adaptive embedding capabilities, manually designed watermarking techniques remain highly valued. The transparency, lower computational overhead, and ease of debugging associated with manually crafted approaches are particularly beneficial in resource-constrained environments typical of medical imaging systems.

2.3 Compression and Encryption in E-Health Systems

As e-health systems continue to evolve, the need to secure vast amounts of medical data has driven the integration of advanced compression and encryption techniques. These methodologies are essential for safeguarding patient privacy and ensuring the efficient storage and transmission of medical images across distributed networks. This section explores recent advances in compression and encryption methodologies related to e-health systems, focusing on their application in watermarking and secure data management.

2.3.1 The Role of Compression in Medical Image Security

Medical images are often high-resolution and require significant storage space, making data compression an indispensable tool in e-health systems. Compression techniques such as DCT, DWT, and FDCuT are routinely employed to reduce data redundancy without significantly affecting image quality. These techniques improve storage efficiency and facilitate faster transmission across healthcare networks, which is vital in telemedicine and real-time diagnostics.

Wang et al. (86) were among the early researchers to explore the use of compression in watermarking techniques. Their work combined zero-watermarking with blockchain technology, ensuring that the medical images remain unaltered while still embedding essential watermark information. Faiza Huma et al. (87) developed an algorithm combining watermarking and encryption techniques to securely conceal a patient's confidential information. The study proposed generating an initialization vector (IV) to encrypt the patient's data using the Advanced Encryption Standard (AES) in output feedback mode. The watermark was embedded into the image using a wavelet-based DWT technique alongside the LSB substitution method.

2.3.2 Encryption Techniques for E-Health Data Security

Encryption plays a critical role in safeguarding sensitive medical data, ensuring the information remains unintelligible even if unauthorized access is gained. Over the years, various encryption algorithms have been integrated into e-health systems to protect medical images and the associated metadata. AES and SHA-256 are among the most commonly used encryption methods in this domain.

In the context of watermarking, several researchers have introduced encryption mechanisms to further secure the embedded watermark. Anand et al. (40), who designed a robust method for embedding patient information into medical images. Their technique involves a multi-level transform strategy that employs the DWT and SVD to combine the advantages of both frequency domains. To further enhance robustness, Hamming coding is applied to the textual watermark data before embedding. After watermark embedding, the image undergoes encryption

using a chaotic encryption algorithm and is compressed via LZW. This approach provides robust watermark extraction while maintaining the integrity and quality of the original image. Similarly, Alsehli Abrar et al. (73) proposed a secure image authentication method where the watermark is first embedded into the third-level DWT coefficients and subsequently encrypted using AES. The encrypted watermark is then hashed using SHA-256 before being stored on a blockchain, adding an additional layer of security.

Encryption is also applied during the compression stage. For instance, Ernawan et al. (88) integrated an adaptive scaling factor in the watermark embedding process based on the host image's DWT-DCT coefficients. Although primarily designed to optimize watermark embedding, the adaptive scaling process inherently complements encryption strategies by ensuring that any modifications to the image remain within acceptable visual thresholds, even after compression.

2.3.3 Integrating Compression and Encryption with Watermarking

The convergence of compression, encryption, and watermarking has given rise to sophisticated hybrid systems that enhance data security while preserving image quality. One notable approach is the integration of zero-watermarking with encryption, as demonstrated by Wang et al. (89) and further expanded in subsequent studies. In these systems, the watermark is not directly embedded into the image data; a key derived from the image's features is stored on a blockchain. The original image remains unaltered, thereby eliminating the compression-induced artifacts that can arise from traditional watermark embedding.

Another example is the method proposed by Chen Lanxiang et al. (90), where the watermark (in the form of a QR code) is generated from concatenated diagnosis results and image hashes. The watermark is then embedded in the DCT domain of the image. Following watermark embedding, the image is encrypted and subsequently stored on a blockchain. This process ensures the image is compact and maintains its integrity and confidentiality.

It is important to note that the synergy between compression and encryption in e-health systems also facilitates efficient data transmission in telemedicine applications. For example, when medical images are transmitted across networks with limited bandwidth, compression ensures quick delivery, while encryption guarantees that the data remains confidential during transit. In scenarios where real-time diagnosis is required, such as in emergency care, the efficiency gained through compression and the security ensured by encryption are critical to maintaining patient trust and data integrity.

2.4 Blockchain in Healthcare: Traceability and Immutability

Blockchain technology has emerged as a transformative tool in healthcare, offering decentralized solutions for ensuring data integrity, traceability, and secure data sharing. The immutable nature of blockchain ledgers provides an ideal platform for managing sensitive medical records, including watermarked medical images and patient identity data. This section reviews key blockchain-based approaches that have been proposed to secure medical data, enhance copyright protection, and facilitate traceability in healthcare systems.

2.4.1 Blockchain for Image Authentication and Copyright Protection

Early efforts to integrate blockchain with medical image security focused on eliminating the need for trusted intermediaries while ensuring data authenticity. In (89) leveraged the Ethereum blockchain combined with IPFS to address challenges associated with data expansion in blockchain systems. Their zero-watermarking approach avoided altering the image data while still embedding a unique signature that could be verified on the blockchain.

Chen et al. (86) proposed a framework for image copyright protection that combined a zero-watermarking technique with blockchain and IPFS. Traditionally, zero-watermarking relied on a trusted third party for storage, which introduced

security and reliability concerns. To address these issues, the authors eliminated the need for a third party by utilizing blockchain's decentralized and tamper-proof features, ensuring secure and dependable storage of zero-watermark data. IPFS enabled efficient storage and sharing of large files, while smart contracts were utilized to manage copyright information, image queries, and transactions, promoting transparency and trust. Another innovative approach is presented by Fang et al. (91), who introduced a block watermarking technique that embeds keys into all image blocks, forming a linear cyclic chain. In this method, each block contains a watermark derived from adjacent blocks, ensuring any tampering can be localized and verified. Block-based watermarking provides enhanced traceability and an effective mechanism for detecting unauthorized modifications when combined with blockchain storage.

In addition to watermarking, Meng et al. (92) proposed a copyright management system that integrates digital watermarking with blockchain technology. Their system also employs perceptual hash functions, QR codes, and decentralized storage via IPFS. Recording watermark information and timestamps on a tamper-resistant blockchain provides robust copyright protection and simplifies the ownership verification process.

2.4.2 Blockchain for Medical Image Traceability and Verification

The traceability of medical images is crucial for ensuring that the images used in diagnosis and treatment are authentic and unaltered. Several studies have explored using blockchain to track and verify medical images throughout their lifecycle.

Mannepalli et al. (93) extended this concept by developing a blockchain-supported framework that integrates invisible watermarking with encryption. In their system, the watermark is embedded into the edge components of the image via edge detection on the DWT coefficients. The encrypted watermark is stored on the blockchain, which provides an additional layer of protection against tampering. Li et al. (94) further advanced blockchain-based methods by proposing a scheme

designed explicitly for compressively sensed images. Their method combines multimedia watermarking with compressed sensing, IPFS, and blockchain technologies. The approach leverages the confidentiality of compressed sensing and the decentralization of blockchain to offer a robust solution for securing large-scale medical image databases.

2.4.3 Combining Blockchain with Encryption and Compression

Integrating blockchain with encryption and compression techniques provides a comprehensive security framework for medical images. Such systems address the dual challenge of maintaining data integrity during storage and transmission and ensuring that the images remain accessible and verifiable across distributed networks.

Alghamdi et al. (95) contributed to this field by presenting a database watermarking method that uses blockchain as a trusted intermediary. Their method reduces reliance on centralized authorities by storing copyright information and verification data on an immutable blockchain ledger.

Blockchain-based systems also address the challenge of scalability. As medical data grows exponentially, decentralized storage solutions such as IPFS, when combined with blockchain, offer a promising solution to handle large datasets by ensuring that compressed and encrypted medical images are stored off-chain (in systems like IPFS). At the same time, critical verification data is kept on-chain. These systems maintain efficiency without sacrificing security.

2.4.4 Challenges and Future Directions

Although blockchain-based systems enhance transparency, several concerns remain unresolved. Scalability is vital as the volume of medical images continues to climb. Large file sizes and the cost of storing data on-chain remain significant barriers, pushing designs toward off-chain solutions like IPFS. In addition, real-time performance is essential for urgent care scenarios, which require further

optimization of consensus mechanisms or protocols that interface with medical imaging archives.

Integration complexities also arise. Legacy healthcare systems, especially smaller clinics, may struggle with adopting novel protocols. Standardized frameworks and interfaces that elegantly merge watermarking, encryption, compression, and blockchain are still in development. Beyond that, privacy laws and regulations differ internationally, complicating uniform deployment.

In the future, converging deep learning with blockchain-based watermarking could automate tamper detection. Machine learning models might learn to **'recognize'** legitimate watermarks and automatically flag unauthorized changes. Similarly, adaptive algorithms that fine-tune compression or encryption parameters in real-time, based on changing bandwidth or user demands, could further streamline the e-health data flows.

2.5 Synthesis and Comparative Analysis

The reviewed literature, as summarized in Tables 2.1 and 2.2, illustrates an evolution from simple watermarking methods to sophisticated hybrid systems that combine watermarking, compression, encryption, and blockchain technologies. Our proposed approaches provide complementary perspectives on securing medical images and ensuring data traceability in e-health systems.

The application of blockchain technology marks a significant advancement in addressing the challenges of data traceability and immutability. Researchers can eliminate reliance on centralized authorities by decentralizing the storage of verification data and embedding critical information (such as watermarks and hashes) onto blockchain ledgers. Blockchain provides an immutable record that can be used to verify image authenticity, trace any modifications, and ensure compliance with regulatory requirements.

The proposed methods, MLSF and IDAW, comprehensively address the significant challenges identified in previous medical image verification and traceability studies. Prior approaches have been hindered by blockchain data expansion, complex implementations, scalability issues, and vulnerability to attacks. At the same

Table 2.1: Summary of Existing Studies on Medical Image Watermarking

Reference	Watermarking Type	Techniques / Domains	Key Advantages	Limitations
Susanto et al. (74)	Non-blind	DCT + Two-level of HWT; focuses on LL2 subband	- Enhances robustness and imperceptibility - Optimizes embedding region	- Requires the original image during extraction - Additional storage overhead
Pandey et al. (75)	Non-blind	Color watermarking in Y channel (YCbCr) + Two-level LWT + SVD	- Preserves diagnostic quality - Suitable for color images	- Needs the original image - Complexity in storage and retrieval
Manasi Jana et al. (76)	Non-blind	Self-embedding fragile watermark; AMBTC-based tamper detection; 4×4 blocks	- Enables localization of tampering - Partial recovery possible through self-embedding	- Original image required for exact recovery - Overhead from storing block features
Lu et al. (77)	Non-blind (Dual-Image RDH)	Two-digit base-9 encoding + reversible data hiding in two separate cover images	- Increases embedding capacity significantly - Maintains overall image quality	- Requires two cover images - Still dependent on original references for complete reversibility
Laouamer et al. (78)	Non-blind	LBP for ROI identification; linear interpolation for embedding	- Good preservation of texture details - Maintains medical diagnostic features	- Must have an original image for extraction - Lacks additional encryption
Soleymani et al. (79)	Blind	ACM + FDCuT in high-frequency bands	- Strong image scrambling via ACM - High imperceptibility in high-frequency embedding	- Vulnerable if uniform regions are chosen inadvertently - No explicit integration with encryption or blockchain
Hebbache et al. (80)	Blind	Image gradients + DWT; embeds watermark in LL band using 3×3 blocks selected by gradient data	- Robust against disruptions by targeting gradient-based blocks - Uses LSB for minimal visual distortion	- Gradient-based block selection may be imprecise - No separate encryption or blockchain
Kahlessenane et al. (38)	Blind	DWT + ZigZag scanning in LL subband; patient data hash embedding	- Large embedding capacity - Low distortion by reorganizing LL coefficients	- Not combined with encryption - Single-transform approach can be less robust under severe attacks
Nazari et al. (81)	Blind	IWT, LSB, chaotic sequences; ROI vs. non-ROI separation	- Protects ROI by excluding it from embedding - Chaotic sequences add encryption randomness	- Complexity from separate ROI handling - Blind mode may reduce robustness under heavy modifications
Kumar et al. (82)	Semi-blind	LWT + alpha blending + edge detection + entropy + ACM	- Minimizes reliance on full host image - Targets visually active regions to reduce distortion	- If reference data is compromised, a scheme may be vulnerable - No blockchain-based long-term traceability
Jana et al. (83)	Semi-blind	Image interpolation + bit reversal permutation + encryption	- High embedding capacity - Eliminates the need for an original image via an interpolated cover	- Interpolation overhead - Lacks a broader security framework
Zear et al. (84)	Semi-blind	3-level LWT, DCT, SVD, plus MD5 hashing and Hamming coding	- Multiple transforms enhance resilience - MD5 + Hamming coding increases the security of textual watermark	- Partial host-image data still used - No blockchain for external traceability

Table 2.2: Summary of Existing Studies on Medical Image Watermarking (Continued)

Reference	Watermarking Type	Techniques / Domains	Key Advantages	Limitations
Munir et al. (85)	Semi-blind	Spatial-domain watermark + chaotic map + differential evolution	- Chaos-based scrambling offers good security - Does not require storing the original image	- Complexity in DE parameter tuning - No explicit compression or advanced encryption
Wang et al. (89)	N/A (Compression + Blockchain)	Zero-watermarking + blockchain + IPFS; minimal image alteration	- Image remains unaltered - Decentralized verification removes reliance on TTP	- No direct watermark embedding in the image - Potential IPFS overhead and complexity
Faiza Huma et al. (87)	N/A (Encryption)	DWT + LSB substitution + AES in output feedback mode	- Solid confidentiality for patient info - Combines wavelet embedding + encryption	- No blockchain integration - Storage scaling issues not directly addressed
Anand et al. (40)	Blind / Encryption-Integrated	DWT + SVD + chaotic encryption + LZW compression; Hamming coding for watermark text	- Robust synergy of transforms and encryption - Effective against channel noise	- Lacks blockchain for traceability - Potentially high computational overhead
Alsehli Abrar et al. (73)	N/A (Encryption + BC)	3-level DWT embedding + AES + SHA-256 + blockchain	- Multi-layer security approach - Tamper-proof via blockchain	- Single-transform approach - Potential scaling issues for large data volumes
Ernawan et al. (88)	N/A (Encryption)	Adaptive scaling factor in DWT-DCT domain; complements encryption	- Embedding intensity scaled adaptively - Maintains fidelity post-compression	- No blockchain for external verification - Not explicitly a blind or semi-blind scheme
Chen et al. (86)	N/A (Blockchain)	QR code watermark + DCT embedding + encryption + blockchain	- Integrates watermark + encryption + BC - Improved tamper resistance	- Possible overhead if the QR region is targeted - No mention of transform synergy (e.g., wavelet + DCT)
Fang et al. (91)	N/A (Blockchain)	Block watermark + linear cyclic chain; blockchain storage of keys	- Local tampering easily detected - High traceability of each block	- Potential overhead from block-wise indexing - Not specialized for wavelet or transform-based embedding
Meng et al. (92)	N/A (Blockchain)	Digital watermark + blockchain + perceptual hashes + QR codes + IPFS	- Robust copyright management - Timestamping and tamper-resistant storage	- High multi-tech complexity - Potential data expansion in large repositories
Mannepalli et al. (93)	N/A (Blockchain)	Invisible watermarking + edge detection (DWT) + blockchain	- Suited for tamper detection - Data on-chain to ensure authenticity	- Does not detail wavelet subband selection or compression - Overhead if many edges are watermarked
Li et al. (94)	N/A (Blockchain)	Multimedia watermarking + compressed sensing + IPFS + blockchain	- Addresses large-scale data - Decentralized authentication	- High complexity - Real-time or partial reference not detailed
Alghamdi et al. (95)	Database Watermarking	Blockchain as trusted intermediary; copyright info stored on-chain	- Tamper-proof ledger reduces single-point failure - Simplifies verification	- Not specifically transform-based for medical imaging - Overhead can be large with big databases

time, reliance on machine learning and intricate transformations often resulted in excessive computational overhead.

Our MLSF framework strategically integrates blockchain, watermarking, compression, and AES-256 encryption to enhance overall security, integrity, and traceability in real-world applications. It also aims to minimize computational overhead and simplify deployment in standard clinical workflows, which is particularly beneficial for hospitals managing large imaging databases.

Complementarily, our IDAW method introduces two critical innovations: first, by applying the Arnold Cat Map to shuffle the host image, it embeds the watermark during the iterative process, thereby achieving minimal distortion through the optimal iteration selection; and second, by concentrating on embedding within non-flat regions specifically those characterized by edges and contours as determined by wavelet analysis it significantly improves robustness while minimizing visual impact. MLSF and IDAW collectively overcome previously reported shortcomings by merging these conceptual pillars. High-level encryption, blockchain-based traceability, wavelet-domain insertion, and iterative chaotic scrambling converge to produce an integrated framework that meets the complex needs of e-health security.

2.6 Conclusion

This chapter reviewed foundational and emerging scholarship on medical image security, spotlighting the interplay among watermarking, compression, encryption, and blockchain-based traceability. Each watermarking category, non-blind, blind, and semi-blind, offers distinct strengths and constraints, revealing trade-offs in storage feasibility, computational overhead, imperceptibility, and tamper resilience. Meanwhile, compression and encryption remain vital in e-health, expediting the secure transmission of large images. Blockchain adds decentralized, immutable records that bolster trust among healthcare stakeholders by eliminating single points of failure.

Although research has advanced considerably, the continuing shift of medical systems to digital platforms, ongoing imaging innovations, and the global push for

data exchange underscores the need for solutions capable of handling enormous data volumes. Additionally, as machine learning–driven watermarking evolves, interpretability and efficient resource use remain essential, preventing undue complexity.

Against this backdrop, the methods proposed in this thesis MLSF and IDAW approaches address these complexities by embedding watermarks in minimally distorted regions, leveraging transforms and chaos-based encryption, and integrating blockchain verification. They offer practical avenues toward more secure, reliable medical imaging workflows. They pave the way for data protection and real-world healthcare adoption.

Chapter 3

The Proposed Contributions

This chapter outlines the significant contributions of this research in advancing medical image watermarking for secure e-health applications. The presented contributions stem from two published works addressing critical data security, integrity, and robustness challenges. The contributions are organized into thematic areas reflecting the advancements made in this thesis.

3.1 Introduction

The contributions presented in this chapter collectively address significant challenges in secure medical imaging. This research enhances the robustness, security, and traceability of medical image watermarking by developing novel frameworks and techniques, offering scalable and efficient solutions for secure e-health applications.

The first significant contribution of this research is developing a multi-layered security framework for medical image security. The framework integrates multiple technologies, including compression, digital watermarking, symmetric encryption, and blockchain, to ensure the security and traceability of medical images. Using the DWT and LSB techniques, a compressed fingerprint watermark is embedded into the LL2 sub-band of the host image. This approach achieves remarkable imperceptibility, evidenced by a peak signal-to-noise ratio (PSNR) of 63.24 dB and a structural similarity index (SSIM) of 1. Blockchain technology is employed with AES-256 encryption and IPFS decentralized storage to enhance data integrity

and prevent tampering. This ensures the reliability and transparency of data in e-health systems, offering a secure and scalable solution for real-world medical image management.

A second key contribution is designing a robust semi-blind watermarking technique that combines ACM and DWT to embed palmprint watermarks. This technique balances imperceptibility and robustness, addressing critical challenges in mitigating integrity attacks. The experimental results demonstrate excellent performance, with a PSNR of 53.95 dB and an SSIM of 0.99996, indicating minimal distortion in the host image after watermark embedding. The technique is computationally efficient, with embedding and extraction times of 0.01218 seconds and 0.006875 seconds, respectively, making it particularly suitable for real-time applications. By leveraging ACM's chaotic properties and the multi-resolution capabilities of DWT, the method ensures resilience against noise interference, compression, and filtering attacks.

This research further contributes by enhancing the robustness of medical image watermarking against a wide range of common attacks. The techniques proposed in this work effectively safeguard watermarked images from adversarial manipulation, including compression and noise interference. Robustness is achieved by embedding the watermark in the DWT-transformed host image's stable and low-frequency LL2 sub-band, ensuring resistance to high-frequency distortions. Using AES-256 encryption and blockchain technology adds a layer of security, ensuring immutability and traceability.

Preserving the diagnostic quality of medical images has been a critical focus throughout this research. Both proposed methods were rigorously evaluated using standard quality metrics such as PSNR and SSIM to ensure that the embedded watermarks did not compromise the visual or diagnostic integrity of the medical images. By targeting the LL2 sub-band for watermark embedding, the research achieves a high degree of imperceptibility while maintaining the original image's usability for diagnostic purposes.

Finally, the proposed frameworks and techniques were designed with practical applications in mind, particularly for e-Health systems. The MLSF integrates seamlessly with hospital IT systems and insurance platforms, providing a secure

and transparent mechanism for sharing sensitive medical images. With its computational efficiency, the semi-blind watermarking technique is especially suited for deployment in resource-constrained environments, ensuring that advanced security measures are accessible in diverse healthcare settings. These contributions collectively address the challenges of security, robustness, and scalability, making significant advancements in medical image watermarking for secure e-health applications.

3.2 Proposed Schemes

3.2.1 The Multi-Layered Security Framework Specifications

The proposed Multi-Layered Security Framework (MLSF) incorporates structured procedures, as depicted in Figure 3.1, which outlines the watermark embedding process. Initially, the watermark, represented by a fingerprint, undergoes preprocessing, converting it into a binary image. The BSIF technique is then applied to extract distinctive features, resulting in a binary matrix representation of these features. A second-level Discrete Wavelet Transform is performed for the host image before embedding the watermark using the method described in Equation (96). This section elaborates on the MLSF watermarking algorithm, divided into two primary phases: embedding and extraction. Inserting and retrieving the watermark involves multiple sequential steps, culminating in the encryption of the watermarked image and its secure storage within a blockchain system. This approach ensures robust data integrity, authentication, and protection against unauthorized access.

3.2.1.1 Binary Matrix Compression with Integrity Verification

Compressing a Binary Statistical Image Features-based watermark prior to its integration into the host medium is essential for optimizing imperceptibility and ensuring robustness against distortion or tampering (97). This preprocessing step reduces the watermark's payload, thereby minimizing its perceptible impact on the host media while retaining its structural and informational integrity.

The proposed methodology involves decomposing the binary matrix into two distinct vectors, $\boldsymbol{H}$ (horizontal summary) and $\boldsymbol{V}$ (vertical summary), which collectively encapsulate the spatial distribution of the binary data. The compression efficiency of this approach is quantified by the ratio $R_{yy} = \frac{100}{m \times n}$, where m and n denote the dimensions of the initial binary matrix (98). This mathematical framework ensures a balance between data compactness and fidelity, enabling seamless embedding without compromising the watermark's detectability or resilience in subsequent authentication processes.

Algorithm 2 Binary Matrix Compression

Require: Binary matrix M of size $m \times n$, where $M[i][j]$ represents the element at the i^{th} row and j^{th} column

Ensure: Vectors H and V, and hash value $Hash(M)$

1: Initialize $H = [0] * m$, where m is the number of rows in M $V = [0] * n$, where n is the number of columns in M

2: Compute Horizontal Summary H

3: **for** each row i in M, calculate $H[i]$ as follows **do**

$$H[i] = \sum_{j=1}^{n} M[i][j]$$

▷ where $H[i]$ represents the total count of 1's in the i^{th} row

4: **end for**

5: Compute Vertical Summary V

6: **for** each column j in M, calculate $V[j]$ as follows **do**

$$V[j] = \sum_{i=1}^{m} M[i][j]$$

▷ where $V[j]$ represents the total count of 1's in the j^{th} column

7: **end for**

8: Generate Hash of Matrix M Compute $Hash(M)$, a unique identifier for M

9: Return the horizontal and vertical summaries (H and V), and $Hash(M)$

Algorithm 2 optimizes the storage requirements for the matrix M by compressing it into its row and column summaries (H and V), while ensuring data integrity and uniqueness through the incorporation of $Hash(M)$. This approach is particularly advantageous for applications that demand efficient storage and robust integrity verification, such as blockchain-based data storage systems.

The recovery process, outlined in Algorithm 3, reconstructs the original binary matrix M from its compressed representation, which includes the horizontal and vertical summaries (H and V) and the hash value $Hash(M)$. By leveraging these summaries and the hash, the algorithm identifies a matrix configuration corresponding to the compressed data.

Algorithm 3 Binary Matrix Recovery

Require: Vectors H and V, and hash value $Hash(M)$
Ensure: Binary matrix M of size $m \times n$
1: **Initialize** an empty matrix M' of size $m \times n$ with all elements set to zero
2: **function** RECONSTRUCT MATRIX
3: **for** each possible configuration of M' that matches the summaries H and V **do**
4: **Fill** M': Ensure the sum of 1's in each row and column matches $H[i]$ and $V[j]$ respectively.
5: **Compute** $Hash(M')$: Calculate the hash of the current configuration of M'.
6: **Check Match**: If $Hash(M') = Hash(M)$, then M' is the correct reconstruction of M.
7: **end for**
8: **end function**
9: **Return** M': Once a match is found where $Hash(M') = Hash(M)$, return M' as the reconstructed matrix

The described methodology employs the horizontal and vertical summaries (H and V) in conjunction with the cryptographic hash value $Hash(M)$ to reconstruct the original matrix. This is achieved by systematically exploring potential matrices that satisfy the predefined constraints derived from these parameters. The algorithm guarantees the fidelity of the recovered matrix M' to the original matrix M by validating the congruence of the computed summaries and the hash value, ensuring compliance with the integrity conditions.

This reconstruction mechanism holds significant importance in domains necessitating rigorous data integrity assurance, such as blockchain-based systems, where precise and dependable data reconstruction is essential for preserving transactional transparency and trustworthiness.

$$M' = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

H (count of $1's$ in each row) is:

$$H = [3, 2, 4, 2, 3]$$

V (count of $1's$ in each column) is:

$$V = [3, 3, 3, 3, 2]$$

To reconstruct M, the process involves identifying a 5×5 matrix M' that aligns with the given row and column summaries H and V and matches the hash value $Hash(M)$.

During this process, each candidate matrix M' is evaluated to ensure it satisfies the specified number of $1's$ in each row and column, as defined by H and V. Additionally, if the hash value is available, it is verified that the hash of M' corresponds to $Hash(M)$, ensuring the accuracy of the reconstruction.

The time required to regenerate the watermark for a matrix of dimensions $W \times W$ can be determined using Equation (3.1):

$$T(W) = 2^{W^2} \times t_{\text{process}} \tag{3.1}$$

In this equation, 2^{W^2} represents the total number of possible matrices of size $W \times W$, while t_{process} denotes the time required to process each matrix. The processing time t_{process} is defined as the sum of t_{hash}, the time taken to compute the hash, and t_{compare}, the time required for comparison, both of which are constant values.

3.2.1.2 Embedding Process

A two-level DWT is applied to the host image, decomposing it into four distinct frequency sub-bands: LL2 (approximation), HL2 (horizontal details), LH2 (vertical details), and HH2 (diagonal details). The watermark is embedded within the LL2 sub-band, as it retains the most significant structural information of the original image in the spatial domain. The mathematical formulation of the DWT is expressed in Equation (3.2), providing a systematic approach to frequency domain transformation for watermarking applications.

$$C(j,k) = \sum_{n} \sum_{m} x(n,m)\psi_{j,k}(n,m) \tag{3.2}$$

In this formulation, $\psi_{j,k}(n,m)$ represents the wavelet basis functions, while $C(j,k)$ denotes the corresponding wavelet coefficients. Embedding the watermark within the LL2 sub-band, as defined in Equation (1.2), ensures the preservation of perceptual quality while enhancing robustness against various image processing operations.

The LL2 sub-band is particularly suitable for watermarking applications due to its high structural stability and reduced susceptibility to compression artifacts and high-frequency distortions. This characteristic makes it an optimal domain for embedding imperceptible yet resilient watermark information.

The watermark, represented by the vectors H and V, is embedded into the LL2 sub-band using the LSB modification technique, as defined by Equation (3.3). The modified pixel value P'_j is obtained by embedding a bit d_i into the original pixel P_j using the following operation:

$$P'_j = (P_j \,\&\, \sim 1)|d_i \tag{3.3}$$

where:

- P'_j denotes the pixel value after embedding the watermark bit.
- The bitwise AND operation (&) is used to clear the least significant bit (LSB) of P_j.

- The expression ~ 1 generates a bitmask that ensures the LSB is set to zero.
- The bitwise OR operation (|) assigns the LSB of P'_j to the watermark bit d_i.

This approach ensures efficient watermark embedding while maintaining the integrity and imperceptibility of the host image, thereby enhancing robustness against potential image manipulations.

Algorithm 4 Watermark Embedding

Require: Fingerprint image W, host image, and predefined parameters
Ensure: Watermarked image

1: Apply the BSIF method to the fingerprint image W to obtain the binary feature image W_BSIF
2: Compute the hash $Hash(W_BSIF)$ using the following equation:

$$Hash(M) = SHA - 256(\text{W_BSIF})$$

3: Perform matrix compression as described in Section 3.2.1.1 to derive the horizontal and vertical feature vectors H and V:

$$H[i] = \sum_{j=1}^{n} M[i][j] \quad , \quad V[j] = \sum_{i=1}^{m} M[i][j]$$

4: Apply second-level DWT to the host image and select the LL2 sub-band
5: Embed Vectors H and V into LL2 using the LSB method Equation (1.3)
6: Apply 2nd-level inverse DWT to obtain the final watermarked image

Algorithm 4 implements a systematic approach for embedding a watermark into the host image. Initially, the BSIF method is applied to the fingerprint image to generate its binary feature representation, followed by the computation of a cryptographic hash for integrity verification. A compression algorithm is then utilized to derive the horizontal and vertical feature vectors, H and V, from the binary feature matrix. These vectors are embedded within the LL2 sub-band of the host image using the LSB substitution technique. Finally, a second-level inverse DWT is performed to reconstruct the watermarked image while ensuring imperceptibility and robustness.

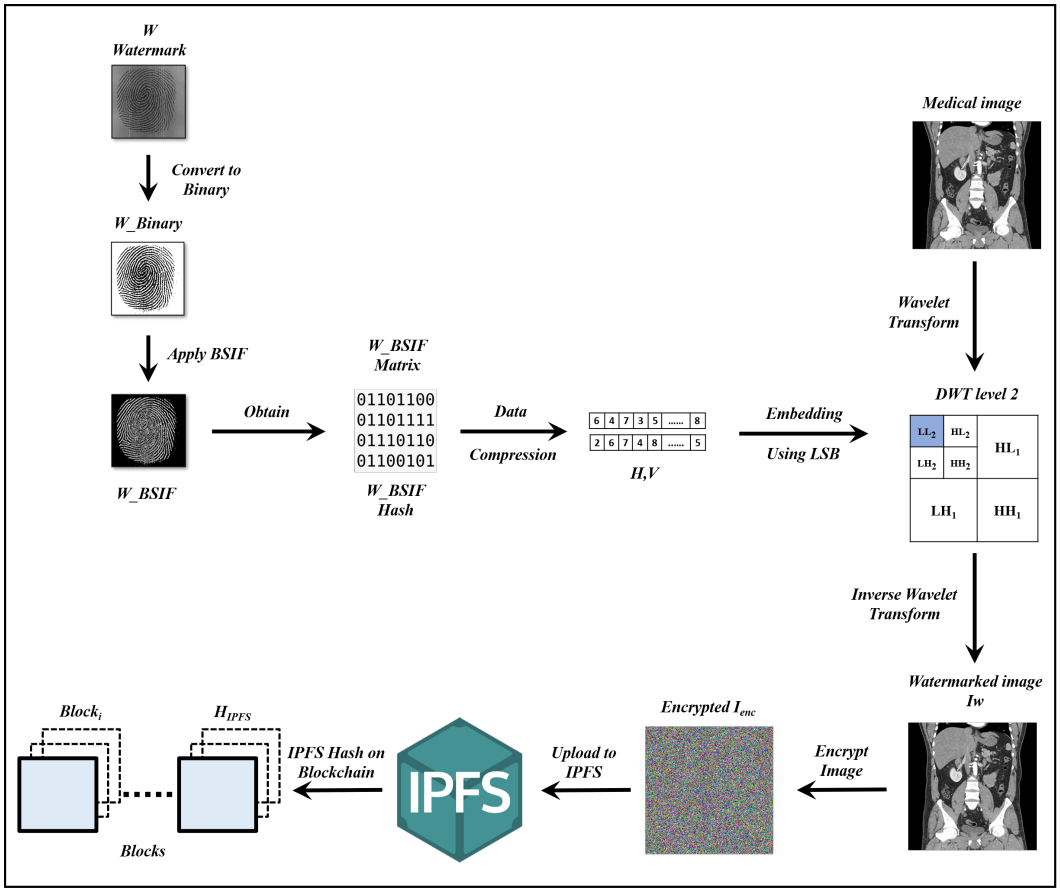


Figure 3.1: A Global Overview of the Blockchain-based Watermarking Process.

3.2.1.3 Secure Storage of Watermarked Images with Blockchain and IPFS

A secure and resilient storage framework for watermarked images can be established by integrating blockchain technology with the InterPlanetary File System (IPFS) and digital watermarking techniques. Specific security measures must be implemented to safeguard the confidentiality and integrity of images stored on IPFS. Given specific images' critical nature and sensitivity, particularly in medical applications, encryption or access control mechanisms are essential to prevent unauthorized access.

An encrypted storage scheme is proposed to enhance data security, ensuring that images remain protected while maintaining controlled visibility. In this approach, stored images are encrypted prior to being uploaded to the IPFS network, rendering them inaccessible without the appropriate decryption key. Upon retrieval, authorized users must possess the corresponding cryptographic key to decrypt and access the original image. This methodology strengthens data security, facilitates efficient image management, and ensures robust authentication of watermarked images. The procedural steps for implementing this secure storage strategy are outlined in Algorithm 5.

The secure storage and verification process for watermarked images begins with the input of the watermarked image (I_w), associated metadata (Info), and an encryption key (K). To ensure confidentiality, the image undergoes encryption using the Advanced Encryption Standard (AES), yielding the encrypted watermarked image I_{enc}, computed as:

$$I_{\text{enc}} = \text{AESencrypt}(I_w, K).$$

The encrypted image I_{enc} is then uploaded to the InterPlanetary File System (IPFS), generating a unique content identifier (CID), denoted as H_{IPFS}. A perceptual hash function is applied to I_w to further establish a unique reference, producing a unique identifier (UID).

A structured record, defined as $R = \{\text{UID}, \text{Info}, H_{\text{IPFS}}\}$, is subsequently created and recorded on the blockchain. This submission generates a blockchain transaction (T_x), ensuring the stored watermarked image's integrity, authenticity, and traceability.

Algorithm 5 Secure Storage of Watermarked Images.

Require: Watermarked image I_w, additional information $Info$, encryption key K

Ensure: Transaction ID Tx, IPFS hash H_{IPFS}

1: Encrypt the watermarked image I_w using the key K to obtain the encrypted image I_{enc}.
2: Upload I_{enc} to IPFS and receive the IPFS hash H_{IPFS}.
3: Generate a unique identifier (UID) using a perceptual hash function (e.g., DHA) on I_w.
4: Create a record R containing UID, $Info$, and H_{IPFS}.
5: Submit the record R to the blockchain and obtain the transaction ID Tx.

The integration of blockchain technology within the proposed MLSF provides a robust mechanism for safeguarding medical images through the following key functionalities:

- **Preservation of Image Integrity:** Blockchain ensures the immutability of medical images by preventing unauthorized alterations or tampering, thereby maintaining their authenticity after storage.
- **Decentralized Trust Management:** The distributed nature of blockchain facilitates secure image sharing among institutions without reliance on a centralized authority, thereby enhancing trust and security in inter-organizational data exchange.
- **Automated Access Governance:** Smart contracts enforce secure, automated access control mechanisms, regulating permissions dynamically and eliminating the need for manual intervention.

- **Transparent and Immutable Audit Trails:** Every interaction with stored image data is permanently recorded on the blockchain, ensuring comprehensive traceability of access and modifications, thereby enhancing accountability and compliance.

This structured approach leverages blockchain's cryptographic security and decentralized architecture to strengthen the reliability, privacy, and accessibility of medical image management.

A structured four-step process, depicted in Figure 3.2, is designed to secure watermarked images within the proposed framework. The process begins with encrypting each watermarked image, enhancing security by restricting access to authorized users. Advanced Encryption Standard (AES) encryption maintains data confidentiality and prevents unauthorized disclosure.

Upon encryption, the secured image is uploaded to the IPFS and assigned a unique content identifier (CID). This CID is generated from the file's cryptographic hash (99), enabling efficient and decentralized retrieval from any participating node within the IPFS network (100).

The generated hash is subsequently recorded on a blockchain to reinforce data integrity and ensure an immutable record of image ownership and storage location. This process establishes a transparent and tamper-proof ledger, safeguarding the stored watermarked images' authenticity, integrity, and copyright.

The MLSF provides significant advantages for medical imaging systems, particularly in facilitating secure image exchange, mitigating fraudulent activities, and maintaining data integrity. Its inherent scalability, supported by blockchain and IPFS, enables the efficient handling of large datasets typical of hospital information systems and insurance platforms, ensuring secure and verifiable medical data management.

AES is employed in encrypting watermarked images (101), providing high cryptographic security. The watermarked image is converted into an unreadable format through AES encryption, ensuring that only authorized entities possessing the correct decryption key can retrieve its original content. This encryption mechanism

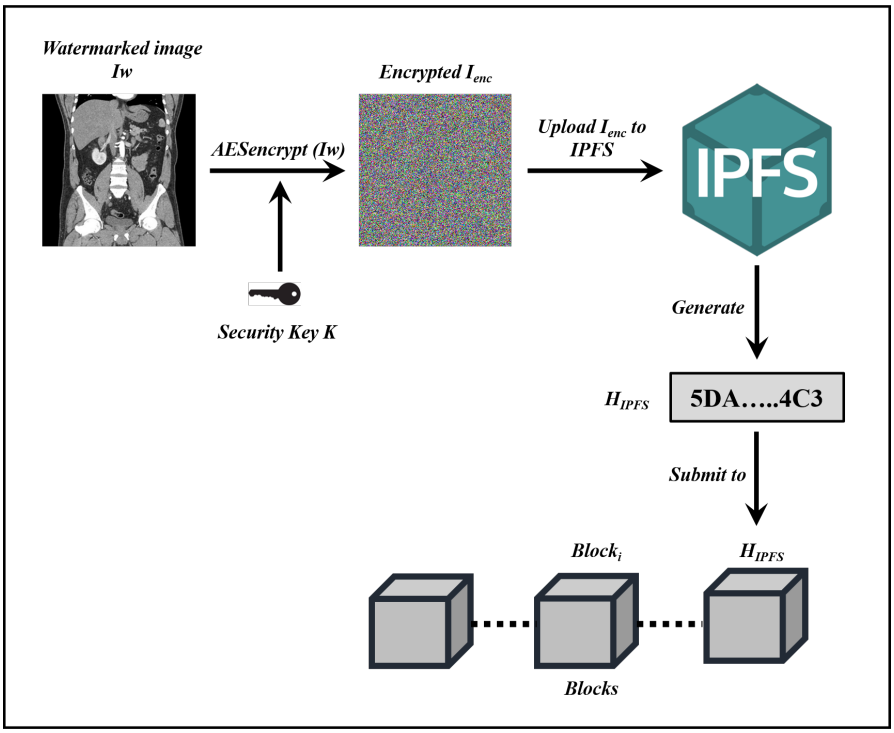


Figure 3.2: Blockchain and IPFS Integration Diagram to Store Watermarked Images.

enhances data confidentiality while reinforcing resistance against unauthorized access and tampering, thereby preserving the integrity and security of the embedded watermark.

3.2.1.4 Extraction Process

Figure 3.3 presents the structured process for extracting embedded watermarks. The encrypted watermarked image (I_{enc}), securely stored and shared via the blockchain, undergoes decryption using the AES-256 algorithm with the corresponding cryptographic key (Key). The decryption operation is expressed as:

$$I_w = \text{AESdecrypt}(I_{\text{enc}}, Key)$$

where I_w represents the retrieved watermarked image.

Following decryption, a second-level of DWT is applied to I_w to achieve multi-resolution decomposition. The LL2 sub-band, which contains the embedded feature vectors H and V, is isolated for further processing. The LSB extraction method, formulated in Equation (3.4), is then employed to recover the watermark by extracting the vectors H and V from the LL2 sub-band. This approach ensures the accurate retrieval of the embedded watermark while maintaining the integrity of the host image.

$$d_i = P'_j \,\&\, 1 \tag{3.4}$$

The following equation governs the extraction of the watermark bit d_i from the least significant bit of the modified pixel value P'_j. The extracted bit sequence is represented as $d_i = [d_1, d_2, \ldots, d_{N_H+N_V}]$, where N_H and N_V correspond to the lengths of the horizontal and vertical feature vectors, respectively.

The reconstruction of the watermark components is defined as follows:

- The horizontal feature vector is reconstructed as:

$$H = D[1 : N_H]$$

- The vertical feature vector is reconstructed as:

$$V = D[N_H + 1 : N_H + N_V]$$

This process ensures the accurate retrieval of the embedded watermark, preserving the structural integrity of the extracted information. When the lengths of the embedded feature vectors H and V are predetermined, they function as additional cryptographic keys for watermark extraction. The parameter N_H denotes the length of H in elements, while N_V represents the length of V in bits, facilitating precise reconstruction of the embedded watermark.

The structured procedure for extracting the watermark is outlined in Algorithm 6, ensuring methodical retrieval and verification of the embedded information.

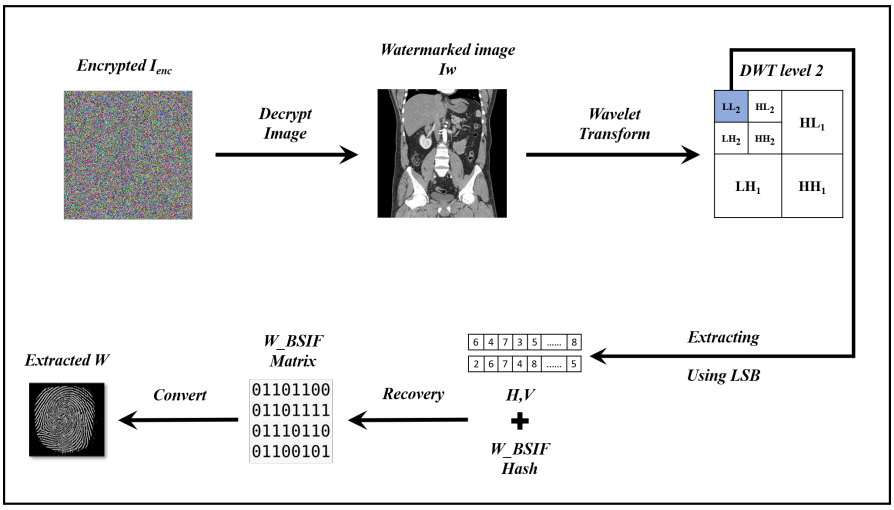


Figure 3.3: The Extraction Steps of the Multi-Layered Security Framework.

Algorithm 6 Watermark Extraction Process

Require: Watermarked image I_w

Ensure: Extracted binary watermark matrix

1: Apply second-level DWT to I_w and isolate the LL2 sub-band.
2: Extract the feature vectors H and V from the LL2 sub-band using LSB extraction method, as formulated in Equation (3.4).
3: Reconstruct Matrix M' from the extracted vectors H and V.
4: Check the match between $Hash(M)$ and $Hash(M')$. Repeat step 3 until the correct M' is obtained
5: Transform the reconstructed matrix M' to retrieve (W_BSIF) extracted.

MLSF ensures the reliable recovery of both the encrypted watermarked image and the extracted BSIF watermark. The encrypted watermarked image is securely stored and distributed via blockchain and IPFS, guaranteeing data integrity and retrieval in the event of corruption or malicious attacks 3.2.1.3.

For the BSIF watermark extraction, the recovery process involves verifying the integrity of the reconstructed binary feature matrix by comparing its cryptographic hash hash(M) with the hash of the reconstructed matrix hash(reconstruct M'). This validation ensures the accurate retrieval of the embedded watermark, maintaining robustness and reliability throughout the extraction process.

3.2.2 Improved DWT and ACM Watermarking Approach Specifications

This subsection delineates the technical specifications of the proposed IDAW watermarking framework, detailing its constituent components and methodological implementation. The scheme employs a structured approach, commencing with the application of ACM to the host image to introduce a level of transformation that enhances security. Subsequently, a single-level DWT is applied to the transformed image to facilitate multi-resolution analysis, optimizing the embedding process. The watermark is then systematically embedded using mathematically defined operations to ensure robustness and imperceptibility. This section provides a comprehensive exposition of the watermarking algorithm, encompassing both the embedding and extraction procedures, which are meticulously structured into sequential stages to maintain methodological integrity and computational efficiency.

3.2.2.1 Embedding Process

The initial phase of the watermark embedding process involves the application of the Arnold Cat Map to the host image, introducing a transformation that reorganizes pixel positions in a deterministic yet seemingly random manner. This transformation is mathematically expressed as iteration $i = \text{ACM}(I, i)$, where I represents the original image and i denotes the iteration index. Following this transformation, a single-level DWT is applied to decompose the transformed image into its respective frequency subbands, enabling efficient multi-resolution representation. The wavelet decomposition facilitates subsequent watermark embedding while preserving image integrity and enhancing robustness against distortions.

Equation (1.1) formally specifies the transformation coefficients. For a given input image matrix I at a particular iteration, the application of DWT results in the decomposition of the image into four distinct subbands: LL, LH, HL, and HH. These subbands correspond to different frequency components and directional details within the image, effectively capturing structural variations across multiple resolutions and orientations (10).

In the subsequent stage, the watermark W undergoes preprocessing using a Gabor filter, which enhances its feature extraction capability by capturing local texture details and prominent line structures within the palmprint. This initial transformation facilitates the identification of significant spatial variations, thereby improving the robustness of the watermarking process. The filtered output is mathematically represented as:

$$G_{\text{filter}}(P) = W_{\text{G}}$$

Following this, the processed watermark $G_{\text{filter}}(P)$ is converted into a binary format to ensure consistency in embedding:

$$W_{\text{binary}} = \text{convert_to_binary}(W_{\text{G}})$$

Subsequently, the binary watermark is embedded into the high-frequency HH subband of the transformed image iteration using a weighted linear combination, as expressed in Equation (3.5):

$$iw = (1 - t) \times W + t \times HH, \quad \text{where} \quad t \in]0, 1[. \tag{3.5}$$

Here, t serves as a tunable parameter governing the trade-off between watermark visibility and imperceptibility, ensuring minimal perceptual distortion while maintaining the integrity of the embedded watermark.

In this process, the parameter t is set to 0.98, ensuring an optimal balance between watermark visibility and imperceptibility. The parameter t is constrained within the range $0 < t < 1$, allowing for controlled modulation of the watermark's perceptibility. Following the embedding phase, the Inverse Discrete Wavelet Transform is applied to reconstruct the modified image. Specifically, IDWT is performed on the coefficient set (LL, LH, HL, iw), where iw represents the modified high-frequency subband incorporating the embedded watermark W within the HH component of the transformed host image (102). For $j \geq j_0$, the IDWT reconstruction process is mathematically defined as:

$$f(x) = \frac{1}{\sqrt{M}} \sum_{k} W_{\phi}(j_0, k)\phi_{j_0,k}(x) +$$

$$\frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_{k} W_{\psi}(j, k)\psi_{j,k}(x) \tag{3.6}$$

where $f(x)$, $\phi_{j_0,k}(x)$, and $\psi_{j,k}(x)$ are functions of the discrete variable $x = 0, 1, 2, \ldots, M-1$, with decomposition levels denoted by $j = 0, 1, 2, \ldots, J-1$ and frequency subbands indexed by $k = 0, 1, 2, \ldots, 2^j - 1$. The transformation coefficients are formally defined in Equation (3.6), ensuring an accurate reconstruction of the watermarked image while maintaining the integrity of embedded information.

Once the watermarked iteration is generated, it undergoes an additional transformation using ACM to finalize the iterative process, producing the fully watermarked image. The ACM is applied to the pixel coordinates of the host image, performing a deterministic scrambling operation that enhances security and resistance to attacks. The transformation is mathematically defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod M$$

where $\begin{bmatrix} x \\ y \end{bmatrix}$ denotes the original spatial coordinates of a pixel, $\begin{bmatrix} x' \\ y' \end{bmatrix}$ represents the transformed coordinates after applying ACM, and M corresponds to the image dimensions. This iterative mapping introduces a pseudo-random permutation of pixel positions while maintaining reversibility, facilitating secure watermark embedding and extraction.

This process is iteratively executed across multiple ACM transformations, where at each iteration $i+1$, the watermark embedding is adjusted to refine the transformation effect. The procedure continues until the predefined number of iterations is completed, generating a sequence of watermarked images corresponding to different ACM iterations. To determine the most perceptually optimized result, the Peak Signal-to-Noise Ratio (PSNR) is computed for each watermarked image.

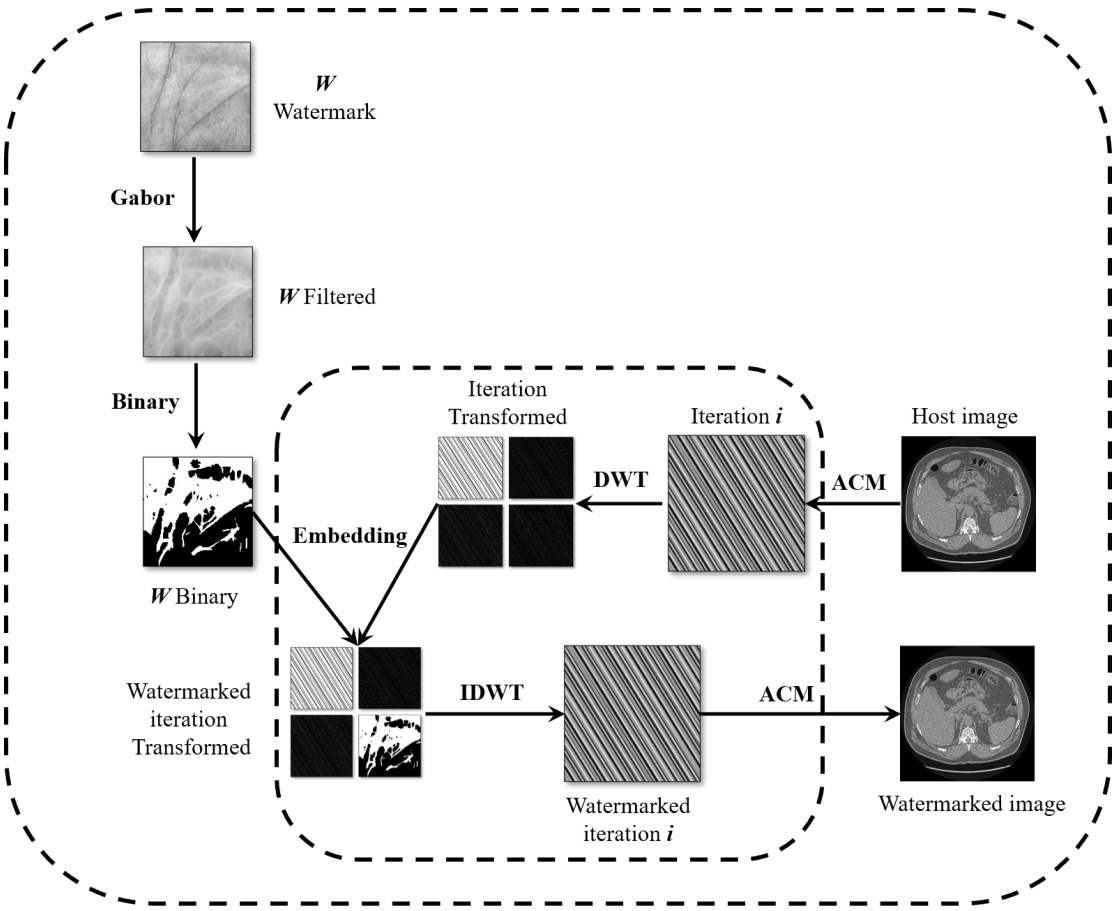


Figure 3.4: The Embedding Process of IDAW.

The iteration yielding the highest PSNR value is identified as optimal, ensuring minimal distortion while maintaining watermark robustness and imperceptibility.

Algorithm 7 Watermark Embedding Algorithm.

1: ACM(I,i) = iteration i: Apply ACM to the host image and stop at a specific iteration, referred to as iteration i.
2: Apply DWT (Single-Level DWT) to each block obtained in step 1 for image iteration i. The matrix yields DWT coefficients and iDWT results.
3: For watermarking, apply a Gabor filter to the palmprint, then convert it to a binary image to obtain a prepared watermark.
4: Insert the binary watermark W into iDWT using the following equation: $iwDWT = (1 - t) \times W + t \times HH$, where $iwDWT$ represents watermarked matrices. To make it human-readable, an additional step is needed.
5: Apply the IDWT to all blocks to obtain a human-readable image for watermarked iteration i.
6: Continue applying ACM to iteration i to obtain the watermarked image.

Note: In step 4, t is a given value within the range $\in]0, 1[$.

The primary procedural steps of the watermark embedding technique are outlined in Algorithm 7. This embedding framework operates within the spatial-frequency domain, where the parameter t is critical in controlling watermark visibility and imperceptibility. Empirical analysis suggests that optimal results are obtained when t approaches 1, ensuring minimal distortion of the host image. Conversely, smaller values of t lead to increased perceptual degradation. The watermark is strategically embedded into the high-frequency HH subband of the transformed image to enhance resilience against signal processing attacks while maintaining visual fidelity.

3.2.2.2 Extraction Process

The watermark extraction procedure consists of multiple sequential stages, utilizing both the embedded watermark (binary format) and the watermarked image. The extraction process commences with applying ACM to the watermarked image, iteratively reversing the transformation until a predefined iteration i is reached. At this stage, the corresponding watermarked iteration i is reconstructed. Subsequently, a single-level DWT is applied to decompose the retrieved iteration, facilitating the isolation of the frequency subbands. The extracted watermark is

then obtained using Equation (3.7), ensuring accurate retrieval while preserving the structural integrity of the host image. In this process, the parameter t is set to 0.98, adhering to the range $0 < t < 1$ to maintain the optimal balance between watermark visibility and robustness. The extraction mechanism plays a critical role in watermarking applications, ensuring the integrity and recoverability of the embedded watermark across various operational scenarios.

$$wa = t \times W - \frac{(1-t)}{t} \times HH \tag{3.7}$$

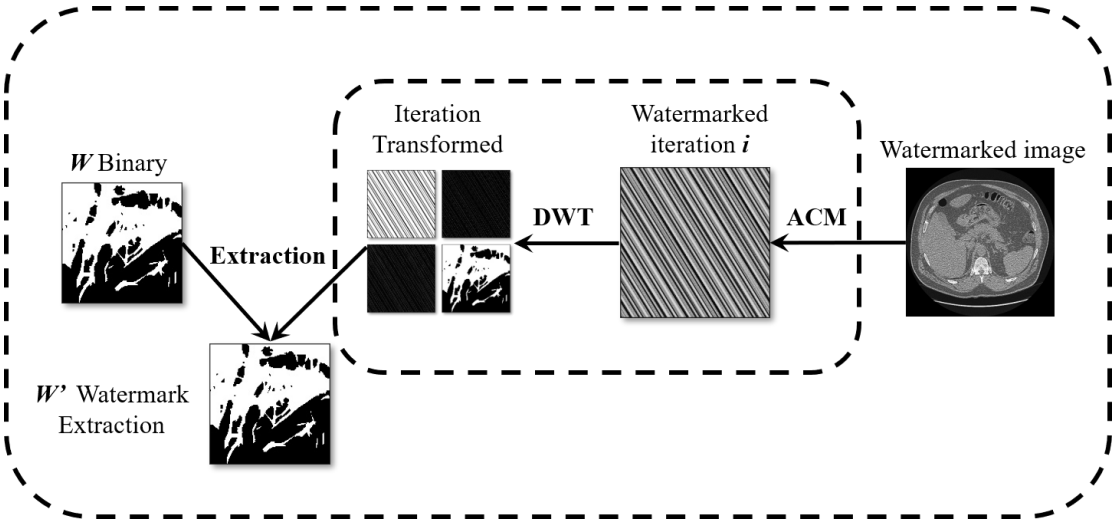


Figure 3.5: The Extraction Process of IDAW.

Algorithm 8 Watermark Extraction Algorithm.

Note: Consider the watermark image (Binary Watermark) and the watermarked image.

1: Apply the ACM to the watermarked image until a specific iteration i.
2: Obtain the watermarked iteration i.
3: Apply the DWT with a one-level transformation to the iteration.
4: Get the watermarked iteration i transformed.
5: Use the equation: $wa = t \times W - ((1-t)/t) \times HH$ to extract the watermark.
6: Ensure the retrieval of the watermark image from the watermarked image.

Note: The parameter t ranges between 0 and 1.

The watermark extraction procedure is formally outlined in Algorithm 8. During the extraction phase, both the original watermark and the watermarked image—potentially subjected to various attacks—are utilized to recover the embedded watermark. The extraction process employs the same parameter t as in the embedding phase to ensure consistency and accuracy in retrieval. Notably, the mathematical formulation governing the extraction does not introduce distortions in the recovered watermark or the reconstructed host image, thereby preserving the fidelity of the extracted watermark while maintaining the original image's perceptual quality.

3.3 Implementation and Experimental Evaluation

In alignment with the methodologies discussed in the two referenced studies, our implementation centers on embedding a fingerprint-based watermark into medical images to enhance security while safeguarding diagnostic fidelity. The primary objective is twofold: first, to maintain image integrity for accurate clinical interpretations; and second, to incorporate a robust identification mechanism that authenticates ownership and prevents unauthorized distribution. Drawing on the design principles highlighted in the previous works, the approach addresses common security vulnerabilities, such as unauthorized tampering and data leakage, by leveraging cryptographic protections and resilient watermark insertion strategies.

3.3.1 Implementation

Implementation of robust and secure watermarking techniques is crucial for maintaining the confidentiality and authenticity of medical images. This study builds upon two influential research works that demonstrated the effectiveness of fingerprint-based watermarking in medical imaging scenarios. By integrating advanced encryption methods, these strategies ensure minimized distortion in diagnostic regions while preserving essential patient data. The proposed approach employs a fingerprint image as a watermark, embedded within medical images to provide

reliable identity verification. This section outlines the dataset, programming environment, and computational procedures involved in our system.

3.3.1.1 Dataset Description and Image Types

For first contribution, our analysis involved a curated selection of 200 images referenced in (103). These images underwent preprocessing to remove borders, standardize dimensions to 256×256 pixels, and convert them into BMP format, as depicted in Figure 3.6. The larger CT KIDNEY DATASET: Normal-Cyst-Tumor and Stone, acquired from PACS across multiple hospitals in Dhaka, Bangladesh, consists of 12,446 unique CT scans. Radiologists and medical technologists verified each image to confirm one of four diagnoses: cyst, normal finding, stone, or tumor. The dataset includes coronal and axial cuts from contrast and non-contrast CT scans, emphasizing the whole abdomen and urogram. Specifically, it is categorized into 3,709 cysts, 5,077 normal findings, 1,377 stones, and 2,283 tumors.

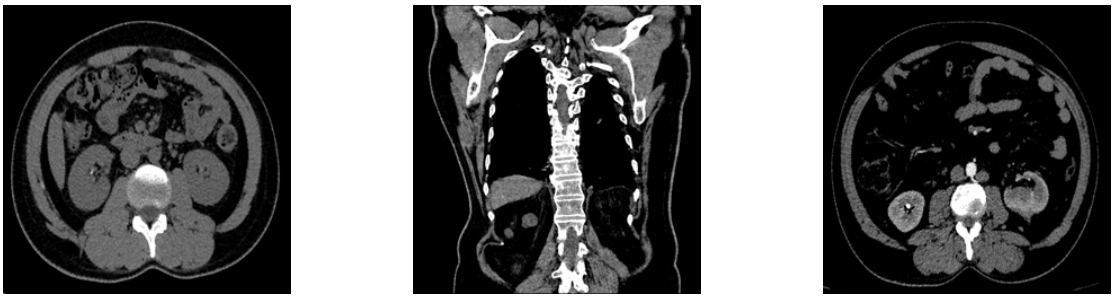
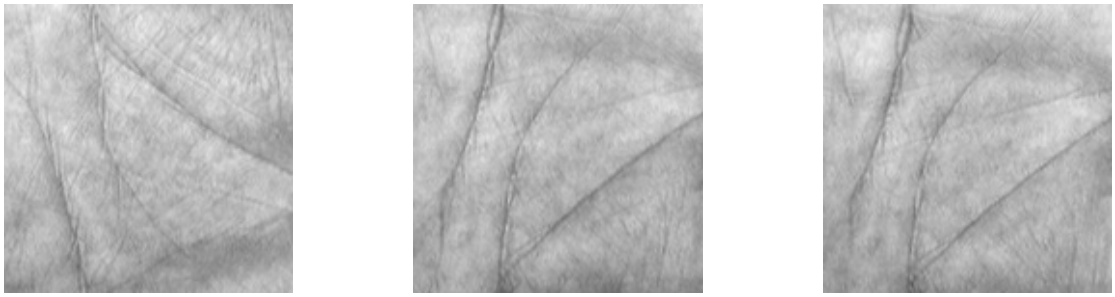


Figure 3.6: Samples of Used Human Brain MRI Image Dataset.

For watermarking purposes, the experiments utilized the FVC2002 fingerprint database (104), a commonly referenced source in biometric research. This repository is partitioned into two groups (A and B), each subdivided into four datasets (DB1, DB2, DB3, and DB4). It contains 120 unique fingers, each captured in 12 impressions (totaling 1,440 images), collected from 30 volunteers. The FVC2002 database offers a comprehensive benchmark for evaluating fingerprint recognition and feature extraction methods such as BSIF, making it well-suited for use as a robust watermark.

A publicly available palmprint dataset, PolyU (PolyU II) (105), was selected to serve as a watermark source for the IDAW approach. Developed by The Hong

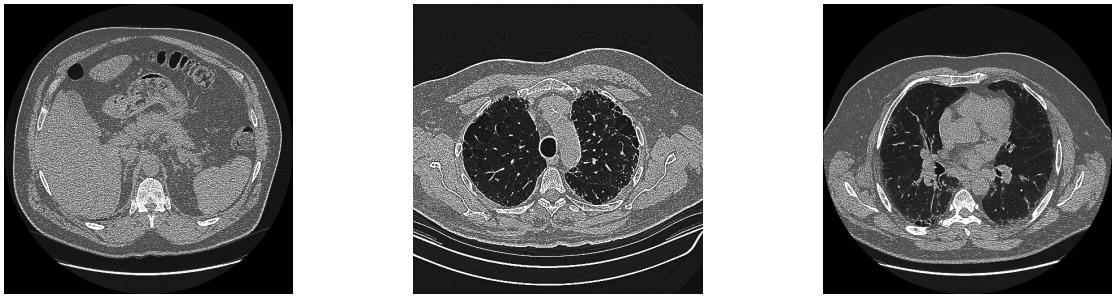
Kong Polytechnic University, this repository contains complete palmprint images valuable for biometric authentication. Since PolyU II images are exclusively provided in full-palm formats, a cropping step was employed to extract 256×256 pixel squares, ensuring optimal watermark placement. Figure 3.7 showcases representative samples from PolyU II.



(a) (b) (c)

Figure 3.7: Illustrative Samples of The PolyU II Palmprint Database.

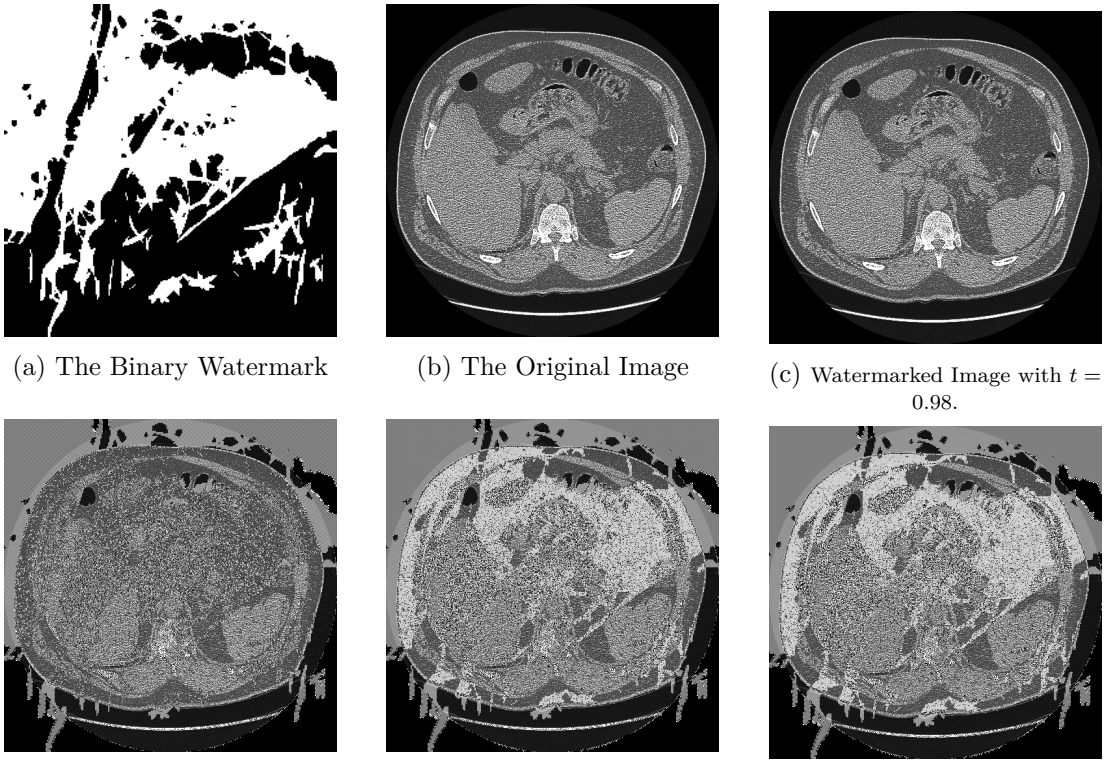
For the medical image component of the study, 200 grayscale images were obtained from (106), each originally in DICOM format at a resolution of 512×512 pixels. These images were derived from the Pulmonary Fibrosis Progression competition's training dataset. To maintain consistency and facilitate analysis, the DICOM files were converted into grayscale PNG images using windowing and normalization procedures provided by the Fast.ai medical imaging library. This standardized conversion ensured each image was suitably processed for subsequent watermark embedding trials.



(a) (b) (c)

Figure 3.8: Gray-scale Medical Image Sample from The Pulmonary Fibrosis Progression Dataset.

Utilizing the IDAW method, we experimented with various visibility threshold parameter values, specifically setting t at 0.1, 0.2, 0.5, and 0.98. Based on our results, we observed that the watermark remained imperceptible and yielded better outcomes when $t = 0.98$ (approaching 1), compared to the visible watermarks at $t = 0.1$ and $t = 0.2$, as well as the semi-invisible watermark at $t = 0.5$. Furthermore, the extracted watermarks were identical to the original ones. The results are illustrated in Figure 3.9.



(a) The Binary Watermark

(b) The Original Image

(c) Watermarked Image with $t = 0.98$.

(d) Watermarked Image with $t = 0.5$.

(e) Watermarked Image with $t = 0.2$.

(f) Watermarked Image with $t = 0.1$.

Figure 3.9: Results of Utilizing Various Visibility Factors (t) to Embed Watermarks.

Table 3.1 demonstrates that the LoG filter is more effective for BSIF applications than the Gaussian-like filter. Although the Gaussian-like filter excels at reducing noise, its smoothing effect tends to blur edges, which compromises both edge preservation and detail enhancement. In contrast, the LoG filter, while offering only moderate noise reduction, significantly improves edge retention and enhances fine details qualities that are crucial for robust feature extraction in BSIF.

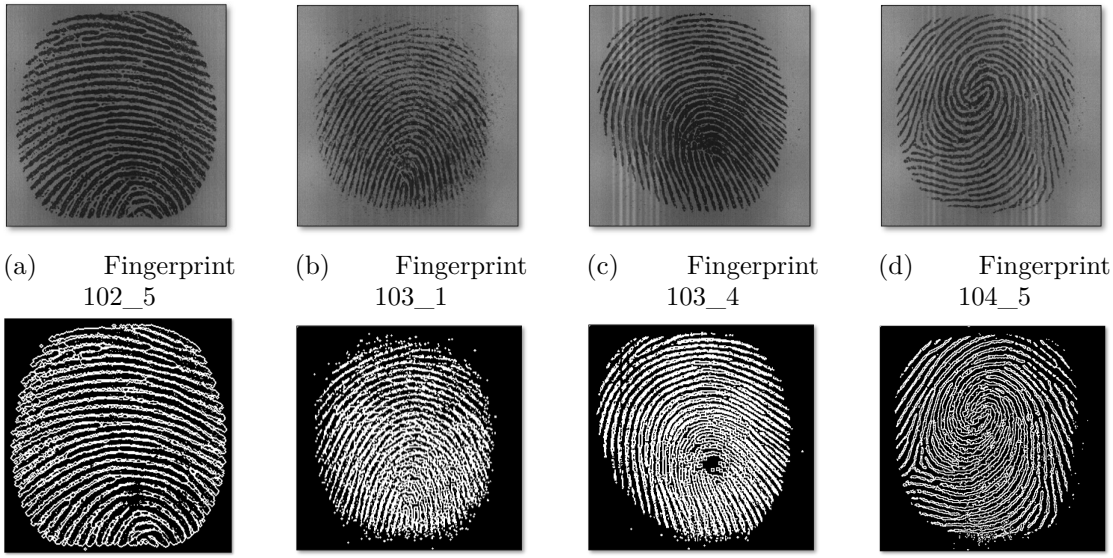
Table 3.1: Gaussian-like Filter and LoG Filter Comparisons.

Aspect	**Gaussian-like Filter**	**Laplacian of Gaussian (LoG) Filter**
Filter Matrix	$\begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & -2 & -1 & 0 \\ -1 & -2 & 16 & -2 & -1 \\ 0 & -1 & -2 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix}$
Primary Function	Smoothing, noise reduction	Edge detection, noise reduction
Noise Reduction	High	Moderate
Edge Preservation	Low (blurs edges)	High (enhances edges)
Detail Enhancement	Low	High
Suitability for BSIF	Basic feature extraction	Enhanced feature extraction
Use Case	Initial smoothing, reducing noise	Highlighting fine details, preserving edges

Figure 3.10 presents fingerprint images in BMP format with dimensions of 300 × 300 pixels, demonstrating how BSIF is applied using a LoG filter on fingerprint datasets. The convolution process with the LoG filter isolates specific features from the binary images, thereby enhancing the fingerprint patterns for improved identification and analysis. Additionally, BSIF reduces the image size by roughly 69.25% compared to the original, maintaining critical fingerprint features while lowering the data storage requirements.

Their performance evaluation revealed impressive data compression rates: 77.34% for a 64 × 64 matrix and an even higher 88.08% for a 128 × 128 matrix. These results are derived using a mathematical formula that computes the compression rate, as shown in Equation:

$$\frac{(m' + n' + |Hash(M)|) \times 100}{m \times n}$$



(a) Fingerprint 102_5 (b) Fingerprint 103_1 (c) Fingerprint 103_4 (d) Fingerprint 104_5

(e) BSIF 102_5 (f) BSIF 103_1 (g) BSIF 103_4 (h) BSIF 104_5

Figure 3.10: Performed BSIF Feature Extraction on Fingerprint Images.

In this equation, m and n represent the dimensions of the original matrix, while m' and n' correspond to the dimensions after compression.

Using this matrix-based method to compress watermarks significantly reduces data volume (see Figure 3.11), thereby boosting storage and transmission efficiency within blockchain systems. Incorporating a hash guarantees that the compressed data remains unique, which in turn makes it easier to accurately restore the original watermark after decompression. Overall, this approach improves both data integrity and performance, playing a vital role in maintaining secure and reliable digital transactions.

3.3.1.2 Device Characteristics and Computational Environment

All experiments were performed on a desktop workstation with an Intel Core i7 processor operating at 3.60 GHz, 16 GB of RAM, and an NVIDIA GeForce RTX GPU for accelerated image manipulation. The system ran on a 64-bit Windows 11 operating system, providing stability and compatibility with the selected software stack. This configuration allowed efficient handling of large medical images and

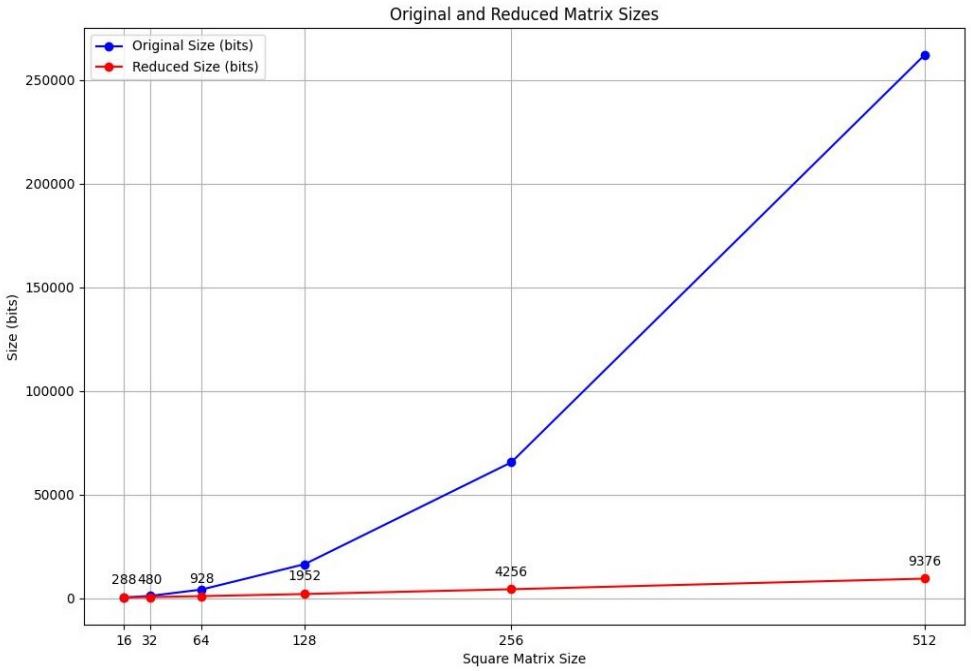


Figure 3.11: Comparison between original and reduced matrix sizes in bits.

rapid execution of the watermark embedding and verification modules. A local server environment was also used to manage dataset storage, ensuring a secure and organized workspace.

In order to standardize the experimental procedures, images were cropped to 64×64 and 128×128 pixel squares for watermark embedding. This approach facilitates direct comparisons of results by creating a consistent baseline and enables thorough evaluation of the watermarking algorithm's performance under varying conditions, such as image compression or diverse attack scenarios. Moreover, using smaller image dimensions simulates real-world compression challenges often encountered in medical and biometric applications, thereby confirming the algorithm's effectiveness even when data is reduced.

Figure 3.12 illustrates the incorporation of a biometric fingerprint, processed with BSIF, into a medical image as a watermark. Following this embedding process, the watermarked image undergoes an encryption procedure to safeguard the privacy and integrity of the underlying medical data.



(a) (b) (c) (d)

Figure 3.12: Watermark Embedding and Encryption Processes in Medical Images.

3.3.2 Experimental Evaluation

The experimental evaluation of our proposed watermarking approachs employs key metrics PSNR, SSIM, and NCC to comprehensively assess performance. These metrics ensure visual fidelity, imperceptibility, and robustness against distortions. While PSNR and SSIM evaluate image quality (107), NCC validates watermark integrity (108), emphasizing the reliability of ownership verification (109). Together, they provide a holistic framework for evaluating systems effectiveness (13).

3.3.2.1 Quality and Robustness Evaluation Metrics

Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Normalized Cross-Correlation (NCC) are widely recognized metrics in watermarking research for quantifying imperceptibility, visual fidelity, and watermark retrieval reliability (107; 109). PSNR measures the ratio between the highest possible pixel intensity squared and the Mean Squared Error (MSE) between original and watermarked images. Mathematically, it is expressed in Equation (3.8).

$$\text{PSNR} = 10 \cdot \log_{10} \left(\frac{\text{MAX_PIXEL}^2}{\text{MSE}} \right) \tag{3.8}$$

where a higher value indicates minimal distortion (110). However, while PSNR captures pixel-level discrepancies effectively, it does not fully account for human

visual perception (107). SSIM, defined by Equation (3.9), addresses this limitation by evaluating luminance, contrast, and structural information in local image patches (111). Specifically,

$$\text{SSIM} = \frac{(2\mu_x\mu_y + C1)}{(\mu_x^2 + \mu_y^2 + C1)} \cdot \frac{(2\sigma_{xy} + C2)}{(\sigma_x^2 + \sigma_y^2 + C2)} \tag{3.9}$$

where μ_x and μ_y represent mean intensities, σ_x^2 and σ_y^2 denote variances, and C_1, C_2 are stability constants (13; 10). This holistic assessment aligns more closely with how the human eye discerns differences in visual content. NCC, denoted by Equation (3.10), measures the correlation between the original watermark and its extracted counterpart to gauge watermark retrieval accuracy (112; 108). A higher NCC implies robust watermark recovery despite attacks such as compression or filtering, thereby verifying the integrity and authenticity of embedded information. Concretely,

$$\text{NCC} = \frac{\sum_{i=1}^{N}(I_{o,i} \cdot I_{w,i})}{\sqrt{\sum_{i=1}^{N}(I_{o,i})^2} \cdot \sqrt{\sum_{i=1}^{N}(I_{w,i})^2}} \tag{3.10}$$

captures the resilience of the watermark against signal degradation (13; 1). Hence, PSNR and SSIM collectively reveal the overall imperceptibility of the embedded watermark, while a high NCC confirms the watermark's robust recoverability under standard transformations (113). By unifying these metrics, watermarking systems can be thoroughly evaluated for visual fidelity, diagnostic integrity, and authentication reliability, ensuring effective protection of embedded information in diverse imaging contexts.

3.3.3 Imperceptibility Measurements

The experimental results in Table 3.2 demonstrate that the MLSF technique effectively preserves image quality during watermark embedding. With an average PSNR of approximately 63.2367 dB and SSIM values consistently above 0.9999, the watermarked images retain near-identical structural integrity compared to

their originals. These metrics indicate negligible perceptual degradation, underscoring the method's capacity to balance robust security with imperceptibility. Overall, the proposed approach significantly enhances watermark performance.

Table 3.2: Imperceptibility Results of the Multi-Layered Security Framework.

S.No	Image	PSNR (dB)	SSIM
1	Airplane	63.8986	1
2	Barbara	63.2497	0.99998
3	Boat	63.6754	0.99996
4	Lena	63.5067	1
5	Liftingbody	63.7457	0.99998
6	Pepper	63.9404	1
7	Cyst- (1)	62.3050	0.99994
8	Normal- (100)	62.6414	0.99996
9	Tumor- (1024)	62.7558	0.99994
10	Normal- (1001)	62.6480	0.99998

Table 3.3 and Figure 3.13 summarize the outcomes of applying watermarks of varying sizes (64×64, 128×128, 256×256, and 512×512 pixels) using a binary matrix compression approach.

Table 3.3: Performance Metrics of Watermark Compression and Embedding in Host Images.

Image	W	Size W (KB)	Size M (Byte)	Reduction	Rate %	PSNR	SSIM
256×256	64×64	5.05	512	116	77.34	62.96	1.00
	128×128	17.01	2048	244	87.90	58.02	1.00
	256×256	65.05	8192	532	93.50	55.73	0.9999
	512×512	257	32768	1172	96.48	53.16	0.9998
512×512	64×64	5.05	512	116	77.34	67.058	1.00
	128×128	17.01	2048	244	87.90	64.08	1.00
	256×256	65.05	8192	532	93.50	60.93	0.9999
	512×512	257	32768	1172	96.48	58.04	0.9999



(a) 64 px (b) 128 px (c) 256 px (d) 512 px

Figure 3.13: Different Sizes of Watermark.

The results demonstrate a significant reduction in watermark size, with compression rates spanning from 77.34% to 96.48%. Notably, despite the aggressive compression, the quality of the watermarked images remains high, as evidenced by PSNR values ranging from 53.16 to 67.06 dB, which confirm excellent image fidelity. Moreover, SSIM values remain consistently close to 1, indicating strong structural similarity between the compressed and original images. Overall, these findings underscore the effectiveness of the proposed compression technique in achieving substantial data reduction while preserving image quality. These findings confirm that the compression method effectively preserves critical image quality while achieving significant size reduction.

Table 3.4 presents a comprehensive evaluation of the IDAW concept, designed to achieve a high degree of imperceptibility in watermark embedding. The results indicate that our watermarking scheme maintains excellent visual fidelity with minimal degradation in the watermarked images. By optimizing the parameter t to approach 1 (specifically, $t = 0.98$), the embedding process is finely tuned to preserve the original image content. The reported PSNR values, ranging from 52.01000 to 53.95001 dB, reflect a strong resemblance between the original and watermarked images, while the SSIM scores consistently exceed 0.9999, confirming near-perfect structural similarity. These metrics demonstrate minimal visual impact and highlight the resilience of the method under various conditions, making it highly suitable for secure and quality-critical applications.

Table 3.4: Performance Metrics for Watermark Embedding.

S.No	Image	PSNR (dB)	SSIM	NCC
1	Lena	53.94404	0.99996	0.9999878
2	Pepper	52.01000	0.99994	0.9999899
3	Barbara	53.88076	0.99996	0.9999928
4	Airplane	53.95001	0.99995	0.9999960
5	Eight	53.94398	0.99996	0.99999535
6	Liftingbody	52.86642	0.99987	0.9997472

3.3.4 Robustness Measurements

Watermark extraction results from medical images and standard images such as Boat, Lena, Pepper, Barbara, and Airplane validate the proposed approach. In the MLSF framework, perfect recovery is achieved by decrypting a shared watermarked encrypted image on IPFS and extracting the H and V components. The reconstruction of the matrix using Hash(M) enables conversion into a binary image. In particular, the BSIF watermark is extracted with a PSNR of ∞ and an SSIM of 1, demonstrating exceptional precision and confirming the effectiveness of our technique under attack-free conditions, thus proving robustness.

In Table 3.5, the watermarks extracted from images like Lena, Pepper, Barbara, and Airplane demonstrate remarkable fidelity to the originals. The PSNR values, averaging around 50 dB, indicate that the extraction process incurs minimal distortion. Furthermore, the SSIM and NCC scores, consistently near 1.0, confirm nearly perfect structural and content preservation. These results validate the effectiveness of the proposed IDAW approach, as it reliably retrieves the embedded watermarks with exceptional accuracy and integrity in attack-free conditions.

Table 3.5: Watermark Extraction Results.

S.No	Image	PSNR (dB)	SSIM	NCC
1	Lena	49.02833	0.999990	0.9999954
2	Pepper	48.64467	0.999987	0.9999943
3	Barbara	47.84994	0.999982	0.99999166
4	Airplane	50.50734	0.999997	0.9999991
5	Eight	51.03107	0.999999	0.9999990
6	Liftingbody	50.65065	0.999998	0.9999993

Figure 3.14 illustrates modifications applied to the watermarked medical image Cyst_512, simulating common distortions. The robust performance of the watermark under adversarial conditions clearly confirms the technique's effectiveness and overall stability in maintaining watermark integrity. These results underscore the method's resilience.

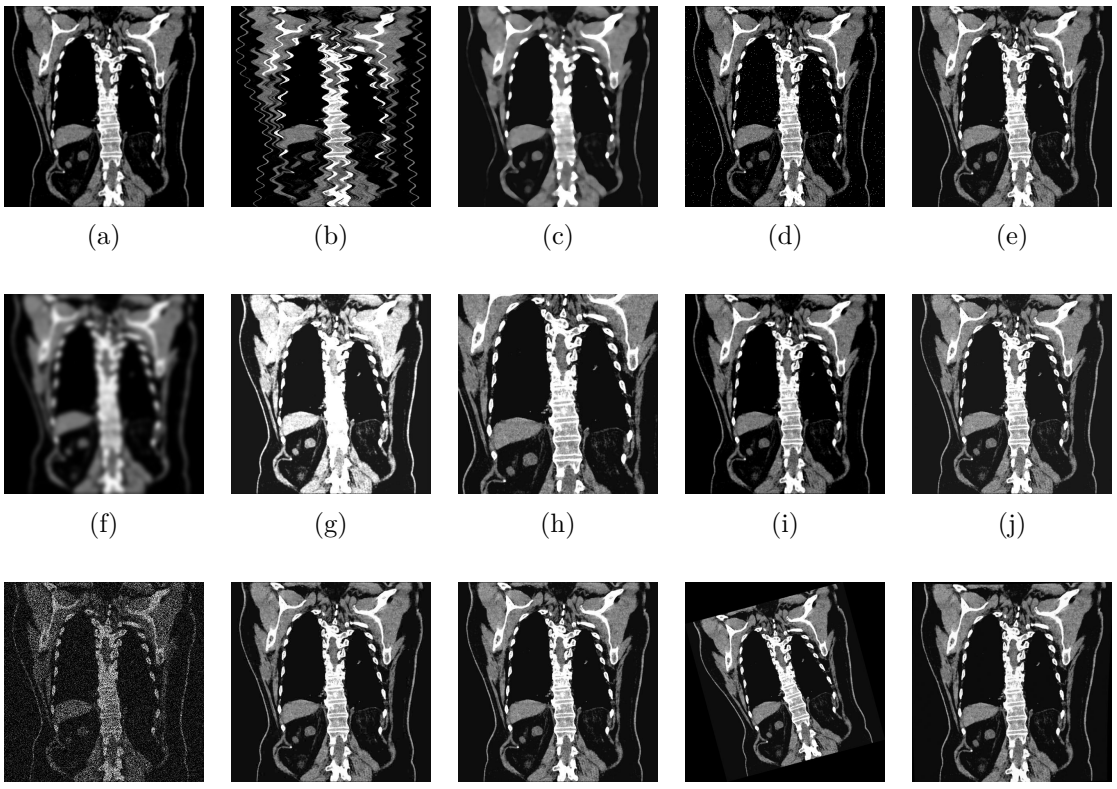


Figure 3.14: Robustness Against JPEG and Image Processing Attacks.

Table 3.6 and the accompanying analysis demonstrate that the MLSF approach exhibits robust performance against a variety of image attacks. In particular, the method achieves near-perfect watermark recovery under JPEG_90 and PSNR_90 conditions, with NCC values of 0.9990 and minimal BERs of 0.0050 and 0.0010. Moreover, it shows strong resistance to blurring, rescaling, and convolution operations. Although aggressive attacks such as CROP_75 and ROT_15 pose greater challenges, the overall performance remains effective across diverse distortions. These balanced results in imperceptibility and robustness confirm that MLSF is well-suited for secure watermarking applications in real-world scenarios. These

impressive results not only preserve watermark integrity but also effectively counteract typical signal processing distortions, ensuring performance in real-world security applications.

Table 3.6: Robustness measurement against different attacks.

S.No	Attacks	NCC	BER	MSE
1	Gaussian Blur 10%	0.9200	0.1800	45.0
2	Bending_attack	0.9400	0.0600	90.0
3	MEDIAN_9	0.99200	0.0200	17.0
4	Salt_pepper 15%	0.8700	0.2100	110.0
5	ROTSCALE_0.75	0.9100	0.0900	150.0
6	Blurred	0.9650	0.0250	35.0
7	CONV_1	0.9850	0.0350	25.0
8	CROP_75	0.7200	0.2400	130.0
9	Rescaled	0.9850	0.0150	25.0
10	PSNR_90	0.9990	0.0010	6.5
11	NOISE_20	0.8400	0.0600	90.0
12	JPEG_20%	0.9500	0.0500	75.0
13	JPEG_90%	0.9990	0.0050	5.5
14	ROT_15	0.7800	0.2300	110.0
15	RNDDIST_1.1	0.9600	0.0400	60.0

Table 3.7 presents a detailed evaluation of the IDAW approach under a diverse set of image attacks, including geometric distortions, filtering, noise, and compression. The experimental results indicate that the proposed method exhibits remarkable robustness across various manipulations. Under geometric attacks such as Scaling_1.5x and Shear_20, the watermarked images achieve PSNR values of approximately 49.27 dB and 49.49 dB, respectively, with SSIM and NCC values consistently exceeding 0.99995, thereby preserving spatial integrity. Similarly, signal processing attacks like Gaussian Blur yield PSNR values near 49.46 dB with near-perfect SSIM scores, underscoring the method's resistance to filtering effects. Although the Noise_80 attack leads to a substantial decline in PSNR to around 28 dB, SSIM and NCC remain high, indicating that despite reduced overall image quality, the embedded watermark's integrity is largely maintained. These results validate the reliability of IDAW for robust watermark embedding and extraction. However, the vulnerability to high noise levels suggests an avenue for further improvement. Future work should focus on enhancing noise resistance

to ensure both robust watermark protection and superior image quality under severe attack conditions. These findings offer a promising foundation for developing next-generation secure watermarking systems.

Figure 3.15 shows that, despite JPEG compression degrading the watermarked image, the proposed method exhibits impressive robustness in watermark extraction. For instance, at a quality level of 10, the watermarked image has a PSNR of 26.61 and SSIM of 0.7616, yet the extracted watermark attains a PSNR of 37.73 and SSIM of 0.99991. Similar trends across compression levels confirm the method's durability, with quality 100 yielding an extracted watermark PSNR of 49.92 and SSIM of 0.99999. Overall, the method is effective.

3.3.5 Computational Complexity and Practical Feasibility

Encrypting a watermarked image with AES requires roughly 0.00754 seconds, and decryption takes about 0.00476 seconds, highlighting the efficiency of the AES process. In our MLSF framework for secure medical image storage, these minimal processing times ensure that encryption and decryption do not create bottlenecks.

Similarly, embedding a compressed watermark takes approximately 0.012 seconds, while extraction is completed in about 0.008 seconds. These rapid processing times are significantly faster than those reported in other studies (114) and (115), where embedding times were recorded at 1.865 and 0.6 seconds, and extraction times at 1.916 and 0.7 seconds, respectively. Such performance demonstrates that the watermarking process has a negligible impact on overall system efficiency. In a practical healthcare environment, this framework can be integrated into existing systems like PACS and EMR, thereby enhancing the secure management of medical images while safeguarding data integrity and patient privacy.

However, implementation challenges remain, such as ensuring compatibility with various imaging formats, maintaining low latency, and meeting stringent regulatory standards like HIPAA and GDPR. Addressing these issues will be essential to fully leverage the benefits of the proposed approach in real-world applications.

Table 3.7: Robustness Measures Against Different Attacks.

Attacks	Lena			Pepper			Barbara			Airplane		
	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC
Scaling_1.5x	49.274310	0.999970	0.999980	49.725450	0.999978	0.999998	50.000045	0.9999996	0.9999986	50.031678	0.999973	0.9999998
Shift_20	47.768534	0.999975	0.999990	47.387111	0.999970	0.999985	47.511895	0.999965	0.999980	47.246287	0.999968	0.999983
Blur_1.5	49.465167	0.999990	0.999920	49.243336	0.999910	0.999980	48.799674	0.999970	0.999900	48.577843	0.999975	0.999905
S_pepper_10	31.228046	0.999850	0.999880	31.126621	0.999840	0.999870	30.822346	0.999830	0.999860	30.923771	0.999835	0.999865
HistEq	36.511214	0.999950	0.999970	36.400418	0.999945	0.999965	36.068031	0.999940	0.999960	36.178827	0.999943	0.999963
Shear_20	49.490170	0.999960	0.999980	49.288529	0.999955	0.999975	48.881793	0.999950	0.999970	49.085161	0.999953	0.999973
Noise_80	28.137196	0.996883	0.998502	28.499743	0.997135	0.998622	28.192497	0.996923	0.998521	28.029403	0.996804	0.9984644
Rot_45	46.954995	0.999974	0.999987	46.135368	0.999966	0.999983	45.380707	0.999957	0.999979	44.813301	0.999949	0.9999754
JPEG_90	49.233671	0.999991	0.999996	48.553835	0.999987	0.999994	36.449226	0.999558	0.999785	50.234194	0.999996	0.9999984
PSNR_90	49.028336	0.9999912	0.999995	48.644678	0.999987	0.9999943	36.581342	0.999572	0.999791	50.437433	0.999997	0.999999
CROP_50	51.031071	0.999999	0.999999	45.010471	0.999953	0.999976	45.015212	0.999953	0.999932	51.031071	0.9999995	0.9999996
Median_9	49.155983	0.999991	0.999995	50.958401	0.999999	0.999999	51.023143	0.9999995	0.999983	50.9584013	0.9999993	0.9999999

The IDAW technique's time complexity was assessed by measuring the average duration needed for both watermark embedding and extraction. Experimental results indicate that embedding a watermark takes approximately 0.01218 seconds on average, while extraction requires about 0.006875 seconds. This minimal processing time demonstrates that our method is both reliable and rapid, making it well-suited for real-time applications.

The primary contributor to IDAW's complexity is the embedding stage, which follows an $O(N^2 + N \log N)$ computational model. In this model, the $O(N^2)$ component reflects the workload from ACM iterations, whereas the $O(N \log N)$ term accounts for the DWT operations. The extraction process exhibits a similar complexity, highlighting these steps as the main factors influencing the algorithm's overall efficiency.

Moreover, the watermark insertion equation itself is highly efficient, operating within $O(N)$ due to its reliance on simple arithmetic. This optimized step minimizes computational overhead and significantly enhances the overall speed of the watermarking process.

3.3.6 Comparative Study

In this comparative study, we evaluate the performance of our proposed MLSF and IDAW frameworks. Key metrics including PSNR, SSIM, NCC, and resilience under various attacks are examined. Our integrated approach demonstrates superior imperceptibility and robustness compared to existing methods.

3.3.6.1 Imperceptibility

As Table 3.8 illustrates, the Multi-Layered Security Framework outperforms comparable approaches in imperceptibility, achieving a PSNR of 63.2367 dB and an SSIM of 0.9999. In contrast, Abrar et al. (73) and Chen et al. (90) report PSNR values of 47.699 dB and 39.2792 dB, with corresponding SSIMs of 0.995 and 0.9735, respectively. These metrics confirm that MLSF effectively preserves image quality. Overall, these results underscore the significant improvement offered by our approach.

Table 3.8: The Performance Comparative Study.

S.No	Approach	PSNR (dB)	SSIM
1	(73)	47.699	0.995
2	(40)	44.1944	0.9961
3	(90)	39.2792	0.9735
4	(115)	51.14	0.9969
5	MLSF	**63.2367**	**0.9999**

Table 3.9 presents a comparative study of watermarking quality for the Lena image, using PSNR, SSIM, and NCC metrics. The proposed IDAW framework achieves a PSNR of 53.9440 dB, an SSIM of 0.99996, and an NCC of 0.9999878, outperforming other methods. For example, (116) reports a PSNR of 51.8941 dB, while (117) and (118) yield lower values. Moreover, our ablation study confirms that the combined use of ACM and DWT significantly enhances performance compared to their individual application. This integrated approach guarantees exceptional watermark quality while ensuring a minimal perceptual impact, making it remarkably suitable for sensitive applications. These findings emphasize the importance of integrating ACM with DWT, as separate implementations yield lower PSNR and SSIM values. Overall, the IDAW framework demonstrates significant potential for secure watermarking applications that demand robust performance and minimal perceptual degradation.

Table 3.9: Watermarked Image Quality: PSNR, SSIM, and NCC Comparison.

Approach	PSNR	SSIM	NCC
IDAW	**53.9440**	**0.99996**	0.9999878
(116)	51.8941	0.9998	0.9999
(117)	47.8980	0.9992	0.9941
(118)	35.4765	0.9977	0.9981
(82)	44.7457	0.9999	**1**
(119)	49.1100	0.9998	0.9998
(75)	49.8400	0.9900	0.9900
(85)	41.0200	0.9900	0.9900
(79)	40.1300	0.9980	-

3.3.6.2 Robustness

Table 3.10 demonstrates that MLSF outperforms comparable methods, achieving infinite PSNR and an SSIM of 1.0 for extracted watermarks. In contrast, Sajeer et al. (120) report a PSNR of 52.71 dB and SSIM of 0.9912, while Arora et al. (121) and Hosny et al. (122) obtain PSNRs of 54.98 dB and 55.34 dB with SSIMs of 0.9997 and 0.9999. These results confirm the exceptional quality and robustness of our framework indeed.

Table 3.10: PSNR and SSIM Values Comparison of the Extracted Watermarks.

S.No	Approach	PSNR (dB)	SSIM
1	(120)	52.71	0.9912
2	(121)	54.98	0.9997
3	(122)	55.34	0.9999
4	MLSF	∞	**1.0**

Our evaluation of robustness demonstrates that the proposed IDAW approach consistently outperforms alternative methods, as evidenced by Table 3.11. Under Noise_80, our PSNR of 28.1372 dB surpasses others, while a remarkable 46.9550 dB under Rot_45 contrasts sharply with lower values from competitors. Moreover, our PSNR of 51.0311 dB under CROP_50 highlights the superior resilience and effectiveness of our combined technique compared to standalone DWT and ACM methods, further validating its robust and consistently superior overall performance.

Table 3.11: Comparison of PSNR Values for Different Attacks.

Approach	Noise_80	Rot_45	JPEG_90	PSNR_90	CROP_50	Median_9
IDAW	**28.1372**	**46.9550**	**49.2337**	**49.0283**	**51.0311**	**49.1560**
(117)	27.8473	2.3541	12.5423	-	20.4512	14.6408
(116)	19.1126	12.3800	43.8853	-	17.2401	28.7697
(82)	13.8395	12.5441	37.0235	-	15.8038	33.7449
(123)	-	26.7190	45.6165	-	27.4545	40.7819

Table 3.12 demonstrates that the proposed IDAW approach consistently achieves exceptional NCC values under various attacks, indicating nearly perfect similarity

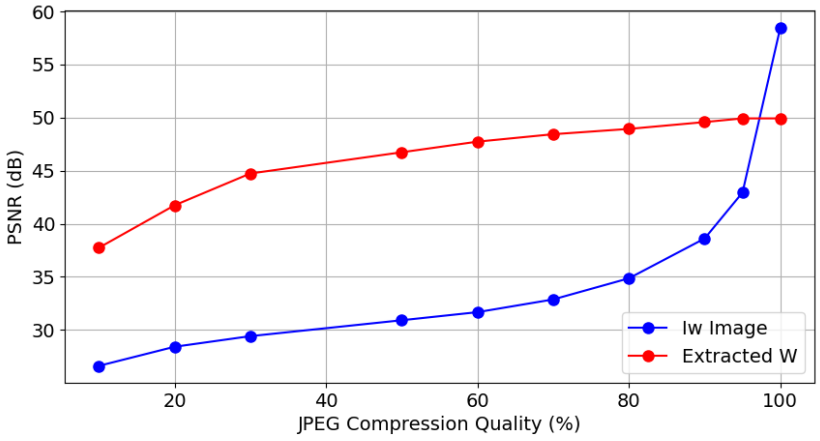
between the original and extracted watermarks. For instance, under the Noise_80 attack, our method attains an NCC of 0.9985, significantly outperforming 0.7669 reported by (117). Similarly, in Rot_45 and JPEG_90 attacks, our NCC values are 0.99998 and 0.99999 respectively, while under CROP_50, an NCC of 0.99999 is achieved. These results confirm the superior robustness and resilience of our framework. Overall, findings validate the superiority of our approach.

Table 3.12: Comparison of NCC Values for Different Attacks.

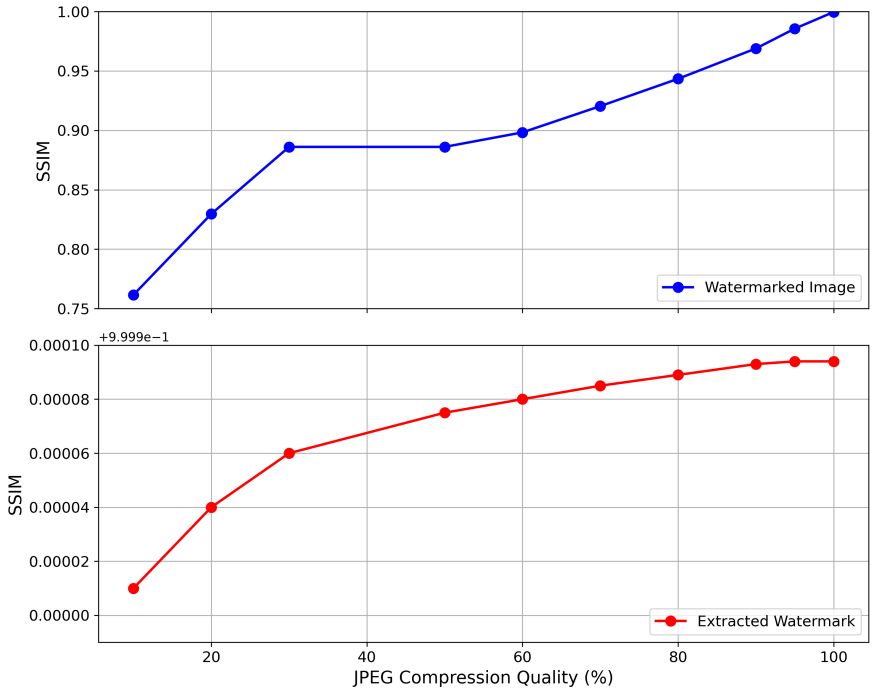
Approach	Noise_80	Rot_45	JPEG_90	PSNR_90	CROP_50	Median_9
IDAW	**0.9985**	**0.99998**	**0.99999**	**0.99999**	**0.99999**	**0.99999**
(117)	0.7669	0.5428	0.4578	-	0.4567	0.4919
(116)	0.9867	0.9929	0.9998	-	0.9945	0.9950
(82)	0.9715	0.9450	0.9996	-	0.9998	0.9646
(123)	0.9883	0.9797	0.9996	-	0.9998	0.9787

3.4 Conclusion

This chapter has presented significant contributions toward enhancing medical image watermarking for secure e-health applications. The proposed Multi-Layered Security Framework and improved DWT and ACM watermarking approach demonstrate superior imperceptibility, robustness, and computational efficiency compared to existing methods. The integration of encryption, blockchain, and IPFS ensures data integrity and traceability, while advanced compression techniques optimize storage and transmission. These findings provide a solid foundation for secure, reliable medical image management, opening avenues for future improvements in noise resistance and system scalability.



(a) PSNR



(b) SSIM

Figure 3.15: Comparison of The Obtained PSNR and SSIM for JPEG Compression.

Chapter 4

Case Studies of Watermarking in Healthcare

This section aims to help healthcare practitioners select the appropriate watermarking techniques for medical images.

4.1 Introduction

Medical images play a critical role in modern healthcare by providing detailed insights for accurate diagnosis, treatment planning, and patient management. Their integrity is paramount; even minor alterations can lead to misinterpretation and incorrect treatments. Digital watermarking, which embeds secure, imperceptible information into images, has emerged as a vital technology for ensuring authenticity, integrity, and privacy in medical imaging. This chapter presents a collection of real-life applications and case studies highlighting various watermarking techniques. The studies include reversible schemes for full image recovery, adversarial watermarks to counter unauthorized AI analysis, and adaptive methods balancing robustness with image quality. These examples offer valuable insights into practical implementations, challenges, and emerging trends in healthcare data security, guiding future improvements.

This thesis focused on developing an advanced adaptive watermarking method that considers the unique requirements of medical imaging. The proposed techniques are designed to enhance both the watermark's robustness and the medical image's

fidelity, contributing to the secure and reliable use of digital imaging technologies in healthcare settings.

4.2 Real Applications of Watermarking in Healthcare

The practical application of watermarking techniques in healthcare has gained significant attention due to the increasing demand for enhanced security and integrity of medical images. As medical imaging technologies advance and digital healthcare solutions are adopted, ensuring medical data security, authenticity, and privacy becomes more critical. Watermarking is a robust and versatile approach to address these challenges, offering a reliable means to embed secure information within medical images without compromising their diagnostic quality. This section explores the diverse real-world scenarios where watermarking has proven beneficial in healthcare, demonstrating its value as a key component of modern medical data management and security frameworks.

- **Protection of Sensitive Health Records:** Recent advances in digital watermarking have demonstrated substantial promise in enhancing the security and integrity of medical images. In clinical settings, watermarking is employed to securely embed patient identity, clinical history, and treatment protocols directly into medical images. For example, Pallaw et al. (35) developed a robust watermarking scheme using nature-inspired optimization to embed fingerprint features into low-frequency subbands, ensuring that sensitive metadata is concealed even when images are transmitted over unsecured networks. This method not only protects patient data but also provides a reliable means to verify the authenticity of medical images, aligning with regulatory requirements such as HIPAA.
- **Integrity Verification During Transmission:** Another significant application is the verification of image integrity during transmission. Watermarking techniques can detect any unauthorized modifications that occur during image exchange. Zarrabi et al. (124) proposed a reversible watermarking approach using distortion compensation in the wavelet domain, which enables

the exact recovery of the original image after extraction. Such techniques are instrumental in telemedicine, where even slight alterations can compromise diagnostic outcomes.

- **Telemedicine Security:** In addition, watermarking has been integrated with telemedicine systems to secure remote diagnostics. For instance, the Universitat Oberta de Catalunya (UOC) implemented a digital watermarking solution in 2024 to protect medical documents and images exchanged via telehealth platforms, ensuring that any tampering or unauthorized access is promptly detected (125). This application is crucial in environments where medical images are frequently shared between providers, laboratories, and specialists.

- **Usage Monitoring and Traceability:** Moreover, watermarking techniques ensure traceability and data provenance in distributed healthcare systems. (126) proposed embedding a unique device fingerprint into medical images before storage, which facilitates subsequent verification of the image source. This approach is particularly relevant for mobile imaging devices and telemedicine applications, where data origin must be reliably authenticated.

- **Protection of Intellectual Property Rights:** Watermarking also supports intellectual property protection in healthcare. As medical imaging technology and diagnostic algorithms continue to evolve, securing proprietary information becomes essential. By embedding ownership data directly within digital images, watermarking deters infringement and provides verifiable evidence of originality. Hassani Allaf and Aït Kbir (127) reviewed several watermarking applications for medical image exchange security, underscoring the role of embedded watermarks in authentication and copyright protection.

- **Enhanced Security in Healthcare Software:** Furthermore, watermarking contributes to enhanced security in healthcare software systems. Many healthcare applications that handle sensitive medical images integrate watermarking with traditional security measures such as encryption and access control to provide an extra layer of protection against data breaches. This multi-layered security approach helps ensure that even if one method is compromised, the overall integrity of the medical data remains intact.

- **Integration with PACS:** Finally, watermarking is seamlessly integrated with PACS, which are widely used to store and manage medical images. By embedding watermarks into images without significant processing overhead, these systems benefit from improved security while maintaining optimal performance. These real-world applications demonstrate that digital watermarking has become an indispensable tool for securing medical images. From protecting sensitive health records and verifying image integrity to preventing unauthorized AI analysis and ensuring data provenance, watermarking techniques are proving vital in modern e-health systems (128; 35; 125; 124).

4.3 Case Studies and Examples

Digital watermarking is being adopted by hospitals and research universities worldwide to secure medical images. These implementations focus on protecting patient data, verifying image authenticity, and enabling safer telemedicine. Below are key institutions and case studies demonstrating real-world medical image watermarking and its applications and benefits.

4.3.1 Christian Medical College (CMC), Vellore (India)

CMC Vellore, India's leading hospital and medical institution, implemented a pilot watermarking system within its Transfusion Medicine department. In collaboration with Liverpool Hope University, researchers developed software to embed patient details and diagnostic results directly into blood smear images (129). The watermark, inserted in the image's frequency domain, remains intact despite compression or filtering, ensuring metadata integrity. This approach preserves patient IDs and test results within the image, enhancing security and traceability. Clinicians noted improved workflow as images remained confidential, unaltered, and self-contained, eliminating reliance on separate databases and enhancing diagnostic efficiency.

4.3.2 National Technical University of Athens & Hippokratio Hospital (Greece)

In a telemedicine pilot in Athens, researchers from the National Technical University of Athens, in collaboration with the Breast Unit of Hippokratio University Hospital, demonstrated the practical application of digital watermarking for remote diagnostics. Invisible watermarks with patient details, ID numbers, and clinic information were embedded in mammogram images transmitted from a rural health center to city specialists. Clinicians used digital keys to verify authenticity and unlock embedded notes. During a four-week trial involving 39 cases, staff reported that the system was user-friendly, enhanced data security, and maintained image integrity.

4.3.3 Ongoing Adoption in Research and Practice

Recent advances in digital watermarking have demonstrated substantial promise in enhancing the security and integrity of medical images. In one notable case study, the Universitat Oberta de Catalunya (125) implemented a digital watermarking solution to protect medical documents. This system embeds imperceptible watermarks into medical images and records, securely encoding patient identity, clinical history, and treatment protocols to ensure data confidentiality even during transmission over telemedicine networks. The watermark acts as a tamper-evident audit trail, deterring unauthorized alterations and meeting regulatory requirements such as HIPAA. Their studies (published in 2024) stress that embedding watermarks in all medical images can guarantee authenticity and integrity of health data.

In another example, Wei et al. (130) introduced an adversarial watermarking scheme to thwart unauthorized AI analysis by embedding subtle perturbations that mislead deep learning models, thereby reducing diagnostic errors from fake news propagation. Together, these case studies illustrate the practical viability of digital watermarking as a multi-layered security measure that protects health records from fraud and enhances data integrity and trust in modern e-health systems. These studies offer evidence for the broader adoption of watermarking in practice.

Healthcare organizations acknowledge the multifaceted benefits of digital watermarking techniques. Recent medical guidelines advocate the use of visible watermarks to deter misuse of clinical images and protect patient data. For example, a 2024 editorial in a dermatology journal recommends that physicians apply a watermark to images prior to distribution, mitigating risks associated with unauthorized copying or redistribution of patient photographs (131). Visible watermarks, such as institutional logos or text overlays, assert ownership and authenticity, thereby reducing the likelihood of fraudulent exploitation. In contrast, invisible digital watermarks embedded within image data address advanced security concerns by detecting tampering, verifying image origin, and ensuring that patient information remains inherently linked to the image. Collectively, these watermarking strategies are transitioning from experimental research into practical applications within medical workflows.

4.4 Key Applications and Benefits

Actual implementations of medical image watermarking have shown several real applications and benefits:

- **Image Integrity & Tamper Detection:** Embedded watermarks act as an authenticity seal. Hospitals like CMC Vellore used them to ensure images and their findings cannot be altered without detection (129). Any change to the image would disturb the watermark, alerting it to tampering. This is vital for the legal and diagnostic integrity of radiology images.
- **Secure Data Embedding:** Patient identifiers, reports, or hospital logos can be in the image file. This was demonstrated in both the Indian and Greek cases, where patient data and reports were hidden in the images for secure transfer (129; 34). It ensures the correct context (patient info, origin, diagnosis) stays with the image, even across different systems, reducing misidentification and the need for separate paperwork.
- **Telemedicine and Remote Consultation:** Watermarking has proven especially valuable in telemedicine by protecting images sent over the internet. The Athens pilot showed that doctors could confidently exchange

watermarked mammograms, knowing that only authorized clinicians with the key could access the embedded data (26). This provides end-to-end authentication in teleradiology – the remote specialist can verify the image is original and unmodified from the source clinic. Such secure image exchange builds trust in tele-diagnosis, enabling wider adoption of remote healthcare.

- **Preserving Privacy and Confidentiality:** By embedding sensitive data (like patient name or ID) invisibly, watermarking avoids sending that data in plain text or separate files. The watermark can even be encrypted. The Greek study participants felt this approach guaranteed patient privacy while still attaching the needed info for diagnosis (132). Only those with the decryption key can extract the patient's details, adding a layer of privacy beyond standard encryption of channels.

- **Non-Repudiation and Audit Trails:** Hospitals have found that watermarks can serve as a permanent record of who created or altered an image. For example, using a hospital's digital signature or logo as part of the watermark means the image itself carries proof of its source (127). This can prevent disputes (non-repudiation) – neither the sending nor receiving party can deny the authenticity of the image. It also aids audit logs: combined with timestamps or serial numbers embedded, one can trace an image's history directly from the pixel data (129).

- **Maintaining Diagnostic Quality:** An important benefit confirmed by university studies is that robust watermarking techniques can be designed to avoid affecting the diagnostically important parts of the image. Techniques like Region of Interest (ROI) protection or reversible watermarking mean doctors see no visible difference (133). This ensures security measures do not compromise patient care. In trials, radiologists had unchanged opinions with watermarked images, indicating that these methods are viable for clinical use.

- **Efficient Image Management:** Embedding information can streamline workflows. The telemedicine pilot noted more efficient image archiving and retrieval, since images were essentially self-descriptive with key data inside them (133). Likewise, CMC's lab found it convenient that processed results were stored in the image for later review (129). Watermarking thus can

reduce reliance on external databases and keep images and their data in sync, which is beneficial for PACS and long-term records management.

4.5 Discussion

These sources collectively demonstrate the breadth of real applications of digital watermarking in healthcare. From reversible watermarking that ensures full recovery of medical images to adversarial schemes designed to thwart unauthorized AI analysis, these studies provide robust evidence of the technique's effectiveness in maintaining data integrity and authenticity. Additionally, the integration of watermarking with blockchain and advanced optimization algorithms, as shown in several studies, emphasizes the move toward comprehensive security frameworks in telemedicine. These real-world applications not only highlight the current state of the art but also illuminate promising directions for future research and clinical implementation.

4.6 Future Trends and Innovations

- **Adaptive Watermarking Models:** Develop AI-driven systems that dynamically adjust watermark embedding parameters to enhance resilience against diverse attack patterns and high noise conditions.
- **Multi-Modal Biometric Integration:** Incorporate additional biometric modalities, such as iris scans, voiceprints, and gait analysis, in conjunction with traditional fingerprint and palmprint methods to improve authentication robustness.
- **Quantum-Safe Cryptography:** Investigate and integrate postquantum encryption algorithms to ensure that the security of the watermark remains effective in the face of emerging threats from quantum computing.
- **Federated Blockchain Networks:** Design lightweight, decentralized blockchain architectures with efficient consensus mechanisms to reduce latency and improve scalability in medical image sharing.

- **Clinical Validation and Interoperability:** Conduct large-scale clinical trials and evaluate integration with DICOM standards and EHR systems, ensuring ethical AI practices in tamper detection and secure data exchange.

4.7 Conclusion

The reviewed real applications underscore digital watermarking's pivotal role in enhancing medical image security. As demonstrated by these studies, watermarking has been successfully applied in various healthcare contexts from protecting patient data during telemedicine to ensuring the provenance of medical images using blockchain. These cases validate that watermarking, particularly when combined with advanced transforms, biometric data, and cryptographic techniques, is an effective means to address the multifaceted security challenges of modern e-health systems.

Conclusion

This dissertation addresses the critical challenge of securing medical images in e-health applications through advanced digital watermarking techniques. The research question centers on how innovative watermarking methodologies can be developed to ensure robust protection, integrity, and authenticity of medical images while preserving diagnostic quality. The proposed approach integrates DWT, LSB embedding, and biometric features (fingerprints and palmprints) to embed imperceptible watermarks. Additionally, blockchain technology and IPFS are incorporated to enhance traceability and decentralized security. Methodologically, the study introduces two frameworks: MLSF, which combines compression, encryption, and blockchain, and the IDAW scheme, optimizing watermark resilience through chaotic transformations. Experimental evaluations demonstrate exceptional performance, with MLSF achieving a PSNR of 63.24 dB and SSIM of 1.0, ensuring near-perfect imperceptibility. IDAW exhibits robustness against compression, noise, and geometric attacks, maintaining a PSNR of 53.95 dB and SSIM of 0.99996. These results validate the frameworks' ability to balance security, diagnostic fidelity, and computational efficiency, positioning them as viable solutions for modern healthcare systems.

This research advances medical image security through three key innovations.

- **Integrated Security Framework:** The MLSF merges digital watermarking, biometric verification, and blockchain for end-to-end defense. By embedding compressed fingerprint data within the low frequency subbands of DWT, encrypting through AES-256, and employing Ethereum-based IPFS storage, the framework ensures immutability and auditability of medical images, an unprecedented integration in healthcare.

- **Biometric-Driven Watermarking:** The IDAW introduces semi-blind watermarking that combines palmprint biometrics, Arnold Cat Map scrambling, and wavelet-based embedding. This approach achieves minimal distortion while safeguarding images against adversarial attacks, ultimately improving patient identification accuracy.
- **Compression and Efficiency Innovations:** A binary matrix compression strategy reduces watermark payloads by up to 96.48% while preserving feature integrity. With embedding and extraction times recorded at 0.012 and 0.007 seconds, respectively, these advancements demonstrate exceptional computational efficiency.

Collectively, these contributions help fill a gap in the literature where most prior efforts concentrated on single-domain watermarking or overlooked the potential of blockchain for decentralized verification. By empirically demonstrating the practical feasibility of multi-layered security, the thesis substantiates a new paradigm wherein watermarking is no longer viewed in isolation but is integrated within a broader cybersecurity strategy for e-health infrastructures.

Implications

Theoretically, this work expands the scope of digital watermarking theory by integrating chaotic transformations with multi-resolution analysis DWT. The iterative application of ACM to balance imperceptibility and robustness provides a mathematical foundation for future chaos-based security models. Additionally, the compression technique for binary matrices introduces a novel paradigm for optimizing data storage in blockchain networks, contributing to information theory.

The frameworks offer deployable solutions for healthcare practitioners to secure telemedicine platforms, EHRs, and teleradiology systems. Hospitals can utilize MLSF to authenticate medical images during cross-institutional sharing, mitigating the risks of data breaches. The biometric component ensures patient-specific watermarking. Furthermore, the computational efficiency of IDAW makes it suitable for integration into existing PACS without disrupting clinical workflows. This

research supports the global adoption of e-health by enhancing trust in digital diagnostics.

Limitations

Despite its potential, this research faces several limitations that warrant further investigation. First, **the computational overhead** of multi-domain embedding and real-time encryption may impede adoption in resource-constrained settings. At the same time, **user acceptance** could be hindered if new protocols disrupt routine workflows. Additionally, the study relies on curated datasets that might not capture the full diversity of medical imaging modalities or biometric variations globally. Although robust against common attacks, the proposed frameworks exhibit reduced efficacy under **extreme manipulations**. **Scalability remains** a concern, as blockchain-based storage on IPFS can induce latency in low-bandwidth regions. Finally, evolving regulatory standards and blockchain technologies may necessitate **continual re-engineering** for compliance and enhanced security in practical deployment.

This dissertation bridges critical gaps in medical image security by harmonizing advanced watermarking techniques with decentralized technologies. Its contributions enhance the theoretical underpinnings of data protection and provide pragmatic tools for safeguarding patient privacy in an increasingly digital healthcare landscape. As cyber threats evolve, the proposed methodologies offer a resilient foundation for future advancements, ultimately fostering safer, more reliable e-health ecosystems worldwide.

Bibliography

[1] Poonam Kadian, Shiafali M Arora, and Nidhi Arora. Robust digital watermarking techniques for copyright protection of digital data: A survey. *Wireless Personal Communications*, 118:3225–3249, 2021.

[2] Asma Albassam, Fatima Almutairi, Nouf Majoun, Reem Althukair, Zahra Alturaiki, Atta Rahman, and M Mahmud. Integration of blockchain and cloud computing in telemedicine and healthcare. *IJCSNS*, 23(6):17–26, 2023.

[3] Xiaoyi Zhou, Yue Ma, Qingquan Zhang, Mazin Abed Mohammed, and Robertas Damaševičius. A reversible watermarking system for medical color images: balancing capacity, imperceptibility, and robustness. *Electronics*, 10(9):1024, 2021.

[4] Jian Rong and Yutong Liu. Advances in medical imaging techniques. *BMC Methods*, 1(1):10, 2024.

[5] Caroline Omoanatse Alenoghena, Adeiza James Onumanyi, Henry Ohiani Ohize, Achonu Oluwole Adejo, Maxwell Oligbi, Shaibu Ibrahim Ali, and Supreme Ayewoh Okoh. ehealth: A survey of architectures, developments in mhealth, security concerns and solutions. *International Journal of Environmental Research and Public Health*, 19(20):13071, 2022.

[6] A robust authentication and access control protocol for securing wireless healthcare sensor networks. *Journal of Information Security and Applications*, 52:102502, 2020.

[7] Kiran Maharana, Surajit Mondal, and Bhushankumar Nemade. A review: Data pre-processing and data augmentation techniques. *Global Transitions Proceedings*, 3(1):91–99, 2022.

[8] Sondes Ksibi, Faouzi Jaidi, and Adel Bouhoula. A comprehensive study of security and cyber-security risk management within e-health systems:

Synthesis, analysis and a novel quantified approach. *Mobile Networks and Applications*, 28(1):107–127, 2023.

[9] Marco Eichelberg, Klaus Kleber, and Marc Kämmerer. Cybersecurity protection for pacs and medical imaging: deployment considerations and practical problems. *Academic radiology*, 28(12):1761–1774, 2021.

[10] Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Omar Aldabbas, Muath Alshaikh, Abdelkader Laouid, and Mohammad Hammoudeh. A multi-layered security framework for medical imaging: Integrating compressed digital watermarking and blockchain. *IEEE Access*, 12:187604–187622, 2024.

[11] Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Muath AlShaikh, Khaled Chait, and Mohammad Hammoudeh. An efficient semi-blind watermarking technique based on acm and dwt for mitigating integrity attacks. *Arabian Journal for Science and Engineering*, pages 1–21, 2025.

[12] Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Khaled Chait, and Muath AlShaikh. A blind digital watermarking approach using palmprint-embedded local binary patterns and arnold cat map transformations. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pages 1–8. IEEE, 2024. `https://doi.org/10.1109/PAIS62114.2024.10541138`.

[13] Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Muath AlShaikh, and Khaled Chait. An adaptive image watermarking based on bellman-ford algorithm. In *Proceedings of the 7th International Conference on Future Networks and Distributed Systems*, ICFNDS '23, pages 357–365. ACM, 2023. `https://doi.org/10.1145/3644713.3644762`.

[14] Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Ahcene Bounceur, and Mostefa Kara. A decentralized gps positioning consensus based on secure image watermarking for uav networks. In *2024 1st International Conference on Innovative and Intelligent Information Technologies (IC3IT)*, pages 1–6, 2024.

[15] Saja Theab Ahmed, Dalal Abdulmohsin Hammood, Raad Farhood Chisab, Ali Al-Naji, and Javaan Chahl. Medical image encryption: a comprehensive review. *Computers*, 12(8):160, 2023.

[16] Sunpreet Sharma, Ju Jia Zou, Gu Fang, Pancham Shukla, and Weidong Cai. A review of image watermarking for identity protection and verification. *Multimedia Tools and Applications*, 83(11):31829–31891, 2024.

[17] Shi Dong, Khushnood Abbas, Meixi Li, and Joarder Kamruzzaman. Blockchain technology and application: an overview. *PeerJ Computer Science*, 9:e1705, 2023.

[18] National Library of Medicine. Medpix database, 2023. `https://medpix.nlm.nih.gov/`.

[19] Barsha Abhisheka, Saroj Kumar Biswas, Biswajit Purkayastha, Dolly Das, and Alexandre Escargueil. Recent trend in medical imaging modalities and their applications in disease diagnosis: a review. *Multimedia Tools and Applications*, 83(14):43035–43070, 2024.

[20] Jun Li, Junyu Chen, Yucheng Tang, Ce Wang, Bennett A Landman, and S Kevin Zhou. Transforming medical imaging with transformers? a comparative review of key properties, current progresses, and future perspectives. *Medical image analysis*, 85:102762, 2023.

[21] Gazi Imtiyaz Ahmad, Jimmy Singla, and Kaiser J Giri. Security and privacy of e-health data. *Multimedia Security: Algorithm Development, Analysis and Applications*, pages 199–214, 2021.

[22] Bin Zhang, Bahbibi Rahmatullah, Shir Li Wang, AA Zaidan, BB Zaidan, and Penghui Liu. A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations. *Multimedia Tools and Applications*, pages 1–40, 2023.

[23] Ashima Anand and Amit Kumar Singh. Watermarking techniques for medical data authentication: a survey. *Multimedia Tools and Applications*, 80(20):30165–30197, 2021.

[24] Wenbo Wan, Jun Wang, Yunming Zhang, Jing Li, Hui Yu, and Jiande Sun. A comprehensive survey on robust image watermarking. *Neurocomputing*, 488:226–247, 2022.

[25] Anna Melman and Oleg Evsutin. Methods for countering attacks on image watermarking schemes: Overview. *Journal of Visual Communication and Image Representation*, page 104073, 2024.

[26] Solihah Gull and Shabir A Parah. Advances in medical image watermarking: a state of the art review. *Multimedia Tools and Applications*, 83(1):1407–1447, 2024.

[27] Hanan S Alshanbari. Medical image watermarking for ownership & tamper detection. *Multimedia tools and applications*, 80(11):16549–16564, 2021.

[28] K Balasamy and S Suganyadevi. A fuzzy based roi selection for encryption and watermarking in medical image using dwt and svd. *Multimedia tools and applications*, 80(5):7167–7186, 2021.

[29] Narima Zermi, Amine Khaldi, Med Redouane Kafi, Fares Kahlessenane, and Salah Euschi. A lossless dwt-svd domain watermarking for medical information security. *Multimedia Tools and Applications*, 80:24823–24841, 2021.

[30] Mohamed Saber, El-Sayed M El-Kenawy, Abdelhameed Ibrahim, and Marwa M Eid. Watermarking system for medical images using optimization algorithm. *Fusion: Practice & Applications*, 10(1), 2023.

[31] Priyanka Singh, K Jyothsna Devi, Hiren Kumar Thakkar, and Ketan Kotecha. Region-based hybrid medical image watermarking scheme for robust and secured transmission in iomt. *IEEE Access*, 10:8974–8993, 2022.

[32] Zhen Dai, Chunyan Lian, Zhuohao He, Huailong Jiang, and Yifan Wang. A novel hybrid reversible-zero watermarking scheme to protect medical image. *IEEE Access*, 10:58005–58016, 2022.

[33] Med Sayah Moad, Mohamed Redouane Kafi, and Amine Khaldi. Medical image watermarking for secure e-healthcare applications. *Multimedia Tools and Applications*, 81(30):44087–44107, 2022.

[34] Kamred Udham Singh, Hatem Salem Abu-Hamatta, Abhishek Kumar, Achintya Singhal, Mamoon Rashid, and AK Bashir. Secure watermarking scheme for color dicom images in telemedicine applications. *Computers, Materials and Continua*, 70(2):2525–2542, 2021.

[35] Vijay Krishna Pallaw, Kamred Udham Singh, Ankit Kumar, Teekam Singh, Chetan Swarup, and Anjali Goswami. A robust medical image watermarking scheme based on nature-inspired optimization for telemedicine applications. *Electronics*, 12(2):334, 2023.

[36] Kun Hu, Xiaochao Wang, Jianping Hu, Hongfei Wang, and Hong Qin. A novel robust zero-watermarking algorithm for medical images. *The Visual Computer*, 37(9):2841–2853, 2021.

[37] Priyank Khare and Vinay Kumar Srivastava. A secured and robust medical image watermarking approach for protecting integrity of medical images. *Transactions on Emerging Telecommunications Technologies*, 32(2):e3918, 2021.

[38] Fares Kahlessenane, Amine Khaldi, Redouane Kafi, and Salah Euschi. A dwt based watermarking approach for medical image protection. *Journal of Ambient Intelligence and Humanized Computing*, 12(2):2931–2938, 2021.

[39] Muath AlShaikh, Lamri Laouamer, Laurent Nana, and Anca Christine Pascu. Efficient and robust encryption and watermarking technique based on a new chaotic map approach. *Multimedia Tools and Applications*, 76:8937–8950, 2017.

[40] Ashima Anand and Amit Kumar Singh. An improved dwt-svd domain watermarking for medical information security. *Computer Communications*, 152:72–80, 2020.

[41] Junxiu Liu, Jiadong Huang, Yuling Luo, Lvchen Cao, Su Yang, Duqu Wei, and Ronglong Zhou. An optimized image watermarking method based on hd and svd in dwt domain. *IEEE Access*, 7:80849–80860, 2019.

[42] Fauzia Yasmeen and Mohammad Shorif Uddin. An efficient watermarking approach based on ll and hh edges of dwt–svd. *SN Computer Science*, 2(2):82, 2021.

[43] Nayeem Hasan, Md Saiful Islam, Wenyu Chen, Muhammad Ashad Kabir, and Saad Al-Ahmadi. Encryption based image watermarking algorithm in 2dwt-dct domains. *Sensors*, 21(16):5540, 2021.

[44] Seddeq E Ghrare, A Adim Mohamad Alamari, and Hajer Abdulhkim Emhemed. Digital image watermarking method based on lsb and dwt hybrid technique. In *2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, pages 465–470. IEEE, 2022.

[45] Ashwani Kumar. A review on implementation of digital image watermarking techniques using lsb and dwt. *Information and Communication Technology for Sustainable Development: Proceedings of ICT4SD 2018*, pages 595–602, 2020.

[46] Amaal Ghazi Hamad Rafash, Enas Mohammed Hussein Saeed, and Al-Sharify Mushtaq Talib. Development of an enhanced scatter search algorithm using discrete chaotic arnold's cat map. *Eastern-European Journal of Enterprise Technologies*, 6(4):114, 2021.

[47] Rinaldi Munir et al. A secure fragile video watermarking algorithm for content authentication based on arnold cat map. In *2019 4th International Conference on Information Technology (InCIT)*, pages 32–37. IEEE, 2019.

[48] Mehdi Letafati and Safa Otoum. On the privacy and security for e-health services in the metaverse: An overview. *Ad Hoc Networks*, page 103262, 2023.

[49] Ziadeddine MAKHLOUF, Abdallah MERAOUMIA, Laimeche LAKHDAR, and Mohamed Yassine HAOUAM. Enhancing medical data security in e-health systems using biometric-based watermarking. *Applied Computer Science*, 20(1):28–55, 2024.

[50] S Prasanth Vaidya. Fingerprint-based robust medical image watermarking in hybrid transform. *The Visual Computer*, 39(6):2245–2260, 2023.

[51] Ravinder Kumar. Orientation local binary pattern based fingerprint matching. *SN Computer Science*, 1(2):67, 2020.

[52] UD Dixit and MS Shirdhonkar. An improved fingerprint-based document image retrieval using multi-resolution histogram of oriented gradient features. *International Journal of Engineering*, 35(4):750–759, 2022.

[53] Ahlem Adjimi, Abdenour Hacine-Gharbi, Philippe Ravier, and Messaoud Mostefai. Mutual information based feature selection for fingerprint identification. *Informatica*, 43(2), 2019.

[54] Emanuela Marasco, Stefany Cando, Larry Tang, and Elham Tabassi. Cross-sensor evaluation of textural descriptors for gender prediction from fingerprints. In *2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)*, pages 55–62. IEEE, 2019.

[55] Ram Prakash Sharma and Somnath Dey. A comparative study of hand-crafted local texture descriptors for fingerprint liveness detection under real world scenarios. *Multimedia Tools and Applications*, 80(7):9993–10012, 2021.

[56] Abdelouahab Attia, Mourad Chaa, Zahid Akhtar, and Youssef Chahir. Finger knuckle patterns based person recognition via bank of multi-scale binarized statistical texture features. *Evolving Systems*, 11(4):625–635, 2020.

[57] Sergei V. Fotin, David F. Yankelevitz, Claudia I. Henschke, and Anthony P. Reeves. A multiscale laplacian of gaussian (log) filtering approach to pulmonary nodule detection from whole-lung ct scans. *arXiv preprint arXiv:1907.08328*, 2019.

[58] Gang Wang, Carlos Lopez-Molina, and Bernard De Baets. Automated blob detection using iterative laplacian of gaussian filtering and unilateral second-order gaussian kernels. *Digital Signal Processing*, 96:102592, 2020.

[59] Shivanand Gornale, Abhijit Patil, and Mallikarjun Hangarge. Palmprint biometric data analysis for gender classification using binarized statistical image feature set. In *Data Science: Theory, Algorithms, and Applications*, pages 157–167. Springer, 2021.

[60] Nadia Amrouni, Amir Benzaoui, Rafik Bouaouina, Yacine Khaldi, Insaf Adjabi, and Ouahiba Bouglimina. Contactless palmprint recognition using binarized statistical image features-based multiresolution analysis. *Sensors*, 22(24):9814, 2022.

[61] Xu Liang, Jinyang Yang, Guangming Lu, and David Zhang. Compnet: Competitive neural network for palmprint recognition using learnable gabor kernels. *IEEE Signal Processing Letters*, 28:1739–1743, 2021.

[62] Ismail Taha Ahmed, Baraa Tareq Hammad, and Norziana Jamil. Common gabor features for image watermarking identification. *Applied Sciences*, 11(18):8308, 2021.

[63] Palak Jain and Umesh Ghanekar. Robust watermarking technique for textured images. *Procedia Computer Science*, 125:179–186, 2018.

[64] Amit Kumar Singh, Ashima Anand, Zhihan Lv, Hoon Ko, and Anand Mohan. A survey on healthcare data: a security perspective. *ACM Transactions on Multimidia Computing Communications and Applications*, 17(2s):1–26, 2021.

[65] Vani Rajasekar, J Premalatha, and K Sathya. Cancelable iris template for secure authentication based on random projection and double random phase encoding. *Peer-to-Peer Networking and Applications*, 14(2):747–762, 2021.

[66] Ashima Anand and Amit Kumar Singh. Health record security through multiple watermarking on fused medical images. *IEEE Transactions on Computational Social Systems*, 9(6):1594–1603, 2021.

[67] Salman Shamshad, Khalid Mahmood, Saru Kumari, Chien-Ming Chen, et al. A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, 55:102590, 2020.

[68] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy for healthcare blockchains. *IEEE Transactions on Services Computing*, 15(6):3668–3686, 2021.

[69] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3):1–34, 2019.

[70] Nida Fatima, Parul Agarwal, and Shahab Saquib Sohail. Security and privacy issues of blockchain technology in health care—a review. *ICT Analysis and Applications*, pages 193–201, 2022.

[71] Bingqi Liu, Mingzhe Liu, Xin Jiang, Feixiang Zhao, and Ruili Wang. A blockchain-based scheme for secure sharing of x-ray medical images. In *Security with Intelligent Computing and Big-data Services: Proceedings of the Second International Conference on Security with Intelligent Computing and Big Data Services (SICBS-2018) 2*, pages 29–42. Springer, 2020.

[72] Divyanshu Awasthi, Priyank Khare, Vinay Kumar Srivastava, and Amit Kumar Singh. Anfis optimization-based watermarking for securing integrity of medical images with blockchain authentication. *Computers and Electrical Engineering*, 118:109451, 2024.

[73] Abrar Alsehli, Abdul Wadood, and Sanaa Ghouzali. Secure image authentication using watermarking and blockchain. *Intelligent Automation & Soft Computing*, 28(2), 2021.

[74] Ajib Susanto, Eko Hari Rachmawanto, Christy Atika Sari, et al. A robust non-blind image watermarking method using 2-level hwt-dct. In *2018 International Seminar on Application for Technology of Information and Communication*, pages 304–308. IEEE, 2018.

[75] Sanjay Patsariya and Manish Dixit. A new block based non-blind hybrid color image watermarking approach using lifting scheme and chaotic encryption based on arnold cat map. *Traitement du Signal*, 39(4):1159–1168, 2022.

[76] Manasi Jana, Biswapati Jana, and Subhankar Joardar. Local feature based self-embedding fragile watermarking scheme for tampered detection and recovery utilizing ambtc with fuzzy logic. *Journal of King Saud University-Computer and Information Sciences*, 34(10):9822–9835, 2022.

[77] Tzu Chuen Lu, Thanh Nhan Vo, and Biswapati Jana. Dual-image reversible data hiding based on encoding the numeral system of concealed information. In *2023 15th International Conference on Advanced Computational Intelligence (ICACI)*, pages 1–7. IEEE, 2023.

[78] Lamri Laouamer. New informed non-blind medical image watermarking based on local binary pattern. *Traitement du Signal*, 39(5), 2022.

[79] Seyyed Hossein Soleymani, Amir Hossein Taherinia, and Amir Hossein Mohajerzadeh. Waca: a new blind robust watermarking method based on arnold cat map and amplified pseudo-noise strings with weak correlation. *Multimedia Tools and Applications*, 78:19163–19179, 2019.

[80] Khaled Hebbache, Belal Khaldi, Oussama Aiadi, and Ali Benziane. A dwt-based approach with gradient analysis for robust and blind medical image watermarking. *Applied Sciences*, 14(14):6199, 2024.

[81] Mahboubeh Nazari and Mahshid Mehrabian. A novel chaotic iwt-lsb blind watermarking approach with flexible capacity for secure transmission of authenticated medical images. *Multimedia Tools and Applications*, 80(7):10615–10655, 2021.

[82] Sanjay Kumar and Binod Kumar Singh. An improved watermarking scheme for color image using alpha blending. *Multimedia Tools and Applications*, 80:13975–13999, 2021.

[83] Manasi Jana, Biswapati Jana, Tzu-Chuen Lu, Pabitra Pal, Sharmistha Jana, and Subhankar Joardar. A secured reversible data hiding technique for multiple secrets using image interpolation with bit reversal permutation. 2022.

[84] Aditi Zear and Pradeep Kumar Singh. Secure and robust color image dual watermarking based on lwt-dct-svd. *Multimedia Tools and Applications*, 81(19):26721–26738, 2022.

[85] Aulia Arham and Novia Lestari. Secure medical image watermarking based on reversible data hiding with arnold's cat map. *International Journal of Advances in Intelligent Informatics*, 9(3), 2023.

[86] Tao Chen, Zhao Qiu, Gengquan Xie, Lin Yuan, Shaohua Duan, Hao Guo, Dahao Fu, and Hancheng Huang. A image copyright protection method using zero-watermark by blockchain and ipfs. *Journal of Information Hiding and Privacy Protection*, 3(3):131–142, 2021.

[87] Faiza Huma, Maryeama Jahan, Ismat Binte Rashid, and Mohammad Abu Yousuf. Wavelet and lsb-based encrypted watermarking approach to hide patient's information in medical image. In *Proceedings of International Joint*

Conference on Advances in Computational Intelligence: IJCACI 2020, pages 89–104. Springer, 2021.

[88] Ferda Ernawan, Dhani Ariatmanto, and Ahmad Firdaus. An improved image watermarking by modifying selected dwt-dct coefficients. *IEEE Access*, 9:45474–45485, 2021.

[89] Baowei Wang, Shi Jiawei, Weishen Wang, and Peng Zhao. A blockchain-based system for secure image protection using zero-watermark. In *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 62–70. IEEE, 2020.

[90] Lanxiang Chen, Wutong Bai, and Zhiqiang Yao. A secure and privacy-preserving watermark based medical image sharing method. *Chinese Journal of Electronics*, 29(5):819–825, 2020.

[91] Wangsheng Fang, Yuyao Wang, and Xiangyu Wang. Image tampering location and restoration watermarking based on blockchain technology. In *Big Data Analytics for Cyber-Physical System in Smart City: BDCPS 2019, 28-29 December 2019, Shenyang, China*, pages 420–428. Springer, 2020.

[92] Zhaoxiong Meng, Tetsuya Morizumi, Sumiko Miyata, and Hirotsugu Kinoshita. Design scheme of copyright management system based on digital watermarking and blockchain. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 359–364. IEEE, 2018.

[93] Praveen Kumar Mannepalli, Vineet Richhariya, Susheel Kumar Gupta, Piyush Kumar Shukla, and Pushan Kumar Dutta. Block chain based robust image watermarking using edge detection and wavelet transform. 2021.

[94] Ming Li, Leilei Zeng, Le Zhao, Renlin Yang, Dezhi An, and Haiju Fan. Blockchain-watermarking for compressive sensed images. *IEEE Access*, 9:56457–56467, 2021.

[95] Ahmed S. Alghamdi, Surayya Naz, Ammar Saeed, Eesa Al Solami, Muhammad Kamran, and Mohammed Saeed Alkatheiri. A novel database watermarking technique using blockchain as trusted third party. *Computers, Material and Continua (CMC)*, 70(1):1585–1601, 2022.

[96] S. Abolfazl Hosseini and Parya Farahmand. An attack resistant hybrid blind image watermarking scheme based on combination of dwt, dct and pca. *Multimedia Tools and Applications*, 83(7):18829–18852, 2024.

[97] Sahar Haddad, Gouenou Coatrieux, Alexandre Moreau-Gaudry, and Michel Cozic. Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains. *IEEE Transactions on Information Forensics and Security*, 15:2556–2569, 2020.

[98] Abdelkader Laouid, Kara Mostefa, Mohammed Al-Khalidi, Khaled Chait, Mohammad Hammoudeh, and Ahmed Aziz. A binary matrix-based data representation for data compression in blockchain. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*, pages 307–314. IEEE, 2023.

[99] Nayana N. Kumar, R. Senthil Kumar, Riya Rajshekhar Basale, and Mohammed Saffath. Decentralized storage of educational assets using nfts and blockchain technology. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pages 260–266. IEEE, 2022.

[100] N. Sangeeta and Seung Yeob Nam. Blockchain and interplanetary file system (ipfs)-based data storage system for vehicular networks with keyword search capability. *Electronics*, 12(7):1545, 2023.

[101] Sondes Ajili, Mohamed Ali Hajjaji, and Abdellatif Mtibaa. Crypto-watermarking algorithm using weber's law and aes: a view to transfer safe medical image. *Scientific Programming*, 2021:1–22, 2021.

[102] Vildan Atalay Aydin and Hassan Foroosh. Motion compensation using critically sampled dwt subbands for low-bitrate video coding. In *2017 IEEE International Conference on Image Processing (ICIP)*, pages 21–25. IEEE, 2017.

[103] M. Islam and MHK Mehedi. Ct kidney dataset: Normal-cyst-tumor and stone. *Kaggle.com*, 2, 2021.

[104] Dario Maio, Davide Maltoni, Raffaele Cappelli, James L. Wayman, and Anil K. Jain. FVC2000: Fingerprint verification competition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(3):402–412, 2002.

[105] Hong Kong Polytechnic University. Polyu-iitd contactless palmprint images database (version 3.0), 2017. https://www4.comp.polyu.edu.hk/~csajaykr/palmprint3.htm.

[106] kaggle. Pulmonary fibrosis progression png training set, 2020. https://www.kaggle.com/datasets/qitvision/pulmonary-fibrosis-progression-png-training-set.

[107] K. Prabha and I. Shatheesh Sam. An effective robust and imperceptible blind color image watermarking using wht. *Journal of King Saud University-Computer and Information Sciences*, 34(6):2982–2992, 2022.

[108] Shabir Ahmad Parah, Farhana Ahad, Javaid Ahmad Sheikh, and G Mohiuddin Bhat. On the realization of robust watermarking system for medical images. In *2015 Annual IEEE India Conference (INDICON)*, pages 1–5. IEEE, 2015.

[109] Afrig Aminuddin and Ferda Ernawan. Ausr2: Image watermarking technique for authentication and self-recovery with image texture preservation. *Computers and Electrical Engineering*, 102:108207, 2022.

[110] De Rosal Igantius Moses Setiadi. Psnr vs ssim: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*, 80(6):8423–8444, 2021.

[111] Umme Sara, Morium Akter, and Mohammad Shorif Uddin. Image quality assessment through fsim, ssim, mse and psnr—a comparative study. *Journal of Computer and Communications*, 7(3):8–18, 2019.

[112] Mario Gonzalez-Lee, Hector Vazquez-Leal, Jose Francisco Gomez-Aguilar, Luis J Morales-Mendoza, Victor Manuel Jimenez-Fernandez, Juan R Laguna-Camacho, and Celia M Calderon-Ramon. Exploring the cross-correlation as a means for detecting digital watermarks and its reformulation into the fractional calculus framework. *IEEE Access*, 6:71699–71718, 2018.

[113] Christy Atika Sari, Eko Hari Rachmawanto, et al. Robust and imperceptible image watermarking by dc coefficients using singular value decomposition. In *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, pages 1–5. IEEE, 2017.

[114] Ertugrul Gul and Serkan Ozturk. A novel hash function based fragile watermarking method for image integrity. *Multimedia Tools and Applications*, 78:17701–17718, 2019.

[115] Aditya Kumar Sahu. A logistic map based blind and fragile watermarking for tamper detection and localization in images. *Journal of Ambient Intelligence and Humanized Computing*, 13(8):3869–3881, 2022.

[116] Sanjay Kumar and Binod Kumar Singh. Dwt based color image watermarking using maximum entropy. *Multimedia Tools and Applications*, 80:15487–15510, 2021.

[117] Redouane Kaibou, Mohamed Salah Azzaz, Mustapha Benssalah, Djamel Teguig, Hocine Hamil, Amira Merah, and Meriam Tinhinane Akrour. Real-time fpga implementation of a secure chaos-based digital crypto-watermarking system in the dwt domain using co-design approach. *Journal of Real-Time Image Processing*, 18(6):2009–2025, 2021.

[118] Omer Faruk Saritas and Serkan Ozturk. A color channel multiplexing approach for robust discrete wavelet transform based image watermarking. *Concurrency and Computation: Practice and Experience*, 34(25):e7255, 2022.

[119] Ahmed A Mohammed, Bilal A Jebur, and Karam M Younus. Hybrid dct-svd based digital watermarking scheme with chaotic encryption for medical images. In *IOP Conference Series: Materials Science and Engineering*, volume 1152, page 012025. IOP Publishing, 2021.

[120] M. Sajeer and Ashutosh Mishra. A robust and secured fusion based hybrid medical image watermarking approach using rdwt-dwt-msvd with hyper-chaotic system-fibonacci q matrix encryption. *Multimedia Tools and Applications*, 82(24):37479–37501, 2023.

[121] Shaifali M. Arora et al. A dwt-svd based robust digital watermarking for digital images. *Procedia Computer Science*, 132:1441–1448, 2018.

[122] Khalid M. Hosny and Mohamed M. Darwish. Resilient color image watermarking using accurate quaternion radial substituted chebyshev moments.

ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 15(2):1–25, 2019.

[123] Jinan N Shehab, Hussein A Abdulkadhim, and Yousif Allbadi. Blind image watermarking scheme based on lowest energy contourlet transform coefficient and modified arnold cat/ikeda maps. *Indonesian Journal of Electrical Engineering and Computer Science*, 21(1):196–207, 2021.

[124] Hamidreza Zarrabi, Mohsen Hajabdollahi, SM Reza Soroushmehr, Nader Karimi, Shadrokh Samavi, and Kayvan Najarian. Reversible image watermarking for health informatics systems using distortion compensation in wavelet domain. In *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 798–801. IEEE, 2018.

[125] European Universities Association. Digital watermarking to prevent fraud: from medical images to fake news, 27 juin 2024. `https://www.uoc.edu/en/news/2024/digital-watermarking-to-protect-medical-documents`.

[126] Vijay Kumar and Kolin Paul. Medical image data provenance for medical cyber-physical system. *arXiv preprint arXiv:2403.15522*, 2024.

[127] A Hassani Allaf and M Ait Kbir. A review of digital watermarking applications for medical image exchange security. In *Innovations in Smart Cities Applications Edition 2: The Proceedings of the Third International Conference on Smart City Applications*, pages 472–480. Springer, 2019.

[128] Ashima Anand, Amit Kumar Singh, Zhihan Lv, and Guarav Bhatnagar. Compression-then-encryption-based secure watermarking technique for smart healthcare system. *IEEE MultiMedia*, 27(4):133–143, 2020.

[129] Atulya K. Nagar, Robinson Thamburaj, F. Sheeba, P. M. Maqlin, Titus Thevarthundiyil, and J. J. Mammen. Segmentation and watermarking of peripheral blood smear images, 2013. `https://impact.ref.ac.uk/casestudies/CaseStudy.aspx?Id=42638`.

[130] Xingxing Wei, Bangzheng Pu, Shiji Zhao, Chen Chi, and Huazhu Fu. Preventing unauthorized ai over-analysis by medical image adversarial watermarking. *arXiv preprint arXiv:2303.09858*, 2023.

[131] Kelita A Waterton, Stephanie Chan, Jane Yoo, Diane Jackson-Richards, and Naiara S Barbosa. Best practices for clinical image collection and utilization in patients with skin of color, 2024.

[132] Rasha Thabit. Review of medical image authentication techniques and their recent trends. *Multimedia Tools and Applications*, 80(9):13439–13473, 2021.

[133] Kaiser J Giri, Zubair Jeelani, Javaid Iqbal Bhat, and Rumaan Bashir. Survey on reversible watermarking techniques for medical images. *Multimedia Security: Algorithm Development, Analysis and Applications*, pages 177–198, 2021.