

الجمهورية الجزائرية الديمقراطية الشعبية

DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

جامعة أبي بكر بلقايد - تلمسان

Abou Bekr Belkaid University -Tlemcen-

Faculty of Technology



THESE

Presented to obtain the degree of DOCTORATE Third Cycle

In: Biomedical Engineering

Speciality: Biomedical Informatics and Telemedicine

By: ABDI Hadjer

Topic

Medical Imaging Data Security

Publicly defended, on 1st June 2024, to the jury composed of :

Mr. Hadj Slimane Zine Eddine	Professeur	Univ. Tlemcen	President
Mr BOUKLI HACENE Ismail	Professeur	Univ. Tlemcen	Supervisor
Mr. Bendelhoum Mohammed Sofiane	MCA	University Center of El Bayadh	Examiner
Mr. Bengana Abdelfatih	MCA	Univ. Tlemcen	Examiner

Abstract

Telemedicine leverages advanced technologies to enhance healthcare, making it more accessible and cost-effective. This includes improved sharing of medical imaging data for accurate diagnoses and treatments. However, data exchange raises privacy and security concerns.

This thesis aims to enhance medical imaging data security by embedding digital watermarks and the Electronic Patient Record (EPR) within images, ensuring data integrity and confidentiality. It combines Lifting Wavelet Transform (LWT) and Fast Walsh Hadamard Transform (FWHT) for robustness and imperceptibility, with additional security via Error Correcting Code (ECC) and chaotic encryption.

The Artificial Bee Colony (ABC) algorithm further enhances performance. Testing on various datasets showed the method's superiority over traditional techniques using metrics such as PSNR, SSIM, NC, and BER.

Keywords: Medical Images, Medical Data Security, Data Integrity, Digital Watermarking, Encryption, Lifting Wavelet Transform, Fast Walsh Hadamard Transform, Artificial Bee Colony.

ملخص

يعتمد استخدام الطب عن بعد على التقنيات المتقدمة لتحسين الرعاية الصحية وجعلها أكثر سهولة وأقل تكلفة. يتضمن ذلك تحسين مشاركة بيانات التصوير الطبي من أجل تشخيص وعلاج أكثر دقة. ومع ذلك، يثير تبادل البيانات مخاوف بشأن الخصوصية والأمان.

تهدف هذه الأطروحة إلى تعزيز أمن بيانات التصوير الطبي من خلال تضمين علامات مائية رقمية والسجل الطبي الإلكتروني (EPR) داخل الصور، مما يضمن سلامة البيانات وسرية المريض. تجمع الدراسة بين تحويل موجة الرفع (LWT) وتحويل والش هادامارد السريع (FWHT) لتحقيق المتانة وعدم الإدراك، مع تعزيز الأمان باستخدام رمز تصحيح الخطأ (ECC) والتشفير الفوضوي. علاوة على ذلك، تعمل خوارزمية مستعمرة نحل العسل الاصطناعي (ABC) على تحسين أداء النظام بشكل أكبر. وأظهرت الاختبارات التي أجريت على مجموعات بيانات مختلفة تفوق هذه الطريقة على الأساليب التقليدية باستخدام معايير مثل PSNR , SSIM , NC , BER.

الكلمات المفتاحية: الصور الطبية، أمن البيانات الطبية، سلامة البيانات، العلامات المائية الرقمية، التشفير، تحويل المويجات الرفعية، تحويل والش هادامارد السريع، مستعمرة النحل الاصطناعية.

Résumé

La télémédecine exploite les technologies avancées pour améliorer les soins de santé, les rendant plus accessibles et rentables. Cela inclut une meilleure partage des données d'imagerie médicale pour des diagnostics et traitements précis. Cependant, l'échange de données soulève des préoccupations en matière de confidentialité et de sécurité.

Cette thèse vise à améliorer la sécurité des données d'imagerie médicale en intégrant des filigranes numériques et le dossier médical électronique (DME) dans les images, garantissant l'intégrité et la confidentialité des données. Elle combine la transformation en ondelettes par relèvement (LWT) et la transformation rapide de Walsh-Hadamard (FWHT) pour la robustesse et l'imperceptibilité, avec une sécurité supplémentaire via le code de correction d'erreurs (ECC) et le cryptage chaotique.

L'algorithme de la colonie d'abeilles artificielle (ABC) améliore encore les performances. Les tests sur divers ensembles de données ont montré la supériorité de la méthode par rapport aux techniques traditionnelles en utilisant des métriques telles que PSNR, SSIM, NC et BER.

Mots Clée : Images médicales, Sécurité des données médicales, Intégrité des données, Tatouage numérique, Chiffrement, Transformation en Ondelettes par Lifting, Transformation de Walsh Hadamard Rapide, Colonie d'Abeilles Artificielles

Dedication

À mon père, son amour inconditionnel et son soutien indéfectible ont été les fondements de mon parcours académique. Sa présence bienveillante a été la boussole qui a guidé chacun de mes pas vers la réussite. Sans lui, je n'aurais jamais été où je suis aujourd'hui. Un homme exceptionnel et source inépuisable d'inspiration.

À ma mère, sa bienveillance infinie a été la toile douce qui a tissé les moments de ma vie, me fournissant force et réconfort.

À mon frère *HABIB*, son soutien inébranlable et son encouragement ont éclairé chaque étape de cette aventure.

À mon cher mari *ABEDEASSEMAD*, pour son amour constant, son soutien, et surtout, sa patience remarquable

À tous ceux qui ont généreusement apporté leur soutien tout au long de cette aventure. Un merci particulier à *THAMI, ABDEALLATIF, TOURKIA*, la famille *CHALABI, et SAFYA*. Votre contribution a grandement enrichi cette expérience.

À mes chères amies *SOUMEYA, MERIEM et CHAIMA*.

À toute ma famille et belle famille.

ABDI-Hadjer

Acknowledgments

First and foremost, I wish to extend my deepest gratitude to Mr. I. BOUKLI HACENE, Professor at Abou-Bekr Belkaïd University, for his invaluable guidance and unwavering support throughout the entirety of this research endeavor. His profound wisdom and extensive knowledge, coupled with his high expectations and constructive critiques, have steered me through this work. The numerous discussions throughout this journey were highly enriching and fruitful. He adeptly initiated me into the spirit of research with rigor and efficiency, while also sharing his experience and expertise in this field of scientific inquiry.

I extend my sincere thanks to Pr. Hadj Slimane Zine Eddine, for graciously presiding over the thesis jury. I appreciate his valuable support and contribution to this academic work.

Dr. Bendelhoum Mohammed Sofiane and Dr. Bengana Abdelfatih had the honor of reviewing this thesis. I extend my heartfelt gratitude for their thorough examination, insightful comments, and valuable contributions.

I would like to express sincere gratitude to all of the Biomedical Engineering Laboratory members for their support. I want to extend my heartfelt gratitude to Chaima CHERFI, Meriem SAIM, Amina BENAHMED, Fatiha YOUBI, and Hafida BELFILALI, whose great contributions played a pivotal role in the success of this journey.

Lastly, I extend my sincere thanks to all those who have assisted and supported me throughout this period. Your contributions, whether direct or indirect, have been invaluable.

Contents

List of Figures	i
List of Tables	iv
List of Algorithms	v
Abbreviations	vi
General Introduction	1
1 MEDICAL DATA SECURITY (BASIC NOTION)	5
1.1 Introduction	6
1.2 Medical Imaging Security	6
1.2.1 Medical Data Security Threats	7
1.2.2 Medical Imaging Modalities	7
1.2.2.1 Magnetic Resonance Imaging	8
1.2.2.2 Radiography	9
1.2.2.3 Computed Tomography Scan	10
1.2.2.4 Ultrasound Imaging	11
1.2.3 Main Requirements of Data Security	13
1.2.3.1 Data Availability	13
1.2.3.2 Data Integrity	13
1.2.3.3 Data Confidentiality	14
1.3 Digital Watermarking	14
1.3.1 Image Watermarking Algorithm	15
1.3.1.1 Watermark Embedding Process	16

1.3.1.2	Watermark Extraction process	16
1.3.2	Algorithm Classification	17
1.3.2.1	Cover Type	17
1.3.2.2	Watermark Visibility	17
1.3.2.3	Watermark Robustness	17
1.3.2.4	Embedding Domain	18
1.3.3	Digital Watermarking Requirements	19
1.3.3.1	Imperceptibility	19
1.3.3.2	Robustness	19
1.3.3.3	Embedding Capacity	19
1.3.4	Digital Watermarking Applications	19
1.3.4.1	Content Authentication	20
1.3.4.2	Ownership Protection	20
1.3.4.3	Transaction Tracking	20
1.4	Image Encryption	20
1.4.1	Algorithm	21
1.4.1.1	Encryption Process	21
1.4.1.2	Decryption Process	21
1.4.2	Classification	21
1.4.2.1	Symmetric Encryption	22
1.4.2.2	Asymmetric Encryption	23
1.5	Conclusion	23
2	LITERATURE REVIEW	24
2.1	Introduction	25
2.2	Problematic and solution	25
2.3	Literature Review	27
2.3.1	Medical image watermarking techniques	27
2.3.2	Electronic Patient Record	30
2.3.3	Meta-Heuristic Algorithms	32
2.4	Challenges and Future Directions	37
2.5	Conclusion	37
3	WATERMARKING ALGORITHMS BASED ON WAVELET DO-	
	MAIN TRANSFORM	39
3.1	Introduction	40
3.2	The Wavelet Transform	40
3.2.1	2D-Discrete Wavelet Transform	41

3.2.1.1	2D-Discrete Wavelet Transform Limtes	44
3.2.2	The Lifting Scheme	44
3.2.2.1	Lifting Scheme Properties	46
3.2.3	Wavelet Families	47
3.2.3.1	Haar Wavelets	47
3.2.3.2	Daubechies wavelets	48
3.2.3.3	Symlet wavelets	48
3.2.3.4	Biorthogonal wavelets	49
3.2.3.5	Coiflet Wavelets	49
3.2.3.6	Meyer wavelets	49
3.3	Evaluation Measures	52
3.3.1	Peak Signal-to-Noise Ratio	52
3.3.2	Structural Similarity Index	53
3.3.3	Normalized Correlation	53
3.3.4	Bit Error Rate	54
3.4	Watermarking Algorithm Based On Wavelet Domain	54
3.4.1	1 st Experiment: Wavelet Selection	55
3.4.1.1	Imperceptibility And Robustness Results	56
3.4.1.2	Results Discussion	62
3.4.2	2 nd Experiment: LWT-Based watermarking	63
3.4.2.1	Imperceptibility And Robustness Results	63
3.5	Conclusion	67

4 EXPLORING HYBRID TECHNIQUES AND OPTIMIZATION ALGORITHMS IN MEDICAL IMAGE WATERMARKING 69

4.1	Introduction	70
4.2	Hybrid Watermarking Techniques	71
4.2.1	Fast Walsh-Hadamard Transform	71
4.2.1.1	Hadamard Matrices	72
4.2.1.2	The Fast Walsh-Hadamard Structure	72
4.2.1.3	The Fast Walsh-Hadamard Scheme Properties	73
4.2.2	Singular Value Decomposition	73
4.2.2.1	The Mathematical Perception Behind The SVD	74
4.2.2.2	Characteristics Features of SVD	74
4.2.2.3	SVD Limitation	75
4.2.3	Discrete Cosine Transform	75
4.2.3.1	Formulation	75
4.2.3.2	Properties of DCT	76

4.2.3.3	DCT Limitation	77
4.2.4	Comparative Analysis of Hybrid Approaches	77
4.2.4.1	Error-Correcting Code	77
4.2.4.2	Chaotic maps	79
4.2.4.3	Speeded-Up Robust Features	81
4.2.4.4	Methodology	82
4.2.4.5	Result and Discussion	82
4.3	Optimization Techniques in Watermarking	96
4.3.1	Artificial Bee Colony Algorithm	96
4.3.1.1	General Scheme	96
4.3.2	Methodology:	98
4.3.3	Results and Discussion	99
4.4	Conclusion	109
Conclusion		110
ANNEXES		114
A	Medical Images Data Set	114
A.1	Magnetic Resonance Imaging	114
A.2	Ultrasound	116
A.3	X-ray	117
A.4	CT-scan	118
Bibliography		119
Publications		128

List of Figures

1.1	Normal and Abnormal X-ray Images[1]	7
1.2	Brain MRI Image [2]	8
1.3	Chest X-Ray Image[1]	9
1.4	Brain CT-Scan Image [3]	10
1.5	Ultrasound Image[4]	12
1.6	A general Scheme of The Watermarking System	16
1.7	Symmetric Key Encryption	22
1.8	Asymmetric Key Encryption	23
2.1	Evolution of the Number of Research Papers on Medical Data Security Since the 1990s	26
3.1	Discrete Wavelet Decomposition	43
3.2	Two-level Decomposition of Wavelet Transform	43
3.3	Lifting Wavelet Decomposition	45
3.4	Some Wavelet Families.	51
3.5	Medical Images Used for the Test [2, 3, 1, 5]	56
3.6	Medical Image Watermarking Algorithm Based on 2D-DWT	58
3.7	Imperceptibility Performance of Each Wavelet	61
3.8	Robustness Performance of Each Wavelet (NC Results)	62
3.9	Watermarking Algorithm Based on LWT	64
4.1	The Effect of Arnold's Cat Map on the Watermark After N Iterations	81
4.2	LWT/FWHT Based Watermarking Algorithm: Embedding Process	85
4.3	LWT/FWHT Based Watermarking Algorithm: Extraction Process	85
4.4	Imperceptibility Performance For Normal Medical Images	86

4.5	Imperceptibility Performance For Abnormal Medical Images	87
4.6	NC and SSIM Performance for Normal Medical Images: Filtering Attacks	90
4.7	NC and SSIM Performance for Normal Medical Images: Noise Addition Attacks	90
4.8	NC and SSIM Performance for Normal Medical Images: Geometric, Compression and Histogram Attacks	91
4.9	NC and SSIM Performance for Abnormal Medical Images: Filtering Attacks	91
4.10	NC and SSIM Performance for Abnormal Medical Images: Noise Addition Attacks	92
4.11	NC and SSIM Performance for Abnormal Medical Images: Geometric, Compression and Histogram Attacks	92
4.12	BER Performance for Normal Medical Images	93
4.13	BER Performance for Abnormal Medical Images	94
4.14	ABC-Based Watermarking Algorithm	99
4.15	NC and SSIM Performance for Normal Medical Images After Optimization: Filtering Attacks	101
4.16	NC and SSIM Performance for Normal Medical Images After Optimization: Noise Addition Attacks	101
4.17	NC and SSIM Performance for Normal Medical Images After Optimization: Geometric, Compression and Histogram Attacks	102
4.18	NC and SSIM Performance for Abnormal Medical Images After Optimization: Filtering Attacks	102
4.19	NC and SSIM Performance for Abnormal Medical Images After Optimization: Noise Addition Attacks	103
4.20	NC and SSIM Performance for Abnormal Medical Images After Optimization: Geometric, Compression and Histogram Attacks	103
4.21	BER Performance for Normal Medical Images	104
4.22	BER Performance for Abnormal Medical Images	105
4.23	Comparative Performance Analysis: Evaluating the Imperceptibility of the Proposed Method Before and After ABC Optimization	106
4.24	Comparative Performance Analysis: Evaluating the Robustness of the Proposed Method Before and After ABC Optimization	107
4.25	Source of MRI Images for Watermarking Algorithm	115
4.26	A Sample of MRI Images Selected from the Four Folders	115
4.27	Source of Ultrasound Images for Watermarking Algorithm	116
4.28	A Sample of Ultrasound Images	116

4.29 Source of X-ray Images for Watermarking Algorithm	117
4.30 A Sample of X-ray Images	117
4.31 Source of CT Scan Images for Watermarking Algorithm	118
4.32 A Sample of CT scan Images	118

List of Tables

1.1	Requirements of Medical Data Security	14
2.1	A Comprehensive Summary of the Latest Advancements in Medical Image Watermarking Techniques	38
3.1	Comparison of 2D-DWT and LWT	44
3.2	The Impact of Wavelet Families on the Imperceptibility of Medical Images	59
3.3	The Impact of Wavelet Families on the Robustness of the Extracted Watermark.	60
3.4	PSNR and SSIM Results of the Watermarked Image	66
3.5	Robustness Results of the Watermarked Image	67
4.1	Imperceptibility Assessment of LWT-FWHT Watermarking Algorithm on Normal and Abnormal Medical Images	84
4.2	Comparison of the Proposed Technique With Existing Techniques	95
4.3	Robustness of Proposed Technique and Existing Techniques for Non-medical Image	95
4.4	Robustness of Proposed Technique and Existing Techniques Under Different Attacks	95
4.5	ABC Parameters	98
4.6	Imperceptibility Performance After Using ABC Optimization Algorithm	100
4.7	Comparison of the Proposed Technique With Similar Schemes in Terms of PSNR Using Standard Images	107
4.8	Robustness Comparison: Evaluating the Performance of the Proposed Technique Against Similar Schemes Using Standard Images	108

List of Algorithms

1	Embedding rules	55
2	Extraction rules	57
3	LWT Based Embedding Algorithm	65
4	LWT Based Extraction Algorithm	66
5	LWT/FWHT Based Embedding Algorithm	83
6	LWT/FWHT Based Extraction Algorithm	84

LIST OF ABBREVIATIONS

A

ABC Artificial Bee Colony

AES Advanced Encryption Standard

AIC Security requirements: Availability, Integrity, and Confidentiality

B

BER Bit Error Rate

BCH Bose–Chaudhuri–Hocquenghem

BiorN Biorthogonal wavelets of order N

C

CT Computed Tomography

CoifN Coiflet wavelets of order N

D

dB Decibel

DCT Discrete Cosine Transform

DFT Discrete Fourier Transform

DbN Daubechies wavelets of order N

DWT Discrete Wavelet Transform

E

ECC Error Correcting Code

EPR Electronic Patient Record

F

FWHT Fast Walsh-Hadamard Transform

G

GA Genetic Algorithm

I

ICA Independent Component Analysis

IMARC Group The International Market Analysis Research and Consulting Group

IoT Internet of Things

J

JPEG Joint Photographic Experts Group

L

LSB Least Significant Bit

LWT Lifting Wavelet Transform

LZW Lempel-Ziv-Welch

M

MD5 Message Digest Algorithm 5

MFrLFMs Multi-Channel Fractional Legendre-Fourier Moments

MRI Magnetic Resonance Imaging

N

NCC Normalized Cross-Correlation

NC Normalized Correlation

P

PRNG Pseudo-Random Number Generator

PSBFO Particle Swarm Bacterial Foraging Optimization

PSNR Peak Signal-to-Noise Ratio

PSO Particle Swarm Optimization

Q

QIM Quantization Index Modulation

R

ROI Region of Interest

RONI Region of No-Interest

S

SSIM Structural Similarity Index

SURF Speeded-Up Robust Features

SVD Singular Value Decomposition

U

USD United States Dollar

US Ultrasound

W

WHT Walsh-Hadamard Transform

WPT Wavelet Packet Transform

WT Wavelet Transform

General Introduction

With the appearance of digitization and automated data processing, the healthcare sector has taken advantage of the new technologies of information and communication where a new practice of medicine has been developed known as Telemedicine. This innovative practice of medicine leverages advanced technologies to facilitate remote patient care, breaking down geographical barriers and enhancing accessibility to healthcare services.

The term 'Telemedicine' encompasses a broad concept, including various medical practices such as teleconsultation, tele-expertise, tele-monitoring, etc. The primary objective of these practices is to enable patients to receive remote care, bringing about significant positive changes across the health sector. Firstly, telemedicine enhances access to information, helping healthcare professionals stay well-informed for better decision-making. Additionally, it facilitates the delivery of care in ways that were once challenging, expanding healthcare services. This not only improves access to services but also increases overall care delivery. Lastly, the integration of technology leads to a reduction in healthcare costs, making quality healthcare more sustainable and accessible to a broader population [6].

At the same time, the incorporation of Telemedicine into healthcare practices brings about various shifts in how medical data is handled, providing greater availability and accessibility compared to previous approaches.

Medical data can take many forms, including medical images, Electronic Patient Records (EPR) containing personal information, blood test results, and recordings of physiological signals. This multifaceted data compilation provides a comprehensive view of a patient's health, allowing for a more comprehensive approach to medical care and diagnostics.

In the same context, medical imaging data, a type of medical information, plays an important role in diagnosing and treating patients. This category of medical

data includes technologies and tools used to provide precise and detailed images to healthcare professionals. These images aid in the comprehension and evaluation of a patient's internal structures and functions, providing valuable insights into a variety of conditions such as injuries, diseases, tumors, and abnormalities. Such insights enable healthcare professionals to develop precise treatment plans and interventions. Various sophisticated imaging techniques include, but are not limited to, X-rays, computed tomography (CT), magnetic resonance imaging (MRI), and ultrasound. Each modality in medical imaging has distinct characteristics that are shaped by factors such as contrast, resolution, and noise. Furthermore, even within a single imaging modality, there is a diversity of images, emphasizing the nuanced nature of these advanced diagnostic tools [7].

Despite significant advances in the health sector, medical data security remains a critical challenge that requires attention and resolution. Indeed, the use and transmission of medical data in Telemedicine raise important issues, such as the need for robust security measures to protect patient privacy and compliance with applicable healthcare regulations.

Medical data protection is critical because it is highly sensitive and directly affects patients' lives. Regardless of the circumstances, this data should always be kept unchanged and unaltered.

To achieve this objective, the Telemedicine system needs to conform to specific requirements, particularly those pertaining to medical data. The critical requirements include ensuring the integrity of medical data to protect it from modifications, ensuring the confidentiality of patient information by restricting access only to authorized individuals (including patients and healthcare professionals), and ensuring continuous availability, allowing the data to be accessible at any moment.

Security measures in the context of medical imaging data involve a variety of techniques aimed at ensuring the integrity, confidentiality, and availability of medical information.

These technologies include encryption methods for secure data transmission. It is the process of protecting digital images from unauthorized access and maintaining their confidentiality. The use of cryptography algorithms to transform the pixel values or representation of an image in such a way that it becomes incomprehensible without the proper decryption key is involved in this technique.

Furthermore, as another security measure, digital watermarking is frequently used to embed invisible marks within medical images. This process provides a unique form of identification, improving traceability and contributing to the integrity and authenticity of medical images. Meantime, digital watermarking has emerged as a promising solution for securing medical imaging data, offering efficiency as well as

increased security. This security technology is an effective method for preventing unauthorized access to or tampering with critical medical images.

One of the most difficult challenges in medical image watermarking is maintaining the watermark's imperceptibility while avoiding interference with the diagnostic quality of the medical image. Another significant challenge is choosing a technique appropriate to the medical image's specific nature while keeping in mind that each modality has distinctive features.

In this thesis, we are interested in medical imaging data security. The primary goal is to create a strong security system that is specifically designed to protect medical images and the patient's personal information.

In order to achieve this objective, we used digital watermarking technology to embed a digital watermark within the medical image, to protect its integrity and authenticity. In addition, we incorporated the Electronic Patient Record with the medical image to reduce the risk of data loss and ensure patient confidentiality and privacy. To maintain the imperceptibility and robustness requirements of digital watermarking algorithms. This approach involved the integration of the lifting wavelet transform (LWT) in conjunction with the fast Walsh Hadamard Transform (FWHT). Additionally, we heightened the security of our methodology by encoding the EPR using an Error Correcting Code (ECC) and encrypting the watermark image through a chaotic encryption process.

To organize and address specific elements within our bibliographies and simulations, we have structured this memory into distinct chapters. Each chapter is devoted to a distinct theme that intricately contributes to our research's general topic.

In the first chapter, we explored various medical imaging modalities, emphasizing the distinctive features that characterize medical images including resolution, contrast, and noise. Following that, we provided a thorough explanation of the requirements for securing and protecting medical imaging data. Lastly, we provided a theoretical overview of image security, with a particular emphasis on digital watermarking and encryption. We offered a thorough discussion of techniques, algorithms, and the classification of each security measure.

In the second chapter, we discussed the difficulties associated with securing medical imaging data. We introduced digital watermarking as a promising solution for improving the efficiency and security of target data. It is important to note that this conclusion was reached after a thorough review of the literature presented in this chapter.

In the third chapter, we conducted a study to examine the influence of the wavelet transform on digital watermarking algorithms. We began by discussing the theoretical aspects of the wavelet technique, including the discrete wavelet transform and

the lifting wavelet transform, as well as various wavelet families. The theoretical aspects were then applied to a medical image watermarking simulation. Our goal was to identify the best wavelet family and wavelet transform for the medical image watermarking algorithm using rigorous analysis.

In the fourth chapter, we introduced a hybrid security system based on the Lifting Wavelet Transform (LWT) and the Fast Walsh-Hadamard Transform (FWHT). This system's security was enhanced with additional safeguards such as Error Correcting Code (ECC) and chaotic encryption. Following that, we investigated Meta-heuristic algorithms to optimize the proposed system, with a particular emphasis on the ABC algorithm.

The final section of our research is dedicated to summarizing the findings in the field of medical data security, providing a synthesis, and illuminating future directions for this field of study.

Chapter : 1

***MEDICAL DATA SECURITY (BASIC
NOTION)***

Contents

1.1	Introduction	6
1.2	Medical Imaging Security	6
1.2.1	Medical Data Security Threats	7
1.2.2	Medical Imaging Modalities	7
1.2.3	Main Requirements of Data Security	13
1.3	Digital Watermarking	14
1.3.1	Image Watermarking Algorithm	15
1.3.2	Algorithm Classification	17
1.3.3	Digital Watermarking Requirements	19
1.3.4	Digital Watermarking Applications	19
1.4	Image Encryption	20
1.4.1	Algorithm	21
1.4.2	Classification	21
1.5	Conclusion	23

1.1 Introduction

The usage of information and communication technology in the healthcare sector has grown, enabling patients and medical personnel to transfer, store, and exchange medical information. This evolution is evident in the implementation of a Hospital Management System (HMS), which handles the medical, administrative, and financial procedures of health facilities. Additionally, e-health applications have extensively utilized Internet of Things (IoT) technology to enhance healthcare services.

Nevertheless, medical data has become exposed to the risk of unlawful attacks, which endanger patients' lives by leading to incorrect diagnoses or inappropriate treatments. This raises concerns about the security of this sensitive information. Although security techniques used for the protection of medical data have undergone significant development due to the technological revolution, it remains challenging to optimize and enhance these techniques to keep up with the continuous evolution of healthcare services.[8, 9].

In this chapter, we will discuss the different types of medical imaging modalities and highlight the unique features that distinguish medical images. Additionally, we will explore the fundamental requirements necessary to ensure the protection and security of this valuable data.

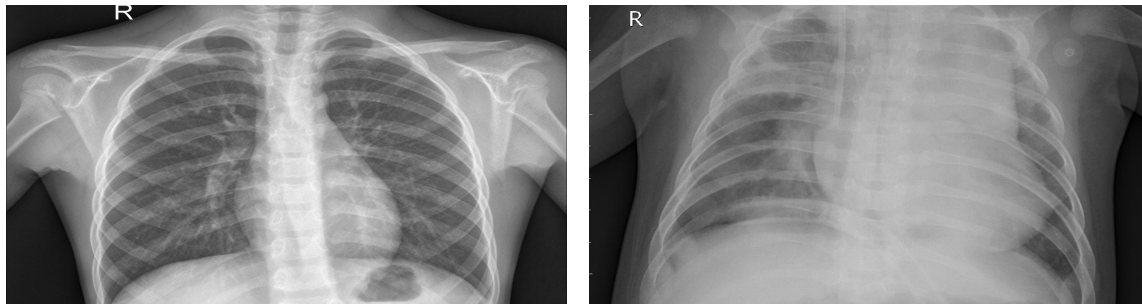
1.2 Medical Imaging Security

Medical imaging describes the technologies and tools used to provide healthcare professionals with detailed and accurate images that aid in understanding and assessing a patient's internal structures and functions and obtain valuable insights into various conditions, including injuries, diseases, tumors, and abnormalities, enabling them to formulate appropriate treatment plans and interventions. [7]

These advanced imaging techniques include a wide range of modalities such as X-rays, computed tomography (CT), magnetic resonance imaging (MRI), and ultrasound, among others. Each modality within medical imaging exhibits unique characteristics that are influenced by various factors, including contrast, resolution, and noise. Furthermore, even within the same imaging modality, there exists a diversity of images. For instance, a chest X-ray of a healthy individual possesses different characteristics when compared to a chest X-ray of a patient diagnosed with pneumonia (Figure 1.1).

Developing security systems for medical imaging faces the challenge of adapting to the diverse range of imaging modalities and their specific requirements simultaneously.

The goal is to create a system that can effectively handle the varying characteristics of different imaging modalities while ensuring robust security measures.



(a) Normal chest X-ray, the lungs appear clear with no visible areas of abnormal opacification.

(b) Bacterial pneumonia, focal lobar consolidation is commonly observed.

Figure 1.1: Normal and Abnormal X-ray Images[1]

1.2.1 Medical Data Security Threats

The impact of attacks on medical data security goes far beyond the simple technical aspects, profoundly affecting patients, healthcare professionals, and the healthcare system as a whole. The consequences of such attacks can include critical medical errors, misdiagnosis, and even inappropriate treatment. Patients, by entrusting their sensitive medical information, are the first potential victims. Cases of medical identity theft can lead to serious complications, compromising the confidentiality of medical histories and exposing individuals to financial and health risks. For healthcare professionals, loss of data integrity can lead to reduced patient confidence, legal disputes, and major ethical challenges. Finally, at a systemic level, successful attacks can paralyze hospital operations, leading to delays in care, financial disruption, and a deterioration in the overall quality of healthcare services. It is therefore imperative to recognize and explore these wider implications to raise awareness of the crucial importance of medical data security in maintaining public health and trust in the healthcare system.

1.2.2 Medical Imaging Modalities

Each medical imaging technique provides unique insights into the organ under examination, displaying specific details in the corresponding medical image. The choice of imaging modality depends on the clinical question, the organ of interest, and the desired information.

In this section, we introduce various imaging modalities along with their corresponding image characteristics, such as contrast, resolution, and noise.

1.2.2.1 Magnetic Resonance Imaging

Magnetic Resonance Imaging (MRI) is based on nuclear magnetic resonance (NMR), which creates a detailed image of the internal anatomy of the body [10]. MRI is characterized by the ability to generate multi-sequences for the body area and high-resolution images, which means 3D representation and better resolution for soft tissue contrast, leading to a more accurate diagnosis.

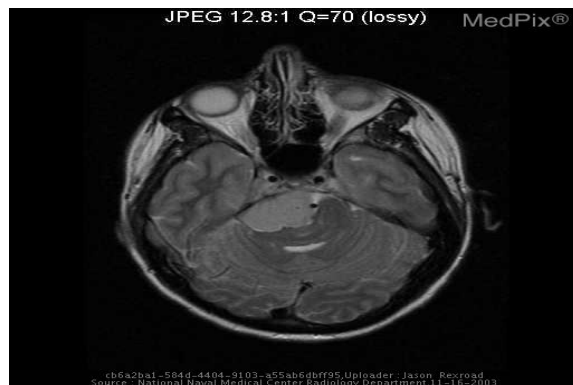


Figure 1.2: Brain MRI Image [2]

- **Resolution:**

The MRI image resolution depends on numerous factors. Yet, there are two resolution parameters for producing the images: the basic and the phase resolution. The basic resolution is the spatial resolution of MRI images. This resolution relies on various factors like the magnetic field strength, gradient performance, and the coil design of the MRI scan. The phase resolution represents the MRI system's ability to depict each voxel's spatial magnetic resonance signal. It is influenced by several other factors such as the receiver bandwidth, the matrix size, and the field of view.

- **Contrast:**

MRI image contrast helps in differentiating the various tissues based on their inherent properties. It is the visual differences in signal intensity between different structures within the imaged area. Various factors influence this fundamental aspect, including tissue properties, pulse sequence, magnetic field strength, repetition time, inversion

recovery, gradient echo, slice thickness, resolution, contrast agents, and motion and artifacts.

- **Noise:**

Generally, noise in MRI images is produced by the static fluctuation of signal intensity and it appears as grains or irregular patterns. There are two main sources of the noise in MRI images: Molecular movement and electrical resistance. It depends on the coil, the bandwidth, and the field strength. The SNR is the standard utilized to measure the performance of the MRI system, particularly for quality assurance, pulse sequence comparison, and radiofrequency comparison. Briefly, a higher SNR indicates a stronger signal relative to noise resulting in a detailed image.

1.2.2.2 Radiography

Conventional radiography measures the attenuation of an X-ray that passes through an item to produce a single image, in order to determine whether a patient has a condition, a foreign object, structural damage, or an anomaly.

- **Resolution:**

The image resolution of a radiographic system depends on various factors. These factors include the size of the focal spot, the patient's characteristics (such as thickness and X-ray scattering), the light scattering properties of the fluorescent screen, the film resolution (determined by grain size), and the sampling step in image intensifier systems and digital radiography.

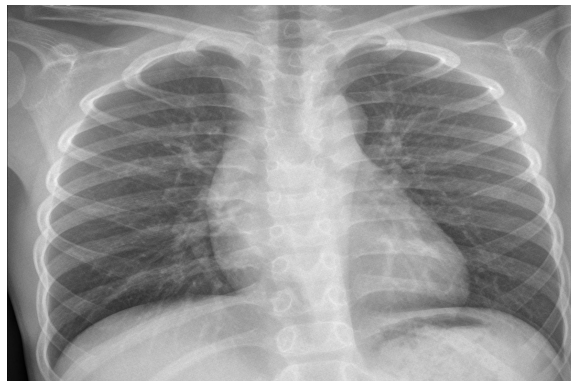


Figure 1.3: Chest X-Ray Image[1]

- **Contrast:**

The contrast in an image is determined by the intensity difference between adjacent regions. The image intensity relies on the attenuation coefficients and thicknesses of different tissue layers along the projection line. The spectrum of the X-ray beam, influenced by the energy of the X-rays, plays a significant role in contrast. Another crucial factor is the absorption efficiency of the detector, which refers to the fraction of radiation absorbed by the detector from the total incident radiation. Higher absorption efficiency contributes to higher image contrast.

- **Noise:**

The primary source of image noise stems from two main factors: the quantum noise properties of X-ray photons and the electronic noise of the detector system. Quantum noise is inherently random and is associated with the fluctuation in the number of photons detected. On the other hand, electronic noise arises from the X-ray detector system itself.

1.2.2.3 Computed Tomography Scan

Computed Tomography Scan or CT-Scan, is a combination of X-Ray technology and computer processing to generate a sequence of cross-sectional images of the organ. Afterward, These images are merged to create a 3D image, providing more information on the organ than plain radiography.

CT scans can produce detailed representation of many structures inside the body, including the internal organs, blood vessels, and bones.



Figure 1.4: Brain CT-Scan Image [3]

- **Resolution:**

A CT scanner's spatial resolution is its capacity to discriminate between two neighboring objects. It is expressed as line pairs per centimeter (lp/cm). The better the spatial resolution, the higher the lp/cm. A CT scan's spatial resolution can be affected by several factors, including the size of the focal spot. The size of the detector channels, the convolution filter, and the interpolation process inherent to the back projection of the voxel size.

- **Contrast:**

The contrast between an item and its background is determined largely by its attenuation qualities and physical parameters such as the X-ray tube's spectrum, the degree of beam hardening, scatter, and detecting non-linearity. Because the images are digital, the displayed contrast is varied by a gray level transformation (e.g., window/level) performed after the image is formed.

As a result, noise is the primary constraint on the perception of low-contrast features. It should be noted that CT has a significantly greater capacity to identify low-contrast features than radiography. The primary difference is that radiography produces projection images with various structures overlaid, whereas CT scans provide images of thin body slices.

- **Noise:**

There are three types of noise in CT: quantum noise or statistical noise, electronic noise, and round-off or quantization noise that results from the limited dynamic range of the detector. The largest source of contribution is quantum noise, which is caused by the statistical character of X-rays.

1.2.2.4 Ultrasound Imaging

It is a non-invasive exam with an excellent temporal resolution, also known as sonography. This technique employs high-frequency sound waves to generate images that indicate morphology, anatomy, cardiac function, blood vessels, and other body organs and tissues [11].

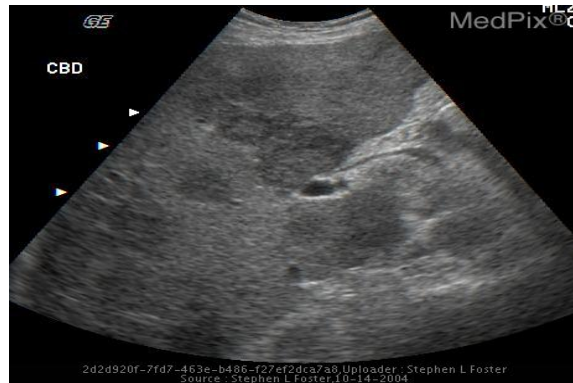


Figure 1.5: Ultrasound Image[4]

- **Resolution:**

In ultrasonic imaging, spatial resolution is divided into three components: axial resolution, lateral resolution, and elevation resolution. The capacity of the system to identify structures along the path of the ultrasound beam is measured by axial resolution, which is largely determined by the wavelength of the ultrasound waves and pulse duration. Lateral resolution refers to the separation of objects positioned side by side across the surface of the image, which is affected by factors such as transducer element size and design. Elevation resolution is concerned with differentiating structures perpendicular to the picture plane. These components in combination determine the system's capacity to deliver high-resolution and detailed ultrasound images, thereby affecting clinical diagnosis and anatomical structure visualization.

- **Contrast:**

Structures that strongly reflect ultrasound, such as calcifications or tissue interfaces, produce bright reflections, in contrast to hypogenic structures like blood, which exhibit weak reflections. The received signal encompasses not only specular reflections but also scatter. The substantial amplitude difference between specular and scatter reflections results in a broad dynamic range. To address this issue, a logarithmic function is typically applied, helping to normalize and enhance the representation of signals across this dynamic range.

- **Noise:**

Speckle noise, a characteristic artifact in medical ultrasound imaging, is an inherent property that can have a negative impact on image resolution and contrast. As a result, the presence of speckle noise can diminish the overall diagnostic value of ultrasound imaging. The noise tends to introduce grainy patterns and can make it more challenging to accurately visualize and interpret the structures within the image. Therefore, efforts are often made to mitigate or minimize speckle noise in order to improve the quality and diagnostic efficacy of ultrasound images.

1.2.3 Main Requirements of Data Security

Data security aims to protect digital information from unauthorized access or manipulation and to prevent data from loss or deterioration by an intentional or unintentional attack. Therefore, a security system must comply with at least three primary requirements known as (AIC) triad: Availability, Integrity, and Confidentiality. [9].

This section provides a detailed explanation of these requirements. In addition, other critical requirements for medical data security are listed in Table 1.1.

1.2.3.1 Data Availability

Medical data must be available to use whenever it is required. Meanwhile, the destruction of data availability leads to the disruption of the proper functioning of the health system, which affects patients' lives in particular and public health in general.

The data availability ensures that the information system remains operational properly by providing the equal distribution of medical data and confirming fair access for all parties. Moreover, the system should keep information and services systems operational during an outage.

1.2.3.2 Data Integrity

The most critical need in the health system is the integrity of medical data. As a matter of fact, any tampering in medical information could lead to serious implications to the patient's health by wrong treatment, improper clinical procedures, or acts. This causes adequate intervention to be delayed [12].

The integrity of medical data can be vulnerable in different situations. Whether is an unintentional human error, transfer error, or interference by an unauthorized

party, health data cannot be tampered with under any circumstances. Consequently, a robust security system consists in determining if the data has not been altered during the communication.

1.2.3.3 Data Confidentiality

Medical data contain personal information, including persons' health state and medical treatment. The sensitivity of this information imposes the provision of the right of privacy for both patients and the medical personal, and no foreign entity can be allowed to access this information[13] .

Confidentiality intends to protect the privacy of persons by allowing access only to authorized individuals to regard and operate personal data while making the information incomprehensible to anyone other than the only parties involved in the medical act.

Table 1.1: Requirements of Medical Data Security

Security Requirements	Description
Authenticity	Is to confirm the identity of all participants by ensuring that a user is who he alleges to be and securing his personal information.[14]
Non-repudiation	Providing proof that an act was completed, whether it was creating, transmitting, or receiving data.[15]
Access Control	Access Control designates and regulates who has access to the system.

1.3 Digital Watermarking

Digital watermarking refers to the process of concealing digital data within multimedia covers which includes documents, videos, images, audio, etc. This strategy is considered as an efficient security technique to confirm the authenticity and the integrity of the cover, as well as the identity of the owners.

The digital watermarking branches from a large concept named information hiding. It is the practice of hiding a secret message into a clear message so that it is not even possible to know its existence.[16].

Despite the fact that Andrew Tirkel and Charles Osborne concept introduced the term "Digital Watermarking" in 1992[17]. Watermarking has existed since the invention of paper. In 1282, the watermark was used to provide information about the paper producer, in in Fabriano, Italy. Through the 18th century, watermarking was used to protect money, legal documentation, and even artwork from falsification, illegitimate use, and theft and it is still in use today[18].

1.3.1 Image Watermarking Algorithm

The digital watermarking algorithm is an overall security system that contains two complementary processes: **Embedding and Extraction** (Figure 1.6).

To ensure the security of data during a transmission operation employing a watermarking system, the sender employs the embedding process. In this step, secret information is seamlessly incorporated into the transmitted data. Subsequently, the receiver utilizes the extraction process to determine and retrieve this embedded information.

On the other hand, major parties must be involved in order for the image watermarking procedure to be completed:

The cover image: The original support to be protected or hide the secret data within.

The watermark: The secret data to be concealed, which is commonly associated with the owner of the cover image.

Secret key: Increase the security of the system so that only the authorized person can complete the procedures.

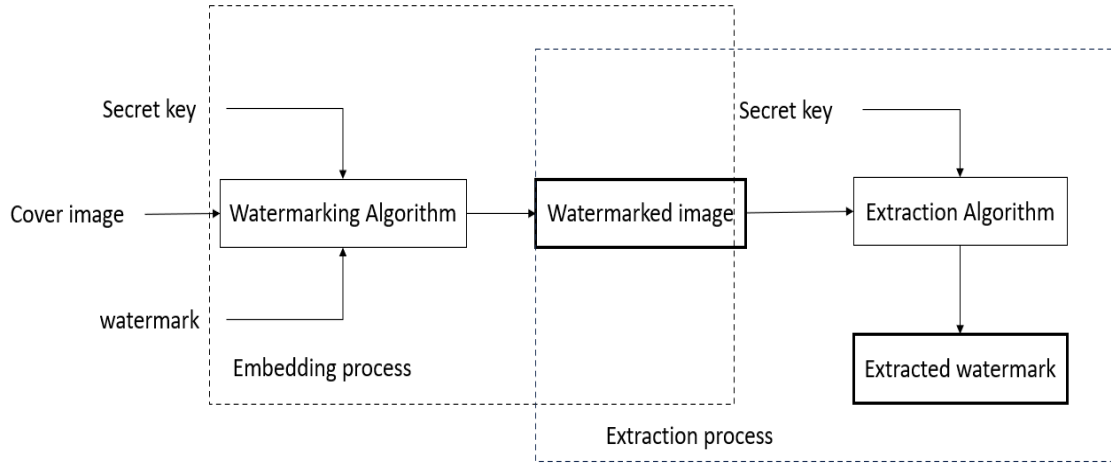


Figure 1.6: A general Scheme of The Watermarking System

1.3.1.1 Watermark Embedding Process

In the embedding process, an embedding function and a secret key are used to hide the watermark in the cover image. As a result, a new image named the **Water-marked image** is generated.

Equation (1.1) is the mathematical representation of the embedding process. Where $F_{Embedding}$ is the embedding function, I is the cover image, W is the secret watermark, K is the secret key, and I' the watermarked image

$$I' = F_{Embedding}(I, W, K) \quad (1.1)$$

1.3.1.2 Watermark Extraction process

The extraction process is the opposite of the embedding process, where the water-marked image and a secret key are used in the extraction function to detect the secret watermark. In the case of a non-blind watermarking algorithm, the original cover image may also be require.

Equation (1.2) is the mathematical representation of the extraction process. Where $F_{Extraction}$ is the detection function, and W' is the extracted secret watermark.

$$W' = F_{Extraction}(I', K) \quad (1.2)$$

1.3.2 Algorithm Classification

A watermarking algorithm is classified based on multiple standard. Meanwhile, the combination of these standard determines the functionality of the watermarking system[19].

1.3.2.1 Cover Type

The watermarking algorithms are classified based on the type of cover multimedia, which could be text, image, video, audio, etc. In fact, data digitization allows for the presence of a large amount of digital multimedia, Which makes it a suitable environment for data hiding, whether to protect the integrity and the authenticity of the cover media or to hide secret information within.

1.3.2.2 Watermark Visibility

The transparency of the watermark is an important aspect when defining the purpose of a watermarking system.

Visible watermarking: Here, the watermark is visible to the human perceptuality. This technique is used for copyright protection, where a visible mark associated with the owner is added to the cover. Nevertheless, this method distorts the multimedia quality and can be removed easily. embedding (Pardhu 2016)capacity. capacity. textbfLSBadding,manipulation (cite: Pardhu 2016 and Bansal 2014)discrete

Invisible watermarking: The secret watermark is hidden in the cover multimedia in this technique and cannot be detected without the appropriate extraction process, making the system more efficient for integrity and authenticity protection. Furthermore, it is almost impossible for an attacker to estimate the existence of the mark, which increases the system's security.

1.3.2.3 Watermark Robustness

Watermarking algorithms are divided into three groups based on the robustness of the system[15, 20]. This corresponds to the algorithm's resistance to attack to the watermarked image.

Robust watermarking: The algorithm is resistant to various types of attacks, including composite attacks. This type of watermarking is used in E-health application, Copyright protection and data hiding.

Semi-fragile watermarking: The watermark is resistant against medium straight attacks such as filtering and compression but fragile against the strongest ones, including geometric attacks. This type of watermarking is mostly used for content authentication.

Fragile watermarking: Medium-strength attacks can easily destroy the watermark, making the system more suitable for tamper detection and authentication.

1.3.2.4 Embedding Domain

In digital watermarking, the digital cover is regarded as a numerical signal, which can be altered to embed the secret data. Hence, the pixels of an image are modified and used as a carrier to hide data. The watermark is actually embedded using either a spatial domain technique, in which the pixels are directly modified, or a transform domain method, which uses the frequency coefficients for embedding[21].

Spatial domain: The watermarking algorithms in this domain are simple and easy to implement by changing the pixel values. Furthermore, this domain offers fast and less expensive processing and more embedding capacity.

The most basic method in spatial domain watermarking is the **LSB** algorithm, which modifies the Least Significant Bit based on the embedded watermark. Patchwork, correlation, pseudo-noise adding and spread spectrum-based techniques are also utilized in spatial domain watermarking. Nonetheless, these techniques are extremely susceptible to manipulation[21, 22].

Transform domain: The algorithms in the transform domain are distinguished by their high compatibility with preserving the quality of the watermarked image while also being resistant to almost every common attack. Furthermore, the computational complexity of these techniques increases the algorithm's security and efficiency.

The cover image is converted from the time/space domain to the frequency domain using one or a combination of transform techniques known as hybrid watermarking in transform domain algorithms. The most commonly used methods for image watermarking are the Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD). Otherwise, the processing time remains a disadvantage of these techniques. Additionally, compared to spatial domain techniques, data embedding has a lower capacity[21, 22, 23].

1.3.3 Digital Watermarking Requirements

The quality of a watermarking algorithm is estimated according to the robustness of the watermark against various malicious attacks, the imperceptibility of the human visual system, and the capacity of data to be embedded. These requirements, however, are mutually incompatible and difficult to achieve at the same time[24].

1.3.3.1 Imperceptibility

Every image application requires the perceptual quality of the watermarked image. Therefore, the hidden watermark should not deteriorate the image's quality. In which the existence of secret data in a low imperceptibility system is easily estimated, lowering security and diverting the scheme from its primary purpose.

1.3.3.2 Robustness

Robustness refers to the extracted watermark's resistance and ability to retain its original state, even if the watermarked image has been subjected to intentional or unintentional attacks.

some level of common operations, data, During transmission or any application that requires some security level, the watermarked image is vulnerable to different types of attacks. These attacks could be common harmless image processing operations including compression, image enhancement, and resizing, or demolition operations for the purpose of destroying the embedded data such as noise addition or geometric attacks [25].

1.3.3.3 Embedding Capacity

The amount of data hidden in the cover image is termed the embedding capacity. Thus, an efficient watermarking system should be able to embed as much data as the carrier allows while maintaining imperceptibility and robustness.

Embedding capacity has a negative impact on the other requirement, as increasing the amount of data reduces both the system's resistance and the quality of the watermarked image.

1.3.4 Digital Watermarking Applications

Due to the advancement of communication technologies, a large amount of digital content and data became available on the internet, exposing it to illegal use and theft.

However, the digital watermarking technique provides high protection for data since it can be useful in different applications (Rashid 2016 digital).

1.3.4.1 Content Authentication

With the widespread use of digital content for sharing and transmission. It became essential to validate the information's integrity and ensure that the data was not manipulated.

In the case of communication, a receiver could benefit from a watermarking system to confirm the authenticity of data by ensuring the integrity of the received information and verifying the identity of the sender. Furthermore, watermarking systems are used to detect regions that have been tampered with or altered in the cover by an unauthorized person.

1.3.4.2 Ownership Protection

The availability of multimedia on the internet made it necessary for owners to protect the copyright of their contents from fraud or unauthorized use. Digital watermarking provides copyright protection, in which the owner could use the extracted watermark as proof of ownership. In addition, by employing a secret key, an unauthorized user is unable to embed, identify, or delete a legitimate watermark.

1.3.4.3 Transaction Tracking

The ability to share content made it challenging for the owners to track their data once it was distributed, making it difficult to identify the source of the information leak. Therefore, digital watermarking is used as a transaction tracking application which is also known as fingerprinting. In reality, before sharing, each copy of the content is marked with a particular mark. The traitor will thus be discovered quickly.

1.4 Image Encryption

Encryption is the technique of transforming information into an illegible format using a secret key. In that case, only authorized parties can return to the original form. Encryption, in general, is a form of cryptography that aims to secure communications and store important data across insecure networks.

Even though the origins of this security technique can be traced back to 1900 BC in ancient Egypt, the concept is still in use today, as it has evolved to conform to the requirements of the modern age of digitization and information technology.

1.4.1 Algorithm

Similar to any other security technique that intends to protect the transmitted and stored data, an encryption system consists of two processes: *Encryption* and *Decryption* process.

1.4.1.1 Encryption Process

During the encryption process, data in their original format, known as *Plaintext*, is converted into unreadable data, known as *Ciphertext*, using a secret key and a set of mathematical rules. This procedure is usually performed on the sender's side or before storing the data.

$$C = E_K(P) \tag{1.3}$$

Where:

- C is the ciphertext.
- E_k is the encryption function with a key K .
- P is the plaintext.

1.4.1.2 Decryption Process

Decryption is the reverse process of encryption, where the '*Ciphertext*' is reverted into its original format '*Plaintext*'.

$$P = D_K(C) \tag{1.4}$$

Where:

- D_k is the decryption function with a key K .

1.4.2 Classification

According to the encryption key, encryption can be categorized into symmetric encryption (secret key) and asymmetric encryption (public key), each with its own variations in terms of implementation in practice. [26]

1.4.2.1 Symmetric Encryption

In this technique (Figure 1.7), a similar secret key is employed for both data encryption and decryption. That further necessitates a secure method to deliver the key to the correspondence sides.

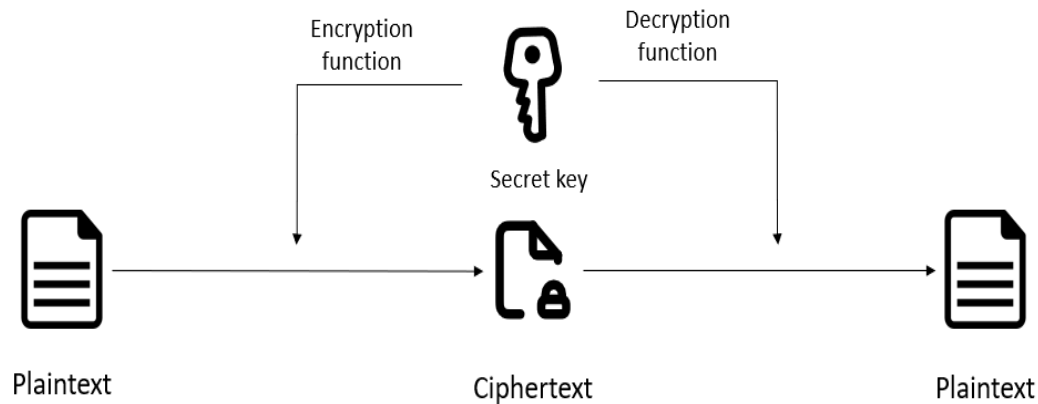


Figure 1.7: Symmetric Key Encryption

According to the input data, symmetric encryption is classified into two types:

Block cipher system: Encryption is performed on a single block of data at a time, with a fixed length of data and a fixed key. Modern block ciphers are structured for blocks of 64, 128, or 256 bits in size. Block-based algorithms such as AES, DES, Blowfish, Triple DES, PRESENT, and KLEIN are featured for high diffusion and strong resistance to tampering. [27].

Stream cipher system: Encryption is performed on stream of bits. stream ciphers have low error propagation since the procedure is executed on one bit at a time and does not affect the entire data. Furthermore, the algorithm's linearity and continuity make it simpler and faster to implement. Common stream cipher encryption techniques include: RS4,

1.4.2.2 Asymmetric Encryption

Also known as pair key encryption, it employs two different keys for the encryption and decryption procedures (Figure 1.8). In the main, a public key is diffused to the authorized parties or shared with the large public and used to encrypt the data. Meanwhile, a private key is kept secret by the owner and used to decrypt the received data.

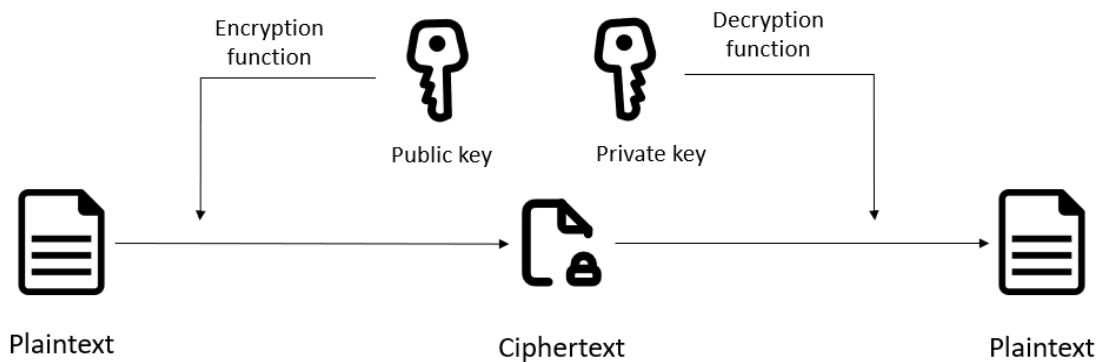


Figure 1.8: Asymmetric Key Encryption

1.5 Conclusion

In this chapter, we emphasize the importance of securing medical data, focusing specifically on medical imaging data. Initially, we pointed out the features of different imaging methods, discussing the unique traits of each. Following that, we delved into the fundamental requirements needed to ensure the protection and security of this valuable data, touching on the technologies utilized for safeguarding medical images. In the next chapter, we will present a state-of-the-art overview, referencing influential works in medical image security that have shaped our research.

Chapter : 2

LITERATURE REVIEW

Contents

2.1	Introduction	25
2.2	Problematic and solution	25
2.3	Literature Review	27
2.3.1	Medical image watermarking techniques	27
2.3.2	Electronic Patient Record	30
2.3.3	Meta-Heuristic Algorithms	32
2.4	Challenges and Future Directions	37
2.5	Conclusion	37

2.1 Introduction

The evolution of digitalizing healthcare services has resulted in the availability of vast amounts of medical data in various formats, improving the quality of care through reduced cost and time for diagnosis and treatment. Furthermore, this evolution has also enabled healthcare providers to share information and collaborate more effectively. Consequently, the worldwide digital health industry reached a value of USD 289 billion in 2021, with projections suggesting a 20.14 % increase from 2022 to 2027, reaching a total of USD 881 Billion, as reported by IMARC Group [28].

In the meantime, the confidentiality of a patient’s personal life, as mandated by the doctor-patient privilege [29], necessitates the implementation of a security system in any healthcare application to preserve privacy. For this purpose, researchers focus on developing robust security systems that can protect the authenticity and integrity of the data. The goal is to prevent unauthorized access and ensure the confidentiality of the patient’s information. The development of these security systems requires a multi-disciplinary approach, involving experts in computer science, cryptography, and medicine, among other disciplines.

The main objective of this chapter is to outline the central issue addressed in this work and present proposed solutions based on a thorough review of the available literature. Initially, we discuss the significance of medical data security, with a particular focus on medical imaging data, highlighting researchers’ strong interest in this critical field. Following that, we provide a comprehensive literature review of the most notable works in this field.

2.2 Problematic and solution

In the era of digital health and Telemedicine, it has become increasingly important to protect medical images through the use of robust security systems. This includes the use of encryption, access controls, digital watermarking, and other security measures to ensure the authenticity and confidentiality of medical images.

Otherwise, the growing number of research papers focused on medical data and image security (Figure 2.1, according to Google Scholar.), reflects the increasing public interest and investment in this field. Meanwhile, digital watermarking emerged as a promising solution for medical imaging data, offering efficiency and security. Researchers are recognizing the potential benefits that can be offered by this technique, in terms of ensuring the integrity and security of patient data and preventing unauthorized access or tampering with medical images.

The figure illustrates the evolution of the number of research papers on medical data security from the 1990s to the date of this research (February 2023). In this study, we utilized keywords such as ('medical' And 'data' And 'security') to identify research papers containing these terms. We employed the Google Scholar search engine, known for its reliability in providing these statistics.

The figure shows the increasing number of research papers in the field of medical security. For instance, the number of research papers using keywords ('medical' And 'data' And 'security') has surged by 108.772% within 10 years and by 568.421% within 20 years. These findings underscore the significance attributed to this field by researchers. Furthermore, our study specifically focuses on medical image security and medical image watermarking, revealing a substantial increase in the number of papers in this domain over the years.

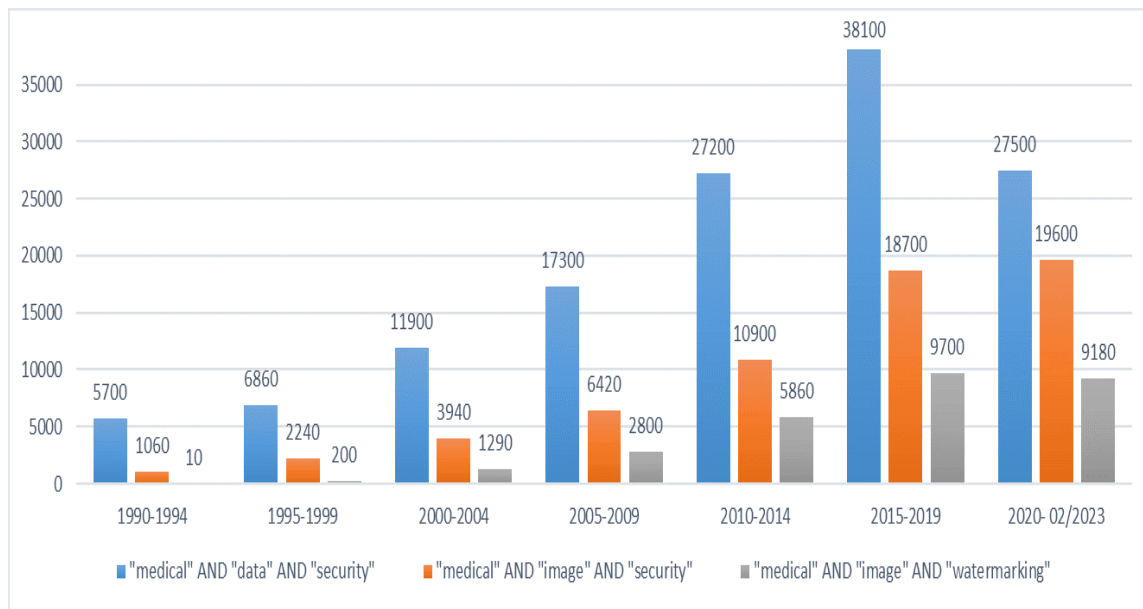


Figure 2.1: Evolution of the Number of Research Papers on Medical Data Security Since the 1990s

One of the most difficult challenges in medical image watermarking is ensuring that the watermark is imperceptible and does not interfere with the medical image's diagnosis. To address this, researchers have developed watermarking techniques that take into account the limitations and perceptual characteristics of the human visual system.

Another challenge is to ensure that the watermark does not degrade the quality of the medical image. To overcome this challenge, researchers have developed various watermarking algorithms that minimize the distortion caused by the watermark while maximizing its robustness to attacks.

Meanwhile, a medical image is a suitable environment to hide additional information about the patient, such as Electronic Patient Records, which can help ensure secure transmission and storage of the EPR. Therefore, it is crucial to select an appropriate embedding technique that provides the maximum capacity for storing such information.

2.3 Literature Review

The sensitivity of medical images requires a careful and considered approach when embedding additional data, in order to ensure the security and protection of sensitive patient information and to maintain the quality and accuracy of the images [30].

This section presents a comprehensive review of the current state-of-the-art medical image watermarking algorithms through a thorough examination of the latest developments and an analysis of different algorithms and techniques' strengths, weaknesses, and limitations.

The comprehensive survey of influential works in both medical and non-medical image security is encapsulated and outlined in Table 2.1.

2.3.1 Medical image watermarking techniques

Transform domain methods have become popular in the field of medical image watermarking due to their ability to provide robust and efficient watermarking solutions [31]. Furthermore, researchers are exploring new ways to improve their performance and security. One promising approach has been to combine different frequency domain methods to create more robust and effective techniques. By combining the strengths of each technique, researchers can address the limitations of individual methods and create systems that are more resilient to attacks, better at preserving image quality, and more efficient in terms of data storage and retrieval. These ad-

vancements have important implications for medical imaging.

In their study, Selvam et al [32]. suggest a reversible watermarking method for medical images that utilize both Integer Wavelet Transform (IWT)[33] and Discrete Gould Transform (DGT)[34]. The authors aimed to enhance the watermarking capacity while eliminating the requirement for extra key information to achieve lossless retrieval.

The proposed hybrid transform-based reversible watermarking technique for medical images in Telemedicine applications involves the following steps: applying Integer Wavelet Transform to the original medical image to obtain high-frequency sub-bands, dividing each sub-band into non-overlapping blocks, applying Discrete Gould Transform to each block to obtain DGT coefficients, embedding the Electronic Patient Record in the DGT coefficients after using a one-to-one mapping function and AES encryption, compressing the generated hash value, encrypted patient information, ROI coordinates points, and doctor authentication code using lossless compression, and embedding the compressed data within the cover image using LSB substitution. In summary, this work achieved :

- A high embedding capacity and a good visual quality of the watermarked image.
- High robustness against common image processing attacks such as JPEG compression, cropping, and rotation.
- A high peak signal-to-noise ratio (PSNR) between the original and extracted medical images and structural similarity index (SSIM) between the original and extracted medical images.
- And finally, the proposed technique is effective for the secure transmission of medical data in Telemedicine applications.

It should be acknowledged that the proposed technique may not offer complete protection against more advanced attacks, such as geometric transformations or content-aware image resizing. Furthermore, the effectiveness of the technique may be dependent on the quality and attributes of the cover image and watermark information.

Rajendiran et al [35]. employed a watermarking system for medical images that utilized a combination of Wavelet Packet Transform (WPT) and Independent Component Analysis (ICA), which demonstrated significant robustness against geometric attacks, according to the results.

The proposed watermarking scheme is tested on a medical image (Doppler) of size

256 × 256 using two-level wavelet packet transform. The LHV2 and HLV2 sub-bands were chosen to embed two watermarks: Watermark1 (ECG), with a length of 128 bits, and Watermark2 (text), with a length of 512 bits. The results of the testing demonstrate that the proposed method is capable of withstanding different attacks, such as Gaussian noise, salt and pepper noise, rotation, and translation. Nevertheless, it should be noted that the proposed method's high computational complexity might render it unsuitable for real-time applications.

Araghi et al.[36] presented a blind image watermarking scheme that enhances the effectiveness of hybrid DWT and SVD-based schemes using the second level of SVD. Additionally, image blocking is introduced to make the capacity independent of host image size, ensuring security and usability in both medical and non-medical images. The proposed watermarking scheme utilizes a hybrid approach of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to embed the watermark. A preprocessing step duplicates the watermark image to the size of the cover image, which is then divided into non-overlapping 16*16 blocks along with the cover image. Image blocking is used to find the optimal block size for embedding the watermark. The embedding process involves applying DWT and SVD on each block and modifying singular values using scaled watermark bits. The scheme ensures security by using a two-level authentication system for watermark extraction to detect false positive and false negative problems.

The proposed scheme was compared to previous schemes using the same hosts and watermark images, as well as attack parameters. The results of the experiments showed that the proposed scheme achieved higher imperceptibility and robustness compared to previous schemes, and its performance was improved compared to conventional DWT+SVD schemes.

Nonetheless, the proposed scheme is not suitable for grayscale images, as it was designed for color images.

Abdel-Aziz et al.[37] propose a new blind watermarking method for color medical images using fast Walsh-Hadamard transformation and multi-channel fractional Legendre-Fourier moments. The proposed method is designed to achieve high robustness and visual imperceptibility compared to other existing watermarking methods. The proposed image watermarking process consists of several key steps. Firstly, the input host color image was decomposed into 4x4 non-overlapping blocks. Subsequently, Multi-Channel Fractional Legendre-Fourier Moments (MFrLFMs) are computed for each block, involving the calculation of fractional Legendre-Fourier moments for individual color channels. Following this, appropriate MFrLFMs coeffi-

icients are selected, and the Fast Walsh-Hadamard Transformation (FWHT) is applied to transform these chosen coefficients into a different domain suitable for watermark embedding. The actual watermark is embedded into the quantized selected MFrLFMs coefficients during the watermark embedding phase. Notably, the proposed method enables blind extraction, eliminating the need for the original host image during extraction, thereby simplifying the process and preserving image quality.

While the proposed method for blind watermarking of color medical images is effective in achieving high robustness and visual imperceptibility, there are some limitations to the method. For instance, the proposed method may not be suitable for all types of medical images. The method is designed to work with color medical images, and it may not be effective for grayscale or other types of medical images.

Anand et al. [38] propose an enhanced watermarking technique in the DWT-SVD domain for ensuring the security of medical information. The proposed method incorporates diverse techniques, including Hamming code, encryption, and compression, to embed multiple watermarks in medical cover images. The outcomes illustrate notable robustness against various attacks, concurrently preserving imperceptibility, security, and achieving a favorable compression ratio.

In this process, a 512×512 MRI image serves as the cover, along with a 256×256 watermark image. The second level of DWT is applied to the cover image, resulting in four sub-bands. SVD is performed on the horizontal and vertical sub-bands from the DWT. The watermark image is divided into halves, W1 and W2, with Hamming code applied to W1. W1 and W2 are embedded into singular matrices obtained from the SVD. The watermarked image is reconstructed using inverse SVD, followed by encryption using Chaotic-LZW or HyperChaotic-LZW. Compression is then applied using Arithmetic coding, LZW, or Chaotic-LZW before transmission.

While the technique aims to maintain imperceptibility, it may still be sensitive to certain types of image modifications or attacks, such as geometric transformations, noise addition, and compression beyond the tested limits.

2.3.2 Electronic Patient Record

Digital watermarking for medical imaging offers a significant advantage by enabling the embedding of patient records within the medical image, thus reducing storage capacity and providing a secure method for transmitting medical data. However, It should not be regarded as the exclusive means of protecting sensitive medical information. It is important to have other security measures in place to ensure the

privacy and confidentiality of patient data. These measures may include encryption and error-correcting codes [39].

Singh et al [40]. presented a watermarking technique that employs the lifting wavelet transform (LWT) and discrete cosine transform (DCT). The authors encrypted the signature watermark using message-digest (MD5) and encoded the patient report using an error-correcting code (BCH).

First, the cover image is transformed into the LWT domain. The LWT coefficients are then partitioned into non-overlapping blocks, and a discrete cosine transform (DCT) is performed on each block to obtain frequency coefficients. Next, utilizing BCH error-correcting code, the signature watermark and the patient report are embedded into the frequency coefficients. Subsequently, an inverse DCT is applied to the modified frequency coefficients to obtain the modified LWT coefficients. Finally, these coefficients are converted back to the spatial domain.

The proposed method superior performance in terms of imperceptibility and capacity compared to similar DWT, DWT-SVD or DWT-DCT-SVD based watermarking techniques.

On the other hand, The performance of the method can be greatly affected by factors such as the gain factor, variations in noise, and the size of the secret information being embedded.

Pradeepkumar et al [41]. proposed a hybrid watermarking technique that utilizes discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) to embed the EPR into the medical image.

The proposed method involves decomposing the medical image through Discrete Wavelet Transform, applying Discrete Cosine Transform within the LH band, and performing Singular Value Decomposition on that particular block. This process is repeated for the watermark image during the embedding phase. To obtain the watermarked image, inverse Singular Value Decomposition and Inverse Discrete Cosine Transform are applied.

The study conducted experiments on many medical images and subjected them to various noise attacks to check the robustness of the proposed methodology. The results showed that the proposed watermarking scheme using Hybrid Transform (DWT+DCT+SVD) is effective in securing Electronic Patient Record (EPR) and medical images against various noise attacks. The study also showed that the proposed method has a high embedding capacity and low distortion rate, making it suitable for practical applications in the healthcare industry.

Despite its effectiveness in watermarking medical images, the proposed method is

susceptible to cropping and rotation attacks, potentially leading to inaccuracies in the extracted Electronic Patient Record (EPR) data and medical images.

Anand et al [42]. introduced a security approach for EPR that combines watermarking, encryption, and error-correcting code (ECC). Firstly, the discrete wavelet transform (DWT) is used to convert the original image into the wavelet domain, followed by selecting the high-frequency sub-bands of the wavelet coefficients for watermark embedding. A binary watermark is generated using a pseudo-random number generator (PRNG) and then scrambled using Arnold’s cat map. The scrambled watermark is embedded into the selected sub-bands using a quantization index modulation (QIM) technique. Next, both the cover image and the generated watermark are encrypted using the Paillier cryptosystem, a probabilistic asymmetric encryption method.

The proposed watermarking technique for tele-health applications is highly robust and satisfies all requirements regarding imperceptibility, robustness, capacity, and security. Additionally, it exhibits superior robustness against diverse attacks compared to prior methods.

2.3.3 Meta-Heuristic Algorithms

Combining medical image watermarking with metaheuristic algorithms can provide a more secure and efficient way of protecting medical images. Through the use of a metaheuristic algorithm to determine the optimal location and strength of the watermark, the watermark can be added to the image in a way that minimizes any distortion or degradation of the image quality. This approach can help ensure that the medical image remains accurate and useful while still being protected from unauthorized access or tampering.

The proposed approach in [43] suggests a medical image watermarking algorithm using wavelet transformation (DWT) with the assistance of singular value decomposition (SVD) and particle swarm optimization (PSO). The present work proposes an algorithm to embed a watermark into medical images with high imperceptibility and robustness against attacks while preserving diagnostic accuracy. The algorithm includes a preprocessing step to remove any noise or artifacts from the original medical image, followed by the application of a DWT to retrieve the invariant wavelet domain. SVD is then applied to the wavelet coefficients to obtain a diagonal matrix of singular values. The watermark is inserted into the selected region using a threshold function that modifies the values of the coefficients. Finally, PSO is employed

to optimize the scaling factors and achieve better performance against various attacks. The watermark is then inserted into a chosen region by altering the coefficient values in the image via a threshold function. The scaling factors are optimized using the PSO algorithm.

The proposed watermarking scheme using evolutionary programming and discrete wavelet transformation achieved high imperceptibility and robustness against various attacks while maintaining diagnostic accuracy. The experimental results show that the proposed algorithm is robust against various attacks such as noise addition, JPEG compression, cropping, rotation, scaling and filtering. The proposed approach achieved better results compared to other watermarking schemes such as Entropy-SVD and SVD-Firefly in terms of similarity

However, this algorithm may have limitations in its applicability to certain types of medical images and its capacity for embedding watermarks. Furthermore, the robustness of the algorithm against some types of attacks may also be limited. Further research is required to explore its performance under diverse scenarios.

Balasamy et al[44] introduce an innovative method for authenticating medical images, which involves using wavelet decomposition and particle swarm optimization (PSO). The proposed method is able to embed watermark with low distortion and also is valuable with respect to robustness, capacity, and imperceptibility.

The presented system's algorithm involves decomposing the original medical image into sub-bands using wavelet decomposition. The HL3 component is further divided into non-overlapping blocks of size 2x2. Chaotic sequences are generated using the tent map and used to encrypt the watermark, which is embedded in the selected blocks using PSO optimization.

The experiments were conducted on various 512x512 medical images of the human body. The results show that the proposed system achieves high embedding capacity, good imperceptibility, and robustness against various attacks. The PSNR values obtained for the watermarked images are high, indicating that the watermark is embedded with low distortion. The NCC values are also high, indicating that the watermarked image is highly correlated with the original image.

A possible limitation could be the sensitivity of the watermark to certain types of image processing operations or attacks that were not considered in the experiments.

Ansari et al [45]. introduced a robust- reversible watermarking scheme based on Slantlet transform and Artificial Bee Colony. The proposed scheme in this study is reversible and was tested on various types of images to evaluate its applicability. Furthermore, the study indicates the necessity to determine an optimal embedding strength value that achieves a balance between the imperceptibility and robustness of the watermark. Thus, artificial bee colony optimization was employed to determine the optimal embedding strength values.

The watermarking algorithm involves the following steps: performing a Slantlet transform on the host image to obtain its sub-bands, selecting the HL and LH sub-bands for watermark embedding, dividing each selected sub-band into non-overlapping blocks of size 8x8, calculating the mean value of each block and using it as a reference value for embedding, calculating the difference between each reference value and its corresponding pixel value in the watermark image, embedding this difference into each pixel of its corresponding block in HL and LH sub-bands using Arnold transform, using Artificial Bee Colony optimization to find optimal values of embedding strength that provide a tradeoff between imperceptibility and robustness, and finally performing inverse Slantlet transform on all sub-bands to obtain the watermarked image.

The study concludes that the proposed scheme provides better performance in terms of imperceptibility and robustness compared to other existing schemes. Nevertheless, The robustness of the proposed scheme may be affected by certain types of image processing attacks that were not considered in this study. Additionally, the imperceptibility of the watermark may be affected by certain types of image distortions or compression techniques.

Swaraja et al [46]. suggest a medical image watermarking algorithm that is blind, robust, secure, and optimized for embedding dual watermarks, specifically EPR, and ROI, using a combination of DWT and Schur transforms with the Particle Swarm Bacterial Foraging Optimization algorithm (PSBFO) algorithm. The system includes features such as authentication, tamper detection, and confidentiality to provide copyright protection, and the results show that the method performs optimally.

The proposed system involves dividing the original image into ROI and RONI parts. The ROI is compressed using the LZW algorithm with a secret key, and the compressed ROI and EPR watermark are embedded into the RONI part using hybrid transforms of DWT and Schur with PSBFO algorithm. Tamper detection and authentication are performed by comparing the retrieved ROI with the original ROI, and localization of tampered pixels is performed by mapping them with pixels con-

cealed as one of the watermarks in the RONI portion.

The attained perceptible quality of the watermarked medical image is accurate and greater than 31.5 dB for the listed checkmark attacks, and the obtained NC values are more than 0.87, which are depicted. The framework also demonstrates superior transparency and robustness against signal and compression attacks compared with related hybrid optimized algorithms.

Hatami et al [47]. introduce a novel intelligent hybrid approach using Contourlet Transform , SVD ,and PSO to enhance robustness against various attacks, while also increasing imperceptibility and embedding capacity. The proposed watermarking scheme involves partitioning the host image into non-overlapping blocks, transferring the selected blocks to the frequency domain using the Contourlet transform, and performing SVD transform on the selected frequency coefficients. The problem is defined as a multi-objective optimization problem, and the optimal values of dynamic scaling factors are calculated using PSO to increase robustness and imperceptibility in the embedding process. In detection, the watermark is extracted from the watermarked image by performing an inverse SVD transform on selected frequency coefficients with extracted scaling factors and the extracted watermark is compared with the original one to determine if tampering has occurred.

The experimental results showed that the proposed algorithm achieved good imperceptibility while maintaining robustness against different attacks such as noise addition, filtering and compression. The capacity of our scheme was also found to be large enough to embed a significant amount of watermark data.

The computational complexity and processing time required for embedding and extracting watermarks from large images could be a potential limitation for the proposed algorithm.

Zhu et al. [48] presents a novel approach to digital watermarking for image copyright protection. The proposed algorithm leverages singular value decomposition (SVD) and integer wavelet transform (IWT) to enhance imperceptibility and robustness. Additionally, a genetic algorithm is employed to optimize the watermark embedding parameters, further improving the algorithm's performance. Overall, the proposed algorithm exhibits promising performance in terms of imperceptibility and robustness, making it a potential solution for digital image copyright protection.

In the proposed image watermarking approach, the carrier image is initially divided into non-overlapping blocks, followed by the application of Integer Wavelet Transform (IWT) to obtain low-frequency and high-frequency sub-bands. Singular Value Decomposition (SVD) is then performed on the low-frequency sub-band of each block

to extract singular values. Subsequently, the watermark is embedded into the maximum energy step of these singular values using quantization. To optimize the balance between watermark robustness and imperceptibility, a genetic algorithm is employed to determine the quantization step size. For watermark extraction, the process involves the inverse SVD and IWT on the watermarked image, facilitating the retrieval of the embedded watermark.

The algorithm's robustness may vary when subjected to complex geometric transformations, and the computational overhead associated with the SVD and IWT operations, especially for large images or real-time applications, could be a limiting factor.

El Houbay et al. [49] propose an optimized image watermarking technique based on Discrete Wavelet Transform (DWT) and Hadamard transform. Genetic Algorithm (GA) is used to optimize the tradeoff between robustness and imperceptibility. Blind property is conducted using the estimation capability of the Decision Tree (DT). The proposed technique is evaluated against several types of attacks: compression, median filtering, salt and pepper noise, histogram equalization, blurring, scaling, painting, and cropping. Experimental results show that the proposed watermarking technique is robust against these attacks while keeping good imperceptibility. The proposed technique outperforms the compared techniques according to robustness, imperceptibility, and capacity.

In this innovative watermarking method, researchers transform the host image using DWT and WHT on specific components. Then, they employ GA to determine adaptive strength values, ensuring a balanced incorporation of the watermark into these components for an optimal tradeoff between robustness and imperceptibility. Importantly, a trained DT enables blind extraction, eliminating the need for the original image during retrieval. The effectiveness of the technique is rigorously assessed by comparing the extracted watermark with the original, showcasing its robust and imperceptible watermarking capabilities.

Overall, while the proposed technique shows good performance in terms of robustness and imperceptibility, The proposed technique may not be suitable for applications that require a high capacity watermarking. In addition, the time consumption of the GA operation can be high.

2.4 Challenges and Future Directions

The progress in security systems utilizing watermarking algorithms is remarkable. The value derived from earlier works significantly enhances the effectiveness of securing medical data, consequently contributing to the improvement of health services. However, research must be continued to address the shortcomings and limitations of the existing approaches.

We will now present some drawbacks that we have attempted to address in this manuscript.

1. The majority of the presented work does not take into consideration the diversity of characteristics in medical images, where each image varies in terms of modalities and content.
2. While transform domain-based algorithms and hybrid techniques have demonstrated great efficiency, with researchers heavily depending on DWT, DCT, and SVD, exploring new techniques and combinations could further enhance the robustness of the algorithm.
3. The capacity of medical images makes it crucial to embed more watermarks, providing a suitable environment for transmitting medical data. This approach helps prevent the loss of sensitive data.
4. The majority of the mentioned transform techniques are not geometrically invariant, indicating their inability to handle geometric attacks. However, the authors do not elaborate on how they addressed this particular challenge

2.5 Conclusion

With the increasing use of technology in healthcare, the need for secure medical image storage and transmission has become a critical issue that researchers and healthcare professionals must address.

In this chapter, we have discussed the various challenges faced in ensuring the security of medical imaging data. Moreover, we have presented a comprehensive literature review to support the proposed solution in the following chapters.

Table 2.1: A Comprehensive Summary of the Latest Advancements in Medical Image Watermarking Techniques

Authors	Embedding Technique	Optimization Technique	Capacity	Imperceptibility	Robustness
Selvam et al [32].	IWT, DGT	/	High	Very-High	Medium
Rajendiran et al [35].	WPT, ICA	/	Medium	High	Medium
Araghi et al[36].	DWT, SVD	/	Medium	Medium	Medium
Singh et al [40].	LWT, DCT + MD5,BCH	/	High	Medium	Medium
Pradeepkumar et al [41].	DWT, DCT, SVD + ECC	/	Medium	High	Medium
Anand et al [42].	DWT+ Turbo-code, Paillier Encryption	/	Medium	Low	Medium
Abdel-Aziz et al.[37]	FWHT ,MFrLFMs	/	Medium	very-High	High
Anand et al. [38]	DWT, SVD, Chaotic-LZW	/	High	Medium	High
Gangadhar et al [43].	DWT, Entropy, SVD	PSO	Medium	High	High
Balasamy et al [44].	DWT +Ten map, Hash Function	PSO	Medium	High	Medium
Ansari et al [45].	SLT + Arnold Transform	ABC	Medium	High	Medium
Swaraja et al [46]	DWT + LZW	PSBFO	High	High	High
Hatami et al [47].	SNT, SVD	PSO	Medium	very-High	High
Zhu et al. [49]	SVD, IWT	GA	Medium	High	High
El Houby et al.[48]	DWT ,WHT, DT	GA	Medium	High	High

Chapter : 3

***WATERMARKING ALGORITHMS BASED
ON WAVELET DOMAIN TRANSFORM***

Contents

3.1	Introduction	40
3.2	The Wavelet Transform	40
3.2.1	2D-Discrete Wavelet Transform	41
3.2.2	The Lifting Scheme	44
3.2.3	Wavelet Families	47
3.3	Evaluation Measures	52
3.3.1	Peak Signal-to-Noise Ratio	52
3.3.2	Structural Similarity Index	53
3.3.3	Normalized Correlation	53
3.3.4	Bit Error Rate	54
3.4	Watermarking Algorithm Based On Wavelet Domain	54
3.4.1	1 st Experiment: Wavelet Selection	55
3.4.2	2 nd Experiment: LWT-Based watermarking	63
3.5	Conclusion	67

3.1 Introduction

Medical images are available in various forms, depending on the imaging modality used for their acquisition. These diverse types of images serve to diagnose and monitor a broad spectrum of health conditions and diseases. In addition, specialized software and systems can store and analyze these images.

Meanwhile, multiple factors, including contrast, dynamic range, spatial resolution, and noise, can influence the quality of medical images [50]. As a result, it becomes challenging for security systems to handle and process the individual characteristics of each image accurately.

As demonstrated in the previous chapter's state-of-the-art, watermarking plays a vital role in safeguarding sensitive medical data. Wavelet transforms have emerged as a promising approach in this field because they can efficiently capture both frequency and spatial information of the data.

In this chapter, we will delve into the impact of different wavelet transforms and families on medical image watermarking algorithms. The chapter begins with a theoretical study that explains various wavelet transforms and families. Subsequently, we will investigate how each wavelet family, including Haar, Daubechies, Symlet, and Coiflet, influences the imperceptibility and robustness of embedded watermarks in medical images. Through rigorous analysis, we aim to identify the most suitable wavelet family for watermarking medical images.

The subsequent section involves a comparative analysis between two wavelet transforms: the second-generation wavelet transform (Lifting Wavelet Transform LWT) and the traditional wavelet transform (Discrete Wavelet Transform DWT). Our objective is to validate the LWT-based algorithm's capabilities in terms of imperceptibility and robustness in comparison to DWT. By doing so, we can ascertain whether the LWT demonstrates superior performance in safeguarding sensitive medical data.

3.2 The Wavelet Transform

The wavelet transform has become increasingly important in various image-related fields, such as compression, denoising, and feature extraction.

A wavelet transform is a mathematical tool used to analyze signals and functions. Similar to the Fourier transform, it decomposes a signal into its constituent parts, but instead of using sine waves, it employs wavelets. Unlike the Fourier transform, which allows analyzing problems either in the time or frequency domain, the wavelet

transform was developed to address issues in the time-frequency domain, enabling simultaneous analysis of both domains. Furthermore, the wavelet transform can be continuous or discrete and is useful for analyzing non-stationary signals.

The earliest known literature on wavelet transform dates back to 1909 [51] when mathematician Alfred Haar proposed the Haar wavelet. However, the term "wavelet" was not used until 1981 when Jean Morlet and Alex Grossmann introduced it and made significant contributions to the development of wavelet theory and its application to seismic wave analysis.

Yves Meyer, another key figure in the development of wavelet theory, constructed the Meyer wavelet in 1985, and in collaboration with Stephane Mallat, proposed the concept of multiresolution in 1988 [52].

The wavelet transform (WT) continues to be a valuable tool in various fields of science and engineering nowadays, finding applications in a wide range of areas such as image and audio compression, data analysis, and pattern recognition. It is a signal processing technique that utilizes wavelets to analyze a signal, such as an image, by decomposing it into different frequency components at various resolution scales. This approach enables the simultaneous examination of the image's spatial and frequency characteristics. The multiresolution property of the wavelet transform allows for a comprehensive understanding of the signal's behavior across different scales, providing a powerful tool for signal analysis and processing.

3.2.1 2D-Discrete Wavelet Transform

The discrete wavelet transform (DWT) is a mathematical transformation that decomposes a given signal into multiple sets. Each set represents a time series of coefficients, capturing the signal's evolution in different frequency bands. Through the DWT, the signal's frequency components can be analyzed and represented across various scales, offering valuable information about its structure and characteristics[53].

When performing a 2-D wavelet decomposition of an image, the result is four distinct decomposed sub-band images. Each of these sub-bands represents different properties of the original image.

- The LL sub-band contains low-frequency components and represents the coarse details and overall structure of the image. It captures low-resolution information.
- The HL sub-band contains high-frequency vertical details combined with low-frequency horizontal details. It represents the image's horizontal edges and

transitions.

- The LH sub-band contains low-frequency vertical details combined with high-frequency horizontal details. It represents the image's vertical edges and transitions.
- The HH sub-band contains high-frequency components and represents fine details, including the image's textures and high-resolution information.

The 2-D discrete wavelet transform (DWT) decomposes an approximation image $S_i(n_1, n_2)$ into four sub-bands based on the following decomposition process:

$$S_{i+1}(n_1, n_2) = \sum_{k_1} \sum_{k_2} H(k_1)H(k_2)S_i(2n_1 - k_1, 2n_2 - k_2) \quad (3.1)$$

$$W_{i+1}^1(n_1, n_2) = \sum_{k_1} \sum_{k_2} H(k_1)L(k_2)S_i(2n_1 - k_1, 2n_2 - k_2) \quad (3.2)$$

$$W_{i+1}^2(n_1, n_2) = \sum_{k_1} \sum_{k_2} L(k_1)H(k_2)S_i(2n_1 - k_1, 2n_2 - k_2) \quad (3.3)$$

$$W_{i+1}^3(n_1, n_2) = \sum_{k_1} \sum_{k_2} H(k_1)H(k_2)S_i(2n_1 - k_1, 2n_2 - k_2) \quad (3.4)$$

where $L(z)$ and $H(z)$ are 1-D wavelet filters. The signal $S_{i+1}(n_1, n_2)$ is an approximation of $S_i(n_1, n_2)$ at a lower resolution. This approximation is computed from $S_i(n_1, n_2)$ by lowpass filtering and decimating by 2 along its rows and columns. The signals $W_{i+1}^1(n_1, n_2)$, $W_{i+1}^2(n_1, n_2)$, and $W_{i+1}^3(n_1, n_2)$ contain the detail of $S_i(n_1, n_2)$ [54].

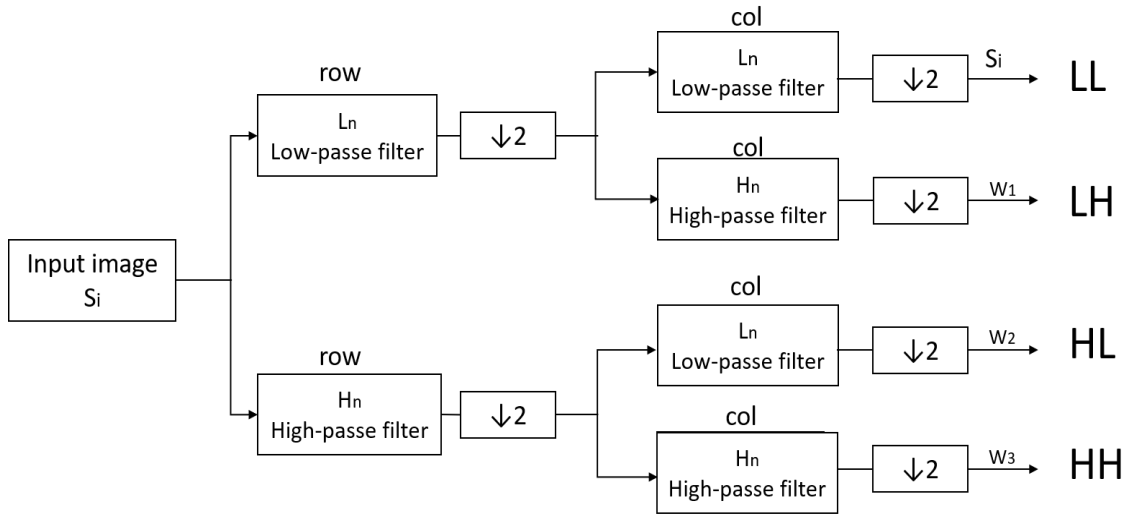


Figure 3.1: Discrete Wavelet Decomposition

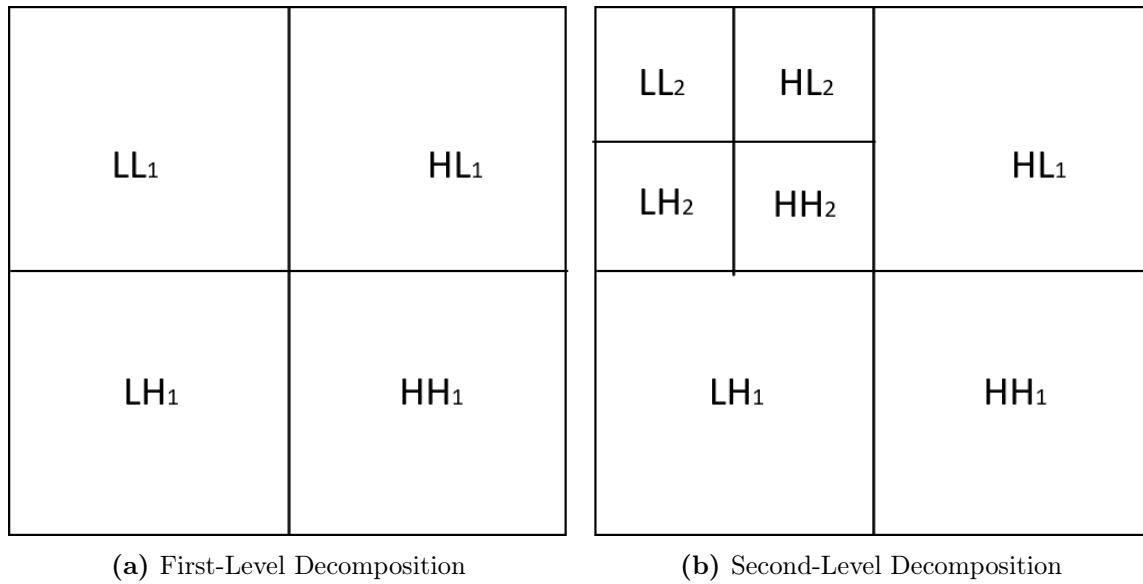


Figure 3.2: Two-level Decomposition of Wavelet Transform

3.2.1.1 2D-Discrete Wavelet Transform Limites

The 2D DWT is a powerful tool that can be used for a variety of purposes. However, it is important to be aware of the limitations of the 2D DWT before using it:

- **Sensitivity to noise:** The 2D DWT is sensitive to noise in the signal. This is because the DWT decomposes the signal into a series of wavelet coefficients, and noise can be amplified in the wavelet coefficients.
- **Computational complexity:** The 2D DWT can be computationally expensive for large signals. This is because the DWT requires the calculation of a large number of wavelet coefficients.

To address this issue, an alternative approach lies in the second-generation wavelet transforms, which offer enhanced efficiency. These transforms employ a lifting scheme to decompose the signal (image) into a set of wavelet coefficients, subsequently enabling the representation of the signal.

LWT is a newer wavelet transform that is more robust to noise. It is also more computationally efficient than 2D DWT for some applications. However, it can be less flexible than 2D DWT and may not be as accurate for some applications.

Table 3.1: Comparison of 2D-DWT and LWT

Feature	2D DWT	Lifting
Robustness to noise	Less robust	More robust
Computational efficiency	Efficient	Efficient for some applications
Flexibility	Flexible	Less flexible
Availability of software	Widely available	Less widely available

3.2.2 The Lifting Scheme

The discrete wavelet transforms, can be implemented using a similar procedure known as "lifting." This approach was introduced by Wim Sweldens in 1996 [55]. The lifting method is used to compute the means part and differences part of the transformed signal, and it allows for a more efficient implementation of the wavelet transform.

Similar to the traditional wavelet transform, the lifting wavelet transform scheme

comprises two stages: the analysis or decomposition stage, and the synthesis or reconstruction stage. Additionally, each stage includes three steps: splitting, predicting, and updating [56].

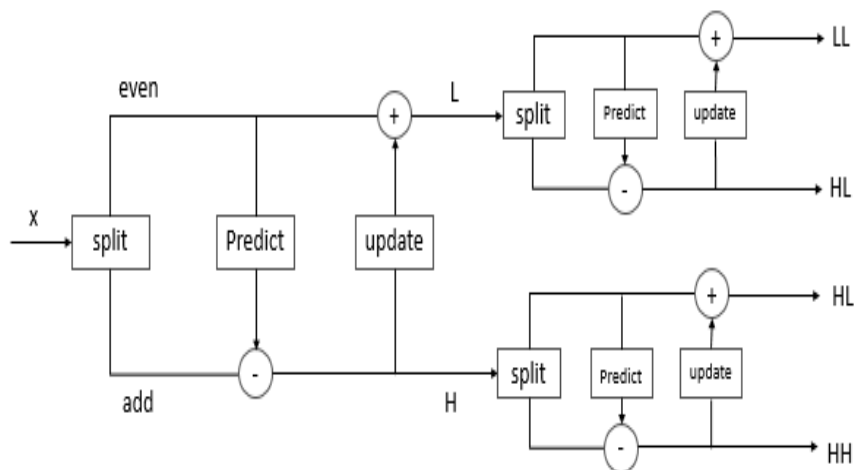


Figure 3.3: Lifting Wavelet Decomposition

- Splitting step: Or the polyphase representation of a signal, it is a crucial concept in the lifting approach. It involves dividing the signal into phases by taking every N -th sample from a given index. For instance, selecting every other sample from $n=0$ gives you the even samples, while taking every other sample from $n=1$ gives you the odd samples. These even and odd polyphase components are then used in the lifting process. Typically, only the even and odd polyphase components are considered, and there can be two phases when the increment between samples is 2:

$$X_{even}(n) = X(2n) \quad (3.5)$$

and

$$X_{add}(n) = X(2n + 1) \quad (3.6)$$

- Predicting step: When a signal has a certain structure, there is usually some correlation between a sample and its neighboring samples. For example, in the case where we predict that the signal is constant, we assume that the value

at sample number $2n$ is the same as the value at sample $2n+1$. We calculate the difference between these two values and replace the value at sample $2n+1$ with this difference. The prediction filter is designed to capture the trend of the signal and remove the redundancy in the signal:

$$H(n) = X_{add}(n) - P[X_{even}(n)] \quad (3.7)$$

Where $P[X_{even}(n)]$ is the predict operator and $H(n)$ is the high-frequency

- **Updating step:** in this final step, the even polyphase component is computed based on a linear combination of difference samples obtained from the predict step. The even polyphase component is obtained by computing a weighted average of these difference samples. The weights used in the computation depend on the chosen lifting scheme and the filter design.:

$$L(n) = X_{even}(n) + U[H(n)] \quad (3.8)$$

where $U[H(n)]$ is the update operator and $L(n)$ is the low- frequency[56].

3.2.2.1 Lifting Scheme Properties

Compared to the traditional wavelet, the lifting wavelet offers several advantages, including:

1. **Computational complexity:** the lifting wavelet approach has a lower computational complexity compared to other wavelet algorithms. This is because the output signal is encoded in the same memory location as the input signal, resulting in more efficient computation and fewer memory requirements.
2. **Perfect reversibility:** the lifting wavelet scheme ensures perfect reversibility, meaning that the original signal can be reconstructed exactly using an inverse algorithm. This property avoids the loss of information and makes it highly suitable for applications requiring security.
3. **Efficiency:** The lifting scheme provides flexibility in choosing wavelet filters and implementation methods, while also requiring fewer operations. Therefore, the lifting wavelet is suitable for processing multidimensional signals, such as images and videos.

3.2.3 Wavelet Families

A wavelet family consists of a group of wavelets that possess common properties, including the length of the support of the mother wavelet, the number of vanishing moments, the symmetry or regularity, as well as the orthogonality or bi-orthogonality of the resulting analysis [57].

The choice of wavelet family plays a critical role in adapting the wavelet transform to suit the specific requirements of an application. Different wavelet families excel in different domains, and factors such as signal characteristics, desired time-frequency resolution, noise sensitivity, and computational efficiency must be considered. By carefully assessing these factors, the most suitable wavelet family can be chosen to effectively analyze and extract relevant information from the data in a given application context.

In the following section, we will highlight several wavelets that have attained substantial prominence and recognition in the field of image processing (Figure 3.4).

3.2.3.1 Haar Wavelets

HAAR wavelets are the first and the simplest type of wavelet, which were developed by Haar Alfred in 1909. The implementation of Haar wavelets follows a similar approach to other wavelet transforms where the discrete signal is divided into two sub-signals with half the length of the original [58].

The Haar wavelet offers multiple benefits, including its simplicity and efficiency. It enables swift computations and facilitates higher compression ratios and improved peak signal-to-noise ratio (PSNR) values. Furthermore, the Haar allows for the recursive amplification of signal details, offering a flexible approach for in-depth analysis [59].

The Haar wavelets are defined by:

$$\psi(0, t) = 1 \quad \text{for } 0 < t \leq 1 \quad (3.9)$$

$$\psi(1, t) = \begin{cases} 1 & \text{for } 0 \leq t < \frac{1}{2} \\ -1 & \text{for } \frac{1}{2} \leq t \leq 1 \end{cases} \quad (3.10)$$

$$\psi(2, t) = \begin{cases} \sqrt{2} & \text{for } 0 \leq t < \frac{1}{4} \\ -\sqrt{2} & \text{for } \frac{1}{4} \leq t < \frac{1}{2} \\ 0 & \text{for } \frac{1}{2} \leq t \leq 1 \end{cases} \quad (3.11)$$

$$\psi(3, t) = \begin{cases} 0 & \text{for } 0 \leq t < \frac{1}{2} \\ \sqrt{2} & \text{for } \frac{1}{2} \leq t < \frac{3}{4} \\ -\sqrt{2} & \text{for } \frac{3}{4} \leq t \leq 1 \end{cases} \quad (3.12)$$

In general, for $2^p + n \leq 1$

$$\psi(2^p + n, t) = \begin{cases} \sqrt{2^p} & \text{for } \frac{n}{2^p} \leq t < \frac{n+\frac{1}{2}}{2^p} \\ -\sqrt{2^p} & \text{for } \frac{n+\frac{1}{2}}{2^p} \leq t < \frac{n+1}{2^p} \\ 0 & \text{elsewhere} \end{cases} \quad (3.13)$$

For $p = 0, 1, 2, \dots$, and $n = 0, 1, 2, 4, \dots, 2^p - 1$ and $0 \leq t \leq 1$.

3.2.3.2 Daubechies wavelets

Daubechies wavelets, introduced by Ingrid Daubechies in 1988, belong to the family of orthogonal wavelets, which implies their lack of correlation with each other. This orthogonality makes them particularly advantageous in applications where the separation of different signal components is crucial.

Similar to the Haar transform, the Daubechies wavelet transform is implemented through a series of decompositions. However, the key distinction lies in the length of the filter, which exceeds two in the case of Daubechies wavelets. Consequently, they exhibit enhanced localization and smoothness properties.

Daubechies wavelets serve as a powerful tool applicable to a wide range of domains. They are well-suited for tasks such as signal processing, image compression, and various applications that require a simultaneous representation of signals in both time and frequency domains [60].

3.2.3.3 Symlet wavelets

The Symlet wavelet family shares similarities with the Daubechies wavelets, possessing both symmetry and excellent time-frequency localization properties. While they aim to approximate orthogonality rather than achieving strict orthogonality, Symlet wavelets introduce additional vanishing moments, enabling better capture of higher-order polynomial trends in signals.

The definition of Symlet wavelet functions relies on their filter coefficients, with the number of vanishing moments determining their order. As a result, Symlet wavelets are widely utilized in signal and image processing tasks such as compression, denoising, feature extraction, and data analysis. Their symmetric nature and strong time-frequency localization properties make them particularly effective in capturing both local details and global trends within signals and images [61].

3.2.3.4 Biorthogonal wavelets

The Biorthogonal wavelets form a family of wavelets specifically designed to possess compact support and orthogonality. In a biorthogonal wavelet system, two sets of wavelet functions exist: the analysis wavelets (typically represented by φ and ψ) and the synthesis wavelets (typically represented by $\tilde{\varphi}$ and $\tilde{\psi}$). The analysis wavelets are used for signal or image decomposition, while the synthesis wavelets are employed for reconstruction.

The primary advantage of biorthogonality lies in its capability for perfect reconstruction. Biorthogonal wavelets were initially introduced by Ingrid Daubechies in 1990 to address certain limitations of orthogonal wavelets, such as susceptibility to noise and challenges in hardware implementation.

Biorthogonal wavelets find extensive applications in diverse fields, including signal processing, image compression, and audio coding. They are particularly well-suited for scenarios where representing a signal accurately in both the time and frequency domains is essential.

3.2.3.5 Coiflet Wavelets

The Coiflets wavelet, developed by Ingrid Daubechies and Ronald Coifman in 1990, shares similarities with Daubechies wavelets but exhibits a higher degree of symmetry. Coiflets have a distinct number of vanishing moments compared to Daubechies wavelets. Specifically, their wavelet functions possess $N/3$ vanishing moments, while the scaling functions have $N/3 - 1$ vanishing moment.

The property of symmetry in Coiflets holds significant value in signal analysis tasks, thanks to the linear phase of the transfer function. Although the Coiflet method may have some limitations in visualizing specific frequencies of interest, its discrete form remains highly advantageous for digital implementations.

In summary, Coiflets serve as a powerful tool applicable to a diverse range of applications. They offer numerous advantages over traditional Fourier transforms, including enhanced flexibility, robustness, and efficiency [62].

3.2.3.6 Meyer wavelets

The Meyer wavelet, introduced by Yves Meyer in 1986, is an orthogonal continuous wavelet. It possesses smooth characteristics and exhibits excellent time-frequency localization properties. Additionally, the Meyer wavelet is biorthogonal, indicating that it is uncorrelated with itself. This feature makes it well-suited for applications

where the ability to distinguish and separate different components of a signal is essential.

The Meyer wavelet and scaling function are defined in the frequency domain:

- Wavelet function

$$\widehat{\psi}(\omega) = (2\pi)^{-1/2} e^{i\omega/2} \sin\left(\frac{\pi}{2} \nu \left(\frac{3}{2\pi} |\omega| - 1\right)\right) \quad \text{if} \quad \frac{2\pi}{3} \leq |\omega| \leq \frac{4\pi}{3} \quad (3.14)$$

$$\widehat{\psi}(\omega) = (2\pi)^{-1/2} e^{i\omega/2} \cos\left(\frac{\pi}{2} \nu \left(\frac{3}{4\pi} |\omega| - 1\right)\right) \quad \text{if} \quad \frac{4\pi}{3} \leq |\omega| \leq \frac{8\pi}{3} \quad (3.15)$$

and

$$\widehat{\psi}(\omega) = 0 \quad \text{if} \quad |\omega| \notin \left[\frac{2\pi}{3}, \frac{8\pi}{3}\right] \quad (3.16)$$

where $\nu = a^4(35 - 84a + 70a^2 - 20a^3) \quad a \in [0, 1]$

- Scaling function

$$\widehat{\phi}(\omega) = (2\pi)^{-1/2} \quad \text{if} \quad |\omega| \leq \frac{2\pi}{3} \quad (3.17)$$

$$\widehat{\phi}(\omega) = (2\pi)^{-1/2} \cos\left(\frac{\pi}{2} \nu \left(\frac{3}{2\pi} |\omega| - 1\right)\right) \quad \text{if} \quad \frac{2\pi}{3} \leq |\omega| \leq \frac{4\pi}{3} \quad (3.18)$$

$$\widehat{\phi}(\omega) = 0 \quad \text{if} \quad |\omega| > \frac{4\pi}{3} \quad (3.19)$$

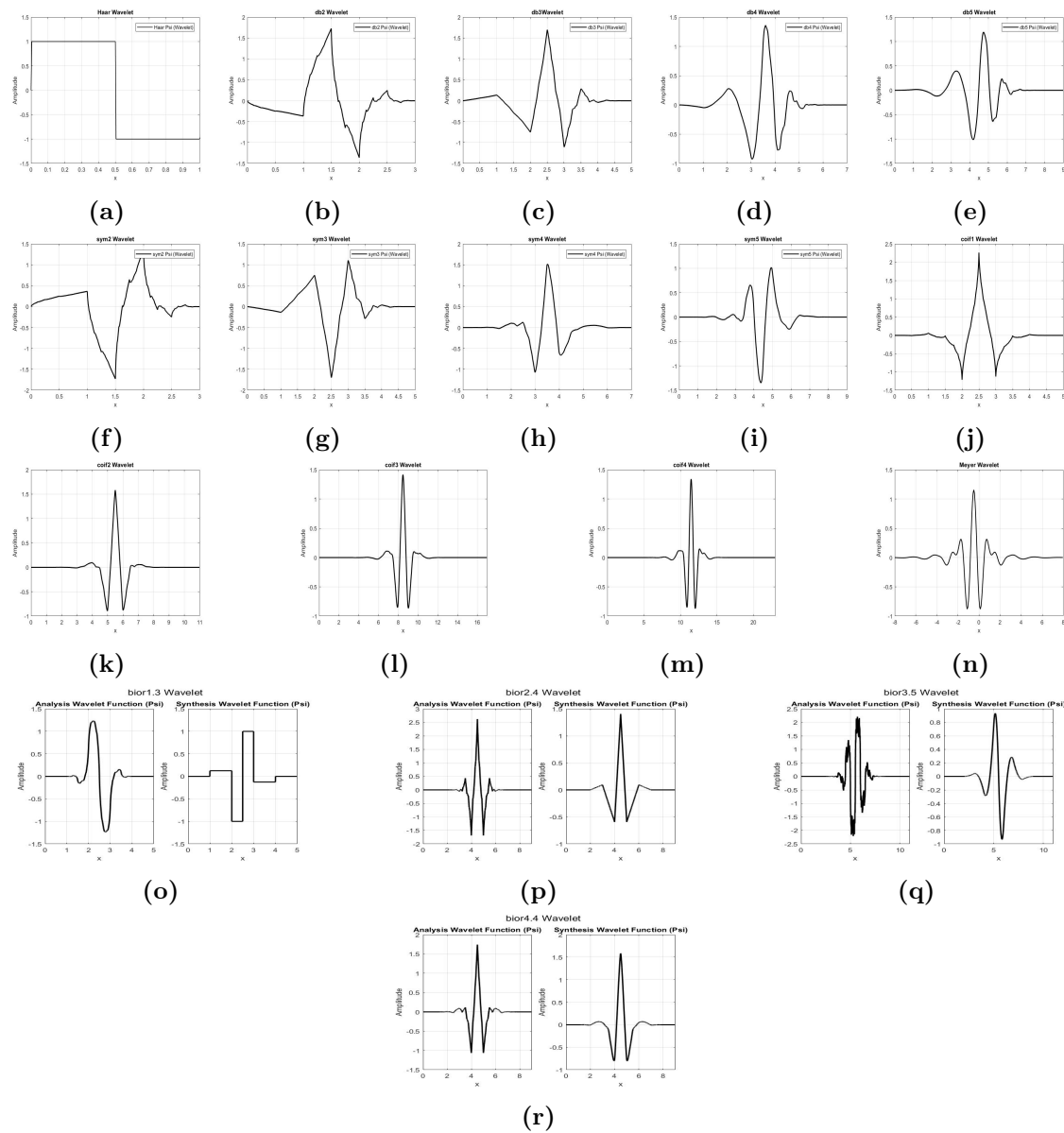


Figure 3.4: Some Wavelet Families.

3.3 Evaluation Measures

Evaluating watermarking algorithms is crucial to assess their performance and determine their suitability for specific applications.

In image watermarking, the quality of both the watermarked image and the extracted watermark is crucial for evaluating the performance of watermarking algorithms. The assessment is conducted by comparing the original data (original image or watermark) with the data obtained after applying the watermarking system (watermarked image or extracted watermark).

The essential parameters for evaluation include PSNR (Peak Signal-to-Noise Ratio), NC (Normalized Correlation), SSIM (Structural Similarity Index), and BER (Bit Error Rate). For accuracy, these metrics should be reported to four decimal places. These standards are widely recognized in watermarking research, and adhering to them enables effective comparison of our system with existing algorithms.

This section introduces the most commonly used measures to evaluate watermarking algorithms.

3.3.1 Peak Signal-to-Noise Ratio

The term "peak signal-to-noise ratio" (PSNR) refers to the ratio between the maximum possible value or power of a signal and the power of distorting noise that affects the quality of its representation.

PSNR serves as a widely used metric for assessing the quality of reconstruction in various applications that require accurate reconstruction and perceptual fidelity, including image compression and transmission.

In the context of a watermarking algorithm, PSNR is employed to evaluate the imperceptibility of the watermark, aiming for it to be invisible to the human eye. This evaluation is carried out by comparing the original image with the watermarked image. A higher PSNR value indicates a higher quality watermarked image, while a low PSNR value suggests that the watermarked image may be visually noticeable, undermining the purpose of watermarking [63].

The PSNR is determined on (db) as :

$$PSNR(I, I_w) = 10 * \log_{10} \frac{max_i^2}{MSE} \quad (3.20)$$

Where: MAX_i represents the largest fluctuation of the input image and MSE is the Mean square error between two images

$$MSE(I, I_w) = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i, j) - I_w(i, j))^2 \quad (3.21)$$

3.3.2 Structural Similarity Index

The Structural Similarity Index (SSIM) is a comprehensive image quality assessment metric that operates on the basis of the human visual system's perception of image quality. It takes into consideration three key aspects of image quality: luminance, contrast, and structure.

SSIM is calculated by comparing two images and generating a similarity score that reflects their level of resemblance. A higher SSIM score indicates a greater similarity between the two images.

SSIM is widely employed as an image quality assessment metric and is considered to be more closely aligned with human perception of image quality compared to other metrics like Peak Signal-to-Noise Ratio (PSNR).

In the context of watermarking, SSIM is utilized to ensure that the presence of a watermark does not significantly degrade the quality of the host image (original image). If the SSIM value falls below a certain threshold, the watermarked image may become visually noticeable, thereby compromising the purpose of the watermarking process [64].

The formula for SSIM is as follows:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3.22)$$

Where μ_x , μ_y , σ_x , σ_y , and σ_{xy} are the local means, standard deviations, and cross-covariance for images x , y , while c_1 and c_2 are constants set to avoid instability.

3.3.3 Normalized Correlation

The normalized correlation coefficient (NC) is a commonly utilized metric to assess the similarity between two images. It quantifies the linear relationship between the pixel intensities of the images and yields a value ranging from -1 to 1. A value of 1 denotes a perfect match, -1 represents a perfect inverse match, and 0 indicates no correlation.

In the context of watermarking algorithms, the NC metric is employed to evaluate the robustness of the extracted watermark by gauging the similarity between the original watermark and the extracted counterpart.

While the NC is a valuable metric for assessing the robustness of a watermarking algorithm, it is important to acknowledge that it is not flawless. The NC solely measures the similarity between images and may be less effective when dealing with textual watermarks. Therefore, it is advisable to employ the NC in conjunction with other metrics for a comprehensive evaluation.

The formula for NC coefficient is as follows:

$$NC = \frac{\sum_{x=1}^M \sum_{y=1}^N w(x, y) \cdot w'(x, y)}{\sum_{x=1}^M \sum_{y=1}^N w^2(x, y)} \quad (3.23)$$

Where $w(x,y)$ presents the watermark image and $w'(x,y)$ is the extracted watermark.

3.3.4 Bit Error Rate

Bit Error Rate (BER) is a metric used to quantify the performance of a digital communication system by measuring the accuracy of transmitted bits compared to the received bits.

The (BER) is used in digital watermarking to measure the number of bits that have been incorrectly extracted from the watermarked signal. It is calculated by dividing the number of incorrect bits by the total number of bits in the watermark.

The BER is calculated by dividing the number of bits that have been corrupted by the total number of bits in the watermark. A low BER value indicates that the watermark has been extracted accurately

The formula for BER is as follows:

$$BER = \frac{\text{number of error bits}}{\text{number of bits}} \quad (3.24)$$

3.4 Watermarking Algorithm Based On Wavelet Domain

Our thesis focuses on the use of a watermarking technique to ensure the security of both medical images and personal patient information. Initially, we used an image watermark to ensure the authenticity and integrity of the medical image. The medical image was then used as a container to securely store and transmit the patient's personal information in the second phase. This method makes it extremely difficult for an attacker to detect the presence of data within the image, adding an extra layer of security.

The wavelet transform has been widely used in image watermarking, owing to its ability to capture both the frequency and spatial characteristics of an image. Furthermore, the wavelet transform allows for the decomposition of the input image into multiple non-overlapping subbands, increasing embedding capacity.

In this section, we will introduce two experiments that explore the utilization of wavelet domain techniques in medical image watermarking algorithms. The primary objective of the first experiment is to examine how the selection of different wavelet families affects the performance of the watermarking algorithm. In the second experiment, we will assess and compare the performance of LWT (Lifting Wavelet Transform) with the traditional wavelet transform 2D-DWT in the context of medical image watermarking.

3.4.1 1st Experiment: Wavelet Selection

In this section, we describe a watermarking algorithm that incorporates a medical image and a binary watermark to ensure integrity protection. To achieve this, we utilized the 2D-DWT as the embedding and extraction technique. The medical image, with a size of 512x512, Figure(3.5), was decomposed into four non-overlapping subbands. Subsequently, the binary watermark image was embedded into the High/Low-frequency vertical details (HL_1) subband using the following rules: Algorithm(1)

Algorithm 1 Embedding rules

```

if  $W == 1$  then
     $HL'_1(1) \leftarrow HL_1(1) + \alpha$ 
     $HL'_1(2) \leftarrow HL_1(2) - \alpha$ 
end if
if  $W == 0$  then
     $HL'_1(1) \leftarrow HL_1(1) - \alpha$ 
     $HL'_1(2) \leftarrow HL_1(1) + \alpha$ 
end if

```

where W is the watermark image, $HL_1(1)$ and $HL_1(2)$ represent the selected coefficients from the HL_1 subband, $HL'_1(1)$ and $HL'_1(2)$ are the modified coefficients, and α denotes the scaling factor.

The extraction phase is the reverse process of the embedding phase. It involves decomposing the watermarked image using the same 2D-DWT algorithm and extracting the watermark using the following rules: Algorithm(2).

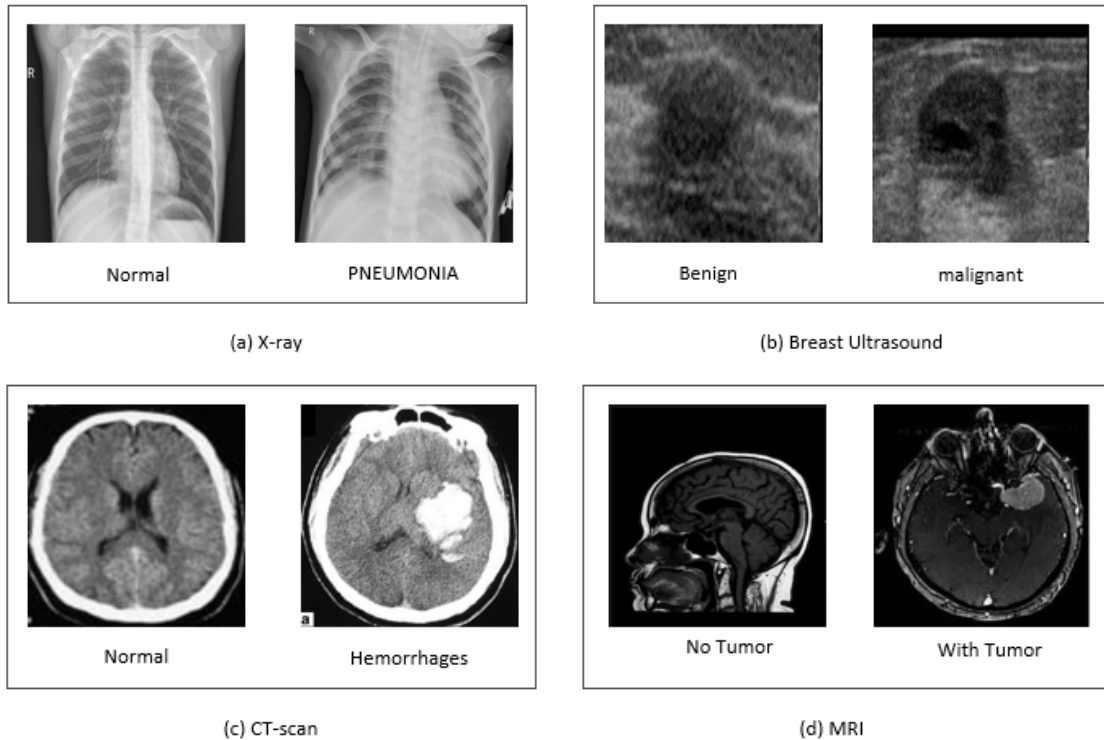


Figure 3.5: Medical Images Used for the Test [2, 3, 1, 5]

In this proposed method, we will evaluate the impact of wavelet families on the watermarking scheme by testing several wavelets and selecting the best wavelet for medical images. The general scheme of the watermarking algorithm is mentioned in Figure(3.6).

3.4.1.1 Imperceptibility And Robustness Results

To study the impact of wavelet families on the imperceptibility and the robustness of watermarked medical images, medical images from different modalities were tested under the same conditions, with a scaling factor of $\alpha = 1$, a binary watermark image of 64x64 pixels, an original image of 512x512 pixels, and a set of 100 images of each modality.

According to the results presented in Table (3.2), the performance of various wavelet families in terms of imperceptibility was evaluated for each modality. The findings revealed that the coiflet 4 wavelet (coif4) outperformed the other wavelet

Algorithm 2 Extraction rules

```
if  $HL_1(1) \geq HL_1(2)$  then  
     $W' \leftarrow 1$   
end if  
if  $HL_1(1) < HL_1(2)$  then  
     $W' \leftarrow 0$   
end if
```

families, exhibiting the highest performance. It achieved a maximum PSNR value of 63.9503 and an SSIM value of 0.9997 for ultrasound images, indicating its ability to reconstruct the original image with near perfection.

The robustness of the extracted watermark was evaluated in terms of the normalized correlation coefficient (NC) and structural similarity index (SSIM), and the results are presented in Table(3.3). It was observed that the Haar wavelet exhibited high performance, with the extracted watermark showing a value close to 1 for both NC and SSIM. This indicates that the Haar wavelet demonstrated strong resilience in preserving the integrity of the watermark.

The effectiveness of a watermarking algorithm relies on finding the right balance between imperceptibility and robustness. This means selecting a wavelet that can accurately reconstruct the watermarked image without compromising the integrity of the embedded watermark.

Figures (3.7) and (3.8) depict the performance of each wavelet in terms of imperceptibility and robustness, respectively. The findings indicate that wavelets such as *coif1*, *coif4*, *db3*, *db4*, *sym3*, *sym4*, and *bior1.3* achieved high levels of imperceptibility but struggled to maintain the robustness required for accurate watermark extraction. On the other hand, wavelets like *haar*, *coif3*, *bior2.4*, and *bior4.4* demonstrated commendable performance in both imperceptibility and robustness, making them favorable choices for watermarking applications.

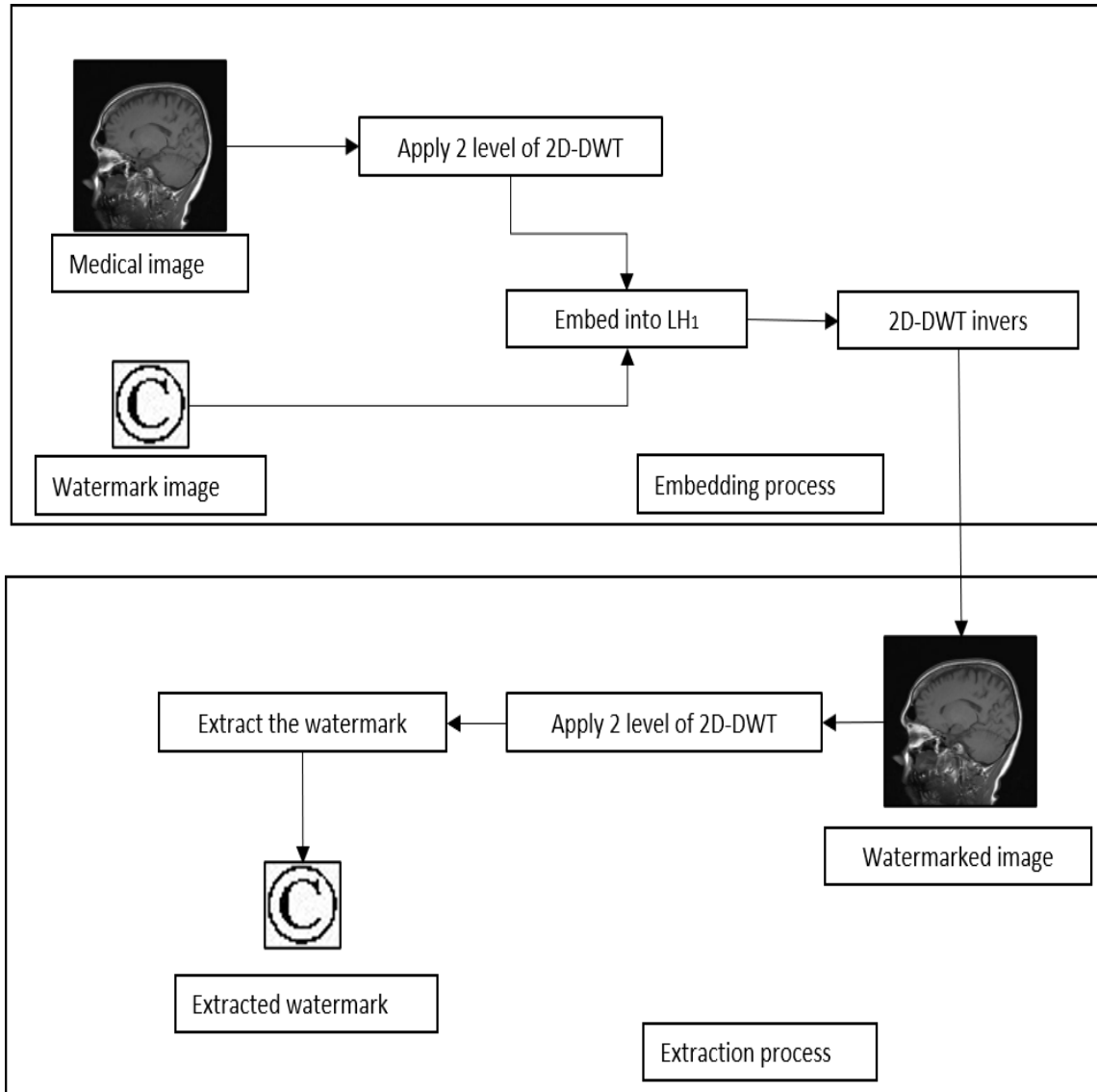


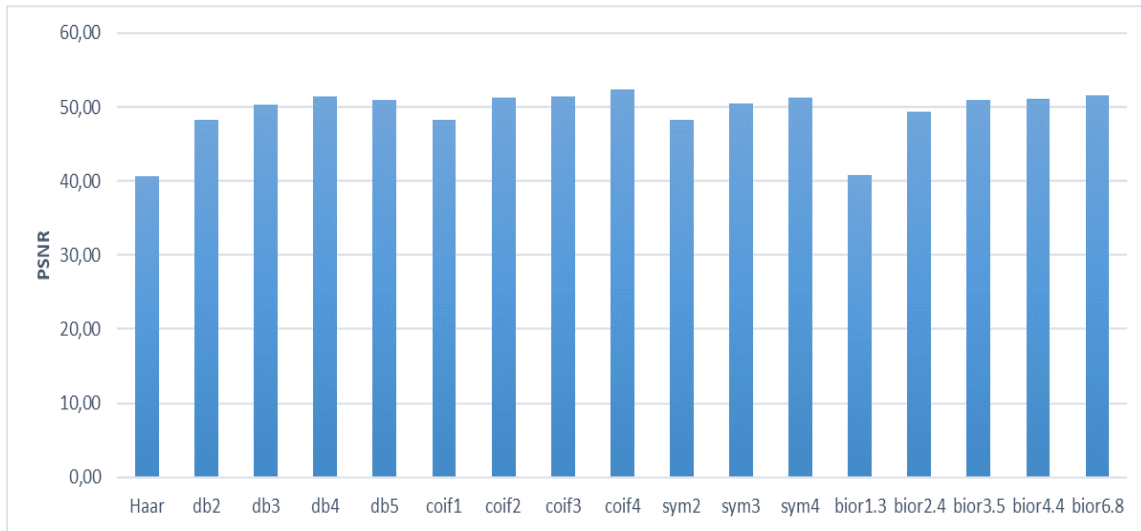
Figure 3.6: Medical Image Watermarking Algorithm Based on 2D-DWT

Table 3.2: The Impact of Wavelet Families on the Imperceptibility of Medical Images

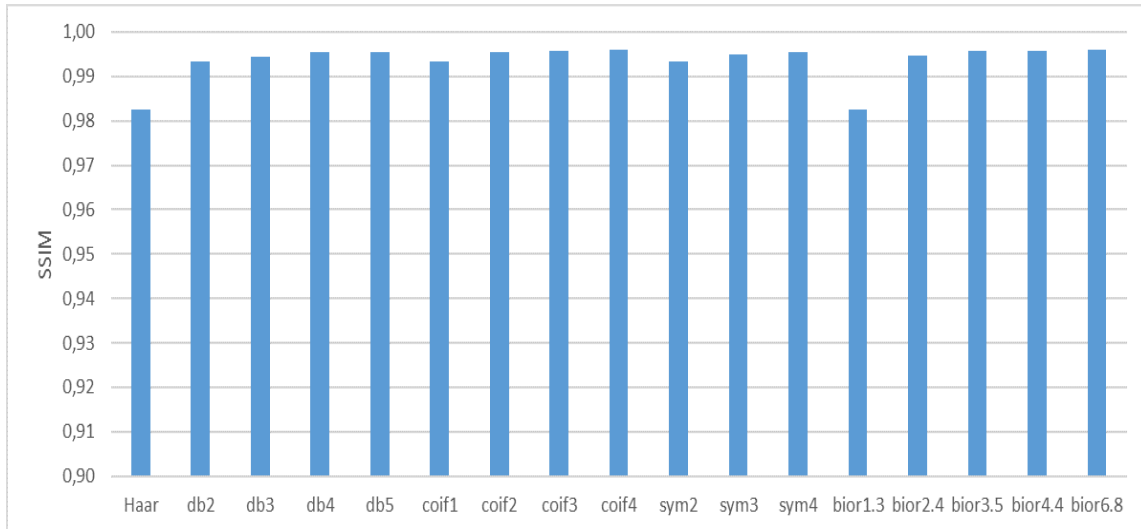
Wavelet	Ultrasound		X-ray		ct		MRI	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Haar	46,5125	0,9886	41,0084	0,9788	36,6562	0,9797	38,2317	0,9835
db2	60,1013	0,9993	43,7875	0,9869	44,3997	0,9930	44,4645	0,9940
db3	62,8863	0,9996	43,7875	0,9869	47,1606	0,9955	47,2643	0,9962
db4	63,6943	0,9997	44,5338	0,9884	48,4808	0,9964	48,7484	0,9970
db5	60,9830	0,9994	44,8948	0,9891	48,8793	0,9966	49,2212	0,9971
coif1	60,3364	0,9994	43,8495	0,9871	44,4594	0,9932	44,5464	0,9942
coif2	63,4504	0,9997	45,0052	0,9892	48,3530	0,9964	48,5795	0,9970
coif3	61,4429	0,9995	45,3247	0,9895	49,2516	0,9969	49,7231	0,9974
coif4	63,9503	0,9997	45,5220	0,9898	49,8422	0,9972	50,3807	0,9978
sym2	60,1013	0,9993	43,7875	0,9869	44,3997	0,9930	44,4645	0,9940
sym3	62,8863	0,9996	44,5338	0,9884	47,1606	0,9955	47,2643	0,9962
sym4	63,4217	0,9997	44,9662	0,9891	48,1817	0,9963	48,3729	0,9969
bior1.3	47,9644	0,9913	40,6455	0,9771	36,4642	0,9791	37,9261	0,9831
bior2.4	60,1765	0,9993	44,4555	0,9882	46,2446	0,9951	46,3613	0,9957
bior3.5	60,1765	0,9993	45,1582	0,9894	49,1413	0,9970	49,6453	0,9975
bior4.4	61,2119	0,9994	45,1751	0,9894	48,8463	0,9968	49,2107	0,9973
bior6.8	61,3409	0,9994	45,4398	0,9897	49,5496	0,9971	50,0473	0,9975

Table 3.3: The Impact of Wavelet Families on the Robustness of the Extracted Watermark.

Wavelet	Ultrasound		X-ray		ct		MRI	
	NC	SSIM	NC	SSIM	NC	SSIM	NC	SSIM
Haar	1,0000	1,0000	0,9991	0,9943	0,9917	0,9873	0,9980	0,9963
db2	0,1382	0,1861	0,1964	0,2453	0,1981	0,2469	0,1495	0,2307
db3	-0,0946	-0,0049	0,1964	0,2453	-0,1796	-0,0281	-0,1739	0,0092
db4	-0,0473	-0,0143	-0,2220	-0,0460	-0,0736	-0,0093	-0,0822	0,0205
db5	0,9727	0,9195	-0,1159	-0,0248	0,9550	0,9160	0,9610	0,9323
coif1	-0,1456	-0,0130	-0,2612	-0,0643	-0,2584	-0,0558	-0,2811	-0,0619
coif2	0,1039	0,1301	0,1855	0,2165	0,1587	0,2011	0,0854	0,1547
coif3	0,9234	0,8606	0,9159	0,8489	0,9196	0,8711	0,9223	0,8850
coif4	-0,0671	-0,0203	-0,1203	-0,0301	-0,0947	-0,0310	-0,0925	-0,0245
sym2	0,1382	0,1861	0,1964	0,2453	0,1981	0,2469	0,1495	0,2307
sym3	-0,0946	-0,0049	-0,2220	-0,0460	-0,1796	-0,0281	-0,1739	0,0092
sym4	-0,0618	-0,0174	-0,1234	-0,0295	-0,0929	-0,0171	-0,0955	0,0012
bior1.3	-0,1770	-0,0465	-0,1720	-0,0304	-0,1578	-0,0208	-0,1820	-0,0006
bior2.4	0,9784	0,9429	0,9689	0,9290	0,9730	0,9442	0,9827	0,9647
bior3.5	0,9784	0,9429	0,1995	0,2042	0,1640	0,1623	0,1051	0,1337
bior4.4	0,9756	0,9330	0,9434	0,9008	0,9554	0,9200	0,9639	0,9403
bior6.8	0,8904	0,8221	0,8809	0,8147	0,8757	0,8136	0,8676	0,8125



(a) PSNR results



(b) SSIM results

Figure 3.7: Imperceptibility Performance of Each Wavelet

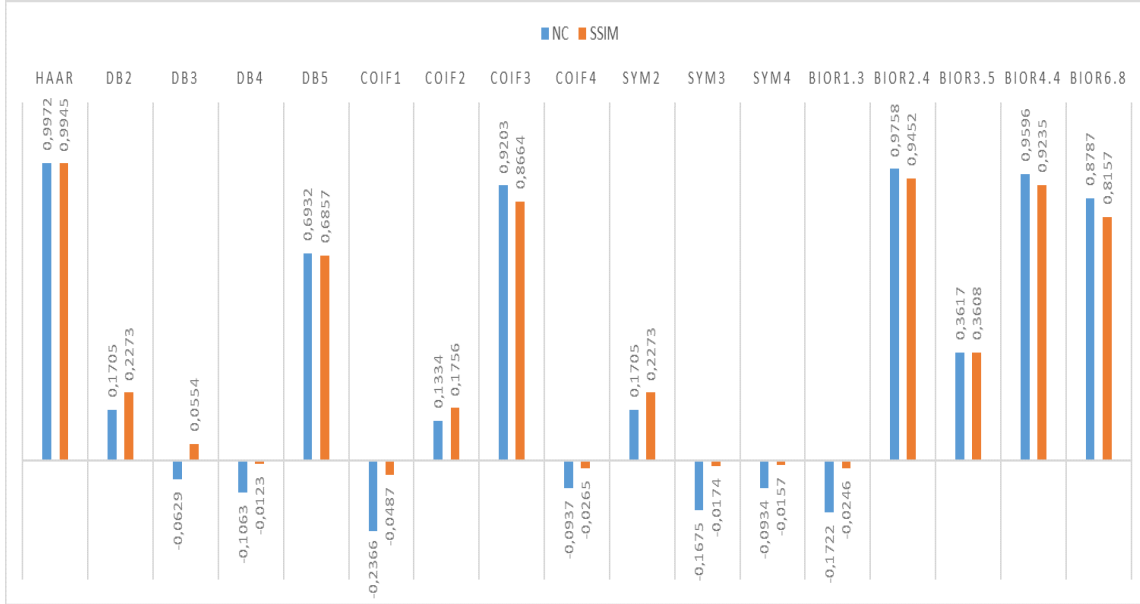


Figure 3.8: Robustness Performance of Each Wavelet (NC Results)

3.4.1.2 Results Discussion

Depending on the results above, the Haar wavelet is the most suitable wavelet for medical image watermarking:

- The Haar wavelet is a simple wavelet that has low computational complexity, making it suitable for real-time applications.
- The Haar wavelet is highly effective in detecting sharp changes or edges in an image. This makes it a great choice for watermarking because it allows for accurate placement of the watermark in areas with strong edges. By leveraging this characteristic, watermarking algorithms can hide the watermark in regions of the image where it is less likely to be noticed, ensuring both the invisibility and effectiveness of the watermark.

Overall, the Haar wavelet is a good choice for medical image watermarking because it provides a good balance between imperceptibility, robustness, and computational complexity.

3.4.2 ^{2nd} Experiment: LWT-Based watermarking

In this algorithm, we utilized the lifting wavelet transform to embed both the watermark image and the personal patient report. From the results obtained, it was determined that the Haar wavelet is the most appropriate choice for this particular algorithm.

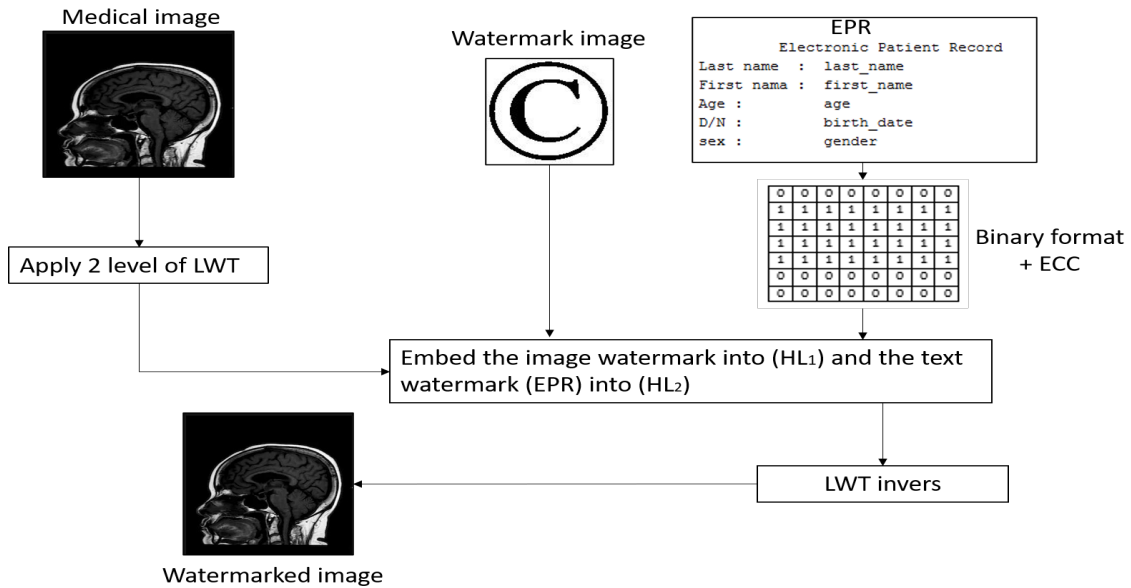
First, two levels of lifting wavelet transform (LWT) were applied to the original image. The watermark image was then embedded in the first high-low frequency (HL_1) vertical details, and the electronic patient report (EPR) was converted into binary format and embedded in the second (HL_2) vertical details. During the extraction phase, the secret information is extracted from the watermarked image by following the guidelines outlined in algorithm 2, which serves as an inverse process. Figure 2 presents a schematic representation of the algorithm, while the detailed algorithms are provided in algorithms 3 and 4.

3.4.2.1 Imperceptibility And Robustness Results

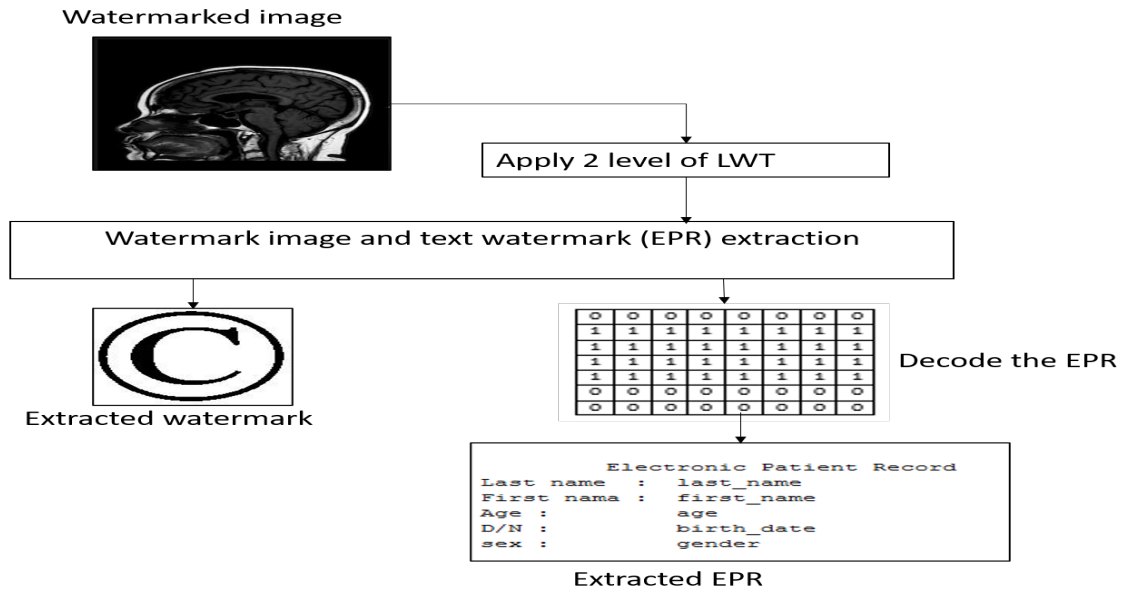
In this experiment, we utilized the same data sets as the previous experiment. Additionally, we included two categories of medical images: normal medical images and medical images exhibiting disease symptoms. This was done to verify the suitability of the watermarking algorithm for various types of medical images. The electronic patient record encompasses crucial information such as the patient's full name, date of birth, and gender.

Within Table 3.4, the imperceptibility of the watermarked images is presented, considering both normal and abnormal images. A dataset of 100 images was used for each modality. Additionally, a comparison was made between the results obtained from the watermarking algorithm being discussed and a DWT-based watermarking algorithm.

The results clearly demonstrate that the watermarking algorithm based on LWT outperforms in terms of imperceptibility. This superiority can be attributed to the characteristics of the lifting wavelet, which makes it more robust and less sensitive to errors in the input data.



(a) Embedding process



(b) Extraction process

Figure 3.9: Watermarking Algorithm Based on LWT

Table 3.5 presents the performance of the LWT-based algorithm in terms of the extracted watermark's robustness, specifically focusing on metrics such as the Nor-

Algorithm 3 LWT Based Embedding Algorithm

Input:

Medical image I ,
Watermark image W ,
Electronic Patient Record EPR

▷ Begin

1: Apply two-level of LWT on I

$$[LL_1, HL_1, LH_1, HH_1] = LWT(I, Haar)$$

$$[LL_2, HL_2, LH_2, HH_2] = LWT(LL_1, Haar)$$

2: Divide HL_1 and HL_2 into (4x4) block

3: Choose two coefficients from each block.

▷ Embedding the watermark image W

4: Embed the watermark image W into the HL_1 subband by applying the rules described in Algorithm 1. This process will generate a modified subband HL'_1 .

▷ Embedding the electronic patient record EPR

5: Convert the Electronic Patient Record (EPR) into binary format, and then encode it using an Error Correction Code (ECC).

6: Follow the embedding rules specified in the Algorithm 1 to modify the HL_2 subband, resulting in a modified subband HL'_2 .

▷ Watermarkd image reconstruction I'

7: Reconstruct the watermarked image (I') using an inverse LWT (Inverse Lifting Wavelet Transform).

$$LL'_1 = ILWT([LL_2, HL'_2, LH_2, HH_2], Haar)$$

$$I' = LWT([LL'_1, HL'_1, LH_1, HH_1], Haar)$$

Algorithm 4 LWT Based Extraction Algorithm

Input:

 Watermarked image I' ,

▷ Begin

1: Apply two-level of LWT on I

$$[LL'_1, HL'_1, LH'_1, HH'_1] = LWT(I', Haar)$$

$$[LL'_2, HL'_2, LH'_2, HH'_2] = LWT(LL'_1, Haar)$$

 2: Divide HL'_1 and HL'_2 into (4x4) block

3: Choose two coefficients from each block.

 ▷ Watermark image W extraction

 4: Extract the watermark image W from the HL'_1 subband by applying the rules described in Algorithm 2.

 ▷ Extraction of the electronic patient record EPR

 5: Follow the embedding rules specified in the Algorithm 2 to extract the EPR

malized Correlation Coefficient (NC) and Structural Similarity Index (SSIM) for the watermark image, along with the bit error rate for the EPR.

The findings demonstrate that the LWT offers significantly higher robustness for the extracted watermarks when compared to DWT. This observation remains consistent across both normal and abnormal medical images, regardless of the imaging modality used.

Table 3.4: PSNR and SSIM Results of the Watermarked Image

Modality	LWT				DWT			
	normal images		abnormal images		normal images		abnormal images	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Ultrasound	43,3943	0,9738	42,0091	0,9711	43,2240	0,9732	41,7074	0,9703
X-ray	39,0095	0,9621	38,9201	0,9636	38,9171	0,9613	39,0597	0,9633
CT	35,2920	0,9615	34,2612	0,9576	34,4979	0,9601	33,6437	0,9563
MRI	36,5372	0,9640	35,2567	0,9610	36,2538	0,9627	35,1340	0,9592

Table 3.5: Robustness Results of the Watermarked Image

Modality	LWT			DWT		
	watermark image		EPR	watermark image		EPR
	NC	SSIM	BER	NC	SSIM	BER
Ultrasound	1,0000	1,0000	0,0000	0,9929	0,9928	0,0000
X-ray	0,9990	0,9939	0,0011	0,9813	0,9771	0,0011
CT	0,9921	0,9870	0,0053	0,9800	0,9744	0,0056
MRI	0,9975	0,9945	0,0074	0,9230	0,9143	0,0066

(a) Normal medical images

modality	LWT			DWT		
	watermark image		EPR	watermark image		EPR
	NC	SSIM	BER	NC	SSIM	BER
Ultrasound	1,0000	1,0000	0,0000	0,9918	0,9914	0,0000
X-ray	0,9985	0,9893	0,0004	0,9756	0,9648	0,0004
CT	0,9815	0,9744	0,0121	0,9781	0,9715	0,0119
MRI	0,9982	0,9953	0,0116	0,9415	0,9345	0,0118

(b) Abnormal Medical Images

3.5 Conclusion

In conclusion, this chapter presented a comprehensive investigation into the application of wavelet-based watermarking algorithms for securing medical images and electronic patient records. The research focused on evaluating the algorithm's ability to meet the requirements of imperceptibility, robustness, and capacity for watermarking applications.

In the initial experiment, we examined the influence of different wavelet families on watermarking algorithms. The findings revealed that the Haar wavelet demonstrated remarkable robustness, making it the optimal choice for watermarking medical images while maintaining their visual quality.

In the second experiment, we compared the performance of two wavelet transforms: the second-generation wavelet transform (Lifting Wavelet Transform LWT) and the traditional wavelet transform (Discrete Wavelet Transform DWT). The results validated that the LWT-based algorithm excels in both imperceptibility and robustness, making it an ideal and effective solution for securing sensitive medical data.

Overall, this chapter's results and analysis set the groundwork for the subsequent chapters, where further investigation and improvements to the watermarking algo-

rithm will be explored to enhance its performance and applicability in real-world medical imaging scenarios.

Chapter : 4

***EXPLORING HYBRID TECHNIQUES AND
OPTIMIZATION ALGORITHMS IN
MEDICAL IMAGE WATERMARKING***

Contents

4.1	Introduction	70
4.2	Hybrid Watermarking Techniques	71
4.2.1	Fast Walsh-Hadamard Transform	71
4.2.2	Singular Value Decomposition	73
4.2.3	Discrete Cosine Transform	75
4.2.4	Comparative Analysis of Hybrid Approaches	77
4.3	Optimization Techniques in Watermarking	96
4.3.1	Artificial Bee Colony Algorithm	96
4.3.2	Methodology:	98
4.3.3	Results and Discussion	99
4.4	Conclusion	109

4.1 Introduction

Utilizing the wavelet domain for medical image watermarking offers several advantages over other techniques, as it exhibits enhanced robustness and efficiency in fulfilling the requirements of watermarking algorithms.

Despite the popularity of wavelet domain watermarking for image embedding, it does come with certain drawbacks. Firstly, the wavelet transform involves a loss of information during image decomposition into wavelet coefficients. Consequently, extracting the watermark becomes more challenging, particularly when the image undergoes quality-degrading attacks.

Another drawback of using the wavelet transform in image watermarking is its lack of shift-invariance, especially when subjected to geometric attacks, making the extraction of the watermark challenging, as the embedded information may be distributed across different wavelet coefficients based on the image's position.

To overcome this issue, hybrid watermarking algorithms offer a possible solution by combining various techniques and embedding domains. The use of multiple approaches can enhance the watermarking algorithm by taking advantage of the strengths of each approach while compensating for their individual weaknesses. This enables the algorithm to become more robust and effective in watermarking, resulting in improved resistance against attacks and better performance during watermark extraction.

Furthermore, optimization algorithms serve as a valuable tool to enhance the effectiveness of watermarking algorithms. These powerful techniques are capable of identifying the optimal embedding parameters, such as the scaling factor and the most suitable location for watermark insertion, leading to more secure and reliable watermark embedding in various applications.

In addressing the challenges inherent in watermarking medical images, the exploration of hybrid techniques and optimization algorithms emerges as critically important. These innovative approaches strategically respond to the limitations associated with wavelet transforms, particularly issues of information loss and translation invariance. Our focus on integrating diverse techniques and employing optimization algorithms aims to maintain the robustness of digital watermarking methods. This is especially crucial in the medical field, where major importance is placed on data security and image integrity. The reliability of digital watermarking techniques is directly related to the confidentiality of medical information and the accuracy of diagnostic results. By offering effective solutions to existing limitations, our research attempts to instill greater confidence in the use of watermarked medical images, thereby reinforcing data security and ensuring the integrity of information crucial

to healthcare professionals and patients. The impact of this investigation extends beyond the realm of research, positively influencing the quality of medical care and the protection of sensitive data within the healthcare sector.

In this chapter, we present an exploration of hybrid medical image watermarking techniques, discussing their advantages and limitations. We also delve into the fundamentals of optimization algorithms and their application to watermarking. Additionally, we investigate how the integration of hybrid and optimization approaches can lead to a robust and imperceptible watermarking framework.

4.2 Hybrid Watermarking Techniques

In a hybrid algorithm, a primary transform, like the wavelet transform, is combined with other transforms, such as Fast Walsh-Hadamard Transform (FWHT), Singular Value Decomposition (SVD), and Discrete Cosine Transform (DCT), to enhance overall performance. By integrating these techniques, the hybrid approach achieves superior security, robustness, and imperceptibility, leveraging the unique strengths of each transform.

In this section, we provide a theoretical background of well-known transforms that are compatible with the Lifting Wavelet Transform (LWT). This approach enhances both imperceptibility and robustness compared to employing a single LWT-based watermarking algorithm. Moreover, the increased complexity of the algorithm contributes to the heightened security of the scheme.

4.2.1 Fast Walsh-Hadamard Transform

The Walsh-Hadamard transform (WHT), also known as the Hadamard transform, is a non-sinusoidal and orthogonal transform that is considered a generalized form of the Fourier transform. The Hadamard transform is named after the French mathematician Jacques Hadamard and is commonly used in various applications, such as image compression, noise reduction, and pattern recognition. The transform is particularly useful in preserving the structure of a sampled image and enabling efficient coding of image data.

There is a faster version of WHT called the Fast Walsh-Hadamard Transform (FWHT). It is a more efficient algorithm used for computing the WHT, offering the advantage of reduced computational complexity and storage requirements.

4.2.1.1 Hadamard Matrices

A Hadamard matrix H is a square matrix of order N composed of elements that are either $+1$ or -1 . The value of N is an integer power of two ($N = 2^k$), and Hadamard matrices are known to exist for values of N up to 200 [65]. The equation represents the Hadamard matrix is:

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} \quad (4.1)$$

Where $K=1, 2, 3, \dots$

For example when $K=1$, the Hadamard matrix H_2 is defined as

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (4.2)$$

And when $K=2$, the Hadamard matrix H_4 is defined as

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (4.3)$$

4.2.1.2 The Fast Walsh-Hadamard Structure

Similar to the Fast Fourier Transform (FFT), the Fast Walsh-Hadamard Transform (FWHT) is a faster version of the Walsh-Hadamard transform. In comparison to the FFT, the FWHT offers advantages such as reduced storage space and faster computation. This is because the FWHT utilizes only real additions and subtractions, while the FFT requires complex values.

Both the FWHT and its inverse (IFWHT) exhibit symmetry and utilize identical calculation processes. For a signal $x(t)$ of length N , the FWHT and IFWHT can be defined as follows:

$$y_n = \frac{1}{N} \sum_{i=0}^{N-1} x_i H(n, i) \quad (4.4)$$

$$x_i = \sum_{n=0}^{N-1} y_n H(n, i) \quad (4.5)$$

Where $i=0, 1, \dots, N-1$ and $H(n,i)$ are Walsh function. The N elements are decomposed into two sets of $N/2$ elements, which are then combined using a butterfly structure to form the FWHT.

4.2.1.3 The Fast Walsh-Hadamard Scheme Properties

The Fast Walsh-Hadamard Transform (FWHT) offers several advantages over the standard Walsh-Hadamard Transform (WHT):

1. **Computationally efficient:** the computational efficiency of the Fast Walsh-Hadamard Transform (FWHT) is attributed to its utilization of simple operations, such as addition and subtraction. This approach requires less processing power, making the FWHT more computationally efficient compared to other techniques.
2. **Low complexity:** the simplicity of the arithmetic operations involved in the Fast Walsh-Hadamard Transform (FWHT) contributes to its low complexity. This characteristic makes FWHT an attractive option for hardware implementation, as it can be efficiently executed on various computing platforms.
3. **Orthogonality:** It implies that the transformed coefficients obtained through the WHT are uncorrelated and possess equal energy. This orthogonality property renders the WHT well-suited for various applications, including data compression and signal processing. By utilizing the orthogonality of the transform, it becomes possible to efficiently represent and manipulate signals while preserving their essential characteristics.
4. **Block division:** It enables the WHT to be divided into smaller blocks, which can be processed independently of each other. This property offers advantages in terms of parallel processing and distributed computing.

4.2.2 Singular Value Decomposition

Singular Value Decomposition (SVD) is a powerful tool in linear algebra, offering numerous attractive properties and geometric features for various applications. Its flexibility is evident in image coding, compression, watermarking, and other domains, making SVD a remarkably effective and useful technique in digital image processing. The SVD helps to improve the robustness and imperceptibility of image watermarking schemes by modifying the coefficients of SVD decomposition of the cover image to embed the watermark signal. SVD coefficients offer high robustness, visual quality, and data payload if there is a minute modification. Therefore, many researchers have proposed SVD-based image watermarking schemes. [66]

4.2.2.1 The Mathematical Perception Behind The SVD

Singular Value Decomposition (SVD) involves decomposing a matrix I of size $m \times n$ into three matrices: U , S , and V^T , where the columns of U and V are orthogonal, and the matrix S is diagonal with positive real entries.

The singular values decomposition of a real matrix can be written as the product.

$$I = USV^T \quad (4.6)$$

where the m by n matrix U and the n by n matrix V satisfy:

$$U^T U = V^T V = V V^T = 1_n \quad (4.7)$$

And:

- U is an $m \times m$ orthogonal matrix, with its columns forming an orthonormal basis for the row space of I .
- S is an $m \times n$ diagonal matrix, containing the singular values of I , arranged in descending order on the diagonal. The singular values are real, positive, and non-negative.
- V^T (V transpose) is an $n \times n$ orthogonal matrix, with its columns forming an orthonormal basis for the column space of I .

4.2.2.2 Characteristics Features of SVD

The SVD offers a unique and valuable advantage as it provides an optimal decomposition of a matrix into three constituent matrices. This property enables numerous applications and benefits, such as:

- **Simplifying Dimensionality:** Singular Value Decomposition (SVD) simplifies high-dimensional data by reducing the number of dimensions, facilitating easier visualization and analysis.
- **Diverse Field Applications:** SVD finds utility in diverse fields, including image processing, natural language processing, and recommendation systems, among others.
- **Enhanced Interpretability:** Extracted singular values and vectors from SVD offer valuable understandings of the data's structure and feature relationships, contributing to improved interpretability.

4.2.2.3 SVD Limitation

Singular Value Decomposition (SVD) is a powerful tool widely utilized in image processing and watermarking, offering numerous applications. However, it is essential to acknowledge that there are also certain drawbacks associated with its use in these particular domains.

- **Computational Complexity:** Implementing the SVD algorithm can be computationally intensive, particularly for large images, which may result in longer processing times.
- **Noise Sensitivity:** The SVD algorithm is susceptible to noise in the image, potentially causing inaccuracies during the watermark detection process.
- **Scale Sensitivity:** Changes in the scale of the image, such as resizing or compression, may affect the accuracy of watermark detection using the SVD algorithm.

4.2.3 Discrete Cosine Transform

The Discrete Cosine Transform (DCT) is a powerful mathematical technique employed in image processing to transform image pixel data from the spatial domain into the frequency domain. This conversion enables the identification of redundancies, patterns, and essential information within the image.

In the context of the Discrete Cosine Transform (DCT), the positioning of coefficients within its matrix follows a pattern that corresponds to the frequency content of the signal being transformed.

therefore, in the DCT matrix, lower-frequency coefficients are positioned in the upper left corner, medium-frequency coefficients occupy the middle area, and higher-frequency coefficients are located in the lower right corner.

4.2.3.1 Formulation

The two-dimensional DCT of an M-by-N matrix A is defined as follows.

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \quad (4.8)$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \leq p \leq M-1 \end{cases} \quad (4.9)$$

$$\alpha_q = \begin{cases} 1/\sqrt{N}, & p = 0 \\ \sqrt{2/N}, & 1 \leq p \leq N-1 \end{cases}$$

Where the DCT coefficients of matrix I are denoted as B_{pq} .

The DCT is a reversible transformation, and its inverse is defined as follows:

$$I_{mn} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \quad (4.10)$$

4.2.3.2 Properties of DCT

The DCT is a powerful tool that has many applications in signal processing. It is a versatile tool that can be used to solve a wide range of problems.

Here are some of the properties of DCT[67]:

- **Decorrelation:** The primary benefit of image transformation through techniques like the DCT is its capacity to eliminate repetitive information among nearby pixels, leading to uncorrelated transform coefficients that can be encoded separately and efficiently.
- **Energy Compaction:** The effectiveness of a transformation scheme is determined by its capability to represent input data with a minimal number of coefficients. This enables the quantization process to remove coefficients with low amplitudes without causing noticeable visual distortion in the reconstructed image. The Discrete Cosine Transform is particularly adept at compacting energy for images with strong correlations, making it an excellent choice for efficient data representation in image compression applications.
- **Separability:** The separability property of the DCT enables the computation of its coefficients in a two-step process through successive 1-D operations on image rows and columns. This property simplifies the computation and enhances the efficiency of both forward and inverse DCT operations, making it a valuable feature in image and video processing algorithms.
- **Symmetry:** The coefficients of the DCT are symmetric about the center of the spectrum, which means that the coefficients from the first half of the spectrum are equal to the coefficients from the second half of the spectrum, but with the opposite sign.
- **Orthogonality:** Orthogonality means that the dot product of any two DCT coefficients is zero if the coefficients are not from the same frequency. This property leads to a reduction in the complexity of pre-computation.

4.2.3.3 DCT Limitation

- **Lossy compression:** The DCT is a type of compression method that results in some loss of information during the compression process. Consequently, it can be challenging to fully restore the original signal from the DCT coefficients.
- **Not robust to noise:** The DCT is not highly resistant to noise, meaning that if the signal is affected by noise, the DCT coefficients will also be influenced, making it difficult to accurately recover the original signal from these coefficients.
- **Not suitable for sharp edges:** The DCT is not well-suited for representing signals with sharp edges due to the smooth nature of its coefficients. As a result, the DCT may struggle to precisely represent the sharp edges present in a signal.

4.2.4 Comparative Analysis of Hybrid Approaches

In this portion, we introduce a hybrid watermarking method designed to enhance the security of medical images. Building upon the preceding chapter, we employed a combination of the lifting wavelet transform (LWT) and the Fast Walsh-Hadamard Transform (FWHT) to insert both a watermark image and the EPR into the medical image.

To enhance the approach's effectiveness, we incorporated extra methods to address potential challenges encountered during the watermarking procedure or in the transmission. These challenges encompass concerns like ensuring the security of the watermark, handling potential errors in the EPR, and countering geometric attacks.

4.2.4.1 Error-Correcting Code

An error-correcting code (ECC) is a method of encoding messages using binary numbers. This technique ensures that even if some bits are accidentally changed, the original message can still be retrieved accurately. ECCs are extensively employed for message transmission, particularly in scenarios involving data storage. They play a crucial role in safeguarding data against corruption.

Principle of error-correcting codes: Error-correcting codes operate by appending extra information (bites), known as redundant or control information, to the message that needs to be sent. This additional data is designed in a way that allows the detection and correction of transmission errors[68].

An elementary illustration of Error-Correcting Code (ECC) involves the replication of individual data elements at a fixed interval (d) for multiple iterations (n). This configuration is referred to as the (n,d) repetition code [69]. In the context of employing a (3,1) repetition code with binary data, each bit is triplicated, resulting in:

$$\begin{aligned}0 &\longrightarrow 000 \\1 &\longrightarrow 111\end{aligned}$$

Consider M as the source message wherein:

$$M = 011010$$

Through the utilization of a (3,1) repetition code, the resultant reserved data R shall manifest as:

$$R = 000111111000111000$$

Types of Error-Correcting Codes: Error-Correcting Codes (ECCs) can be generally sorted into two primary groups: block codes and convolutional codes:

- **Block codes:** In this approach, the original message is divided into unchanging blocks of bits. Additional redundant bits are then introduced to these blocks, serving the purpose of identifying or rectifying errors.

Various types of block codes exist, encompassing:

- Hamming Codes.
 - Reed-Solomon Codes.
 - BCH Codes.
- **Convolutional codes:** In this method, the message is represented as data streams with varying lengths. Parity symbols are produced by applying a specific Boolean function that slides over the data stream. In 1955, Elias put forth the concept of Convolutional codes, and later in 1973, Viterbi introduced a decoding algorithm for it, which came to be known as the Viterbi scheme [70].

BCH Codes: Bose–Chaudhuri–Hocquenghem codes, known as BCH codes, represent a class of error correcting codes (ECC) that possess the capability to rectify multiple errors. These codes owe their name to their creators: Raj Chandra Bose, D. K. Ray-Chaudhuri, and André Leroy Hocquenghem.

BCH codes constitute a category of cyclic error-correcting codes, built through the utilization of polynomials within a finite field, often referred to as a Galois field. Operating as a form of block code, they possess the capability to rectify a predetermined quantity of errors. These codes find widespread application in digital communication systems, effectively guaranteeing the precision of transmitted data.

For an $[n, k]$ BCH code, the requisite message should adopt the format of a binary Galois field array encompassing k columns. Subsequently, the associated code linked to this message adopts the structure of an n -column binary Galois field array. In these Galois field arrays, each row signifies a distinct word[71].

At their core, BCH codes are characterized by:

- Length of codeword: $n = 2^m - 1$
- Number of parity check bits: $n - k \leq mt$
- Minimum distance: $d_{min} \geq 2t + 1$

Where:

m is the degree or integer of the generating polynomial

k is the length of information

t is the maximum number of correctable errors

In the presented approach, the electronic patient record (EPR) encompasses patient personal details represented in textual form, comprising letters and characters. In the initial stages, we employ the 7-bit ASCII code (American Standard for Information Interchange) to transform the EPR content into numerical values, effectively rendering it in binary format.

4.2.4.2 Chaotic maps

In the realm of mathematics, a chaotic map refers to a dynamical system that exhibits sensitivity to its initial conditions. This signifies that even minor alterations in the starting conditions can result in substantial variations in the system's output as time progresses.

Edward Lorenz of MIT is credited with discovering chaos theory in the early 1960s [72] while attempting weather predictions through approximations. Chaos theory explains how apparently random and disorderly outcomes are connected to the underlying patterns that produce them. When we understand the interconnections within a generator, we can study these patterns effectively.

Chaotic maps find utility across diverse domains, encompassing disciplines such as physics, biology, economics, and cryptography. They serve practical roles in the generation of pseudo-random sequences, simulation of intricate phenomena, and reinforcement of security measures [73].

Arnold's Cat Map In the presented approach, a chaotic map was employed to enhance the security of the watermark image. The image pixels were rearranged through the utilization of Arnold's Cat map, a stage acknowledged within chaotic encryption systems as the "confusion phase."

Arnold's Cat Map depicts chaos in a two-dimensional space and can be used to shift the positions of image pixels while keeping all image details intact. This method allows you to rearrange the pixel layout in images without losing any of the original data [74].

The pixel coordinates of an image can be represented as a set :

$$I = \{(x, y) | x, y = 0, 1, 2 \dots N - 1\}.$$

The 2-dimensional image transformation using Arnold's Cat Map can be expressed through the following equation:

$$(x, y) = (2x + y, x + y) \text{ mod } 1. \quad (4.11)$$

where $x(n), y(n) \in [0, 1]$. It can be discretized as:

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \text{ mod}(1) \quad (4.12)$$

and be extended to a more general form:

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq + 1 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \text{ mod}(N) \quad (4.13)$$

where $p, q \in \{0, 1, \dots, N - 1\}$

When employing the Arnold's Cat map for tasks like watermarking or image encryption, $[x(0), y(0)]^T$ commonly signifies the initial pixel position within an image,

whereas $[x(n), y(n)]^T$ represents the pixel position after the n -th iteration of the map.

Figure 1 illustrates the impact of the Arnold's Cat map on the watermark image. It is evident from the figure that the chaotic pattern of the image is influenced by the number of iterations. Moreover, it is possible to restore the original image after a specific count of iterations.

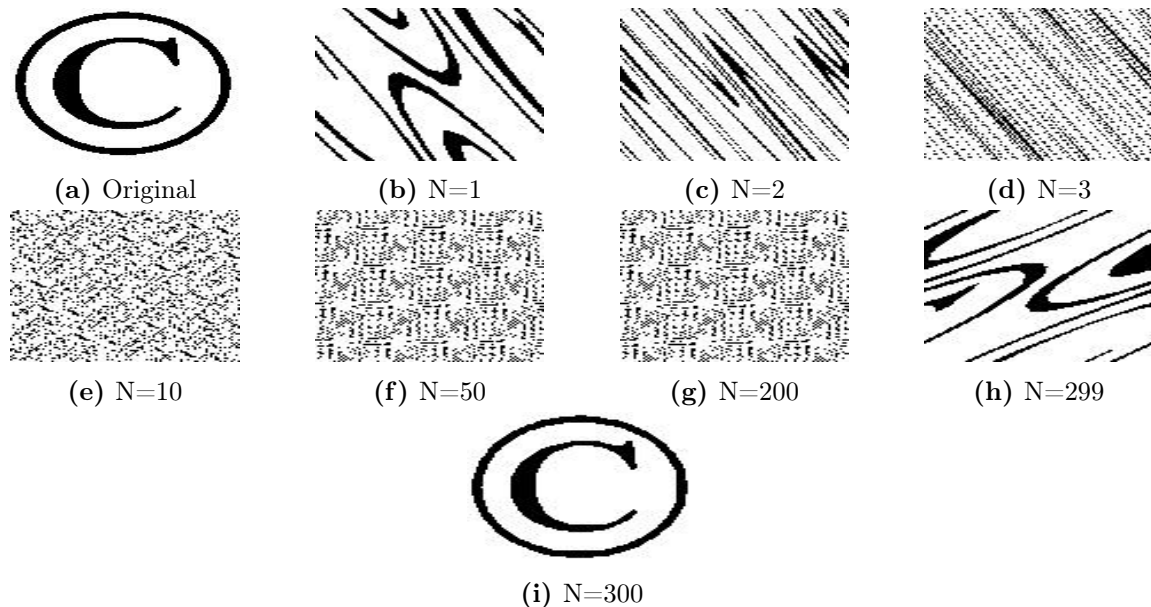


Figure 4.1: The Effect of Arnold's Cat Map on the Watermark After N Iterations

4.2.4.3 Speeded-Up Robust Features

Since the wavelet domain is not geometrically invariant, we must find a way to defend against geometrical attacks. The Speeded-Up Robust Feature (SURF)[75] was used as a result. It is a scale and rotation-invariant detector used in a variety of image processing applications, including object detection, image registration, and classification. The aim is to use the Hessian matrix determinant to extract the feature point and their scale, which reduces the computation time[76, 77].

$$H(P, \delta) = \begin{bmatrix} L_{xx}(P, \delta) & L_{xy}(P, \delta) \\ L_{xy}(P, \delta) & L_{yy}(P, \delta) \end{bmatrix} \quad (4.14)$$

where, $L_{xx}(P, \delta)$, $L_{xy}(P, \delta)$ and $L_{yy}(P, \delta)$ denote the convolution of the second-order Gaussian derivative of the base image at point P . P is the given point. and the

approximate determinant is:

$$\det(H_{approx}) = L_{xx}(P, \delta).L_{yy}(P, \delta) - (0.9 * L_{xy}(P, \delta))^2 \quad (4.15)$$

In our research, we suggest applying the SURF method to recover the angle and scale while using the matching point between the watermarked image and the attacked image.

4.2.4.4 Methodology

We introduce a novel hybrid watermarking algorithm tailored for medical images, leveraging a transform domain approach. Specifically, we combine the techniques of LWT (Lifting Wavelet Transform) and FWHT (Fast Walsh Hadamard Transform) to embed two distinct watermarks. The first watermark involves a binary image that undergoes scrambling through the utilization of Arnold’s Cat map, An implemented measure to increase image security. This binary watermark serves the dual purpose of authenticating the integrity of transmitted medical images. The second watermark consists of text, representing the Electronic Patient Record (EPR). Additionally, to enhance the safeguarding of medical data, the EPR content is subjected to encoding using BCH (Bose-Chaudhuri-Hocquenghem) code, thus fortifying the security measures in place.

Algorithm (5) and Algorithm (6) outline the steps for embedding and extracting, respectively. A graphical illustration of the proposed approach is depicted in Figure 4.2 and 4.3.

4.2.4.5 Result and Discussion

To assess the efficacy of the proposed method, we employed medical images sourced from diverse modalities[2, 3, 1, 5]. Initially, we employed the PSNR and SSIM measures to evaluate imperceptibility. Subsequently, we subjected the watermarked image to various common attacks to estimate its robustness.

Imperceptibility Results: Table 4.1 presents the average imperceptibility results for 100 medical images in each modality, evaluating the visual quality of watermarked images across different imaging methods. Notably, our proposed approach exhibits robust imperceptibility ($PSNR > 35dB, SSIM > 0.9$), indicating the preservation of medical image integrity.

The visual representations of both normal and abnormal medical images are depicted in Figures 4.4 and 4.5, respectively. Notably, the distinction between the

original cover image and the watermarked image is scarcely observable, underscoring the high imperceptibility achieved by the proposed algorithm. This observation reinforces the algorithm's effectiveness in embedding watermarks while preserving the visual integrity of both normal and abnormal medical images.

Algorithm 5 LWT/FWHT Based Embedding Algorithm

Input:

Medical image I ,
 Watermark image W ,
 Electronic Patient Record EPR

▷ Begin

- 1: Apply two-level of LWT on I

$$[LL_1, HL_1, LH_1, HH_1] = LWT(I, Haar)$$

$$[LL_2, HL_2, LH_2, HH_2] = LWT(LL_1, Haar)$$
- 2: Divide HL_1 and HL_2 into (4x4) blocks
- 3: Divide HL_1 and HL_2 into (4x4) blocks and apply FWHT to each block to get WALSH coefficients ($walsh_{coef1}$) and ($walsh_{coef2}$).
- 4: select two coefficients from each block.

▷ Embedding the watermark image W

- 5: Embed the watermark image W into the ($walsh_{coef1}$) subband by applying the rules described in Algorithm 1.

▷ Embedding the electronic patient record EPR

- 6: Convert the Electronic Patient Record (EPR) into binary format, and then encode it using a BCH code
- 7: Follow the embedding rules specified in the algorithm 1 to modify the ($walsh_{coef2}$) subband, resulting in a modified subband HL'_2 .

▷ Watermarkd image reconstruction I'

- 8: Apply WFWT inverse to each modified block and reconstruct the modified subbands HL'_1 and HL'_2
- 9: Reconstruct the watermarked image (I') using an inverse LWT (Inverse Lifting Wavelet Transform).

$$LL'_1 = ILWT([LL_2, HL'_2, LH_2, HH_2], Haar)$$

$$I' = LWT([LL'_1, HL'_1, LH_1, HH_1], Haar)$$

Algorithm 6 LWT/FWHT Based Extraction Algorithm

Input:

 Watermarked image I' ,

▷ Begin

- 1: Apply two-level of LWT on I

$$[LL'_1, HL'_1, LH'_1, HH'_1] = LWT(I', Haar)$$

$$[LL'_2, HL'_2, LH'_2, HH'_2] = LWT(LL'_1, Haar)$$

- 2: Divide
- HL'_1
- and
- HL'_2
- into (4x4) block

- 3: Apply FWHT to each block to get WALSH coefficients (
- $walsh_{coef1}$
-) and (
- $walsh_{coef2}$
-).

 ▷ Watermark image W extraction

- 4: Extract the watermark image
- W
- from the
- HL'_1
- subband by applying the rules described in Algorithm 2.

 ▷ Extraction of the electronic patient record EPR

- 5: Conform to the extraction instructions detailed in the Algorithm's 2 specifications. to extract the
- EPR
-

Table 4.1: Imperceptibility Assessment of LWT-FWHT Watermarking Algorithm on Normal and Abnormal Medical Images

Medical Images	Normal images		Abnormal images	
	PSNR	SSIM	PSNR	SSIM
Ultrasound	43,3943	0,9738	42,0091	0,9711
X-ray	39,0095	0,9621	38,9201	0,9636
CT	35,2920	0,9615	34,2612	0,9576
MRI	36,5372	0,9640	35,2567	0,9610

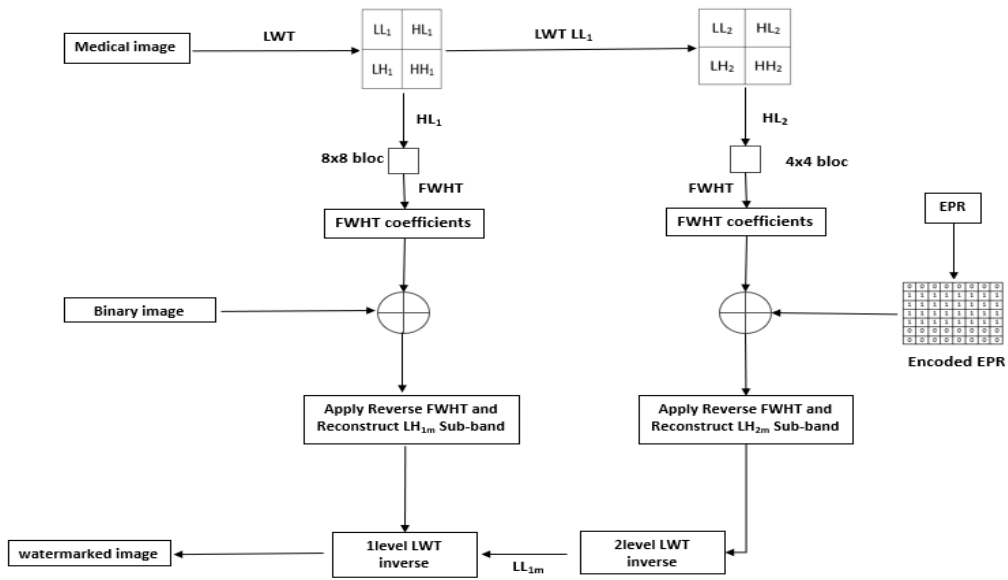


Figure 4.2: LWT/FWHT Based Watermarking Algorithm: Embedding Process

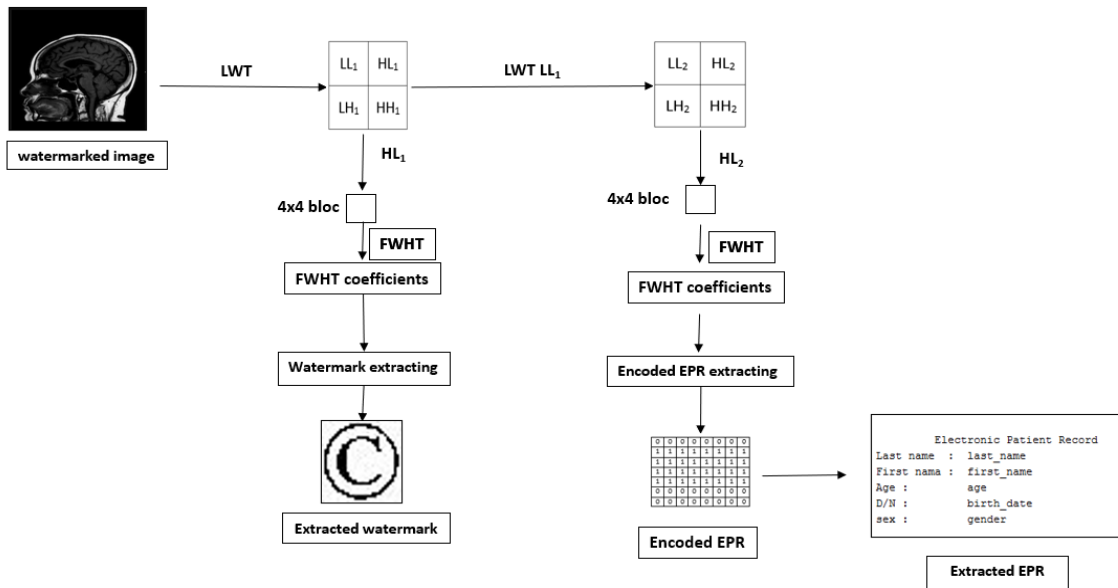
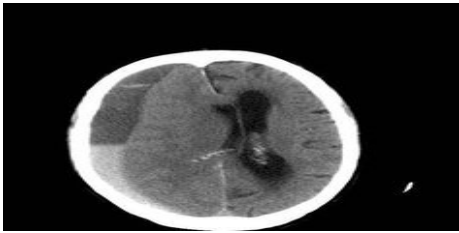
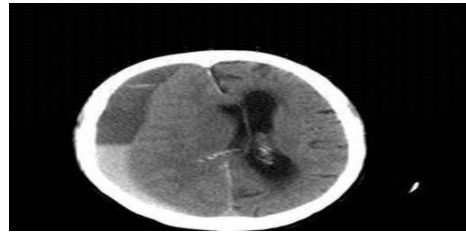


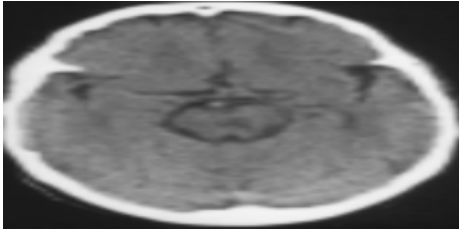
Figure 4.3: LWT/FWHT Based Watermarking Algorithm: Extraction Process



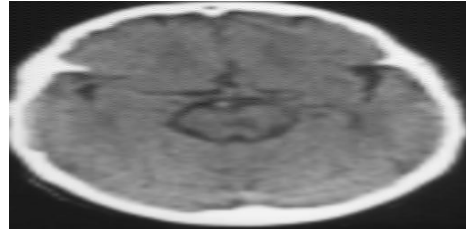
(a) Original image: MRI



(b) Watermarked image: PSNR = 36.0711 / SSIM = 0.9162



(c) Original image: CT scan



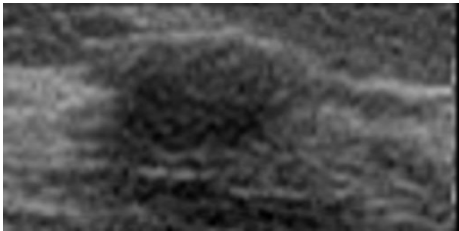
(d) Watermarked image: PSNR = 37.1014 / SSIM = 0.9268



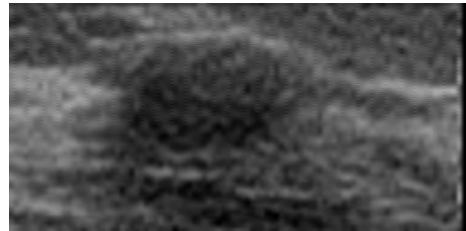
(e) Original image: X-ray



(f) Watermarked image: PSNR = 37.8597 / SSIM = 0.9283

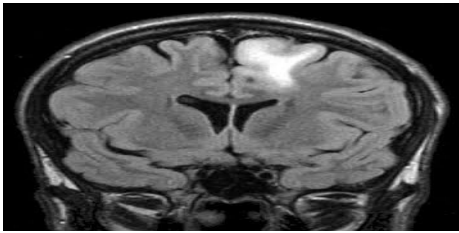


(g) Original image: Ultrasound

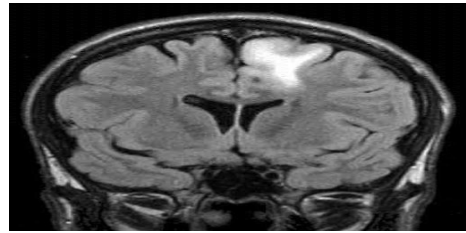


(h) Watermarked image: PSNR = 39.3256 / SSIM = 0.9321

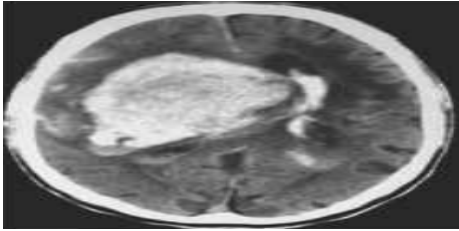
Figure 4.4: Imperceptibility Performance For Normal Medical Images



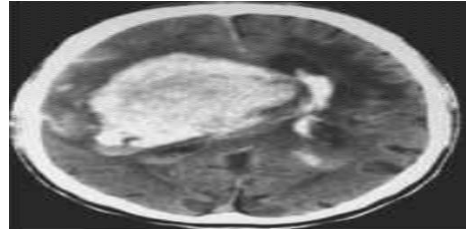
(a) Original image: MRI



(b) Watermarked image: PSNR = 35.1056 / SSIM = 0.9133



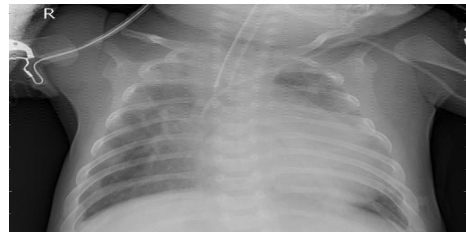
(c) Original image: CT scan



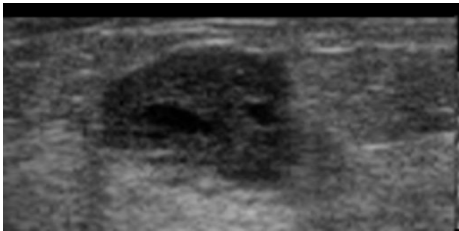
(d) Watermarked image: PSNR = 35.6005 / SSIM = 0.9261



(e) Original image: X-ray



(f) Watermarked image: PSNR = 36.9973 / SSIM = 0.9243



(g) Original image: Ultrasound



(h) Watermarked image: PSNR = 38.9887 / SSIM = 0.9314

Figure 4.5: Imperceptibility Performance For Abnormal Medical Images

Robustness Results: The robustness of the extracted watermark is evaluated by subjecting the watermarked image to various attacks. These attacks simulate potential threats that may compromise the data during transmission or when accessed by unauthorized parties [78].

- **Noise addition:** This attack involves adding noise to the watermarked image. This can be done by adding Gaussian noise, salt and pepper noise, or other types of noise to the image.
- **Filtering:** Filtering involves applying various filters to the watermarked content to remove or distort the embedded watermark. Weiner filters, median filters, and other filtering techniques can be used to reduce the visibility of the watermark.
- **Compression Attacks:** Compression algorithms may introduce artifacts that affect the embedded watermark. Lossy compression, in particular, can lead to information loss and degradation of the watermark's robustness.
- **Histogram Equalization:** Histogram equalization can alter the statistical characteristics of an image, which may affect the visibility and robustness of watermarks.
- **Rotation:** This attack involves rotating the watermarked image. This can be done by rotating the image clockwise or counterclockwise by certain degrees.
- **Scaling:** This attack involves scaling the watermarked image. This can be done by resizing the image to a smaller or larger size.
- **Translation:** Translation attacks involve displacing the watermark within the host signal. Translation specifically refers to moving the watermark horizontally and/or vertically within the image. This type of attack aims to reduce the accuracy of watermark detection by relocating the embedded watermark.

Figures (4.6),(4.7), and (4.8) display the normalized correlation (NC) and structural similarity index (SSIM) results for the extracted watermarks under filtering, noise addition, and geometric attacks, histogram equalization and JPEG compression, respectively, for normal medical images. Where, Figures (4.9),(4.10), and (4.11) display the normalized correlation (NC) and structural similarity index (SSIM) results for the extracted watermarks under filtering, noise addition, and geometric attacks, histogram equalization and JPEG compression, respectively, for abnormal medical images.

The outcomes demonstrate a commendable performance of the proposed method in both scenarios (with no attack and under attacks). Specifically, the normalized correlation (NC) values exceeded 0.6 for all the tested images, indicating a strong correlation. Similarly, the structural similarity index (SSIM) values surpassed 0.8, further affirming the effectiveness of the proposed method in maintaining watermark integrity amidst various attacks.

Figure 4.12 and 4.13 illustrate the Bit Error Rate (BER) for extracted tests from both normal and abnormal images. The results indicate that even under the most severe attacks, the proposed algorithm demonstrates robustness, with BER consistently below 0.2 in the majority of cases.

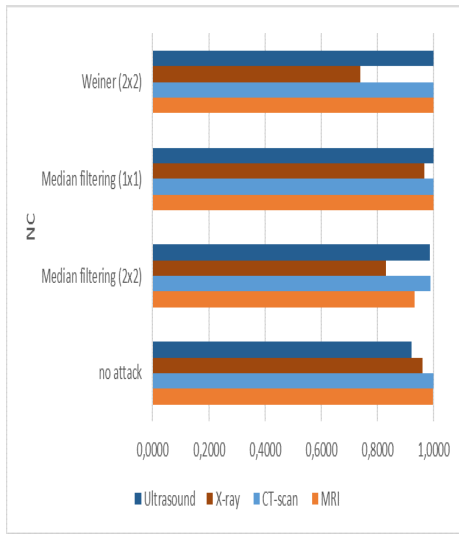
Comparative analysis The comparative evaluation of the proposed methodology was conducted against existing image watermarking techniques implemented in the transform domain, as outlined in Table 4.2.

Anand et al. [38] applied the discrete wavelet transform (DWT) and singular value decomposition (SVD) for medical image watermarking, achieving notable imperceptibility and robustness. El et al. [49] utilized DWT and Walsh-Hadamard transform (WHT) for non-medical image watermarking, attaining a heightened level of imperceptibility. For color medical images, Abdel-Aziz et al. [37] integrated the fast Walsh-Hadamard transform (FWHT) with fractional-order moments, exhibiting resilience against geometric attacks. Zhu et al. [48] proposed an enhanced singular value decomposition-inverse wavelet transform (SVD-IWT) watermarking system, showcasing effective protection against common attacks.

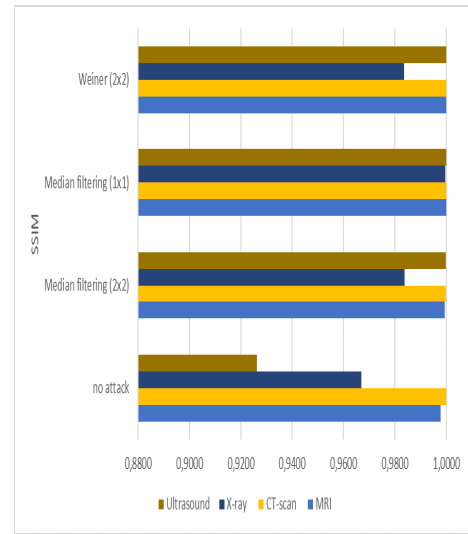
In our proposed scheme, the combination of lifting wavelet transform (LWT) and FWHT was employed for medical image watermarking, resulting in exceptional robustness. Remarkably, we achieved successful embedding of a binary image (64x64) and a text string comprising 68 characters.

The detailed comparative analysis presented in Table 4.3 indicates the superiority of our scheme in terms of both robustness and embedding capacity.

Furthermore, Table 4.4 provides a comparative assessment of the proposed and existing strategies under various attack scenarios. We used the 'Lena' image for the test as a standard image that could be a ground for a comparative study. The results underscore the heightened robustness of the proposed scheme in the face of the majority of tested attacks.

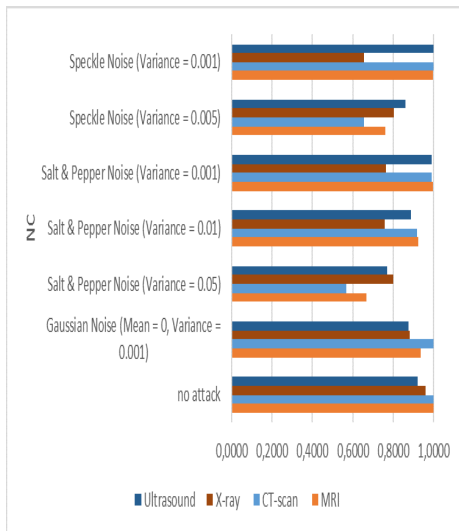


(a) NC results

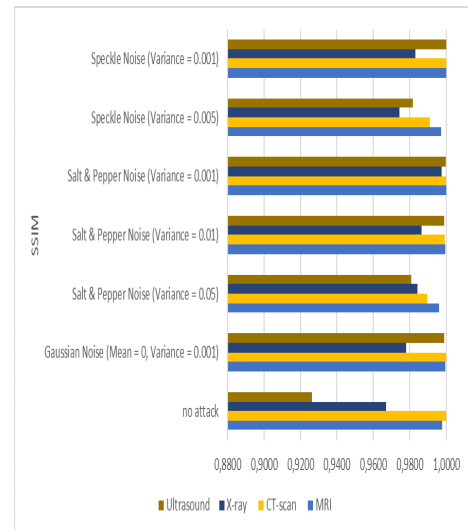


(b) SSIM results

Figure 4.6: NC and SSIM Performance for Normal Medical Images: Filtering Attacks

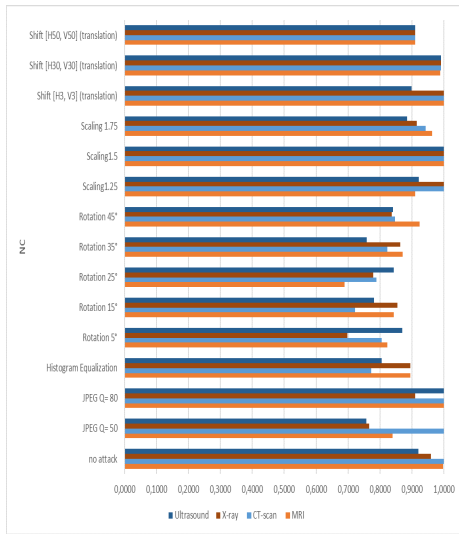


(a) NC results

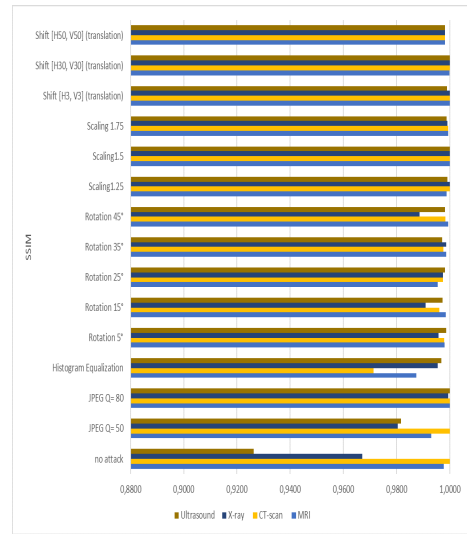


(b) SSIM results

Figure 4.7: NC and SSIM Performance for Normal Medical Images: Noise Addition Attacks

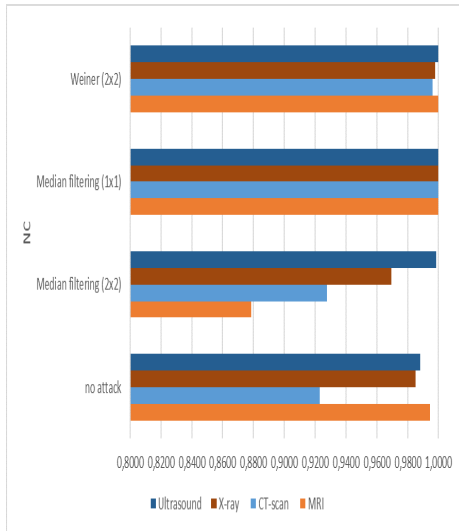


(a) NC results

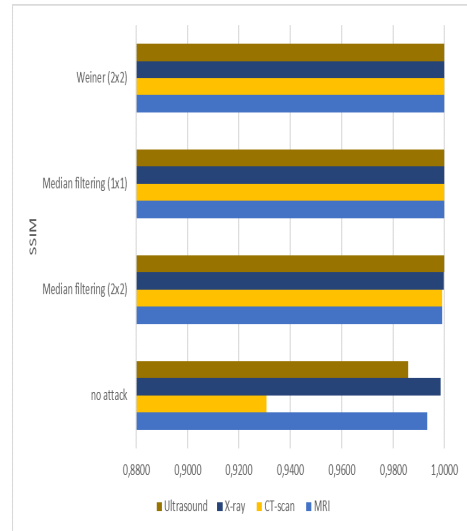


(b) SSIM results

Figure 4.8: NC and SSIM Performance for Normal Medical Images: Geometric, Compression and Histogram Attacks

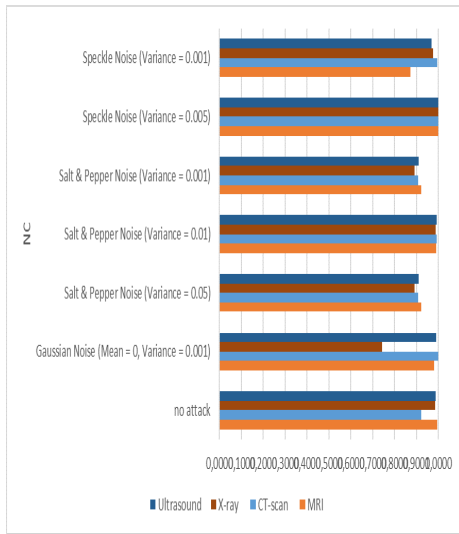


(a) NC results

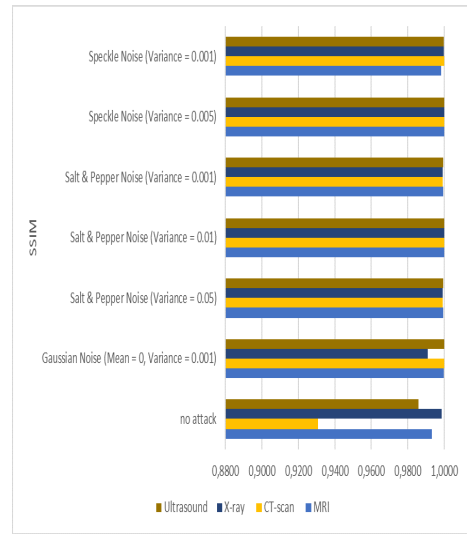


(b) SSIM results

Figure 4.9: NC and SSIM Performance for Abnormal Medical Images: Filtering Attacks

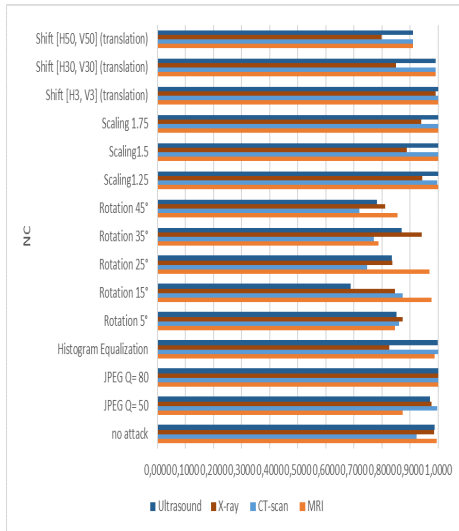


(a) NC results



(b) SSIM results

Figure 4.10: NC and SSIM Performance for Abnormal Medical Images: Noise Addition Attacks



(a) NC results



(b) SSIM results

Figure 4.11: NC and SSIM Performance for Abnormal Medical Images: Geometric, Compression and Histogram Attacks

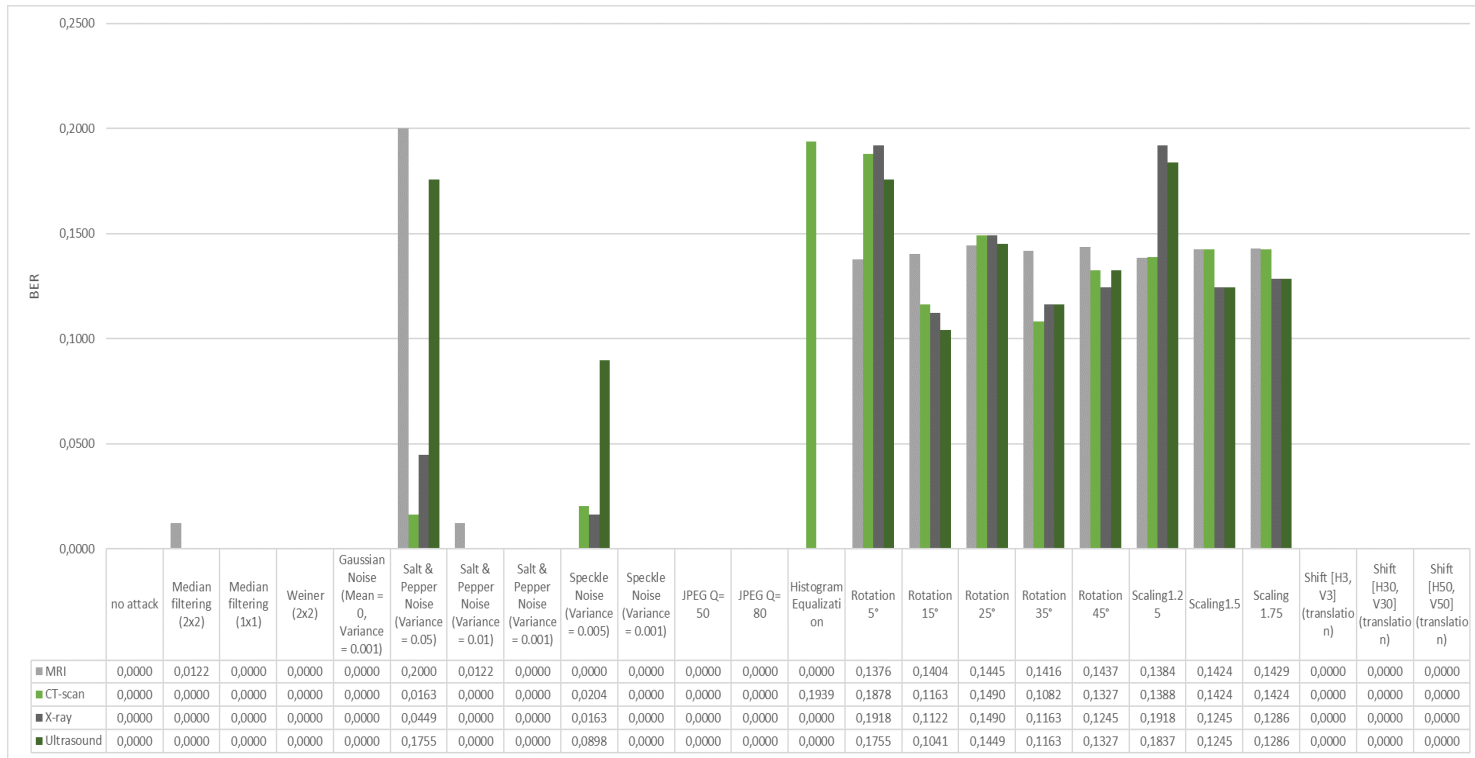


Figure 4.12: BER Performance for Normal Medical Images

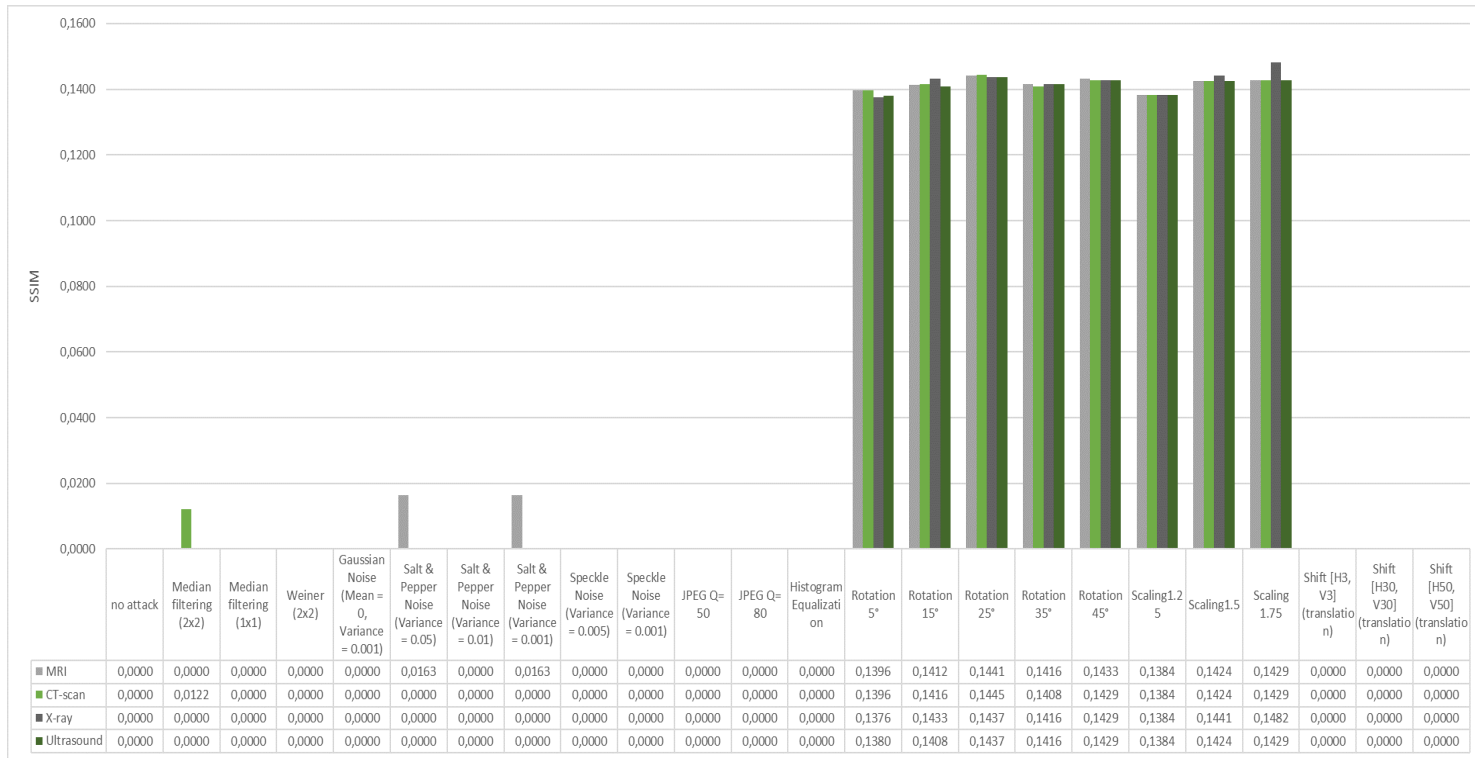


Figure 4.13: BER Performance for Abnormal Medical Images

Table 4.2: Comparison of the Proposed Technique With Existing Techniques

Algorithm	Transform	Medical image	Watermark type	Imperceptibility	Robustness	Watermark capacities	
						Text	Image
Anand et al[38]	DWT/SVD	Yes	Text/image	High	High	12 character	256x256
El Houby et al[49]	DWT/WHT	No	image	Very high	High	-	64x64
Proposed	LWT/FWHT	Yes	Text/image	High	Very high	68 character	64x64

Table 4.3: Robustness of Proposed Technique and Existing Techniques for Non-medical Image

image	proposed		Anand et al[38]		El Houby et al[49]	
	NC	BER	NC	BER	NC	BER
lena	1.0000	0.0000	-	-	0.9998	-
peppers	1.0000	0.0000	-	-	0.9960	-
rice	1.0000	0.0000	0.9999	0.0000	-	-
MRI	1.0000	0.0000	0.9994	0.0000	-	-
cell	1.0000	0.0000	0.9997	0.0000	-	-
cameraman	1.0000	0,0134	0.9982	0.0000	0.9999	-
barbara	1.0000	0.0000	0.9991	0.0000	0.9920	-
baboon	1.0000	0.0000	-	-	0.9950	-

Table 4.4: Robustness of Proposed Technique and Existing Techniques Under Different Attacks

Attacks	Abdel-Aziz[37]	Anand et al[38]	proposed
Rotation	0.9984	0.9221	0.9913
Scaling	0.9984	-	1.0000
Shift	-	-	1.0000
Compression	0.9998	0.9796	1.0000
Histogram	1.0000	0.7223	1.0000
Gaussian noise	0.9989	0.9803	0.9778
Median filtering	0.9984	0.9860	1.0000
Salt & paper	0.9989	0.9879	1.0000
Weiner filter	-	-	0.9714
Speckle noise	-	-	1.0000

4.3 Optimization Techniques in Watermarking

Watermarking technologies play a crucial role in ensuring the integrity of medical images and facilitating the confidential transmission of essential medical data.

However, achieving a balance between robustness and imperceptibility in watermarking algorithms poses a tough challenge. Meanwhile, The judicious selection of an optimal scaling factor stands out as a key consideration in addressing this complex trade-off.

Addressing this concern, researchers have recently explored the integration of nature-inspired optimized algorithms into watermarking schemes [79]. Meta-heuristic algorithms such as Genetic Algorithm (GA) [80], Particle Swarm Optimization (PSO) [81], and Artificial Bee Colony (ABC) [82] are prominent examples widely employed in various aspects of image processing, encompassing compression, segmentation, and watermarking. These endeavors reflect ongoing efforts to enhance the efficacy of watermarking algorithms through the integration of sophisticated optimization techniques.

In this section, we integrated the hybrid algorithm introduced in the preceding section with a meta-heuristic technique to facilitate the automatic selection of the scaling factor.

We propose an optimized image watermarking approach that leverages the Fast Walsh-Hadamard Transform and lifting wavelet transform in conjunction with the Artificial Bee Colony (ABC) algorithm.

4.3.1 Artificial Bee Colony Algorithm

The ABC algorithm is a type of meta-heuristic optimization method that is based on particle swarms (PSO) and was first proposed by Karaboga in 2005[83]. It takes inspiration from the foraging behavior of bees to solve optimization problems.

4.3.1.1 General Scheme

The ABC algorithm comprises the source food, which represents the solution to the problem at hand, and three groups of bees: employed, onlooker, and scout bees.

Initialization Phase: Population vectors (\vec{x}_m) of artificial bees are created, and their positions in the search space represent potential optimization solutions. For initialization purposes, the following equation could be used:

$$x_{mi} = l_i + rand(0.1) * (u_i - l_i) \quad (4.16)$$

Where l_i and u_i represent the upper and lower limits of the parameter x_{mi} .

Employed Bees: Employed bees search (\vec{v}_m) for alternative food sources that provide more nectar (the fitness value of each possible solution). They locate a new food source and then use a fitness function to determine its profitability. The neighboring food source can be identified using the formula provided by the equation.

$$v_{mi} = x_{mi} + \phi(x_{mi} - x_{ki}) \quad (4.17)$$

where (\vec{x}_k) is a randomly chosen food source, i is a randomly selected parameter index, and $\phi(i)$ is a random number between $[-a, a]$.

Onlooker Bees: The onlooker bee is unemployed. Upon receiving information (fitness values) from the employed bees, the onlooker bee uses this information to calculate the probability values, and the quality of the food source is determined by this value. The probability value p_m can be computed using the expression in the equation, with fit_m denoting the fitness value.

$$P_m = \frac{fit_m(\vec{x}_m)}{\sum_{m=1}^{SN} fit_m(\vec{x}_m)} \quad (4.18)$$

Scout Bees: The scout bees are also jobless bees. Once the employed bees find a better food source (solution), they become scout bees who randomly search for and select a new food source. Scout bees can be defined by the previous equation(4.16)

4.3.2 Methodology:

In our proposed watermarking approach (Figure 4.14), the ABC algorithm was employed to select the optimal scaling factor for embedding the watermark image and Electronic Patient Record (EPR) into the medical image. The evaluation of the fitness function was conducted utilizing metrics such as the (PSNR) and (NC), aiming to enhance both imperceptibility and robustness. To fortify the algorithm’s resilience, the watermarked image was subjected to various attacks in our testing protocol.

We initialized the ABC parameters (Table 4.5) based on a series of experiments. The selected parameters worked effectively with our algorithm, in terms of execution time and watermarking system quality.

For the objective function, we incorporated both the embedding and extraction processes to the cover image, and then calculated the PSNR to evaluate the imperceptibility of the watermarked image (I') compared to the cover image (I).

$$imperceptibility = (I, I') \quad (4.19)$$

However, as our objective was to improve the resilience of the technique, we subjected the watermarked image to various attacks, including noise addition, filtering, and RST attacks. Subsequently, we calculated the NC value of the extracted watermarks after each attack to assess the robustness of the method proposed.

$$robustness = \sum_{i=1} NC_i \quad (4.20)$$

To determine the best scaling factor, we computed the fitness function by combining imperceptibility and robustness. In our scheme, we propose to enhance the robustness value by multiplying it by 30, to ensure that its significance is not overlooked.

$$F_i = imperceptibility + (30 * robustness) \quad (4.21)$$

Table 4.5: ABC Parameters

Settings	Values
Colony size	50
Decision Variables (solution)	[0 20]
Fitness function	Imperceptibility, robustness
Objective function	- Embedding process - Attack addition - Extraction process

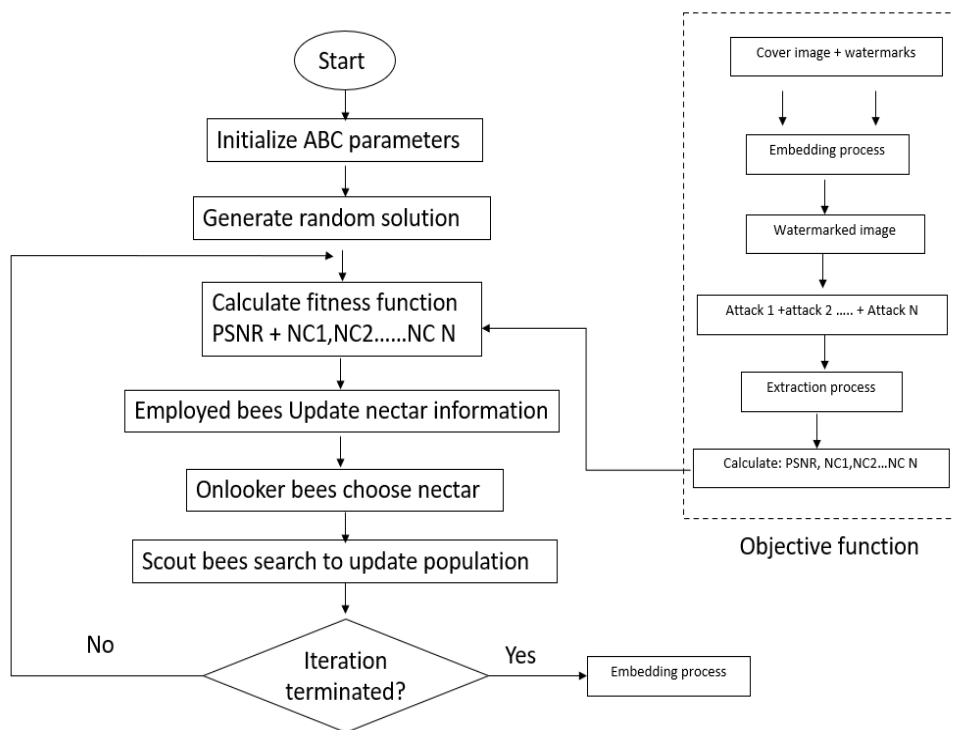


Figure 4.14: ABC-Based Watermarking Algorithm

4.3.3 Results and Discussion

To evaluate the effectiveness of our proposed method, we followed a comprehensive procedure similar to prior studies. Initially, we conducted an imperceptibility assessment using both PSNR and SSIM, comparing the watermarked image to the original. Following that, we tested the robustness of the extracted data, including the watermark image and the EPR, by subjecting the watermarked image to common attacks. The evaluation of the extracted data involved metrics such as NC, SSIM, and BER. Finally, we conducted a comparative analysis to evaluate the performance of our proposed method in comparison to other existing approaches.

Imperceptibility Results: The imperceptibility results are presented in Table 4.6, demonstrating the visual quality of watermarked images under various imaging methods. Notably, our proposed method exhibits robust imperceptibility, with values exceeding ($PSNR > 38dB$, $SSIM > 0.9$), indicating effective medical image integrity preservation.

Table 4.6: Imperceptibility Performance After Using ABC Optimization Algorithm

Medical Images	Normal images		Abnormal images	
	PSNR	SSIM	PSNR	SSIM
Ultrasound	48,1624	0,9903	44,1192	0,9816
X-ray	41,7035	0,9724	40,0273	0,9806
CT	40,2336	0,9821	39,5117	0,9691
MRI	40,4723	0,9748	39,1464	0,9854

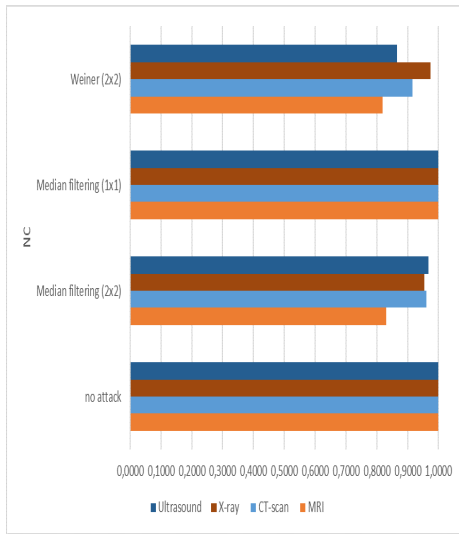
Robustness Results: Figures (4.15),(4.16), and (4.17) display the normalized correlation (NC) and structural similarity index (SSIM) results for the extracted watermarks under filtering, noise addition, and geometric attacks, histogram equalization and JPEG compression, respectively, for normal medical images.

Meanwhile, Figures (4.18),(4.19), and (4.20) display the normalized correlation (NC) and structural similarity index (SSIM) results for the extracted watermarks under filtering, noise addition, and geometric attacks, histogram equalization and JPEG compression, respectively, for normal medical images.

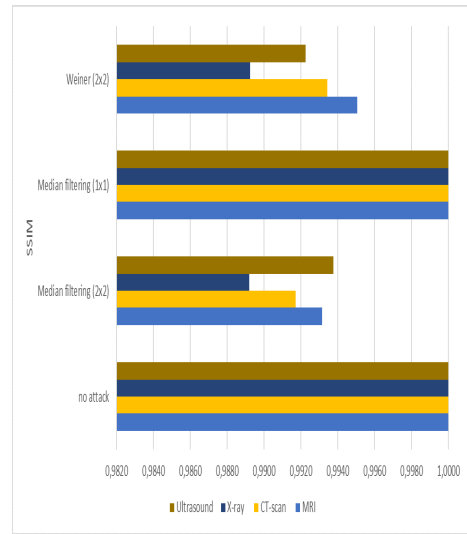
The findings showcase the commendable performance of the proposed method in both scenarios (without attacks and under attacks). Specifically, the NC values exceeded 0.8 for all tested images, indicating a strong correlation. Similarly, the SSIM values surpassed 0.9 reaffirming the effectiveness of the proposed method in preserving watermark integrity despite various attacks.

Figures 4.21 and 4.22 depict the BER for extracted tests from both normal and abnormal images. The results indicate that even under the most severe attacks, the proposed algorithm demonstrates robustness, with BER consistently below 0.1 in the majority of cases.

The performance of the proposed system against composite attacks is detailed in [84]. Specifically, the NC (Normalized Correlation) and SSIM (Structural Similarity Index) of the extracted image, as well as the BER (Bit Error Rate) of the extracted EPR, were evaluated after subjecting the watermarked image to various composite attacks. The results demonstrate that our approach performs well under these conditions.

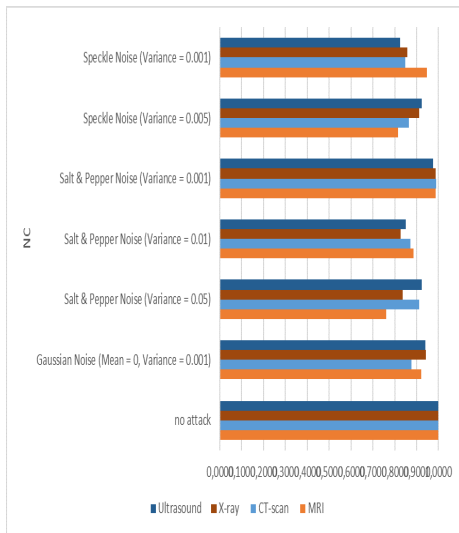


(a) NC results

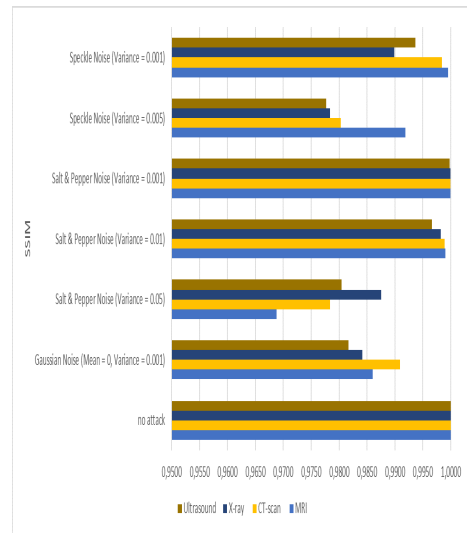


(b) SSIM results

Figure 4.15: NC and SSIM Performance for Normal Medical Images After Optimization: Filtering Attacks

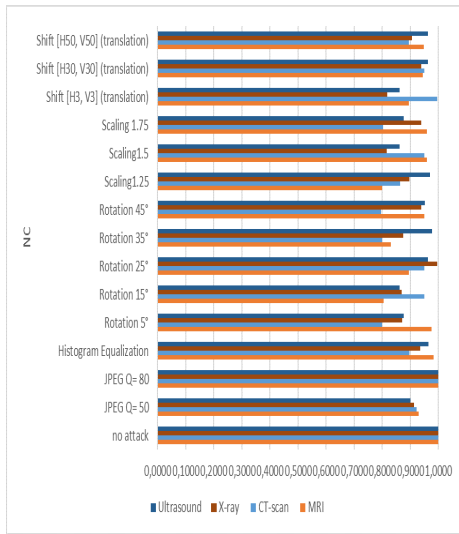


(a) NC results

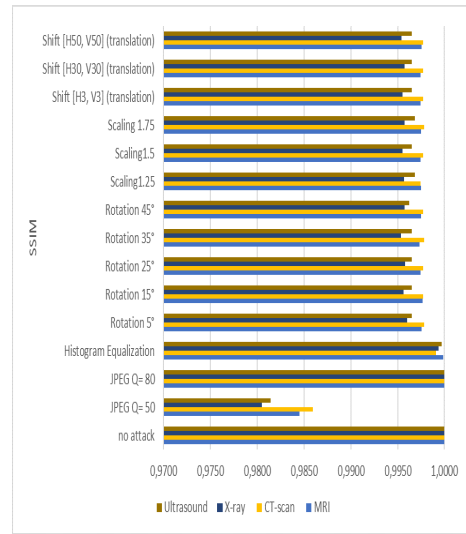


(b) SSIM results

Figure 4.16: NC and SSIM Performance for Normal Medical Images After Optimization: Noise Addition Attacks

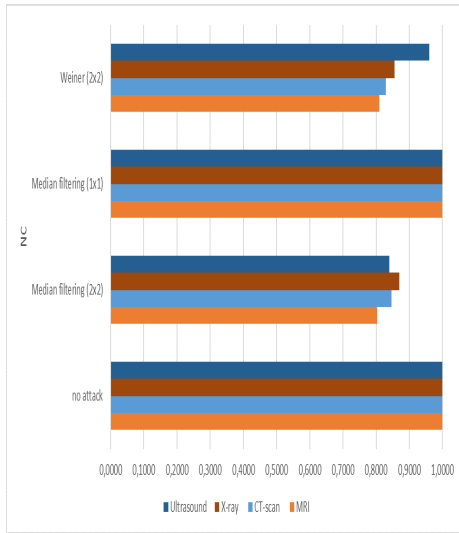


(a) NC results

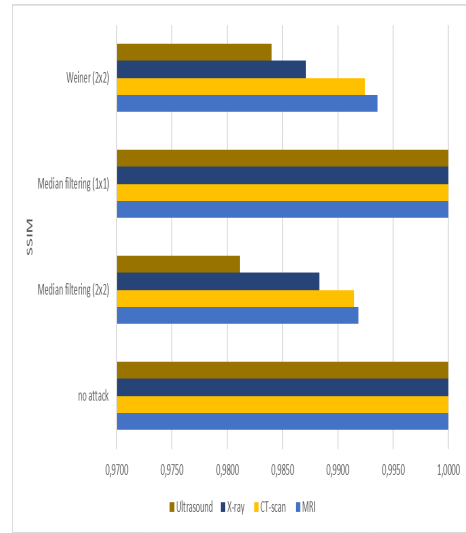


(b) SSIM results

Figure 4.17: NC and SSIM Performance for Normal Medical Images After Optimization: Geometric, Compression and Histogram Attacks

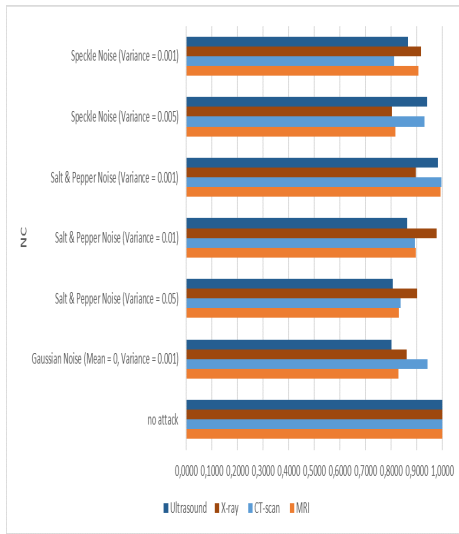


(a) NC results

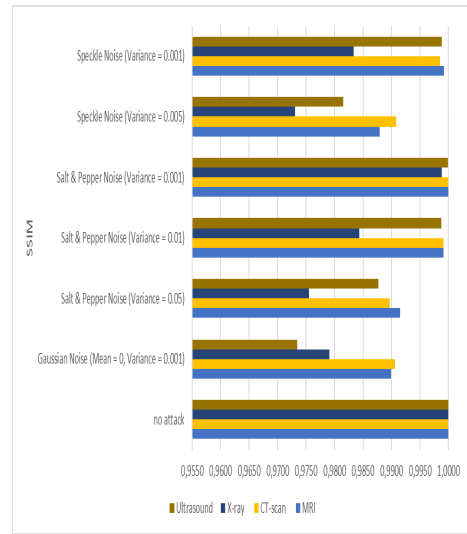


(b) SSIM results

Figure 4.18: NC and SSIM Performance for Abnormal Medical Images After Optimization: Filtering Attacks

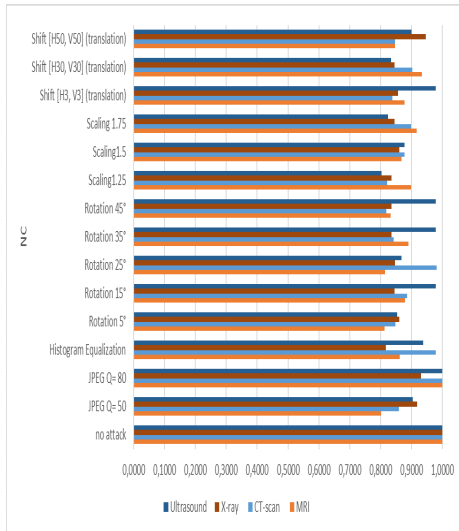


(a) NC results

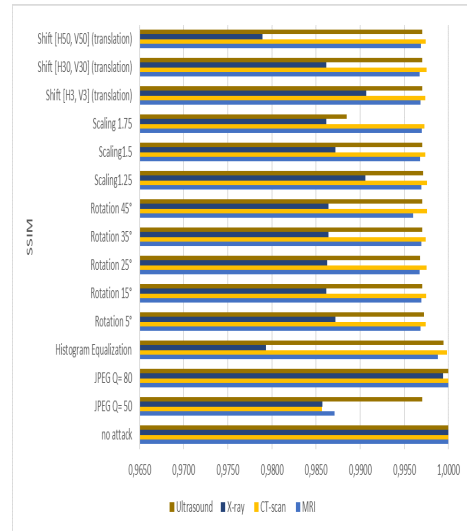


(b) SSIM results

Figure 4.19: NC and SSIM Performance for Abnormal Medical Images After Optimization: Noise Addition Attacks



(a) NC results



(b) SSIM results

Figure 4.20: NC and SSIM Performance for Abnormal Medical Images After Optimization: Geometric, Compression and Histogram Attacks

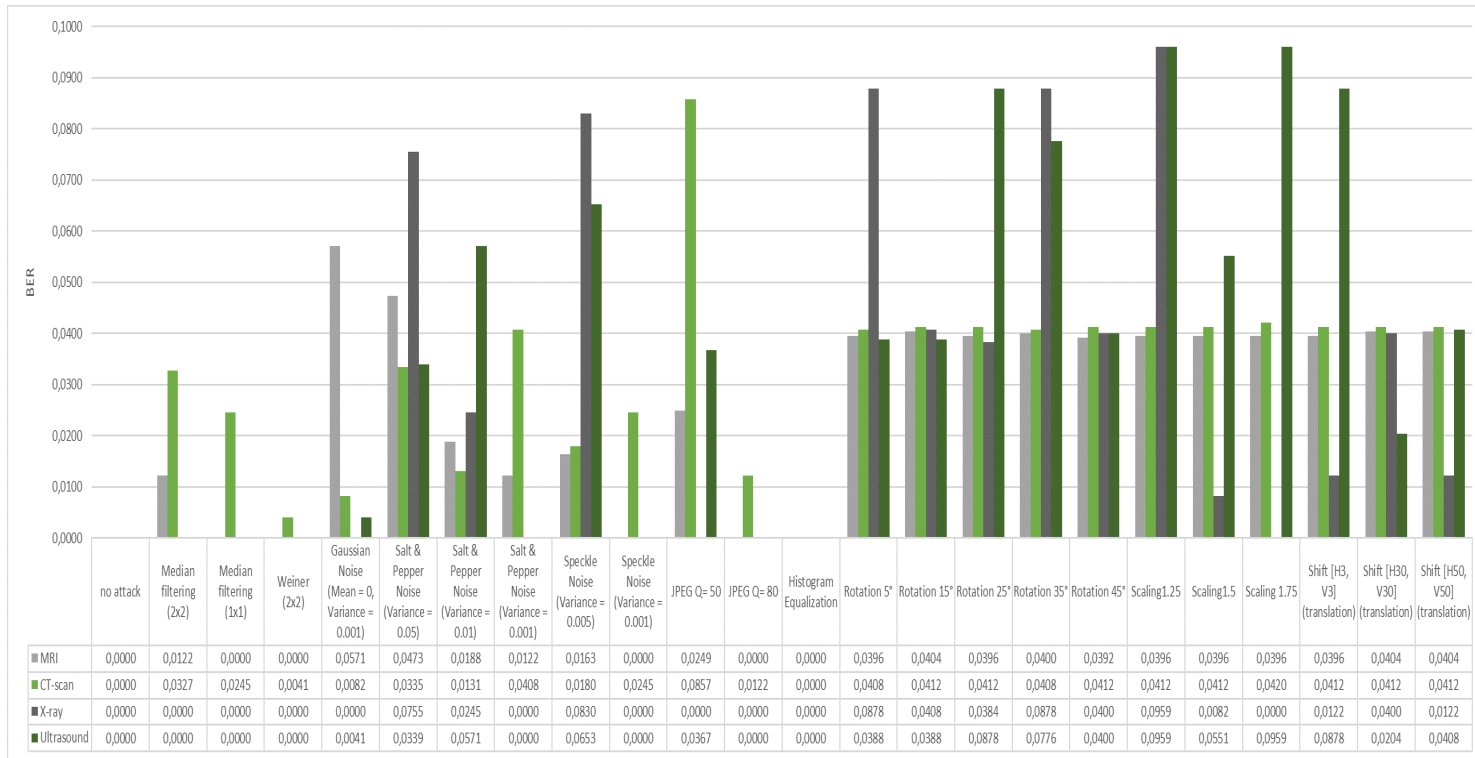


Figure 4.21: BER Performance for Normal Medical Images

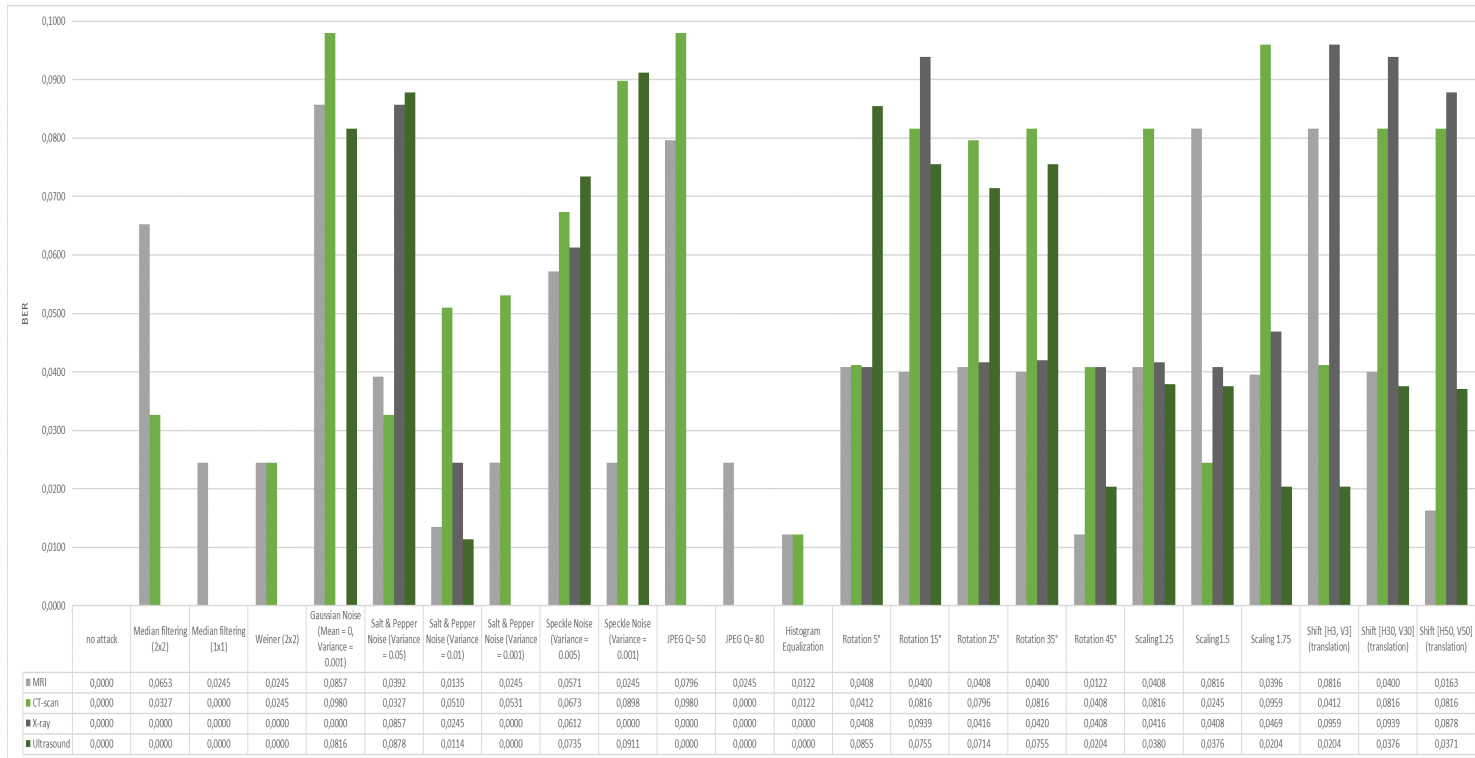


Figure 4.22: BER Performance for Abnormal Medical Images

Comparative analysis: To validate the efficacy of the proposed method, we performed a comparative analysis using the same medical data to compare its performance before and after optimization. Following that, we tested the method with both standard medical and non-medical images, followed by a thorough comparison of the results with existing techniques

Figure 4.23 depicts a comparative performance analysis, assessing the imperceptibility of the proposed method before and after the application of ABC optimization. The graph distinctly exhibits a performance improvement, showcasing the consistent enhancement achieved through the utilization of the ABC algorithm.

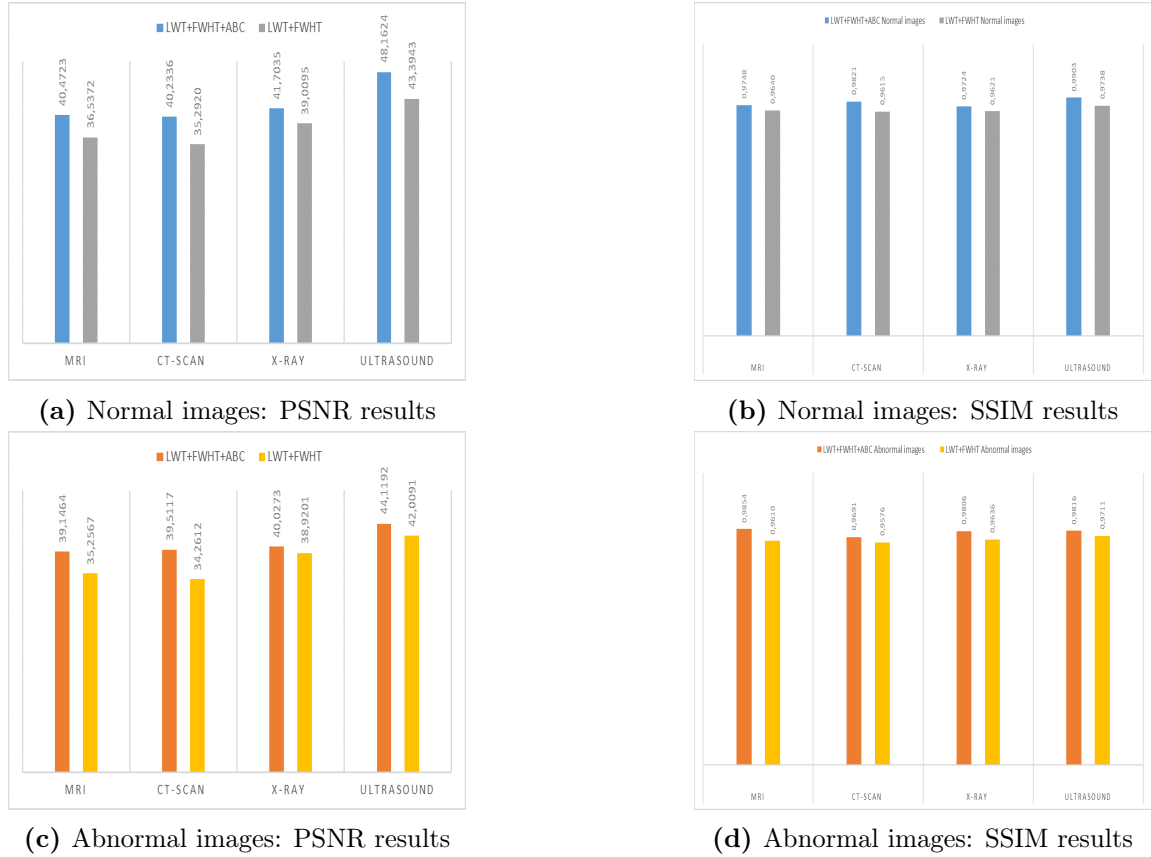


Figure 4.23: Comparative Performance Analysis: Evaluating the Imperceptibility of the Proposed Method Before and After ABC Optimization

Figure 4.24 illustrates the comparative performance analysis, evaluating the robustness of the proposed method before and after applying ABC optimization. The graph clearly demonstrates the enhancement in performance through the utilization

of the ABC algorithm, consistently yielding improved results.

In Table 4.7, we present a comparative analysis in which we evaluate the imperceptibility of the proposed method compared to existing schemes. The results demonstrate the proposed method’s superior performance, highlighting its increased imperceptibility compared to the existing schemes.

In Table 4.8, we present a thorough comparative analysis, assessing the robustness of the proposed method in comparison to existing schemes. The results underscore that the proposed method yields either high or comparable outcomes when compared to the other schemes.

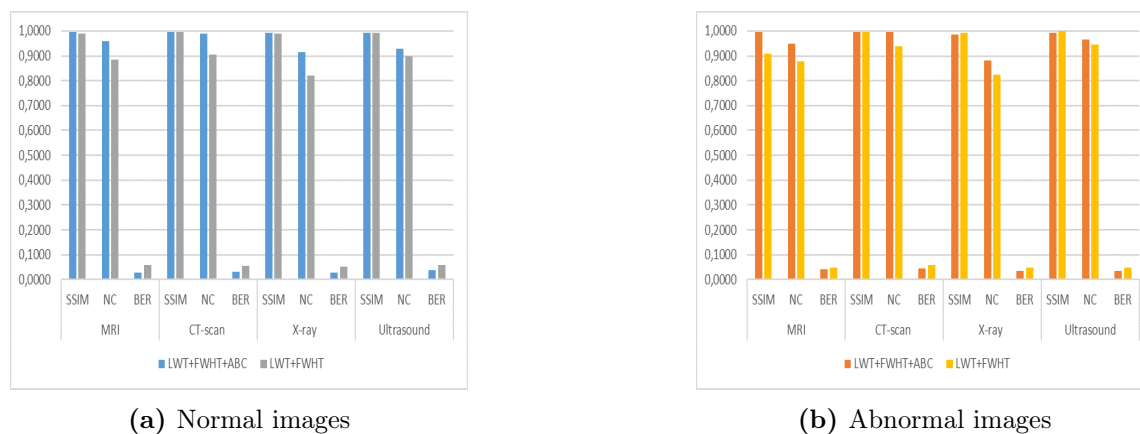


Figure 4.24: Comparative Performance Analysis: Evaluating the Robustness of the Proposed Method Before and After ABC Optimization

Table 4.7: Comparison of the Proposed Technique With Similar Schemes in Terms of PSNR Using Standard Images

Image	Proposed	Zhu et al[48]	El Houby et al[49]
Lena	43,0033	37.23	44,8905
Boats	40,9570	-	-
Barbara	42,5543	-	42,7081
Cameraman	45,6671	-	44,4936
Cell	44,9573	-	-
Moon	39,3589	-	-
MRI	44,1859	-	-
Peppers	44,13485	38,29	43,6299

Table 4.8: Robustness Comparison: Evaluating the Performance of the Proposed Technique Against Similar Schemes Using Standard Images

	Lena			Barbara			Cameraman			peppers		
	Proposed	[48]	[49]	Proposed	[48]	[49]	Proposed	[48]	[49]	Proposed	[48]	[49]
no attack	1,00	-	1,00	1,00	-	0,99	1,00	-	0,9996	1,00	-	1,00
Median filtering	1,00	0,99	0,62	1,00	-	0,62	1,00	-	0,63	1,00	0,99	0,58
Gaussian Noise	0,99	1,00	0,90	0,98	-	0,77	0,99	-	0,90	0,99	1,00	0,76
Histogram Rotation	0,99	-	1,00	0,99	-	0,99	0,96	-	0,97	0,96	-	0,99
Translation	0,91	-	-	0,82	-	-	0,76	-	-	0,97	-	-
Gaussian Noise	0,93	-	-	0,73	-	-	0,95	-	-	0,79	-	-
JPEG	0,93	-	0,90	0,87	-	0,77	0,82	-	0,90	0,96	-	0,90
Weiner	0,91	1,00	1,00	0,81	-	0,78	0,94	-	0,77	0,84	0,9991	1,00
Scaling	0,96	-	-	0,93	-	-	0,48	-	-	0,85	-	-
Average	0,82	1,00	0,87	0,73	-	0,72	0,76	-	0,84	0,98	0,9962	0,72
	0,94	1,00	0,90	0,89	-	0,81	0,87	-	0,83	0,93	1,00	0,85

4.4 Conclusion

In conclusion, this chapter has undertaken a comprehensive exploration of an image watermarking algorithm that integrates hybrid techniques by combining the Lifting Wavelet Transform (LWT) with the Fast Walsh-Hadamard Transform (FWHT). Subsequently, our investigation extended to optimization techniques, incorporating the ABC algorithm alongside the watermarking algorithm.

In our first proposal, we presented a hybrid algorithm that combines the advantages of LWT and FWHT. This fusion combines the effectiveness and simplicity of FWHT with the flexibility and efficiency inherent in LWT, making it ideal for image watermarking applications. The seamless integration of these techniques results in a substantial improvement in both imperceptibility and robustness performance, with outcomes exceeding ($PSNR > 35dB$, $SSIM > 0.9$) for the watermarked images, $NC > 0.6$ for the watermarked images, and $BER < 0.2$ for the extracted EPR.

In the second experiment, we aimed to enhance the performance of the proposed method by introducing a dynamically selected scaling factor based on image characteristics. The results unequivocally show a substantial improvement upon incorporating the ABC optimization algorithm, with notable advancements in both imperceptibility and robustness. The achieved outcomes surpass ($PSNR > 38dB$, $SSIM > 0.9$) for the watermarked images, $NC > 0.8$ for the watermarked images, and $BER < 0.1$ for the extracted EPR.

These findings underscore the significance of hybrid approaches and optimization algorithms in the context of medical image watermarking. Not only does our research contribute to the state of the art by demonstrating substantial improvements, but it also offers promising perspectives for practical applications in the medical field. By focusing on enhancing the security of medical data and preserving image integrity, our approach stands as a meaningful contribution to research in the field, with potential implications for improving healthcare and safeguarding sensitive information.

Moreover, our algorithm's performance was rigorously evaluated across four modalities (MRI, ultrasound, CT, and X-ray) for both normal and pathological images. The results revealed a remarkable improvement in imperceptibility and robustness across all modalities, underscoring the versatility and effectiveness of our hybrid approach. These performance metrics not only validate the relevance and added value of our integrated hybrid approach with an optimization algorithm in the realm of medical image watermarking but also highlight its adaptability across diverse medical imaging modalities.

Conclusion

The widespread use of new information and communication technologies in the healthcare sector improves both access to and availability of medical data. Even though this appears to be a significant benefit development for healthcare services, medical data security must be prioritized for tele-medical system developers.

The diverse nature of medical imaging data, on the other hand, presents a distinct challenge, necessitating a security system that is specifically tailored to the unique characteristics of each image.

We have concluded that the integrity and confidentiality of medical data are the primary requirements that must be protected. Any change in the data could endanger the patient's life by resulting in a misdiagnosis and incorrect treatment. Furthermore, because medical data is personal information, it should only be accessed by authorized individuals, namely healthcare professionals and the patient in question.

Our primary focus has been on meeting these requirements by creating a security system that protects the integrity of medical images while also maintaining the confidentiality of the patient's personal information.

Following a thorough review of the literature on medical imaging data security, we concluded that digital watermarking is an excellent solution for protecting the target data. As a result, we consider this technique to be a primary security measure:

- **Ensures Authenticity and Integrity:** Digital watermarking aids in the authentication of medical images by ensuring that they have not been tampered with or changed.
- **Protects Patient Privacy:** A medical image is a useful tool for embedding information about the patient or the medical facility. This improves data security and prevents unauthorized access.

- **Legal Evidence:** Watermarked images can be used as legal evidence in medical malpractice or dispute cases. The embedded data can be used to trace the images' origins and ownership, increasing their credibility in legal proceedings.

Using watermarking algorithms as a security solution, on the other hand, introduces new challenges, such as the perceptual quality of the medical image, the robustness of extracted watermarks, and the capacity of the cover image. Furthermore, the diverse properties of imaging modalities necessitate the development of an algorithm that is applicable to all types of images.

In this manuscript, we thoroughly addressed these considerations. We investigated watermarking algorithms in the transform domain, which is known for providing robustness and efficiency to watermarking systems. Our study led us to adopt the wavelet transform, which has grown in popularity in a variety of image-related fields.

Initially, we ran a series of experiments to find the best wavelet for medical images. In these experiments, we embedded a watermark image into the medical image. According to the findings, the 'Haar' wavelet outperforms others in terms of imperceptibility and robustness, with $PSNR > 40dB$, $NC > 0.99$.

In the second phase, we compared the traditional discrete wavelet transform (DWT) to the lifting wavelet transform (LWT), known as the second-generation wavelet. We embedded a watermark image as well as the EPR into the medical image in these experiments. Furthermore, we improved the proposed system's security by encrypting the image watermark with Arnold's Cat Map, ensuring the image's confidentiality. Furthermore, we encoded the EPR with a BCH Code, which serves as an error-correcting code. The findings confirmed that the LWT-based algorithm outperforms in both imperceptibility and robustness, making it an ideal and effective solution for securing sensitive medical data, $PSNR > 34dB$, $NC > 0.94$, $BER < 0.0119$.

Following that, we combined the LWT-based wavelet approach with another transform to improve the performance of the watermarking algorithm. We presented a hybrid algorithm that combines the advantages of LWT and FWHT. This hybrid combines the effectiveness and simplicity of FWHT with the flexibility and efficiency of LWT, making it appropriate for image watermarking applications. The seamless integration of these techniques yields a significant improvement in imperceptibility and robustness performance, with outcomes exceeding ($PSNR > 35dB$, $SSIM > 0.9$) for the watermarked images, $NC > 0.6$ for the watermarked images, and $BER < 0.2$ for the extracted EPR.

Lastly, we attempted to improve the proposed method's performance by implementing a dynamic scaling factor selection based on image characteristics. The re-

sults unequivocally show significant improvements following the incorporation of the ABC optimization algorithm, demonstrating improvements in both imperceptibility and robustness. The achieved outcomes surpass ($PSNR > 38dB$, $SSIM > 0.9$) for the watermarked images, $NC > 0.8$ for the watermarked images, and $BER < 0.1$ for the extracted EPR.

In conclusion, this thesis explores a critical topic that is always relevant. Given the rapid advancements in information and communication technologies, it is clear that data protection systems must be constantly developed and reinforced. Medical data, in particular, plays an important role in ensuring patient well-being and must be protected accordingly.

This work demonstrates how watermarking algorithms can improve the security of medical imaging data. The technique not only safeguards the security of medical images but also enables the covert transmission of personal information within the image.

Furthermore, we established the efficacy of the transform domain in watermarking systems, especially when employing hybrid techniques. Combining various techniques simultaneously, such as multiple embedding transforms and encryption approaches, enhances the overall effectiveness of the security system.

The promising findings encourage us to continue our research, with the goal of improving the proposed system by incorporating a strong encryption algorithm for medical images and incorporating artificial intelligence into the system to improve security.

Future Perspectives

The research presented in this thesis has the potential to expand in several directions. The following is a list of possible improvements, applications, and modifications.

- It would be interesting to use a stronger Wavelet Transform, such as the Packet Wavelet Transform, to improve the perceptual quality of the watermarked image. This method allows for greater flexibility when analyzing and decomposing signals.
- It would be interesting to test other wavelet types, such as Biorthogonal Wavelets CDF9/7, known for their favorable properties in image compression, including a nearly symmetric shape and a balance between time and frequency localization[85].
- Combining additional transforms or incorporating further embedding techniques such as SVD may improve the proposed algorithm's robustness.
- An additional suggestion is to use an optimization algorithm to automatically select the wavelet type for each image. This change would improve the algorithm's compatibility with the various features of medical images.
- Also, we may employ AI algorithms to improve the efficiency of watermarking algorithms. This technique can be used to strengthen the algorithm against a variety of attacks, particularly geometric attacks, which are regarded as one of the most difficult challenges for watermarking algorithms.
- On the other hand, our plan involves implementing an effective cryptosystem to encrypt the medical image, therefore improving patient confidentiality and protecting it from any potential unauthorized access or compromise.
- Furthermore, the incorporation of additional security measures, such as robust ECC and encryption algorithms, may improve the security of the proposed system.

ANNEXES

A Medical Images Data Set

In this study, we utilized a collection of (512x512) grayscale medical data images from various modalities, encompassing Magnetic Resonance Imaging (MRI), ultrasound, CT scan, and X-ray images. From each dataset, we selected two types of images. The first type comprises normal images without disease symptoms, while the second type includes abnormal images exhibiting disease symptoms. This selection was made to encompass a diverse range of medical images. Subsequent sections provide a detailed description of the data employed in this manuscript.

A.1 Magnetic Resonance Imaging

We used an MRI data set designed specifically for brain tumor classification[2]. This data set consists of four folders: `no_tumor`, `gglioma_tumor`, `meningioma_tumor`, and `pituitary_tumor`. We chose images from each folder. We selected 100 images from the `no_tumor` folder, which included normal images. Similarly, from the other three folders, each representing a different type of brain tumor, we chose 100 images displaying brain tumor symptoms.

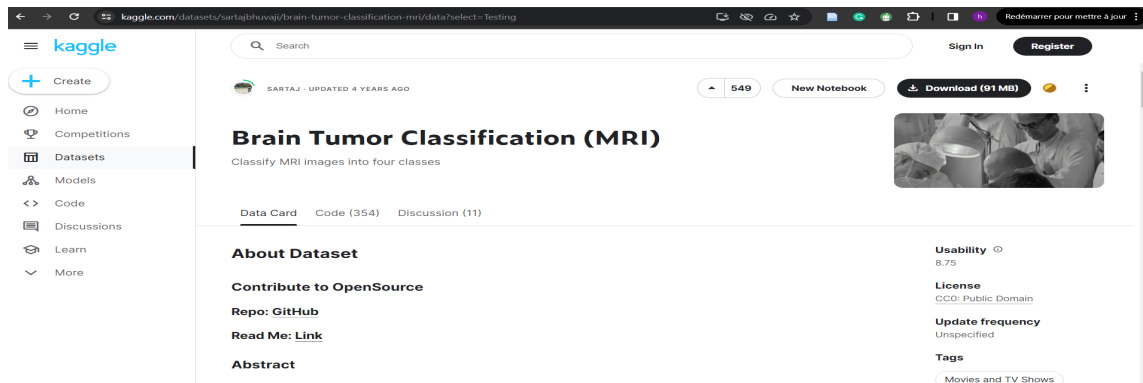


Figure 4.25: Source of MRI Images for Watermarking Algorithm

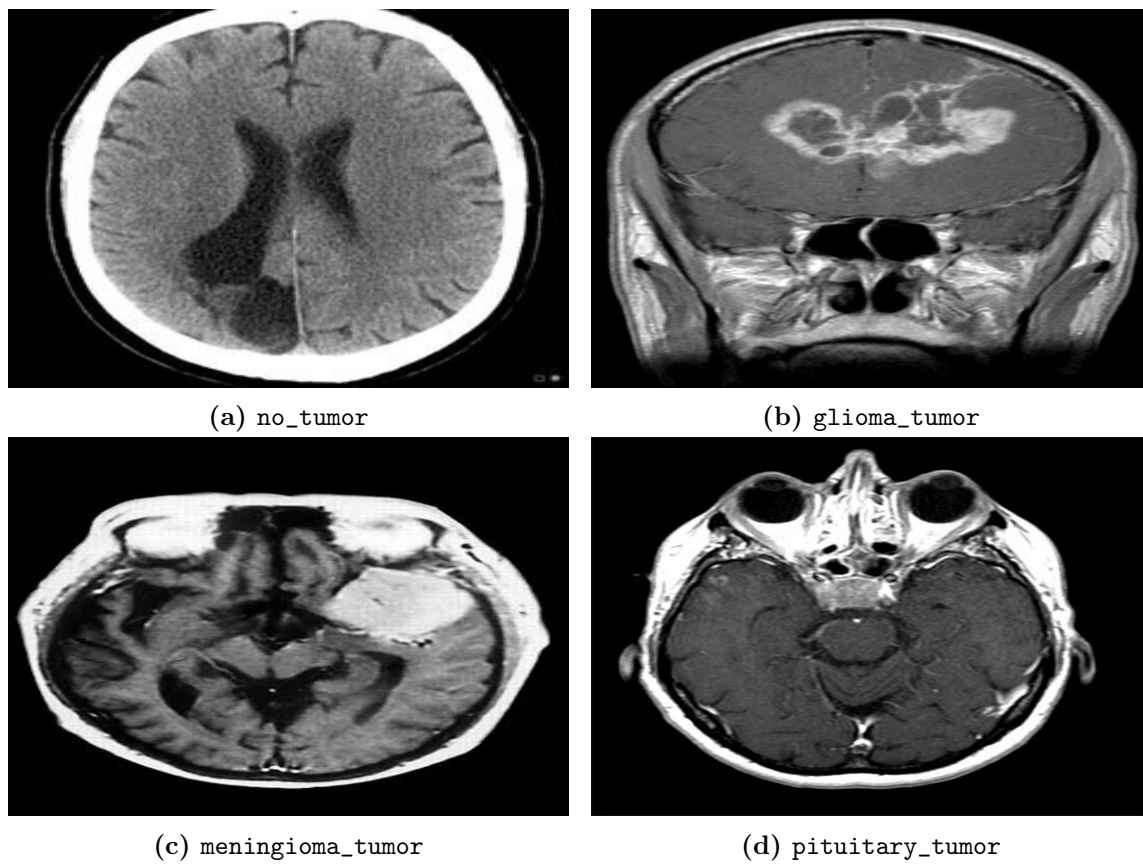
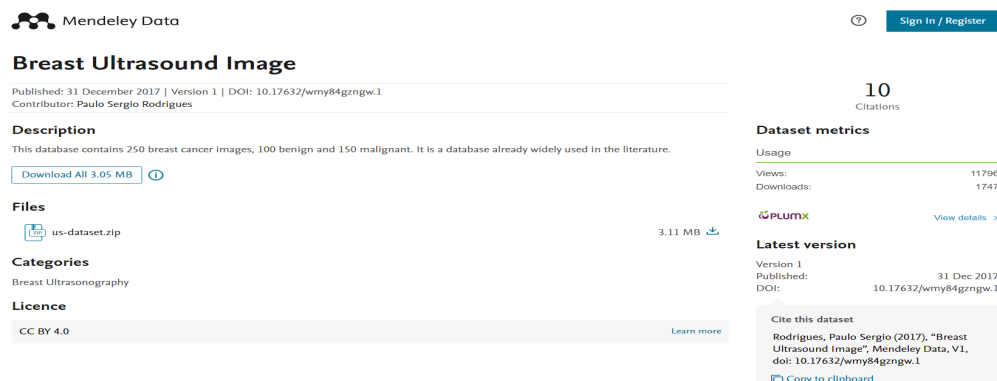


Figure 4.26: A Sample of MRI Images Selected from the Four Folders

A.2 Ultrasound

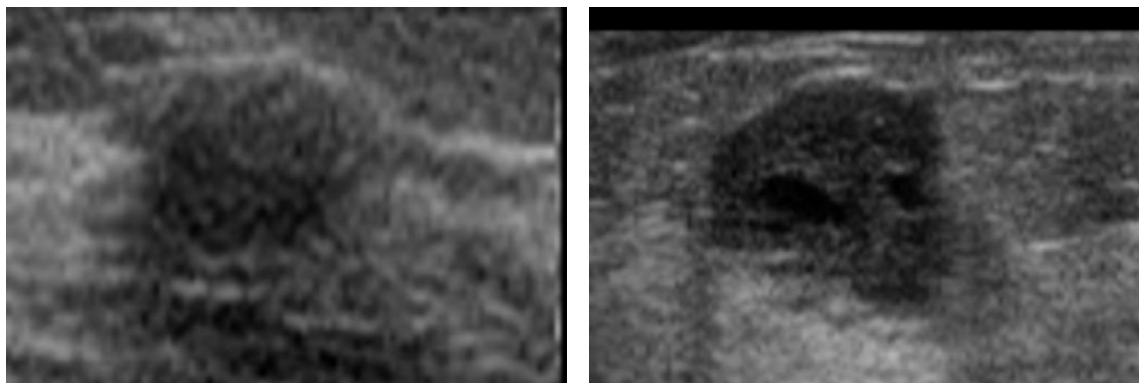
For the Ultrasound dataset, we chose Breast Ultrasound Images available on the Mendeley Data website[5]. This database comprises 250 breast cancer images, with 100 classified as benign and 150 as malignant. Widely utilized in the literature, particularly for breast cancer classification, we selected 100 images from each class for our study.



The screenshot shows the Mendeley Data page for the 'Breast Ultrasound Image' dataset. The page includes the following information:

- Mendeley Data** logo and navigation links (Sign In / Register).
- Breast Ultrasound Image** title.
- Published: 31 December 2017 | Version 1 | DOI: 10.17632/wmy84gzngw.1
- Contributor: Paulo Sergio Rodrigues
- Description:** This database contains 250 breast cancer images, 100 benign and 150 malignant. It is a database already widely used in the literature. A 'Download All 3.05 MB' button is visible.
- Files:** A file named 'us-dataset.zip' is listed with a size of 3.11 MB.
- Categories:** Breast Ultrasonography.
- Licence:** CC BY 4.0.
- Dataset metrics:** 10 Citations, 11796 Views, and 1747 Downloads.
- Latest version:** Version 1, Published: 31 Dec 2017, DOI: 10.17632/wmy84gzngw.1.
- Cite this dataset:** Rodrigues, Paulo Sergio (2017), "Breast Ultrasound Image", Mendeley Data, V1, doi: 10.17632/wmy84gzngw.1. A 'Copy to clipboard' button is present.

Figure 4.27: Source of Ultrasound Images for Watermarking Algorithm



(a) Benign

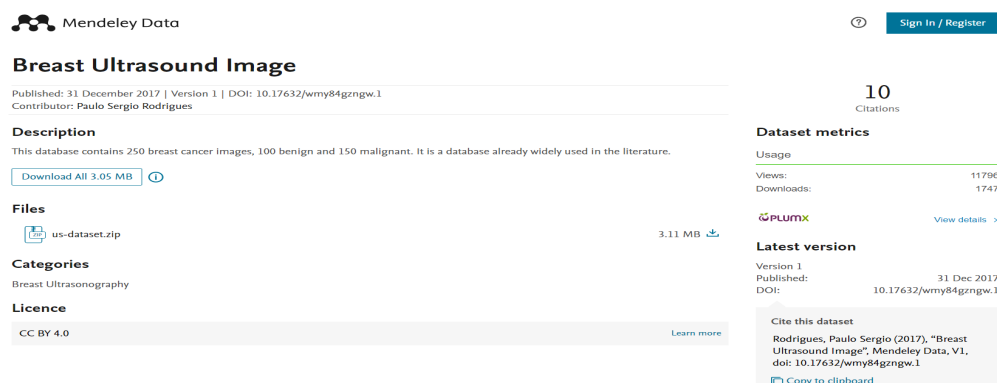
(b) Malignant

Figure 4.28: A Sample of Ultrasound Images

A.3 X-ray

The X-ray images were obtained from a dataset comprising 5,856 validated Chest X-ray images, which were divided into training and testing sets with independent patients. The images are categorized as NORMAL, BACTERIA, and VIRUS.

According to the source, these images (anterior-posterior) were selected from retrospective cohorts of pediatric patients aged one to five years old at Guangzhou Women and Children's Medical Center, Guangzhou[1]. For our study, we specifically chose 100 NORMAL images and 100 images depicting BACTERIA and VIRUS conditions.



The screenshot shows the Mendeley Data page for the dataset 'Breast Ultrasound Image'. The page includes the following information:

- Mendeley Data** logo and navigation links (Sign In / Register).
- Breast Ultrasound Image** title.
- Published: 31 December 2017 | Version 1 | DOI: 10.17632/wmy84gzngw.1
- Contributor: Paulo Sergio Rodrigues
- Description:** This database contains 250 breast cancer Images, 100 benign and 150 malignant. It is a database already widely used in the literature.
- Download All 3.05 MB** button.
- Files:** us-dataset.zip (3.11 MB).
- Categories:** Breast Ultrasonography.
- Licence:** CC BY 4.0.
- Dataset metrics:** 10 Citations, 11796 Views, 1747 Downloads.
- Latest version:** Version 1, Published: 31 Dec 2017, DOI: 10.17632/wmy84gzngw.1.
- Cite this dataset:** Rodrigues, Paulo Sergio (2017), "Breast Ultrasound Image", Mendeley Data, V1, doi: 10.17632/wmy84gzngw.1.
- Copy to clipboard** button.

Figure 4.29: Source of X-ray Images for Watermarking Algorithm

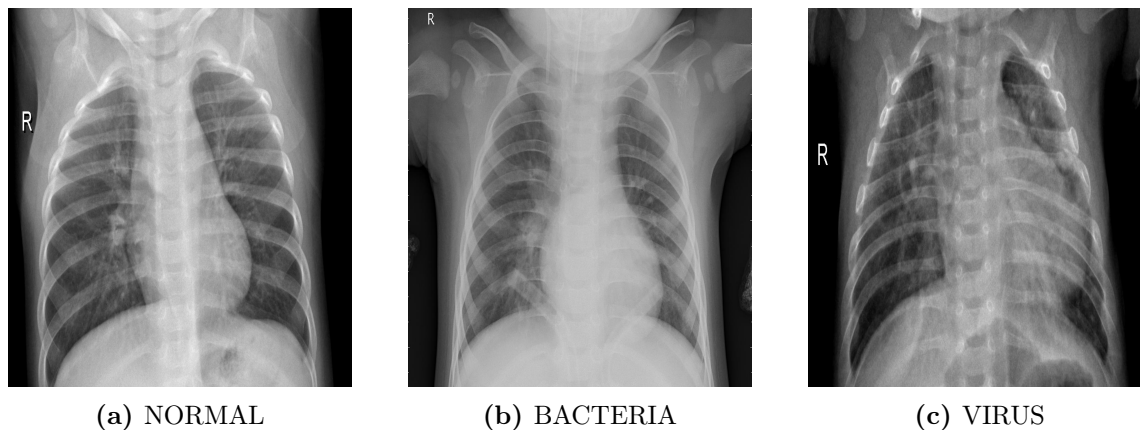
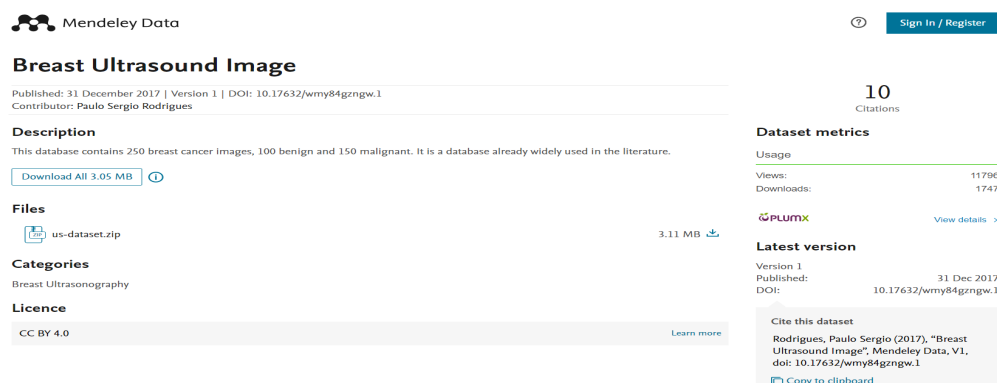


Figure 4.30: A Sample of X-ray Images

A.4 CT-scan

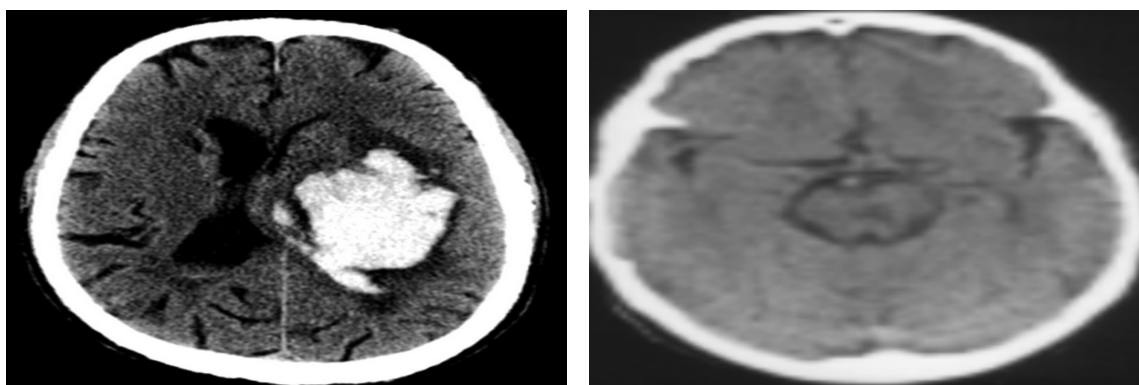
The CT-scan images were sourced from a dataset that includes 100 normal head CT slices and an additional 100 slices depicting hemorrhage, without further categorization of the types of hemorrhage[3]. We utilized the entire dataset to assess and test the proposed algorithm.



The screenshot shows the Mendeley Data page for the dataset "Breast Ultrasound Image". The page includes the following information:

- Mendeley Data** logo and "Sign In / Register" button.
- Breast Ultrasound Image** title.
- Published: 31 December 2017 | Version 1 | DOI: 10.17632/wmy84gzngw.1
- Contributor: Paulo Sergio Rodrigues
- Description:** This database contains 250 breast cancer images, 100 benign and 150 malignant. It is a database already widely used in the literature.
- Download All 3.05 MB** button.
- Files:** us-dataset.zip (3.11 MB)
- Categories:** Breast Ultrasonography
- Licence:** CC BY 4.0
- Dataset metrics:** 10 Citations, 11796 Views, 1747 Downloads.
- PLUMX** logo and "View details" link.
- Latest version:** Version 1, Published: 31 Dec 2017, DOI: 10.17632/wmy84gzngw.1
- Cite this dataset:** Rodrigues, Paulo Sergio (2017), "Breast Ultrasound Image", Mendeley Data, V1, doi: 10.17632/wmy84gzngw.1
- Copy to clipboard** button.

Figure 4.31: Source of CT Scan Images for Watermarking Algorithm



(a) Normal

(b) Hemorrhage

Figure 4.32: A Sample of CT scan Images

Bibliography

- [1] Daniel Kermany, Kang Zhang, Michael Goldbaum, et al. Labeled optical coherence tomography (oct) and chest x-ray images for classification. *Mendeley data*, 2(2), 2018. doi:10.17632/rsbjbr9sj.2.
- [2] Prajakta Bhumkar Sartaj Bhuvaji, Ankita Kadam. Brain tumor classification (mri), 2020. <https://www.kaggle.com/dsv/1183165>. doi:10.34740/KAGGLE/DSV/1183165.
- [3] kaggle.com. Head ct - hemorrhage, (accessed: 2021-02-10). <https://kaggle.com/felipekitamura/head-ct-hemorrhage>.
- [4] The National Library of Medicine. Medpix®[®], 2023. Accessed: January 1, 2023. URL: <https://medpix.nlm.nih.gov/search?allen=true&allt=true&alli=true&query=synpic21672>.
- [5] Paulo Sergio Rodrigues. Breast ultrasound image. *Mendeley Data*, 1, 2017. doi:0.17632/wmy84gzngw.1.
- [6] NM Hjelm. Benefits and drawbacks of telemedicine. *Introduction to Telemedicine, second edition*, pages 134–149, 2017.
- [7] Fahad Shamsad, Salman Khan, Syed Waqas Zamir, Muhammad Haris Khan, Munawar Hayat, Fahad Shahbaz Khan, and Huazhu Fu. Transformers in medical imaging: A survey. *arXiv preprint arXiv:2201.09873*, 2022.
- [8] Elisa Bertino. Data security and privacy in the iot. In *EDBT*, volume 2016, pages 1–3, 2016.

- [9] Chandra Thapa and Seyit Camtepe. Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, 129:104130, 2021.
- [10] Tal Geva. Magnetic resonance imaging: historical perspective. *Journal of cardiovascular magnetic resonance*, 8(4):573–580, 2006.
- [11] Paul Suetens. *Fundamentals of medical imaging*. Cambridge university press, 2017.
- [12] Mohammad Zarour, Mamdouh Alenezi, Md Tarique Jamal Ansari, Abhishek Kumar Pandey, Masood Ahmad, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, 8(3):66–77, 2021.
- [13] Canadian Medical Association et al. Principles for the protection of patient privacy. *Ottawa: Canadian Medical Association*, 2017.
- [14] Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Khaloufi, and Mostafa Saadi. Big data security and privacy in healthcare: A review. *Procedia Computer Science*, 113:73–80, 2017.
- [15] Joint Task Force. Security and privacy controls for information systems and organizations. Technical report, National Institute of Standards and Technology, 2017.
- [16] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. *Digital watermarking and steganography*. Morgan kaufmann, 2007.
- [17] Anatol Z Tirkel, GA Rankin, RM Van Schyndel, WJ Ho, NRA Mee, and Charles F Osborne. Electronic watermark. *Digital Image Computing, Technology and Applications (DICTA '93)*, pages 666–673, 1993.
- [18] Lalit Kumar Saini and Vishal Shrivastava. A survey of digital watermarking techniques and its applications. *arXiv preprint arXiv:1407.4735*, 2014.
- [19] A Al Embaby, Mohamed A Wahby Shalaby, and Khaled Mostafa Elsayed. Digital watermarking properties, classification and techniques. *International Journal of Engineering and Advanced Technology*, 9(3):2742–2750, 2020.
- [20] Om Prakash Singh, Amit Kumar Singh, Gautam Srivastava, and Neeraj Kumar. Image watermarking using soft computing techniques: A comprehensive survey. *Multimedia Tools and Applications*, 80(20):30367–30398, 2021.

- [21] Thottempudi Pardhu and Bhaskara Rao Perli. Digital image watermarking in frequency domain. In *2016 International Conference on Communication and Signal Processing (ICCSP)*, pages 0208–0211. IEEE, 2016.
- [22] Neha Bansal, Vinay Kumar Deolia, Atul Bansal, and Pooja Pathak. Digital image watermarking using least significant bit technique in different bit positions. In *2014 International Conference on Computational Intelligence and Communication Networks*, pages 813–818. IEEE, 2014.
- [23] Manasha Saqib and Sameena Naaz. Spatial and frequency domain digital image watermarking techniques for copyright protection. *Int. J. Eng. Sci. Technol. (IJEST)*, 9(6):691–699, 2017.
- [24] Zhe-Ming Lu and Shi-Ze Guo. *Lossless information hiding in images*. Syngress, 2016.
- [25] Swati Sherekar, V Thakare, Sanjeev Jain, D Ashwini, P Tijare, M Deshpande, et al. Attacks and countermeasures on digital watermarks: classification, implications, benchmarks. *International Journal Of Computer Science And Applications*, 4(2):32, 2011.
- [26] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A Pindar, Nur Shafinaz Ahmad Shakir, and Mustafa Mat Deris. A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, 8(11), 2017.
- [27] Vaishnavi S Shetty, R Anusha, Dileep Kumar MJ, and Prajwal Hegde. A survey on performance analysis of block cipher algorithms. In *2020 International Conference on Inventive Computation Technologies (ICICT)*, pages 167–174. IEEE, 2020.
- [28] IMARC Group. Digital health market: Global industry trends, share, size, growth, opportunity and forecast 2022-2027, 2021. Last accessed 09 February 2023. URL: <https://www.imarcgroup.com/digital-health-market>.
- [29] LII Legal Information Institute. doctor-patient privilege. Last accessed 09 February 2023. URL: https://www.law.cornell.edu/wex/doctor-patient_privilege.
- [30] Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan. *Medical image watermarking*. Springer, 2017.

- [31] Amit Mehto and Neelesh Mehra. Adaptive lossless medical image watermarking algorithm based on dct & dwt. *Procedia Computer Science*, 78:88–94, 2016.
- [32] Priya Selvam, Santhi Balachandran, Swaminathan Pitchai Iyer, and Rajamohan Jayabal. Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. *Optik*, 145:655–671, 2017.
- [33] Steven Dewitte and Jan Cornelis. Lossless integer wavelet transform. *IEEE signal processing letters*, 4(6):158–160, 1997.
- [34] Hoang M Le and Maurice Aburdene. The discrete gould transform and its applications. In *Image Processing: Algorithms and Systems, Neural Networks, and Machine Learning*, volume 6064, pages 156–167. SPIE, 2006.
- [35] Nanmaran Rajendiran, Thirugnanam Gurunathan, and Mangaiyarkarasi Palanivel. Wavelet packet transform-based medical image multiple watermarking with independent component analysis extraction. *International Journal of Medical Engineering and Informatics*, 12(4):322–335, 2020.
- [36] Tanya Koochpayeh Araghi and Azizah Abd Manaf. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on dwt and 2-d svd. *Future Generation Computer Systems*, 101:1223–1246, 2019.
- [37] Mostafa M Abdel-Aziz, Khalid M Hosny, Nabil A Lashin, and Mostafa M Fouda. Blind watermarking of color medical images using hadamard transform and fractional-order moments. *Sensors*, 21(23):7845, 2021.
- [38] Ashima Anand and Amit Kumar Singh. An improved dwt-svd domain watermarking for medical information security. *Computer Communications*, 152:72–80, 2020.
- [39] Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan. Digital image watermarking: concepts and applications. *Medical Image Watermarking: Techniques and Applications*, pages 1–12, 2017.
- [40] Amit Kumar Singh. Robust and distortion control dual watermarking in lwt domain using dct and error correction code for color medical image. *Multimedia Tools and Applications*, 78:30523–30533, 2019.

- [41] G Pradeep Kumar, MD Saranya, KS Tamilselvan, Mazher Iqbal JL, S Kavitha, et al. Investigation on watermarking algorithm for secure transaction of electronic patient record by hybrid transform. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pages 379–383. IEEE, 2020.
- [42] Ashima Anand and Amit Kumar Singh. Joint watermarking-encryption-ecc for patient record security in wavelet domain. *IEEE MultiMedia*, 27(3):66–75, 2020.
- [43] Y Gangadhar, VS Giridhar Akula, and P Chenna Reddy. An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. *Biomedical Signal Processing and Control*, 43:31–40, 2018.
- [44] K Balasamy and S Ramakrishnan. An intelligent reversible watermarking system for authenticating medical images using wavelet and pso. *Cluster Computing*, 22:4431–4442, 2019.
- [45] Irshad Ahmad Ansari, Millie Pant, and Chang Wook Ahn. Artificial bee colony optimized robust-reversible image watermarking. *Multimedia Tools and Applications*, 76:18001–18025, 2017.
- [46] K Swaraja, K Meenakshi, and Padmavathi Kora. An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. *Biomedical Signal Processing and Control*, 55:101665, 2020.
- [47] Einolah Hatami, Hamidreza Rashidy Kanan, Kamran Layeghi, and Ali Harounabadi. An optimized robust and invisible digital image watermarking scheme in contourlet domain for protecting rightful ownership. *Multimedia Tools and Applications*, 82(2):2021–2051, 2023.
- [48] Ting Zhu, Wen Qu, and Wenliang Cao. An optimized image watermarking algorithm based on svd and iwt. *The Journal of Supercomputing*, 78(1):222–237, 2022.
- [49] Enas MF El Houbay and Nisreen IR Yassin. Wavelet-hadamard based blind image watermarking using genetic algorithm and decision tree. *Multimedia Tools and Applications*, 79(37):28453–28474, 2020.
- [50] Xiangyu Ou et al. Recent development in x-ray imaging technology: Future and challenges. *Research*, 2012, 2021.

- [51] Jean Morlet, Georges Arens, Eliane Fourceau, and Dominique Glard. Wave propagation and sampling theory—part i: Complex signal and scattering in multilayered media. *Geophysics*, 47(2):203–221, 1982.
- [52] Stephane G Mallat. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE transactions on pattern analysis and machine intelligence*, 11(7):674–693, 1989.
- [53] Mehdi Hosseinzadeh. Robust control applications in biomedical engineering: Control of depth of hypnosis. In *Control Applications for Biomedical Engineering Systems*, pages 89–125. Elsevier, 2020.
- [54] Chu Yu and Sao-Jie Chen. Vlsi implementation of 2-d discrete wavelet transform for real-time video signal processing. *IEEE transactions on consumer electronics*, 43(4):1270–1279, 1997.
- [55] Wim Sweldens. The lifting scheme: A custom-design construction of biorthogonal wavelets. *Applied and computational harmonic analysis*, 3(2):186–200, 1996.
- [56] Pooneh Bagheri Zadeh, Akbar Sheikh Akbari, Tom Buggy, and John Soraghan. Multiresolution hvs and statistically based image coding scheme. *Multimedia Tools and Applications*, 49(2):347–370, 2010.
- [57] Cristina Stolojescu, Ion Railean, Sorin Moga, and Alexandru Isar. Comparison of wavelet families with application to wimax traffic forecasting. In *2010 12th international conference on optimization of electrical and electronic equipment*, pages 932–937. IEEE, 2010.
- [58] G Lindfield and J Penny. Chapter 8-analyzing data using discrete transforms. *Numerical Methods (Fourth Edition)*, G. Lindfield and J. Penny, Eds, pages 383–431, 2019.
- [59] Hemalatha Kanagaraj and V Muneeswaran. Image compression using haar discrete wavelet transform. In *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, pages 271–274. IEEE, 2020.
- [60] Imran Sharif and Sangeeta Khare. Comparative analysis of haar and daubechies wavelet for hyper spectral image classification. *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, 40(8):937, 2014.

- [61] Hay Mar Soe Naing, Risanuri Hidayat, Rudy Hartanto, and Yoshikazu Miyanaga. Discrete wavelet denoising into mfcc for noise suppressive in automatic speech recognition system. *International Journal of Intelligent Engineering and Systems*, 13(2):74–82, 2020.
- [62] Ali Naji Shaker. Comparison between orthogonal and bi-orthogonal wavelets. *Journal of Southwest Jiaotong University*, 55(2), 2020.
- [63] Asaad F Qasim, Farid Meziane, and Rob Aspin. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, 27:45–60, 2018.
- [64] Amit Kumar Singh, Mayank Dave, and Anand Mohan. Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools and Applications*, 75(14):8381–8401, 2016.
- [65] K Prabha and I Shatheesh Sam. A novel blind color image watermarking based on walsh hadamard transform. *Multimedia Tools and Applications*, 79(9):6845–6869, 2020.
- [66] Sajjad Bagheri Baba Ahmadi, Gongxuan Zhang, and Songjie Wei. Robust and hybrid svd-based image watermarking schemes: A survey. *Multimedia tools and applications*, 79:1075–1117, 2020.
- [67] Syed Ali Khayam. The discrete cosine transform (dct): theory and application. *Michigan State University*, 114(1):31, 2003.
- [68] Ahmed Drissi. The security of cryptosystems based on error-correcting codes. In *Cryptography-Recent Advances and Future Developments*. IntechOpen, 2021.
- [69] James R Wootton and Daniel Loss. Repetition code of 15 qubits. *Physical Review A*, 97(5):052313, 2018.
- [70] Predrag Ivaniš, Dušan Drajić, Predrag Ivaniš, and Dušan Drajić. Convolutional codes and viterbi algorithm. *Information Theory and Coding-Solved Problems*, pages 327–383, 2017.
- [71] P Mozhiarasi and C Gayathri. Analysis on (15, 7) binary bch encoder and decoder for 7-bit ascii characters. *International Journal of Advanced Research in Engineering and Applied Sciences*, 4(4):34–42, 2015.

- [72] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of atmospheric sciences*, 20(2):130–141, 1963.
- [73] Rasika B Naik and Udayprakash Singh. A review on applications of chaotic maps in pseudo-random number generators and encryption. *Annals of Data Science*, pages 1–26, 2022.
- [74] Fei Chen, Kwok-wo Wong, Xiaofeng Liao, and Tao Xiang. Period distribution of generalized discrete arnold cat map. *Theoretical Computer Science*, 552:13–25, 2014.
- [75] Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. Speeded-up robust features (surf). *Computer vision and image understanding*, 110(3):346–359, 2008.
- [76] He Gao and Qing Chen. A robust and secure image watermarking scheme using surf and improved artificial bee colony algorithm in dwt domain. *Optik*, 242:166954, 2021.
- [77] Ali Pourhadi and Homayoun Mahdavi-Nasab. A robust digital image watermarking scheme based on bat algorithm optimization and surf detector in swt domain. *Multimedia Tools and Applications*, 79(29):21653–21677, 2020.
- [78] Tolga Gökozan. Template based image watermarking in the fractional fourier domain. Master’s thesis, Middle East Technical University, 2005.
- [79] Preeti Garg and R Rama Kishore. Literature review of various nature-inspired optimization algorithms used for digital watermarking. *Computational Methods and Data Engineering*, pages 39–52, 2021.
- [80] Sourabh Katoch, Sumit Singh Chauhan, and Vijay Kumar. A review on genetic algorithm: past, present, and future. *Multimedia Tools and Applications*, 80(5):8091–8126, 2021.
- [81] Tareq M Shami, Ayman A El-Saleh, Mohammed Alswaitti, Qasem Al-Tashi, Mhd Amen Summakieh, and Seyedali Mirjalili. Particle swarm optimization: A comprehensive survey. *IEEE Access*, 2022.
- [82] Bahriye Akay and Dervis Karaboga. A survey on the applications of artificial bee colony in signal, image, and video processing. *Signal, Image and Video Processing*, 9(4):967–990, 2015.

- [83] Dervis Karaboga et al. An idea based on honey bee swarm for numerical optimization. Technical report, Technical report-tr06, Erciyes university, engineering faculty, computer . . . , 2005.
- [84] Hadjer Abdi and Ismail Boukli Hacene. A multiple and robust image watermarking approach based on lwt and fwht for medical data security. *Journal of Mechanics in Medicine and Biology*, 23(03):2350011, 2023.
- [85] Boukli Hacene Ismail. *Compression d'images médicales par ondelettes de seconde génération*. PhD thesis, Thèse Pour obtenir le titre de Docteur En Electronique biomédicale . . . , 2014.

Publications

The contributions presented in this thesis and other scientific work appear in the following publications:

International Journals

- ABDI, Hadjer et Ismail Boukli Hacene. A MULTIPLE AND ROBUST IMAGE WATERMARKING APPROACH BASED ON LWT AND FWHT FOR MEDICAL DATA SECURITY. *Journal of Mechanics in Medicine and Biology*, 2023, vol. 23, no 03, p. 2350011. <https://doi.org/10.1142/S0219519423500112>
- ABDI, Hadjer et HACENE, Ismail Boukli. An Optimized Medical Image Watermarking Approach for E-Health Applications. *Medical Technologies Journal*, 2023, vol. 5, no 1, p. 594-603.

International Communication

- Hadjer and B. H. Ismail, " An Optimized Medical Image Watermarking Approach For E-Health Applications" ICHSMT'22: International Congress on Health Sciences and Medical Technologies, Tlemcen, Algeria, 03-05 December 2022
- Hadjer and B. H. Ismail, "A Dual Image Watermarking Scheme Based on WPT And Chaotic Encryption for Medical Data Protection," 2022 7th International Conference on Image and Signal Processing and their Applications (ISPA), 2022, pp. 1-6, [10.1109/ISPA54004.2022.9786355](https://doi.org/10.1109/ISPA54004.2022.9786355).

National Communication

- Hadjer and B. H. Ismail, "A Dual Watermarking Scheme Based On LWT-SVD And Entropy For Medical Images Security," National Conference on Telecommunications and its Applications (CNTA'21) 2021.

Doctoral Days

- ABDI H, BOUKLI HACENE I, "Securing Medical Imaging Data", biomedical engineering doctoral day, JD-GBM 2019, University of Tlemcen.
- ABDI H, BOUKLI HACENE I, " Sécurisation des images médicales: méthode de tatouage numérique", biomedical engineering doctoral day, JD-GBM 2021, University of Tlemcen.

