N^0 d'ordre...../FT/UMBB/2024

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University M'Hamed Bougara of Boumerdes

Faculty of Technology

Doctoral Thesis

Presented by:

Aicha BENYOUCEF

Submitted for the Fulfilment of the Requirements of the

DOCTORATE-LMD degree in

Field: Biomedical Engineering
Option: Biomedical Instrumentation

Biomedical security: Performance study and analysis

In front of a jury composed of:

Mr. MERAIHI Yassine	Professor	UMBB	President
Mr. HAMADOUCHE M'Hamed	Professor	UMBB	Supervisor
Mr. AMMAR Mohammed	Professor	UMBB	Examiner
Mr. RIAHLA Mohamed Amine	Professor	UMBB	Examiner
Mme. BELKACEM Samia	MCA	UMBB	Examiner
Mr. BENLATRACHE Mohamed Salah	MCA	C.U. Mila	Examiner

Academic Year: 2023/2024

ACKNOWLEDGEMENTS

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

First and foremost, I want to thank Allah for providing me with the chance, ability, strength, and determination to accomplish this assignment. without Your driving intervention, my thesis would not have come to fruition.

I would also like to convey my most sincere thanks to my supervisor, **Prof. HAMADOUCHE M'Hamed**, for his great support and guidance during my research, which enormously helped my growth as an independent researcher and to perform without excessive pressure. Being under his direction has been a real joy and honor for me.

Finally, I would also like to thank the Jury, namely, the president, **Prof. MERAIHI Yassine**, from the University of M'Hamed Bouara Boumerdes, and the members, **Prof, AMMAR Mohammed**, from the University of M'Hamed Bouara Boumerdes, **Prof, RIAHLA Mohamed Amine** from the University of M'Hamed Bouara Boumerdes, **Dr, BELKACEM Samia**, the University of M'Hamed Bouara Boumerdes, and **Dr, BENLATRACHE Mohamed Salah** from the University of AbdelHafid Boussouf - Mila.

The present Ph.D. thesis was carried out at the LIMOSE Laboratory, Department of Engineering of Electrical Systems, Faculty of Technologies, University of M'Hamed Bougara Boumerdes.

DEDICATIONS

.

I would like to dedicate this Ph.D. thesis to the soul of my dear father, who was the reason I started my Ph.D. journey, and my mother, who was not stingy with her support and encouragement for me. They are the ones who always believed in me, gave me all the great and precious things, instilled in me the love of science from a young age, always encouraged me to follow my dreams, and supported me every step of the way.

I would also like to dedicate this thesis to my all family and friends and to all those who are dear to me and provided encouragement and motivation during the ups and downs of this research journey.

Aicha BENYOUCEF

الملخص

تبحث هذه الأطروحة في تطوير نهج قوي لتأمين البيانات الطبية من خلال تقنيات العلامة المائية، مع التركيز بشكل خاص على تطبيق تشفير رمز الاستجابة السريعة. يتناول البحث الحاجة الملحة لتحسين التدابير الأمنية في نقل البيانات الطبية وتخزينها، مع الأخذ في الاعتبار مدى تعرض معلومات المريض للوصول والتلاعب غير المصرح به. من خلال مراجعة شاملة للأدبيات وتحليل الأساليب الحالية، تحدد الأطروحة التحديات الرئيسية في وضع العلامات المائية للصور الطبية، بما في ذلك القيود في سعة الحمولة، وعدم القدرة على الإدراك، والمتانة ضد الهجمات.

ولمواجهة هذه التحديات، يقترح البحث نهجًا جديدًا للعلامة المائية يستفيد من تشفير رمز الاستجابة السريعة لتعزيز الأمان والقدرة داخل الصور الطبية. تتضمن المنهجية تضمين تمثيلات رمز الاستجابة السريعة لتقارير اختبار التصوير الطبي $(MITR)$ في المناطق غير المثيرة للاهتمام من الصور الطبية باستخدام تقنيات تحويل المويجات المنفصلة (DWT) وتحليل القيمة المفردة (SVD) . يتم إجراء تقييم الطريقة المقترحة باستخدام مقاييس الأداء مثل نسبة الذروة للإشارة إلى الضوضاء $(PSNR)$ ، ومؤشر التشابه الهيكلي $(SSIM)$ ، ومعامل التطبيع (NC) .

وتظهر النتائج تحسينات كبيرة في سعة الحمولة، وعدم القدرة على الإدراك، والأمن ضد الهجمات المختلفة مقارنة بطرق العلامات المائية الحالية. يوفر النهج المقترح توازنًا بين المتطلبات الأمنية والاعتبارات العملية، مما يجعله مناسبًا للتطبيقات الواقعية في نقل البيانات الطبية وتخزينها. بشكل عام، يساهم هذا البحث في تطوير مجال العلامات المائية للصور الطبية ويضع الأساس للتطورات المستقبلية في مجال الأمن الطبي الحيوي.

الكلمات المفتاحية : الأمن الطبي الحيوي، الصورة الطبية، العلامة المائية الرقمية، الاستجابة السريعة $(QRcode)$ ، التوثيق

ABSTRACT

This thesis investigates the development of a robust approach for securing medical data through watermarking techniques, with a specific focus on the application of QR code encryption. The research addresses the pressing need for improved security measures in medical data transmission and storage, considering the vulnerability of patient information to unauthorized access and manipulation. Through a comprehensive literature review and analysis of existing methods, the thesis identifies key challenges in medical image watermarking, including limitations in payload capacity, imperceptibility, and robustness against attacks.

To address these challenges, the research proposes a novel watermarking approach that leverages QR code encryption to enhance both security and capacity within medical images. The methodology involves embedding QR code representations of Medical Imaging Test Reports (MITR) into the non-interest regions of medical images using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) techniques. Evaluation of the proposed method is conducted using performance metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Normalization Coefficient (NC).

The results demonstrate significant improvements in payload capacity, imperceptibility, and security against various attacks compared to existing watermarking methods. The proposed approach offers a balance between security requirements and practical considerations, making it suitable for real-world applications in medical data transmission and storage. Overall, this research contributes to advancing the field of medical image watermarking and lays the foundation for future developments in biomedical security.

Keywords: Biomedical Security, Medical image, Digital watermarking, Quick Response (QR code), Authentication

RÉSUMÉ

Cette thèse étudie le développement d'une approche robuste pour sécuriser les données médicales en utilisant des techniques de tatouages, avec un accent particulier sur l'application du cryptage du code QR. La recherche répond au besoin pressant d'améliorer les mesures de sécurité dans la transmission et le stockage des données médicales, étant donné la vulnérabilité des informations sur les patients à l'accès et à la manipulation non autorisés. Grâce à un examen approfondi de la littérature et à une analyse des méthodes existantes, la thèse identifie les principaux défis du tatouage d'images médicales, notamment les limites de la capacité de la charge utile, l'imperceptibilité et la robustesse face aux attaques.

Pour relever ces défis, la recherche propose une nouvelle approche du tatouage qui exploite le cryptage des codes QR pour améliorer à la fois la sécurité et la capacité des images médicales. La méthodologie consiste à intégrer des représentations de codes QR de Rapports de Tests d'Imagerie Médicale (MITR) dans les régions sans intérêt des images médicales à l'aide de la Transformée en Ondelettes Discrète (DWT) et des techniques de Décomposition en Valeurs Singulières (SVD). La méthode proposée est évaluée à l'aide de mesures de performance telles que le Rapport Signal/bruit maximal (PSNR), l'Indice de Similarité Structurelle (SSIM) et le Coefficient de Normalisation (NC).

Les résultats démontrent des améliorations significatives de la capacité de la charge utile, de l'imperceptibilité et de la sécurité contre diverses attaques par rapport aux méthodes de filigrane existantes. L'approche proposée offre un équilibre entre les exigences de sécurité et les considérations pratiques, ce qui la rend appropriée pour des applications réelles dans la transmission et le stockage de données médicales. Dans l'ensemble, cette recherche contribue à faire progresser le domaine du tatouages des images médicales et jette les bases des développements futurs en matière de sécurité biomédicale.

Mots clés: Sécurité Biomédicale, Image Médicale, Filigrane Numérique, Réponse Rapide, Authentification

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHMS

LIST OF ACRONYMS

AES **A**dvanced **E**ncryption **S**tandard

AES-GCM **A**dvanced **E**ncryption **S**tandard-**G**alois/**C**ounter **M**ode

AT **A**rnold **T**ransfer

BER **B**it **E**rror **R**ate

CT scan **C**omputerized **T**omography

DCT **D**iscrete **C**osin **T**ransform

DES **D**ata **E**ncryption **S**tandard

DFT **D**iscrete **F**ourier **T**ransform

DICOM **D**igital **I**maging and **CO**mmunications in **M**edicine

DSA **D**igital **S**ignature **A**lgorithm

DNN **D**eep **N**eural **N**etwork

DWT **D**iscrete **W**avelet **T**ransform

ECC **E**lliptic **C**urve **C**ryptography

ECDH **E**llitic **C**urve **D**iffie **H**ellman

EPR **E**lectronic **P**atient **R**ecord

FTBM **F**used **T**ransform-**B**ased **M**ethod

GA **G**enetic **A**lgorithm

HD **H**essenberg **D**ecomposition

HIPAA **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct

HIS **H**ospital **I**nformation **S**ystem

HITECH **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth

HL7 **H**ealth **L**evel **S**even

HVS **H**uman **V**isual **S**ystem

IWT **I**nteger **W**avelet **T**ransformation

JPEG **J**oint **P**hotographic **E**xperts **G**roup

LATESTRNDDIST **LATEST** Small **R**andom **DIST**ortions

LBP **L**ocal **B**inary **B**it

LZW (**L**empel–**Z**iv–**W**elch Compression

LSB **L**east **S**ignificant **B**it

MI **M**edical **I**mage

MITR **M**edical **I**mage **T**est **R**eport

MFRO **M**anta **R**ay **F**oraging **O**ptimization

MRI **M**agnetic **R**esonance **I**maging

MRSVD **M**ulti-**R**esolution **S**ingular **V**alue **D**ecomposition

MSE **M**ean-**S**quare **E**rror

MVs **M**otion **V**ectors

NC **N**ormalized **C**orrelation

NSCT **N**on **S**ub-Sampled **C**ontourlet **T**ransform

OCT **O**ptical **C**oherence **T**omography

PACS **P**icture **A**rchiving and **C**ommunication **S**ystems

PNSR **P**ick **S**ignal to **N**oise **R**ation

QR **Q**uick **R**esponse

QPHT **Q**uaternion **P**olar **H**armonic **T**ransforms

RDWT **R**edundant **D**iscrete **W**avelet **T**ransform

RGB **R**ed-**G**reen-**B**leu component on the color image

RML **R**e**M**ove **L**ines

ROI **R**egion Of **I**nterest

RONI **R**egion Of **N**on **I**nterest

RSVD **R**andomized **S**ingular **V**alue **D**ecomposition

SMFMF **S**witched **M**ode **F**uzzy **M**edian **F**ilter

SSIM **S**tructural **S**imilarity **I**ndex

SVD **S**ingular **V**alue **D**ecomposition

WMI **W**atermared **M**edical **I**mage

ZW **Z**ero-**W**atermarking

CHAPTER 1

INTRODUCTION

Summary

In this chapter, we recall some definitions and concepts of biomedical security and its performance with the fundamental principles of medical imaging, medical image information systems, transmission standards, and medical security. Then we position ourselves concerning the problems we want to solve and the research objectives. Finally, we present the reading structure of the thesis.

1.1 Introduction

Telemedicine revolutionizes healthcare delivery by enabling practitioners to care for patients, remotely, regardless of physical distance. This technology facilitates remote monitoring of patients recovering at home or those facing barriers to accessing traditional healthcare due to geographic or financial limitations. Consequently, telemedicine enhances efficiency, saving time and resources for both patients and healthcare providers. By streamlining hospital and clinic workflows and enabling remote consultations, telemedicine minimizes patient hospitalization, optimizes resource allocation, and reduces the risk of disease transmission. Furthermore, it facilitates collaborative diagnosis by enabling the exchange of patient documents, analyses, and medical images among experts and healthcare facilities [1, 2, 3].

Figure 1.1 illustrates a comprehensive overview of the most prevalent telemedicine services currently available. These services encompass a wide array of healthcare solutions delivered remotely, leveraging technology to bridge the gap between patients and healthcare providers. Figure provides a detailed depiction, including but not limited to virtual consultations, remote monitoring, telepsychiatry, and remote patient education. Through this visual representation, viewers can grasp the breadth and depth of telemedicine services, gaining insights into how technology is revolutionizing healthcare delivery and improving access to quality care[1].

Recently, and exactly in July 2021, the three organizations: Retinal Consultants Medical Group, ACE Surgical Supply, and Three Rivers Regional Commission have recently revealed hacks in which unauthorized parties may have accessed patients' protected health information. The hacking incident in the first one affected 11,603 Patients, when unauthorized individuals had gained access to its computer network, and the second, discovered that her IT environment had been assessed by an unauthorized party who obtained 12,122 patients' health information. also, the health information of 2,000 individuals was attacked in the last company, this information was regrouped into three types of information: the personal such as the name, the address, the username, and the password, and the financial, such as the financial account number, the credit and debit card information, and the medical such as the treatment and diagnosis information, Medicare and Medicaid information. This hacked information can be a risk of identity theft of the patient, phishing, and changing the patient's health information, which can give a wrong diagnosis and treatment [4].

On the other hand, The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act were enacted to address the apprehensions regarding the security and confidentiality of patient health information and biomedical data. These acts introduced a range of security

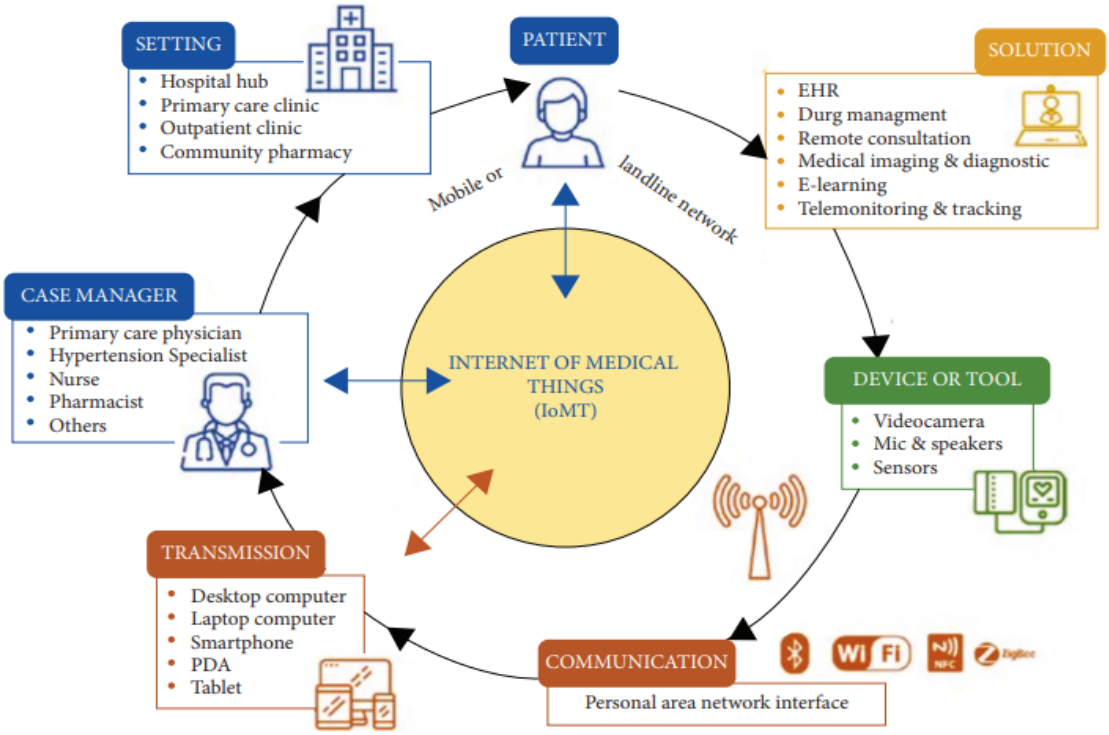

Figure 1.1: A diagram of the most common telemedicine services and their workflow[1]

safeguards with the primary objective of safeguarding electronic patient records (EPR) and ensuring the utmost confidentiality and integrity of the information they encompass [5].

1.2 Biomedical concepts and performance

The biomedical security concept encompasses measures and protocols to safeguard sensitive biomedical data, devices, and systems from unauthorized access, manipulation, or disclosure, including patient health information, research data, and medical records, while performance refers to the effectiveness, efficiency, and reliability of security measures in protecting biomedical data and systems, evaluated through metrics such as intrusion detection accuracy, encryption speed, access control effectiveness, cyber security robustness, and regulatory compliance.

1.2.1 Medical Image Modality

Medical image is a distribution of the physical and functional parts of the human body such as tissues and organs, and it is the result of many medical tools found in hospitals and clinics based on different techniques. In the realm of diagnosis, common imaging modalities encompass radiology, ultrasound imaging (US), computerized tomography (CT), magnetic resonance imaging (MRI), and positron emission tomography (PET). Radiology, among the oldest and most widely employed imaging techniques, relies on X-ray attenuation properties

to visualize the cumulative absorption process of X-rays traversing tissues. Radiographs are created by positioning patients between an X-ray source and a detector. Contrast agents may enhance image quality. CT imaging employs X-rays to generate 3D images of internal anatomy by capturing multiple projections from various angles and reconstructing the volume through tomography. The versatile properties of X-rays render them invaluable for medical diagnostics and treatments [6, 7]. These images are saved and stored in devices or the cloud in a secure way to use in the diagnosis, studies, or transfer between medical centers [8].

1.2.2 Medical Image Information System

Picture Archiving and Communication System

The Picture Archiving and Communication System (PACS), integrated as a module within the radiology information system, serves as a centralized repository for all imaging data, facilitating the creation and transfer of digital radiology images and accompanying reports [9]. This system empowers users to manipulate picture display parameters such as quality, zoom, and contrast, as well as enables image comparison via a workstation computer.

Since the 1980s, PACS has emerged as a viable alternative to traditional film-based imaging, offering numerous advantages. These include optimizing image quality and accessibility, enhancing physicians' productivity and efficiency, fostering seamless communication between clinical units and the radiology department, reducing instances of lost images, expediting the generation and transmission of radiology reports, minimizing physical storage requirements for image archiving, cutting personnel costs and expenses associated with films and related chemicals, mitigating the need for re-imaging and patients' exposure to harmful radiation, and diminishing average patient waiting times [10, 11, 12].

Hospital Information System

Within healthcare organizations, various categories of information systems serve distinct purposes: there are systems tailored for general practitioners as well as specialists such as cardiologists, ophthalmologists, and dentists, alongside systems for hospital units including radiology, functional exploration, and laboratory services. Among these, the Hospital Information System (HIS) holds paramount importance as it forms the backbone of hospital operations. It serves as the overarching framework for the collection, processing, analysis, and reporting of medical data. Specifically, HIS facilitates access to patient records, reports from diverse healthcare services, and billing information. Through electronic patient records, physicians gain comprehensive insights into the care provided to each patient, aiding in informed decision-making and ensuring continuity of care. This system is particularly valuable for monitoring radiology imaging orders and managing billing information. It is commonly

integrated with PACS, which serves as the central component of radiography technical units. [13].

1.2.3 Transmission Standard

Transmitting medical data between different health systems presents challenges for two main reasons: i) medical information systems operate on diverse machine platforms, and ii) medical images originate from various imaging modalities produced by different manufacturers. This underscores the necessity for universally standardized data formats and communication protocols that facilitate seamless interfacing between multiple medical systems.

DICOM Standard

Digital Imaging and Communications in Medicine (DICOM) is the standard for managing medical images. Initially developed by the American College of Radiology and the National Electrical Manufacturers Association in 1985, its primary objective was to enhance interoperability among medical imaging systems. DICOM furnishes comprehensive guidelines on formatting and exchanging medical images and their related data, facilitating seamless integration within and beyond healthcare organizations (e.g., telemedicine). Notably, DICOM ensures scalability, enabling smooth communication among diverse systems and facilitating extensive implementations.[14].

Health Level seven

Health Level Seven (HL7) serves as the benchmark standard for handling non-imaging data, information such as the name, age, phone number, illness information, treatments, doctor name, and other necessary data, encompassing test results, patient demographics, and billing information. Essentially, HL7 comprises a collection of global standards designed for the exchange, management, and integration of clinical and administrative electronic data within healthcare facilities. This fosters interoperability among diverse medical information systems [15].

1.2.4 Biomedical security

To address concerns regarding data breaches and privacy issues, various security measures have been developed. These include: 1) Cryptography: This field focuses on rendering data unintelligible to unauthorized parties. Symmetric encryption involves using a single encryption key for both encryption and decryption, while asymmetric encryption employs different keys for encryption and decryption. 2)Watermarking: A security technique wherein secret data is embedded within a cover medium, such as an image, audio, or video. This embedded data can be retrieved after extraction, providing a means to ensure tamper resistance,

assert intellectual property ownership, and enhance the security of multimedia documents. 3)Steganography: This involves concealing information within a cover medium in a manner that its presence remains undetectable. Digital image steganography offers the potential for secure communication, a crucial aspect in many contemporary applications [16].

1.3 Problem Statement

This thesis focuses on exploring the applications of digital watermarking in medical images as a security measure. The problem statement outlined in the thesis introduction regarding medical image watermarking addresses several issues.

- First, there is a significant problem with the payload capacity, which refers to the amount of data that can be embedded within the medical image without significantly altering its appearance. This capacity directly impacts the imperceptibility of the watermark, meaning the extent to which the watermark is visually undetectable within the image. Imperceptibility is vital in medical image watermarking because it ensures that doctors can accurately interpret the image without being influenced by the presence of the watermark. If the watermark alters the appearance of the image too much, it may impede the diagnostic process and lead to inaccurate assessments of the patient's condition.
- Secondly, there's the challenge of ensuring robustness against various attacks when transmitting the watermarked document through non-secure channels. These attacks could include attempts to remove or alter the watermark, or to degrade the image quality in such a way that the watermark becomes unreadable. The robustness of the watermarking scheme refers to its ability to withstand such attacks and maintain the integrity of the embedded information. However, enhancing robustness often comes at the cost of increased complexity and execution time of the watermarking algorithm. This trade-off between robustness, complexity, and execution time is a key consideration in developing an effective medical image watermarking approach.
- Overall, the problem statement highlights the need to strike a balance between the conflicting requirements of capacity, imperceptibility, and robustness in medical image watermarking. Finding this balance is essential to develop a watermarking technique that meets the needs of healthcare professionals by ensuring accurate diagnosis while also guaranteeing the security and integrity of the medical data during transmission.

1.4 Research Objectives

This research endeavors to instill confidence in digital medical processes by establishing robust authenticity and integrity measures within medical imagery. It seeks to delineate the

essential prerequisites of medical imaging and scrutinize potential security vulnerabilities encountered in routine clinical procedures. This effort will culminate in the development of strategies and methodologies essential for validating the trustworthiness of medical images and meeting the extensive demands of medical imaging workflows. The specific objectives of this research are as follows:

Address the challenge of payload capacity by designing methods capable of accommodating large amounts of data within medical images while maintaining imperceptibility:

This objective involves developing innovative methods or algorithms to increase the payload capacity of the watermarking technique without sacrificing the quality or perceptual fidelity of the medical images. It aims to strike a balance between embedding a significant amount of data while ensuring that the watermark remains invisible or imperceptible to the human eye.

Improve imperceptibility in medical image watermarking to ensure that the presence of embedded data does not compromise the visual quality or diagnostic utility of the image:

Here, the goal is to refine the watermarking process to minimize any perceptible artifacts introduced into the medical images. This requires optimizing the embedding algorithm, selecting appropriate embedding locations, and optimizing the strength of the watermark to minimize any degradation in image quality while maintaining the desired level of robustness.

Enhance the robustness of the watermarking technique to withstand various attacks aimed at altering or removing the embedded information:

Here, the focus is on improving the resilience of the watermarking technique against different types of attacks, such as signal processing attacks, compression, noise addition, or geometric transformations. This may involve incorporating error correction codes, digital signatures, or other techniques to detect and mitigate tampering attempts.

Evaluate the performance and effectiveness of the proposed solution through empirical testing and comparison with existing methods, aiming to achieve a balance between security, capacity, imperceptibility, and robustness in medical data transmission and storage:

This objective involves conducting comprehensive experiments and evaluations to assess how well the proposed watermarking solution performs in real-world scenarios. It includes benchmarking against existing methods, analyzing key performance metrics such as PSNR, SSIM, NC, and assessing the trade-offs between security, capacity, imperceptibility, and

robustness. The aim is to validate the effectiveness and practical utility of the proposed solution in enhancing the security and integrity of medical data transmission and storage systems.

1.5 Contribution

This research introduces contributions and advancements in the field of medical image watermarking. The outcomes and contributions of this study, elaborated in this thesis, have been disseminated through publications in reputable conferences and journal. The primary contributions of this research are outlined as follows:

1.5.1 Publication summary

Paper

Benyoucef, Aicha, and M'Hamed Hamadouche. "Region-Based Medical Image Watermarking Approach For Secure EPR Transmission Applied to e-Health." Arabian Journal for Science and Engineering (2023): 1-13.

The suggested method in this paper introduces a region-based watermarking technique tailored for safeguarding patient Medical Imaging Test Reports (MITRs). This novel approach entails embedding a QR code representation of the MITR within the non-critical regions of the medical image, utilizing frequency domain transformations like discrete wavelet transform and singular value decomposition. This method ensures notable advantages, including heightened payload capacity, authentication, imperceptibility, and resilience against various forms of attacks.

International Conference

Benyoucef, Aicha, and M'Hamed Hamadouche. "RONI-Based Medical Image Watermarking Using DWT and LSB Algorithms." International Conference on Artificial Intelligence and its Applications. Cham: Springer International Publishing, 2021.

We present a robust method for watermarking medical images to safeguard patient data during transmission over non-secure channels. Initially, the original image undergoes enhancement through a sharpening filter to augment contrast, followed by segmentation into two distinct regions using snake segmentation. Subsequently, the watermark, representing the Electronic Patient Record (EPR), is embedded into the frequency domain post-application of Discrete Wavelet Transform (DWT) on the Region of Non-Interest (RONI), employing the least significant bit (LSB). Notably, the RONI typically exhibits a predominantly black background, while the Region of Interest (ROI) contains essential patient

information. This method preserves the quality of the watermarked image, enhancing imperceptibility, security, and authentication.

Benyoucef, Aicha, and M'Hamed Hamadouche. "Medical image watermarking for authentication, integrity, and confidentiality of data." International Congress on Health Sciences and Medical Technologies ICHSMT'22. 2022.

The paper presents the watermarking technique for hiding the patient's information based on hiding the secret information in the RONI of the medical image using the least significant bit (LSB) technique in the spatial domain. The application of the method to various medical images reveals improved imperceptibility and security of the watermark. With high-quality medical image watermarking and unchanged patient illness information, the embedded data are authenticated.

1.6 Thesis Structure

The rest of this thesis is organized as follows. In Chapter 2, after a brief presentation of biomedical security and medical data, we lay out the fundamentalism of Digital watermarking, its requirements, frameworks, classification, and techniques for understanding its application in medical image security. Chapter 3, connected to presents the recent related work in the literature categorized by the medical image watermarking based on domain, medical image watermarking combined with cryptography techniques, and the application of the QR code (Quick Response) in this field. Chapters 4 and 5 present the novel proposed method based on the transform domain and apply the QR code for medical image watermarking, and finished by the thesis conclusion in chapter 6.

CHAPTER 2

DIGITAL IMAGE WATERMARKING

Summary

After a brief presentation of the concepts related to biomedical security and performance, the main objective of this second chapter is to lay the fundamentals of the digital image watermarking necessary for securing the Electronic patient record (EPR) and the information contained in the medical images. First, we summarize the watermarking requirements and the watermarking framework for the embedding and extracting process. Then we present the watermarking classification and its techniques in the spatial and transform domain. Finally, we conclude by presenting the evaluation metrics that allow us to test the performance of watermarking methods.

2.1 Introduction

This chapter on digital image watermarking provides a comprehensive overview of the subject, covering its requirements, framework, classification, techniques, attacks, and metrics. It begins by outlining the necessity for watermarking in digital images to ensure authenticity, integrity, and ownership protection. The framework highlights the significance of efficiently embedding and extracting watermarks while clarifying the basic framework and elements of the watermarking process. Classification explores the various types of digital image watermarking methods, including spatial domain, and transform domain techniques, each with its unique characteristics and applications. Techniques focus on watermark embedding and extraction methods and highlight their strengths and limitations. Attacks analyze potential threats to watermark security, including noise addition, compression, and geometric transformations, which may compromise watermark robustness and imperceptibility. Finally, metrics discuss the quantitative measures used to evaluate watermarking performance providing insights into the effectiveness and reliability of watermarking algorithms. Overall, the thesis chapter offers a comprehensive understanding of digital image watermarking, addressing its key aspects to facilitate further research and application development in the field.

2.2 Digital watermarking

2.2.1 Historical part of digital watermarking

"Digital Watermark" was developed by Andrew Tirkel and Charles Osborne, and Tirkel, Ron Van Schyndel, Rankin, and others successfully embedded and extracted a steganographic spread spectrum watermark for the first time in 1993. [17]. This study investigates the possibility of adding a digital watermark that is "undetectable" on a standard 512*512 intensity picture using an 8-bit grayscale, capable of carrying authentication or authorization codes and intended for usage including copyright enforcement, counterfeit prevention, image labels, and controlled access to image data, with two implementation techniques covered, one using linear addition for enhanced security and bit plane manipulation for quick decoding.

The initial watermarking technique aimed to embed imperceptible patterns or information into images or audio signals, ensuring invisibility or difficulty in detection by humans to maintain media quality and integrity. This facilitated identifying and protecting digital content like images or audio from unauthorized use or distribution, establishing ownership or tracing content origin through unique embedded patterns or information [18].

Digital watermarking offers a means to subtly embed digital data into both digital formats

(images, videos, audio) and traditional media (printed material). The information within the watermark serves to enhance numerous applications including connected content, security, content protection, copy prevention, authentication, and more. One notable benefit of digital watermarking is that the information remains subtly linked to the original medium, whether it's a cover or host [19].

2.2.2 Motivation for digital watermarking

Implementing digital watermarking in medical data can optimize data management processes and enhance efficiency within healthcare organizations by providing a reliable method for identifying and tracking medical data, thereby enabling healthcare providers to efficiently manage and access patient information, leading to quicker and more precise decision-making in clinical settings.

While encryption methods are certainly useful for protecting private medical information, digital watermarking has certain benefits that make it especially appropriate for usage in the medical field.

Digital watermarking's ability to offer traceability and security without changing the original data is one of its main advantages. Embedding undetectable patterns or information directly into the data means that even if the data is accessed by unauthorized parties, the watermark remains intact, providing a subtle but identifiable marker of authenticity. digital watermarking differs from encryption, which scrambles data and makes it unreadable without the right decryption key.

Furthermore, digital watermarking enables the direct embedding of metadata or supplementary details into medical images or records, enhancing data interpretation, fostering collaboration among healthcare professionals, and ultimately enhancing patient care.

Many medical image watermarking methods are proposed to enhance the embedding and extracting of the watermark, but the need to solve the problem of the payload capacity without any distortion of the medical image is still not solved in a good way. This led us to propose methods that can solve this problem corresponding to the watermarking requirements, and find the best balance of the height capacity, great imperceptibility, and robustness of the medical image watermarking.

2.3 Digital watermarking requirement

Designing a comprehensive watermarking approach necessitates the consideration of various critical requirements. These fundamental requirements include reversibility, computational complexity, data payload, security, imperceptibility, resilience, and imperceptibility. These requirements will be explained in more depth in the section that follows.

2.3.1 Security

Watermarking security must be able to resist intentional attacks, which may be divided into three categories [20]: unauthorized detection, unauthorized embedding, and unauthorized removal:

- Unauthorized detection attacks involve attempts by unauthorized users to extract a watermark from digital content without possessing complete knowledge of the embedding algorithm. In these attacks, individuals without proper authorization aim to deduce details about the algorithm through reverse engineering, risking intellectual property and content security. Successful extraction without algorithm knowledge could lead to unauthorized use, distribution, or false claims of ownership. Protecting the secrecy of the embedding algorithm is crucial to thwart such attacks, and security measures, including encryption and continuous monitoring, play a vital role in safeguarding against unauthorized detection and preserving the integrity of digital content.

- Unauthorized embedding attacks involve the malicious insertion of a forged watermark into multimedia data that should originally remain unmarked. In these attacks, a counterfeit watermark is created to mimic a legitimate one, deceiving observers and potentially leading to false claims of ownership or the dissemination of misinformation. The forged watermark is then integrated into digital content, compromising its authenticity and trustworthiness. Such attacks challenge watermarking systems that strive to protect against unauthorized alterations and maintain the reliability of digital media for purposes like copyright protection and content authentication. Robust security measures are essential to detect and thwart these attempts, ensuring that only authorized parties can embed valid watermarks and that unauthorized manipulations are prevented.

- Unauthorized removal attacks refer to attempts to eliminate or tamper with watermarks embedded in digital content. These attacks are carried out to either degrade or completely remove the watermark from the content by 1) Eliminating the attack is based on eliminating the watermark information completely without leaving any traces. 2) Masking attacks involve covering or hiding the watermark within the content in a way that makes it difficult for watermark detection algorithms to identify and

extract it. 3) Collusion attacks occur when multiple copies of watermarked content are combined to weaken or delete the watermark.

2.3.2 Robustness

The robustness requirement refers to the strength of the algorithm or the watermarking approaches against intentional (malicious) and unintentional attacks that can affect the watermark by removing or changing it. It depends also on the signal processing operation needed in the extracting process. Not all digital watermarking approaches should be robust such as fragile watermarking; it depends on its application and usage.

2.3.3 Reliability

This requirement comprises two key principles: authentication and integrity. Authentication entails verifying the origin of data and its associations with a specific user. At the same time, integrity involves demonstrating that the data remains unaltered or unmodified, whether by malicious intent or accidental actions, and has not been played with by unauthorized individuals.

2.3.4 Imperceptibility

The foremost requirement in the digital watermarking proposal is the similarity of the original and watermarked data. In this context, imperceptibility implies that the introduced watermark remains undetected by the human visual system, and there is no distortion of any information within the watermarked data. It is determined by calculating the perceptual similarity between the original and watermarked data.

2.3.5 Data payload / capacity

The number of watermark bits that can be identified and embedded into the original data without degrading its quality can be defined as this requirement. Since watermarks are replicable, having many watermarks adds more data payload and resilience, minimizing the risk of watermarks changing.

2.3.6 Speed / computational complexity

It speaks about how many steps and computations are required for the process of extracting and embedding a watermark, and it directly affects how long the algorithm runs. Requires real-time calculation that is both efficient and time-efficient, i.e., quick and simple.

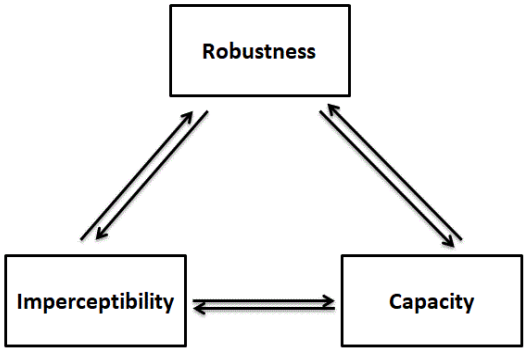

Figure 2.1: Watermarking requirements trade-off

2.3.7 Reversibility

It guarantees the extraction of the watermark in addition to the accurate reconstruction of the original, unchanged data. The watermarked data must be devoid of distortions and the extraction process must be reversible to satisfy this requirement. This is particularly crucial in applications such as telemedicine and remote sensing systems. In tele-diagnosis and treatment within medical data, the data must remain unaltered. Similarly, in remote sensing applications, the data should not change to ensure accurate decision-making processes.

In Figure 2.1, the three essential requirements in the watermarking algorithm are depicted. These requirements are likely to include imperceptibility, robustness, and embedding capacity. The figure suggests that there is a trade-off among these requirements. If emphasis is placed on achieving a large embedding capacity, it may enhance robustness, but at the expense of imperceptibility. Conversely, if the focus is on improving imperceptibility, it might compromise the embedding capacity and, consequently, the robustness of the watermarking algorithm.

2.4 Digital watermarking Framework

Watermark creation, embedding, and extraction are the three essential components that make up the foundational structure for creating a digital watermarking system. The watermark generation process is shown in Figure 2.2, and the phases of embedding and extraction are shown in Figure 2.3.

2.4.1 Digital watermarking generation

The first step to building a digital watermarking scheme is watermark generation; it has some criteria depending on its application: such as the type of data, whether it is text, image, video, audio, or other data, the size of the watermark that will be add on the cover,

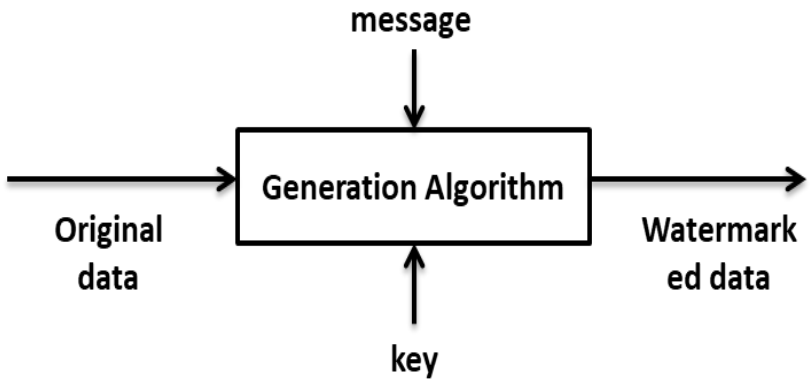

Figure 2.2: Watermark generation

and the target of embedding this digital watermark. In the medical image watermarking application, the watermark can be the electronic patient records (EPR) information such as the name, age, ID, and credit card number, or it can be medical information such as his illness type, treatments, or medical image testing report.

Figure 2.2 illustrates the key parameters essential for generating the watermark—namely the original data, the message, and the selected key for the generation algorithm. The utilization of these watermark generation parameters may vary based on the specific application requirements.

2.4.2 Digital watermark embedding

The second step to building a digital watermarking scheme is the watermark embedding part, which serves as an adding process of the watermark to the cover data (text, image, audio, video) using a secret key for generating the watermarked data by the sender. This embedding process applies some algorithms and watermarking techniques depending on the desired requirements or target application.

2.4.3 Digital watermark extraction

The third step of a digital watermarking scheme involves the extraction of the watermark. This step serves as a testing and verification process conducted by the recipient of the watermarked data to ensure that the watermark remains intact and has not been altered or compromised. This extraction process is the inverse of the embedding algorithm and is applied to retrieve the desired information.

Figure 2.3 presents an embedding and extracting process example for medical image watermarking. The sender side is based on three elements: the cover data, which is the medical image (MI), patient information represents the watermark (W), and the secret wa-

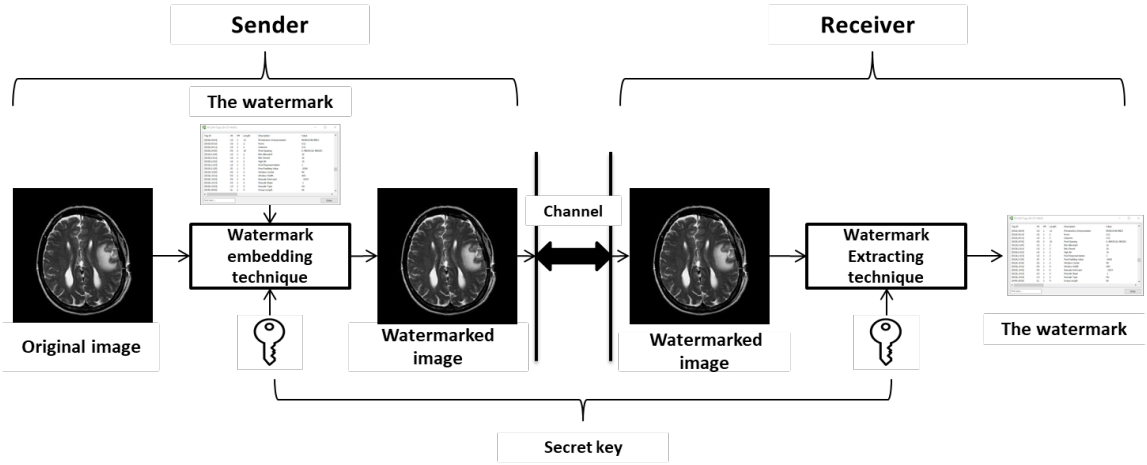

Figure 2.3: Digital image watermarking embedding and extracting process

termarking key (K) to generate the watermarked medical image (WMI) (WMI = [MI, W, K]). The receiver side applies the opposite algorithm and the same secret key (K) to extract the watermark (W) from the watermarked medical image received (WMI) (W = [WMI, K]). The information desired from the watermark extracted depends on the target application and requirement, maybe for the authentication, integrity, or extraction of the hidden secret information.

2.5 Classification digital watermarking

Depending on the different types of data, digital watermarking systems may be divided into various categories, human perception, robustness of the digital watermarking, or the extraction process procedure. All these categories have subcategories that will be discussed in the following part and summarized in figure 2.4.

2.5.1 Data

The digital watermarking classification by data means that the cover and watermark data can be one of these data types: text, image, audio, or video. The cover and watermark data don't need to be the same data type. Digital watermarking, in general, is protecting data from other data from copying, transforming, or changing. When the cover data should be protected, the watermark adds to garnet the sender mark, authentication, and integrity of the owner and avoids copywriting; it's very applicable on the document signature and TV channel. But when the watermark data that should be protected, generally it is an invisible mark or data in the cove to be secure and undetectable, for example, patient information that is sensitive data should be protected and secure then it transmits in the internet.

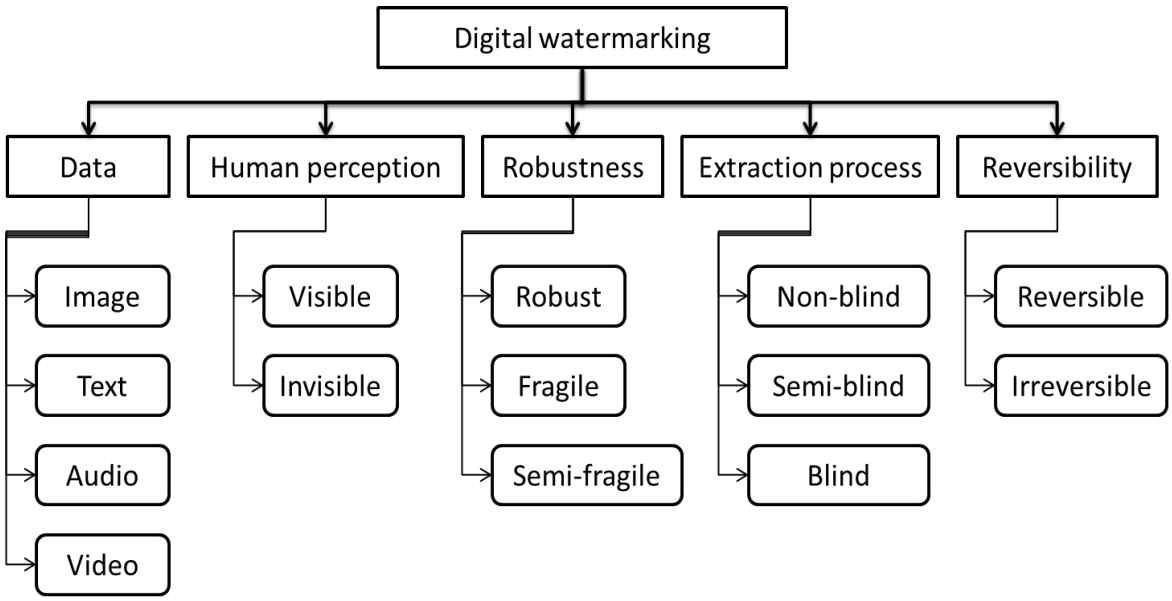

Figure 2.4: Taxonomy of digital image watermarking classification

2.5.2 Human perception

The categorization of digital watermarking based on human perception involves whether the embedded watermark is visible or invisible to the human visual system (HVS). A visible watermark is concealed on the cover data in a manner discernible to human eyes, often representing elements like company logos, ownership information, signatures, etc. In contrast, an invisible watermark is incorporated into the cover data without being perceptible to the HVS; it can only be detected and extracted by specific watermarking techniques and algorithms. This type of watermarking is employed to enhance security and imperceptibility.

2.5.3 Robustness

The digital image watermarking robustness refers to the ability of the approach to repel various attacks in the invisible approaches [21]. It decomposes into four types:

- Robust watermarking techniques are made to withstand a range of data content modifications, including unlawful removal, embedding, and detection assaults, while still accomplishing their initial objectives. For data integrity and authentication reasons, robust techniques are employed to identify stolen data.
- Fragile watermarking methods are designed to safeguard data and have a strong sensitivity to even minor alterations. One advantage of fragile watermarking is its tamper-proof nature; any loss of the watermark indicates the occurrence of tampering.

- Semi-fragile watermarking schemes provide moderate resistance against specific types of attacks. The semi-fragile methods can withstand unintentional modifications, but they are vulnerable to deliberate malicious alterations. This category of approaches is suitable for verifying the reliability, either in terms of authentication or integrity, of data content

- A hybrid approach in digital watermarking involves combining two of the aforementioned types based on the specific application and desired outcomes.

2.5.4 Extraction process

The extraction process in digital watermarking techniques is a very important part [20, 22], and it decomposes into three types:

- Non-blind watermarking techniques are referred to as private techniques because usually the watermark is created from the original data, and it's preferable for tamper-proof applications. To extract the hidden watermark using these methods, it requires the original data, the original watermark, and the key.

- In order to retrieve the hidden watermark from the watermarked data, semi-blind watermarking techniques require both the original watermark and a key. These techniques, sometimes known as semi-private techniques, include the sender and the recipient sharing the original watermark.

- Blind watermarking is a technique used to add a watermark into digital data without requiring the original content, where this last is not needed to verify the presence of the watermark or to extract it, making it more convenient for applications where the original content may not be available or accessible[23].

2.5.5 Reversibility

In the medical field, the paramount requirement for digital watermarking is reversibility, signifying the ability to recover both the original data and the watermark from watermarked data without distortion or modification. This critical feature ensures the preservation of data integrity. Similarly, in the military sector, especially when dealing with sensitive and crucial information, digital watermarking is applied to maintain security.

Conversely, irreversible watermarking involves extracting the watermark and original data but may introduce modifications or changes during the process, offering a distinct approach where preserving the exact original state is not the primary concern. lossless and lossy watermarking is described in the following

2.5.5.1 Lossless watermarking

Lossless watermarking schemes are crucial in applications like medical and military systems, where preserving the original data without distortion is paramount for decision-making. These schemes ensure zero data loss in the absence of attacks, making them highly desirable for sensitive data. They are designed to embed watermarks without altering data content, safeguarding copyright [24]. Two categories within lossless watermarking are zero-watermarking and reversible watermarking.

- Zero-watermarking, with superior robustness, utilizes original data features to create a watermark without modifying the content. Reversible watermarking, requiring a lossless environment for data transfer, aims to recover watermarks even after exposure to unintentional attacks.
- Reversible watermarking is particularly sensitive to intentional or unintentional changes, and approaches capable of conveying embedded watermarks through a lossy environment are termed robust.

2.5.5.2 Lossy watermarking

In lossy watermarking systems, certain characteristics are changed, including frequency domain transform coefficients or the replacement of the Least Significant Bits (LSB) so that the watermark becomes an integrated part of the original data. Because of the changes caused by the embedded watermark, reversing the process is not possible, in opposition to lossless watermarking.

Lossy watermarking is typically employed for data authentication, integrity verification, and ownership identification. While the embedded watermark in lossy schemes may degrade data quality, these schemes exhibit greater robustness compared to their lossless counterparts. This increased robustness is attributed to embedding the watermark strategically, often around edges or other visually significant locations in the original data [25].

2.6 Digital watermarking techniques

There are many digital watermarking techniques depending on the three main domains of embedding watermarks in the original data: spatial, transform, and spread-spectrum. This section presents the different embedding watermark techniques in each domain.

2.6.1 Spatial domain

The techniques applied in this domain are based on embedding the watermark in the cover image by changing its pixel value directly. The algorithms based on these techniques are simple to implement, completely fast, and payload capacity is wide.

Additionally, it is possible to embed watermarks multiple times, enhancing robustness against various attacks, particularly geometric ones such as cropping, translation, and rotation. This lowers the likelihood of completely removing all watermarks, But when it depends on removal attacks such as median filter, sharpening, blurring, and noise addition, it can't survive.

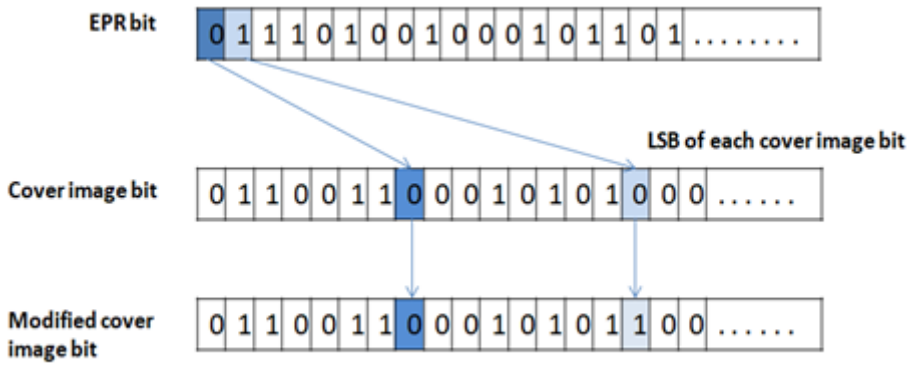

Figure 2.5: The LSB algorithm principle

2.6.1.1 Least significant bit (LSB)

The least significant bit technique is the most watermarking technique applied in the spatial domain. It's based on replacing bit by bit of the least bits of each pixel in the cover image with the most significant bits of the watermark; this last can be a text or other image. The LSB technique provides a highly imperceptible watermarked image with correlation properties for watermark detection, and it represents an inexpensive method with less computationally.

Its widespread use in medical image watermarking relies on the substitution of the least significant bit (LSB) in the medical image with the corresponding bits from the electronic patient record (EPR)[26], Fig.2.5 shows the LSB algorithm principle.

2.6.1.2 Local binary pattern (LBP)

The Local Binary Pattern (LBP) is a highly effective tool for analyzing textures, and patterns and classifying images. Its acceptance is attributed to the operator's invariance property and computational simplicity, making it widely favored. The popularity of this operator further grows due to its discriminative power and straightforward computational approach [27].

LBP codes are employed for watermark bit embedding, offering robustness against contrast adjustment and luminance variation. However, they exhibit fragility when subjected to operations such as filtering and blurring. In essence, LBP-based methods are well-suited for semi-fragile watermarking applications.

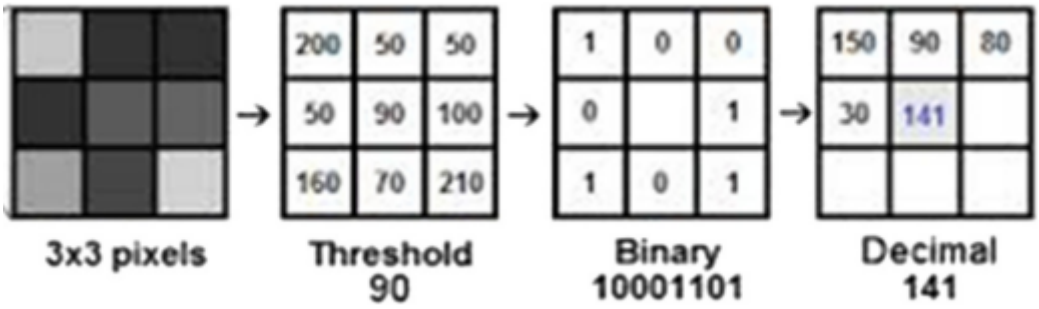

Figure 2.6: The Local Binary Pattern technique [29]

One characteristic utilized in 2D texture analysis and object/pattern detection is the Local Binary Pattern (LBP). It summarizes the local structure of an image by comparing each pixel with its neighbors. The process involves partitioning the image into non-overlapping blocks, calculating local pixel differences within each block, and labeling neighboring pixels based on intensity relative to a threshold. LBP produces an 8-bit binary code (e.g., '10011010') representing the texture spectrum of an image block, with 28 possible combinations from 8 surrounding pixels. These codes, called LBP codes, with 256 gray levels, are commonly used for feature extraction in image classification or recognition [28, 29].

2.6.1.3 Histogram modification

The histogram modification method utilizes pixel values to construct the image histogram, leveraging statistical redundancy to conceal secret data. The watermark can be hidden by manipulating the image histogram's zero and peak points. The histogram's quantity of peak and zero points limits its capability, but its ease of implementation.

The histogram modification method is enhanced through the incorporation of pixel differences or a multi-layer embedding model to boost its performance. This extension involves calculating pixel differences and generating a histogram based on these differences. By embedding secret data, the histogram is shifted, resulting in marked pixel differences. The extraction process, performed in reverse order, requires sending information about peak and zero points to the receiver for reversible recovery.

2.6.2 Transform domain

Transformation methods in signal and image processing provide potent tools for efficient analysis, compression, and feature extraction. These methods unveil concealed patterns and relationships within signals, proving critical for applications in image processing, communication, and data analysis. The mathematical properties of transforms facilitate faster computation while concentrating energy into fewer coefficients enables efficient storage and

transmission. Additionally, the ability to choose relevant coefficients allows for a focused examination of specific aspects of the signal.

This section presents the basic transform methods: Discrete wavelet transform (DWT), Discrete cosines transform (DCT), and Singular value decomposition (SVD).

2.6.2.1 Discrete wavelet transform (DWT)

The Wavelet transform breaks down a signal into fundamental functions known as wavelets, which are finite interval functions with zero mean, ideal for analyzing transient signals. Wavelets serve as a versatile method for representing and analyzing multi-resolution images and applying them to 1D signals.

Wavelets are essential for noise reduction and the recovery of weak signals from noise in signal processing, especially in medical applications. Wavelets are very used in Internet communication for image compression [30].

The discrete wavelet transform converts a discrete-time signal, represented as (x0, x1, ..., xn), into a discrete wavelet representation. Specifically, it transforms the input series into two sets of coefficients: one for low-pass wavelets (L) and another for high-pass wavelets (H), each with a length of n/2. These coefficient series are derived from equations 1 and 2, respectively.

$$Li = \sum_{n=0}^{k-1} x_{2i-1} \times t_n(z) \tag{2.1}$$

$$Hi = \sum_{n=0}^{k-1} x_{2i-1} \times s_n(z) \tag{2.2}$$

In these equations, $t_n(z)$ and $s_n(z)$ represent wavelet filters, where k is the length of the filter, and i takes values from 0 to $[\frac{n}{2}] - 1$. The selection of the filter dictates the shape of the wavelet used for the analysis.

Because of its built-in multi-resolution decomposition, the Discrete Wavelet Transform (DWT) is often used in image processing and compression applications. This method offers different resolutions by analyzing signals at different frequencies. For low-frequency signal components, multi-resolution analysis offers excellent frequency resolution but bad temporal resolution. On the other hand, high-frequency components, produce good time resolution but low-frequency resolution.

In the first level of decomposition for an image of dimensions $M \times N$, DWT splits it into four sub-bands: LL, HL, LH, and HH. Each sub-band, like LL, has dimensions M×N,

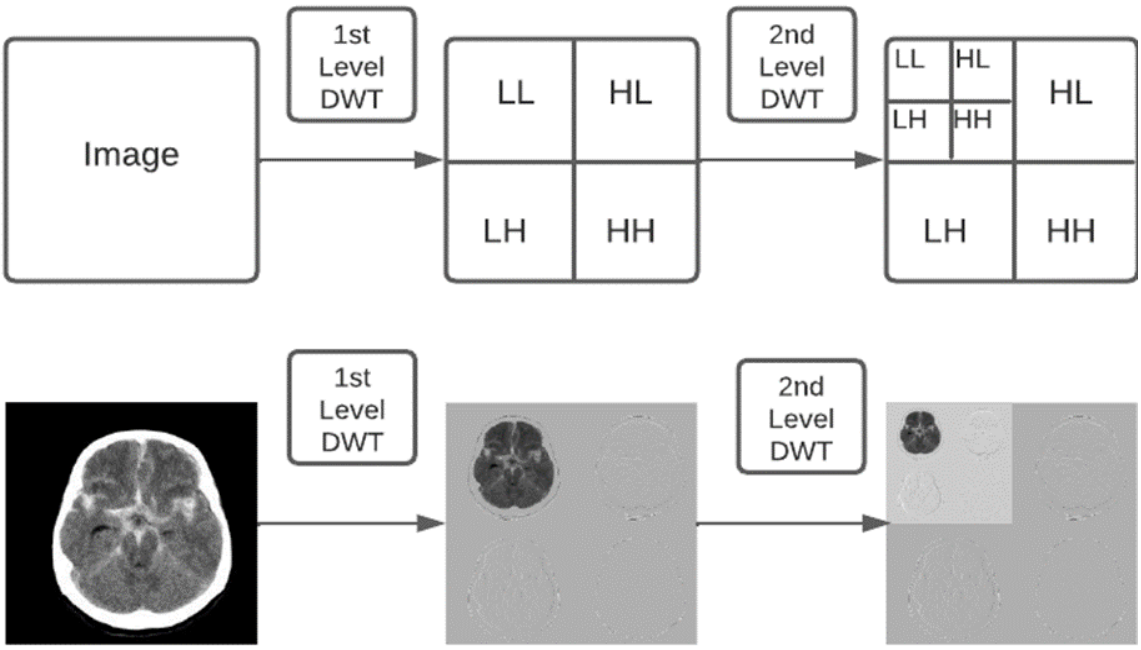

Figure 2.7: Discret wavelet transform 2D, medical image exemple

represented as $LL = LL(i, j) : 0 \leq i \leq M, 0 \leq j \leq N$, with LL(i,j) denoting a pixel value in the i-th row and j-th column of the LL sub-band.

In a wavelet transform, the primary energy of an image is concentrated in the lowest frequency coefficients and is represented by the LL (Low-Low) sub-band. However, the sub-bands denoted LH (Low-High), HL (High-Low), and HH (High-High) provide horizontal detail, vertical detail, and diagonal detail, respectively. High-scale, low-frequency signal components are found in the LL sub-band, whereas low-scale, high-frequency signal components are found in the details sub-bands (HL, LH, and HH).

The LL sub-band can be further subdivided into four sub-bands for further decomposition: LL2, HL2, LH2, and HH2. This process can be iterated until reaching the desired level of decomposition. The graphic shows an example of the two-level wavelet decomposition of a grayscale medical image (Figure 2.7).

The Discrete Wavelet Transform (DWT) finds diverse applications in signal and image processing, including denoising and image compression. When used for concealing secret information in images, DWT efficiently identifies suitable areas for data hiding. While embedding the watermark in the approximate sub-band is noticeable to the human eye, it also ensures a high level of robustness compared to other sub-bands [31].

2.6.2.2 Discrete cosine transform (DCT)

The Discrete Cosine Transform (DCT) is a transform domain technique employing the cosine function as its kernel. It operates on image frequency domains through a 2D DCT, enabling restoration from the DCT domain back to the frequency domain via inverse 2D DCT application.

For an image represented by the function $I(i,j)$ with two space variables i and j, ($i = 0, 1, ...M$) and ($J = 0, 1, ...N$) of size $M\times$ N. The 2D Discrete Cosine Transform (DCT) is acquired through Equation 2.3, while its inverse is obtained via Equation 2.4.

$$C(u,v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I(i,j) cos \frac{\pi(2i+1)u}{2M} \times cos \frac{\pi(2j+1)v}{2N} \tag{2.3}$$

$$I(i,j) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \alpha_u \alpha_v C(u,v) cos \frac{\pi(2i+1)u}{2M} \times cos \frac{\pi(2j+1)v}{2N} \tag{2.4}$$

where $C(u,v)$ is the DCT coefficient of the image $I(i,j)$ in the position u and v.
(u,v) is horizontal and vertical positions ($u = 0, 1, ...M$) and ($v = 0, 1, ...N$).
α_u and α_v values are obtains by the following equations

$$\alpha_u = \begin{cases} \sqrt{\frac{1}{M}}, u = 0 \\ \sqrt{\frac{2}{M}}, 1 \leq u \leq M-1 \end{cases} \tag{2.5}$$

$$\alpha_v = \begin{cases} \sqrt{\frac{1}{N}}, u = 0 \\ \sqrt{\frac{2}{N}}, 1 \leq v \leq N-1 \end{cases} \tag{2.6}$$

Essentially, the 2D DCT process converts the spatial pixels of an image block sized $n \times n$ into frequency domain coefficients. The outcome is an $n \times n$ coefficients matrix comprising one coefficient referred to as DC and 2n-1 coefficients termed ACs. Figure 2.8 illustrates the placement of the DC coefficient and the positions of the AC coefficients within the resulting matrix.

The DC coefficient for each 8×8 sub-block can be calculated in the spatial domain using the equation 2.7[32].

$$DC = \frac{1}{\sqrt{M \times N}} \sum_{i=1}^{M} \sum_{j=1}^{N} I(i,j) \tag{2.7}$$

In this representation, a partitioned block is denoted as a function $I(i,j)$ of two spatial variables i and j where $i = 1, 2, ..., 8$ and $j = 1, 2, ..., 8$ where $I(i,j)$ signifies the pixel value at position (i,j). In an 8-bit depth image, the value of the DC coefficient is influenced by the size of the processed block. For an 8×8 block, the DC coefficient ranges from -1024 to 1016 after adjusting the pixel values by 128.

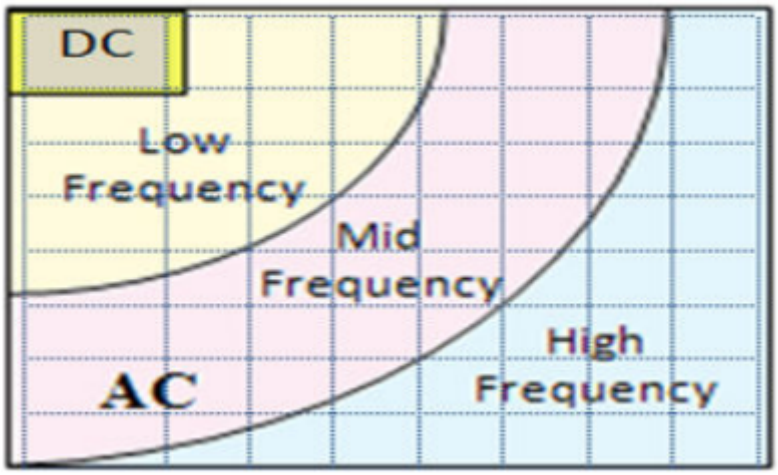

Figure 2.8: Components of the 2D DCT Procedure [21]

The characteristics of DCT coefficients establish a novel feature space for object description, with the DCT process structuring information based on its significance to the Human Visual System (HVS). Notably, crucial values for human perception are positioned in the upper left corner of the coefficients matrix, whereas less critical values are predominantly located in the lower right corner. In terms of texture analysis and HVS considerations, the DC coefficient signifies the average information about the overall magnitude of the processed block, serving as a refined property to delineate the energy of a given block. Blocks with higher energy exhibit more pronounced texture compared to those with lower energy [32].

2.6.2.3 Singular value decomposition (SVD)

The Singular Value Decomposition (SVD) is a mathematical method used to identify low-rank features in high-dimensional data without requiring prior knowledge or being constrained by fundamental physics. This method, widely employed in linear algebra, has proven highly effective in various applications, including image compression, medical image watermarking, and signal processing [33, 34]. the most SVD advantages are represented in the following:

- Any matrix, including non-square matrices, can be treated using SVD to provide a hierarchical data representation.
- Effective data compression is possible when a portion of signal energy is represented by a small number of singular values.
- SVD is known for its computational efficiency. It preserves overall data integrity and exhibits robustness against various image-processing attacks.

Researchers leverage SVD for applications such as image compression, where it helps reduce data while maintaining important features. In medical image watermarking, SVD

aids in embedding and extracting watermarks, ensuring data integrity. Additionally, in signal processing, SVD is applied for tasks such as feature extraction and noise reduction. The versatility, energy concentration capability, and computational efficiency make SVD a valuable tool in diverse fields, providing a powerful approach to analyzing and processing high-dimensional data.

SVD is a mathematical technique used to break down a matrix M of size $n \times n$ into three matrices U, S, and V. The decomposition is expressed as

$$M = USV^T \tag{2.8}$$

Several algebraic features of SVD are advantageous for several image processing tasks, including image enhancement, image reconstruction, and image coding [20]. These properties are outlined below:

- Transpose: A matrix A and its transposition A^t share the same non-zero singular value.
- Translation: A matrix A and its translated version A_{tr} maintain the same non-zero singular value. A_{tr} is derived from A by adding rows and columns composed of zero (black) pixels.
- Rotation: a matrix A and its rotated version A_r have identical non-zero singular values. A_r is obtained from A through rotation by an arbitrary angle O.
- Scaling: For a metric A of dimension $M \times N$ with singular value(σ_1, σ_2,..., σ_n), its scaled counterpart A_s has singular value equal to $(\sigma \times I\sqrt{S_(row)S_(column)})$, where $S_(row)$ is the scaling factor for rows, and $S_(column)$ is the scaling factor for columns.
- Flipping: A metric A and its flipped version A_f exhibit the same non-zero singular values. A_f is obtained by flipping around both vertical and horizontal axes.

The above-mentioned characteristics of Singular Value Decomposition (SVD) are useful for developing watermarking algorithms that aim to protect the watermark from geometric attacks while maintaining the host image's perceived quality. Little perturbations in the singular values do not result in appreciable degradation of the image's quality, and even when these singular values are exposed to different kinds of geometric image processing attacks, their geometric characteristics do not change. [35].

2.6.3 Spread-spectrum domain

The spread-spectrum technique entails transmitting a narrow-band signal over a much broader bandwidth, where signal strength is contingent on frequency, with low-frequency signals harboring more energy than high-frequency ones.

To increase resilience, spread spectrum-based watermarking incorporates the watermark into perceptually significant spectrum areas. Watermarks consisting of long random vectors with low energy are used to provide security, robustness, and imperceptibility.

Throughout the watermark embedding process, the watermark is dispersed across numerous frequency bins, rendering alterations in energy nearly undetectable. In the extraction process, faint signals from diverse bins are amalgamated to create a singular watermark.

The implanted watermark's locations and content are typically known in the watermark verification process. Spread-spectrum can be used in both the frequency and spatial domains.

2.7 Digital image watermarking attacks

The usage and processing of the watermarked data by a third party or an unauthorized one is represented as an attack. These attacks can primarily be categorized as unintentional and intentional (malicious) attacks.

2.7.1 Unintentional attacks

Unintentional attacks encompass all actions directed at eliminating or damaging the watermark present in watermarked data. These attacks can be subdivided into two groups: removal and geometric attacks.

2.7.1.1 Removal attacks

- Gaussian noise

Gaussian noise alters the variations in intensity derived from a Gaussian normal distribution. The noise value is introduced to the pixels of the input image, and its intensity can be controlled by a single parameter ranging from 0 to 100. A value of 0 signifies no noise, while 100 indicates a completely random image [36].

- Median filter

The Median filter attack functions on M×N pixels, replacing each pixel's value with the median intensity of the corresponding region. For instance, when employing Median(3), the operation is applied to a 3×3 pixel area, replacing each pixel's value with the median intensity within that region.

- Sharpening

Sharpening involves improving the quality of a gray-scale or RGB image. By increasing sharpness, the contrast is heightened specifically along edges in the image, while other areas remain unaffected.

- Blurring

A blurring attack is the inverse of the sharpening process. Its impact is to diminish high spatial frequencies. During the blurring process, information from each point is diffused into the surrounding points, resulting in the removal of high-frequency components from the image.

- Histogram equalization

Histogram equalization is a process that transforms intensity values, aligning the histogram of the output image with a specified histogram to enhance image contrast across all possible gray levels. The desired histogram is ideally flat, with an equal number of pixels at each gray level. The ideal number (Id) of pixels at each gray level is computed using the following equation.

$$Id = \frac{M \times N}{L} \tag{2.9}$$

where $M \times N$ is the image size and L is the number of gray levels.

The contrast of an image is determined by the disparity between the maximum and minimum pixel intensities, signifying the range between the darkest and brightest areas. Elevating contrast accentuates the distinction between dark and bright regions, intensifying shadow darkness and brightening highlights.

- JPEG compression

JPEG compression entails a lossy representation of processed pixels, requiring less memory for their storage. Quality factors in JPEG compression typically range from 0 to 100 for example, JPEG(5) denotes a lossy representation of processed pixels with a quality factor of 5 [36]. And it's represented by the following equation:

$$Compressionratio = \frac{Pixel'svalue}{Qualityfactor} \tag{2.10}$$

2.7.1.2 Geometric Attacks

- Scaling

The scaling attack is an attack based on scales a set of pixels up and down in the directions x and y. Its operation is defined by specific scaling factors, denoted as S_x and S_y, along the x and y axes, respectively, and represented as $x' = Sx_x$ and $y' = S_y y$.

- Translation

The translation attack is an attack based on shifts in a set of pixels by a fixed distance in both the x and y directions. The functional representation of translation is given by $x' = x + a$ and $y' = y + b$.

- Rotation

The rotation attack is an attack that involves rotating a set of pixels by an angle θ, either counterclockwise or clockwise, about the origin. The functional form of rotation is represented as:

$$\begin{aligned} x' &= x \times cos\theta + y \times sin\theta \\ y' &= -x \times sin\theta + y \times cos\theta \end{aligned} \tag{2.11}$$

- Croping

The cropping attack is an attack that crops the image by specifying four elements representing the position vector [x_{min}, y_{min}, width, height], which determines the size and position of the crop rectangle. Cropping entails the removal of rows and columns.

- Affine transformation

Affine transformation entails both vertical and horizontal distortion of the image, converting pixels between the x and y directions. The functional representation of Affine transformation is given by

$$\begin{aligned} x' &= a_{11}x + a_{12}y + a_{13} \\ y' &= a_{21}x + a_{22}y + a_{23} \end{aligned} \tag{2.12}$$

- Remove Lines (RML)

This attack eliminates lines in both vertical and\ or horizontal directions, removing sets of pixels in specific rows\ columns of the processed image. The extent of removed rows\columns can be controlled by a parameter α ranging from 10 to 100, representing the frequency of line removal. In this context, α signifies the removal of one line in every α line, subsequently reducing the dimensions of the output image [36].

- Latest Small Random Distortions (LATESTRNDDIST)

The LATESTRNDDIST attack applies a bilinear transformation to the image by displacing its corners by a small random amount. Experimental transformations on the host image can be conducted with various parameters. In the current version of StirMark, the Latest Small Random Distortions also employ a single parameter, which serves as a multiplier for the default parameters, allowing adjustment of the attack's intensity. The available parameter values include {0.6, 1.0, 1.4, 1.8, 2.2, 2.6, 3.0, 3.4, 3.8, 4.2}.

2.7.2 Intentional attacks

The intentional attacks simulated all attempts to modify the embedded watermark, render it ineffective in fulfilling its purpose, compromise the secret key utilized in the watermarking scheme, or insert an alternative watermark into the watermarked data. These attacks can be categorized into two groups: property and cryptographic attacks.

2.7.2.1 Property Attacks

- False positives

This attack entails the attacker extracting the watermark without possessing complete knowledge of the embedding algorithm. In other words, the attacker can identify a watermark in digital data that is ostensibly unmarked and does not legitimately belong to the authorized owner. This allows the attacker to falsely claim ownership of other unauthorized data by easily generating their own watermark. This type of attack is termed an unauthorized extraction attack.

- forgery

The assailant attempts to insert a new watermark of their own instead of removing the existing one. This attack is categorized as an unauthorized embedding attack.

- collusion

In this form of attack, the assailant employs multiple copies of a specific portion of digital data, each possessing a distinct watermark, to assemble a duplicate of the digital data devoid of any watermark. This type of attack is characterized as an unauthorized removal attack.

2.7.2.2 Cryptographic attacks

A prominent cryptographic attack impacting digital watermarking systems is the brute-force attack. This method involves a trial-and-error approach to discern information associated with the digital watermarking system. The attacker generates various guesses for the value of the desired information until the correct one is found. The integrity of a digital watermarking system is compromised if the attacker successfully guesses the secret or public key employed in the embedding/extraction processes. The effectiveness of the watermark against a brute-force attack is contingent on the length of the utilized key or other relevant information, with longer keys providing greater resistance.

2.8 Evaluation metrics

Before judging the effectiveness of the watermarking approaches against potential hacker attacks, The imperceptibility, and robustness of the method were tested in different manners and analyzed by various metrics.

2.8.1 Imperceptibility Test

In e-health and the medical field, the visual quality of medical images is paramount due to the sensitive information they contain. Even minor distortions can impact a doctor's diagnosis significantly. Whether the medical image is transmitted or received from another hospital, ensuring visual quality and imperceptibility is crucial. The two used metrics that can evaluate this requirement are presented in the following.

2.8.1.1 Peak Signal to Noise Ration (PSNR)

The PSNR, measured in decibels, serves as an indicator of the quality comparison between two images: the original and the watermarked version. The mean square difference ratio (MSE) is defined as the ratio of the largest possible mean square difference between two images to the actual mean square difference between them [37]. These parameters are expressed in the following equations.

$$PSNR(I, Iw) = 10 * log_{10} \frac{(MAX_I^2)}{MSE} \tag{2.13}$$

$$MSE = 1/(M * N) \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i,j) - Iw(i,j))^2 \tag{2.14}$$

Where: x,y are (i,j), Iw(i,j) the original image and watermarked one.

2.8.1.2 Structural Similarity Index (SSIM)

The SSIM serves as a commonly utilized full-reference metric to assess the visual quality of images and remote sensing data. Computed block by block, it depends on three components: the similarity of picture block means, the similarity of contrasts, and a correlation factor [38]. The metric is defined by the following equation:

$$SSIM(X, Y) = \frac{((2\mu_x\mu_y + c_1)(2\sigma_x y + c_2))}{((\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2))} \tag{2.15}$$

where: μ_x : *is the mean of X and* μ_y : *is the mean of Y*
σ_x, σ_y *are standard deviations of X and Y respectively.*
σ_{xy}*: the covariance of X and Y*c_1 and c_2 are two constant values used to avoid zero nominator

2.8.2 Robustness Test

The robustness of a watermarking framework or system indicates its ability to withstand various types of attacks during the transmission of the watermarked image over the internet. It ensures that the system can effectively counteract any applied attack, and the receiving part remains capable of extracting the hidden information. The metrics used to evaluate the watermarking framework's robustness are presented in the following.

2.8.2.1 Normalized Correlation Analysis (NC)

The mean squared error serves as a measure to identify distortions between images, representing the average squared difference between the original and watermarked images [37]. Its equation is expressed as follows:

$$NC(W, W") = \frac{(\Sigma_{(}^{m} i_{=}1_{)} \Sigma_{(}^{n} j_{=}1_{)}[W(i,j).W"(i,j)]}{(\Sigma_{(}^{m} i_{=}1_{)} \Sigma_{(}^{n} j_{=}1_{)}[W(i,j)]^2} \tag{2.16}$$

where: W, W' are original and extracted watermarks respectively, m*n: the watermark size.

when: NC=1 specifies that inserted and extracted watermark cannot be distinguished.

And when NC=0 is the smallest possible number that indicates that the original and extracted watermark images are completely distinct.

2.8.2.2 The Bit Error Rate (BER)

The Bit Error Rate (BER) quantifies the percentage of incorrectly extracted watermark bits relative to the total number of original watermark bits. A lower BER indicates a higher level of robustness of the watermark against various attacks. The calculation of BER follows the equation.

$$BER(W, W") = \frac{1}{M \times N}[\Sigma_{(}^{M} i_{=}1_{)} \Sigma_{(}^{N} j_{=}1_{)}(W(i,j) \oplus W"(i,j))] \times 100 \tag{2.17}$$

Here, w(i, j) denotes the pixel at position (i, j) in the original watermark, W"(i, j) signifies the pixel at position (i, j) in the watermarked image (W"), and M×N denotes the size of the watermark.

2.9 Conclusion

Digital watermarking garners significant interest surpassing other protection techniques owing to the escalating concerns surrounding the authenticity, integrity, and copyright protection of digital content. This chapter delineates the motivations driving the adoption of digital watermarking, outlines the requisite elements of digital watermarking systems, and

elucidates the framework underpinning digital watermarking. Furthermore, it delves into the classification of digital watermarking, various techniques employed in digital image watermarking, principles underlying attacks on digital image watermarking systems, and the array of metrics utilized for evaluating the performance of digital image watermarking.

CHAPTER 3

MEDICAL IMAGE WATERMARKING APPROACHES IN THE LITERATURE

Summary

Following the exposition of digital watermarking concepts and their fundamental components, this third chapter provides a survey of recent advancements in medical image watermarking. The overview is structured around three primary categories selected based on their relevance to our research. These categories include medical image watermarking based on application domain (spatial or transform domain), encryption techniques, and approaches using QR codes.

3.1 Introduction

Digital watermarking is utilized across diverse fields and data formats, encompassing images, audio, video, and other multimedia forms, fulfilling numerous objectives like copyright protection and multimedia authentication [39]. Additionally, it finds relevance in telemedicine applications. In these contexts, ensuring image authentication and identification is crucial without imposing significant alterations to the original data. This preserves data integrity for diagnostic purposes in telemedicine and facilitates informed decision-making in remote-sensing imaging systems. In the medical field, the proposed watermarking scheme is reversible, which means the extraction of the patient's information is available. The most important reason to suggest this approach is to hide the essential information in the medical image and make it undetectable by the HVS for many applications.

In this chapter, we present an overview of several medical image watermarking methodologies documented in the literature. These approaches are specifically devised to guarantee image authentication, identification, and security. Notably, these methods are tailored to function within either the spatial or transform domains. The following illustrates the overview.

3.2 Medical image watermarking based on Domain

3.2.1 Medical image watermarking approach on spatial domain

The approaches proposed in the spatial domain are based on the LSB, LBP techniques, and histogram modification summarized in Table 3.1. The proposed work by Sawsan D. Mahmood et al. [40] is the embedding of the watermark in the blue and green component of the oil image using the LSB technique. Gaurav Kumar Soni et al. proposed a watermarking scheme in [41] for medical images to enhance their security when transmitted on the internet using the Genetic Algorithm (GA) and LSB techniques. after creating a barcode 2D image of the patient's information and making it unreadable, they embed it in the medical image using LSB, the watermarked image is encrypted by the GA before sending it. this scheme guarantees the security of both the patient information and the medical image.

Mahboubeh Nazari et al. [42] proposed a medical image watermarking approach for various image modalities, based on embedding the watermark in the region of non-interest by applying the Integer wavelet transform (IWT), LSB, and Chaotic sequence techniques. The test results of this method on medical and non-medical images present that the proposed work enhances the payload capacity and archives the integrity and identity authentication purpose.

Table 3.1: Specifications of several proposed watermarking approaches in Spatial Domain

Work	Type of image tested	Technique used	Application Area	Results	Pros
[40]	OCT images	LSB, Chaotic system	All image	PSNR = 80 dB SSIM = 0.999 NC = 1	Integrity of patient information, Robustness against attacks
[41]	Medical image	LSB, GA	All image	–	High level of security
[42]	MRI, X-Ray, CT scan, Ultra	IWT, LSB, Chaotic- sequence	RONI	PSNR = 75dB, NC = 1	Enhance payload capacity, Information integrity, Authenticity, High imperceptibility
[43]	Chest, Heart, Shoulder, Ort, Knee images	LBP,	All image	PSNR = 50 dB	Hih level of robustness and imperceptibility
[44]	medical image	LBP, DCT, logistic map technology	All image	NC	Robustness against geometric attacks

For the application of the LBP in medical image watermarking is proposed in different works, Lamri Laouamer [43] suggests a watermarking scheme for medical images, as the watermark is constructed from notable features of the host image, specifically utilizing the LBP. Evaluations were conducted by subjecting the watermarked images to various attacks, aiming to extract the attacked watermark. This process aids in determining the robustness of the proposed approach. while Wenyi Liu et al. [44] combine the LBP technique and Dct for embedding the watermark to the medical image.

3.2.2 Medical image watermarking approach on transform domain

The watermarking approaches based on the transform domain are presented in this section and summarized in Table 3.2 where ALI ALZAHRANI et al. [45] introduced a watermarking scheme for embedding the watermark in the RONI of the medical image based on the combination of the three transform techniques; DCT, DWT, and SVD to protect the copyright of medical images. The method operates blindly, obviating the need for a host image to extract concealed information. Furthermore, the proposed approach achieves enhanced levels of imperceptibility and robustness. while Narima Zermi et al. [46] suggested a simple application of the DWT-SVD technique to add the watermark generated by patient information and

Table 3.2: Specifications of several proposed watermarking approaches in Transform Domain

Work	type of image tested	Technique used	Application Area	Results	Pros
[45]	CT scan, ULS, MRI, X-Ray	DWT, DCT, SVD	RONI	PSNR=44.0567 dB, NC = 1.000, BER = 0.000	Higher rate of imperceptibility and robustness
[46]	OCT images	DWT, SVD	All image	PSNR = 57dB, SSIM = 0.9998	Robustness against attacks and authenticity
[47]	Medical and non-medical images	HT, RDWT, SVD, AT	All image	PSNR=57.8677dB, SSIM = 0.9993, NC = 0.9999	Enhanced imperceptibility and robustness
[48]	medical and non-medical	RDWT, RSVD, MRFO	All image	PSNR = 60,97 dB SSIM = 0.9998 NC = 0.9999	A balance among robustness, capacity and imperceptibility
[49]	Medical images	HFQM, RDWT, DWT, MRSVD	All image	PSNR= 90.31dB, SSIM = 1.000, NC = 1.000	Excellent results in imperceptibility and robustness
[50]	CT scan images	RDWT, RSVD, HD, DNN	All image	PSNR=47.0922dB, SSIM=0.9997, NC = 0.9918, BER = 0.000	Higher level of authentication, enhance the security and robustness
[51]	Medical image	DWT, SVD	All image	PSNR= 44.986dB SSIM = 0.997	Imperceptibly and robustness
[52]	Non-medical image	DWT, DCT, SVD	All image	PSNR = 40 dB, SSIM = 0.99	Robustness against various attacks with good imperceptibility
[53]	MRI, CT scan, ultrasound, Doppler, X-ray, Mammograph, skin, retina, PET	DWT, SVD, LZW compression	RONI, ROI	PSNR= 43.99 dB SSIM = 0.9244, NC = 0.9999, BER = 0.000	Scheme has higher, similar robustness against common attacks and higher imperceptibility
[54]	Medical image	IWT, SVD, FPGA	All image	PSNR=47.622829, SSIM= 0.961754, NC = 1.000954	Robustness, security and imperceptibility
[55]	Medical and non-medical images	IWT, MVs	All image	PSNR=53.4976dB, SSIM = 0.9996	Its higher embedding capacity
[56]	OCT images	DWT, SVD, XOR	Hole image	PSNR = 54 dB	Good Imperceptibility

medical image fusion in the cover image.

The redundant discrete wavelet transform (RDWT) has been proposed in many approaches, where Priyank Khare et al. [47] apply it with SVD and homomorphic transform (HT) technique. while Ranjana Dwivedi et al. [48] apply the RDWT with randomized singular value decomposition (RSVD), Henon mapping, and Manta ray foraging optimization (MRFO). but M. Sajeer et al. [49] combined the RDWT with a Hyperchaotic System-Fibonacci Q Matrix (HFQM) encryption system and a Multi-resolution Singular Value Decomposition (MSVD). All these proposed approaches enhanced the robustness and imperceptibility of the medical image watermarking, and execution time process and tested against various attacks to evaluate the shame security.

Anand et al. [50] present a robust and dual watermarking approach for COVID-19 CT scan images based on redundant discrete wavelet transform (RDWT), Hessenberg Decomposition (HD), and randomized singular value decomposition (RSVD). Several watermarks in the form of text and medical images from Electronic Patient Records (EPR) are included on the cover to provide a high degree of authenticity. While Singh et al. [51] proposed a medical image watermarking method based on the frequency domain, this method applies the DWT and SVD techniques to put the watermark image into the medical cover image. It achieves the security of data and robustness against various attacks.

The main goal of the project proposed by Mokashi et al. [52] is to develop a method for cuffing images inside other images utilizing biometric characteristics, specifically fingerprint and signature, and watermarking methods. A combined watermarking approach called DWT-DCT-SVD is planned for picture authentication that is impervious to assaults to achieve this. It combines discrete wavelet transform, discrete cosine transform, and singular value decomposition. Using DWT-DCT-SVD yields the unique values of watermarks 1 (fingerprint) and 2 (signature) in this instance. SINGH et al. [53] proposed a regional watermark based on the watermarked ROI on top of the RONI, with the hospital logo QR and the EPR encrypted in the frequency domain using the DWT-SVD algorithm. This method provides imperceptibility and robustness against different geometric and non-geometric data while ensuring data security.

In the scheme proposed by Arumugham et al. [54] The medical image watermarking is based on two parts, the embedding process of the watermark in the cover image applying the IWT and SVD, then the use of Lü chaotic attractors and Tent map for DICOM image encryption. The method is secure against various attacks. It's achieved imperceptibility, confidentiality, and integrity. But Alquhayz et al. [55] add the watermark image bit in the medical image and the image sequence in the temporal domain by applying seven block-

matching techniques, and frequency domain by using IDW and motion vectors (MVs) to supply a structure for copyright protection and integrity verification.

The approach proposed in [56] by George Klingt et al. is based on the embedding of the EPR text into the OCT image after using the DWT and SVD techniques to achieve a good imperceptibility of the medical data.

3.3 Medical image watermarking combined with encryption techniques

To enhance the security level of the patient information hidden in the medical image, many approaches combine watermarking and encryption techniques. There are two ways or processes for this combination: 1) First process: encrypting the watermark of general data or image representing the EPR, then embedding it in the medical image to increase the security of this information. or 2) Second process: embedding directly the watermark in the cover image, then encrypting the watermarked image, and transmitting it to the open network as an encrypted image. It can enhance the security of the medical image and the watermark within it.

On the other hand, the encryption techniques are decomposed into three categories as presented in Figure 3.1: The classical encryption techniques are combined with many medical image watermarking techniques such as homomorphic encryption [57, 58], and hill cipher encryption [59]. these techniques belong to the substitution encryption technique and it refers to a replacement method that entails substituting the letters, integers, or symbols of the plaintext with alternative counterparts. When the data is viewed as a sequence of bits, substitution involves altering the bit patterns in the plaintext with corresponding cipher text bit patterns.

Table 3.3: Specifications of several proposed watermarking approaches combined with encryption techniques.

Begin of Table					
Work	Type of image tested	Technique used	Application Area	Results	Pros
[57]	Medical image	Homomorphic, chaotic map	ROI, RONI	PSNR=31.1018 SSIM = 0.9866	Increases the security of medical data and improves the visual quality of medical images

Continuation of Table 3.3

Work	Type of image tested	Technique used	Application Area	Results	Pros
[58]	Medical image	Homomorphic encryption, wavelet fast fuzzy algorithm	All image	PSNR=49.55	Medical data hiding security
[59]	Non-medical image	Hill cipher LSB	All image	PSNR=45.2575 MSE = 1.9378	The security of the watermark by encrypting it
[60]	Medical image	AES encryption, AT	All image	PSNR = ∞ SSIM = 1.000	Enhance the security and imperceptibility
[61]	Medical image	AES-GCM, FTBM	RONI	NC = 1.000 BER = 0.000	The approach achieves the imperceptibility, robustness, and security
[62]	medical image	AES, ECC, SHA-256	ROI	PSNR=44.54 NC = 1.000	The scheme based on the face image to improve the security of the crypto-watermarking system
[63]	Medical image	DWT, DCT, RSA	ROI, RONI	NC = 1.000 BER = 0.000	The method is used multiple watermarking and achieves good robustness and imperceptibility
[64]	Medical and Non-medical image	hyper-chaotic system, zero watermarking, RSA, DWT	All image	PSNR=60.52	The technique has been used to secure the communication of multimedia data over 6G networks.
[65]	Non-medical image	DCT, DH key exchange	all image	PSNR=64.13, NC=0.99, SSIM=0.99	Security and robustness against various attacks

Continuation of Table 3.3

Work	Type of image tested	Technique used	Application Area	Results	Pros
[66]	Medical and non-medical image	IWT, SVD, DH KEY exchange	All image	PSNR=61.0689 NC=1.000 SSIM=0.9995	Enhance the secure technique such as confidentiality, authenticity, and non-repudiation with high upload capacity
[67]	Medical image	DCT, DWT, ECDH	All image	–	Provide the confidentiality, authenticity of the medical image
[68]	Medical image	DWT, DCT, Hash function	RONI	PSNR=72.961 NC= 1.000	Increase the security and robustness
[69]	Medical image	ZW, CNN, LBP, Zig Zag, DNA, Hyperchaotic system	All image	Entropy= 8, BER = 0.1000 NC = 0.1000	Hih level of security against various attack types
[70]	Medical image	QPHT, ZW, chaotic system	All image	PSNR=41.2815, BCR=0.9993	Color medical image copyright protection
[71]	Medical image	NSCT, RDWT, SVD	All image	PSNR=38.6088 NC = 0.9988	The approach robust, imperceptible, secure and suitable for medical applications.
[72]	Medical image	SMFMF, DWT, SVD, chaotic systme	All image	PSNR= 49.3, NC = 0.991	Achieves robustness and imperceptibility

End of Table

The modern encryption technique also is combined with medical image watermarking techniques widely, many searches test the symmetric technique which uses the same encryption key to encrypt and decrypt the data such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and X-BOX encryption [60, 61, 62]. the asymmetric en-

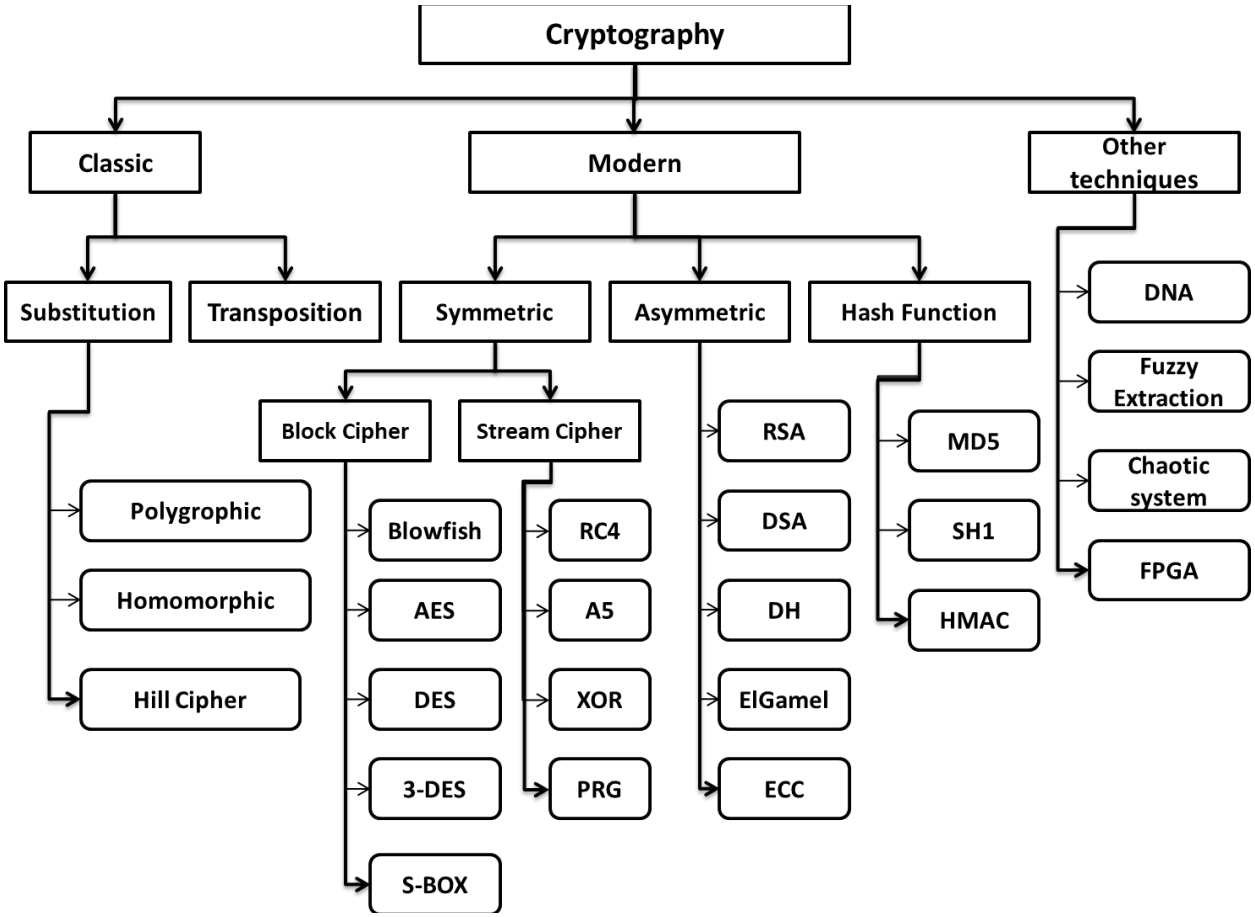

Figure 3.1: Taxonomy of Encryption Technique

cryption algorithm uses two encryption keys, one for the encryption process and the second for decryption; the most techniques combined with medical image watermarking are the RSA encryption algorithm (named by his three creators: Ronald Rivest, Adi Shamir, and Leonard Adleman) [63, 64], Digital Signature Algorithm (DSA) [73], Deffie Hellman, ELGamel, and Elliptic curve cryptography (ECC) [65, 66, 67]. that algorithms applied for encryption key generation or exchange between the sender and the receiver also, used for patient data encryption. and the last encryption algorithm in the modern encryption is the hash function, it's is a one-way function, also named a digest function, and it transforms a message M to a value h called a hash. which can be used to examine the integrity of the data to see whether the message has been damaged or as a digital fingerprint for a message [68].

Other encryption techniques are applied for medical image encryption, but its application with the medical image watermarking is for EPR data encryption such as DNA encryption, [69], chaotic system [70, 71], Fuzzy extraction and FPGA [72, 74].

This combination of the watermarking techniques and encryption algorithm enforces the security of the medical information hidden in the cover image and also it can resist various

attacks in the open network when it transmits. Its strength depends on the difficulty of finding the encryption key and affects the complex process and the execution time, the medical image watermarking approaches based on encryption techniques are summarized in Table 3.3.

3.4 QR code application in the medical image watermarking

The QR code was initially introduced by Denso Wave in 1994 to track vehicle parts. Subsequently, it experienced rapid development and found widespread application across various fields. Phones are widely used as QR code readers due to their capacity to display the code and convert it to a format that may be used. QR codes make it easier to download mobile apps, share contact information, connect to Wi-Fi networks, and retrieve specialized information such as product manuals or website URLs. QR codes are also used for product tracking and authentication, making it possible to easily verify the origin and details of a product [75]. In the security field, the QR code is used for authentication and authorization of a user to verify their identity, temper detection, secure data transfer, and security communication by encrypting and decrypting data using the QR code, also it can be used in steganography and watermarking techniques [76].

In the existing body of literature, it is observed that the utilization of quick response codes in the medical image watermarking application is limited, with only a few studies incorporating its application. where Weixia Chen et al. [77] proposed a medical image watermarking approach based on the QR code resistant to print-scan in the transform domain applying DWT-SVD, the method embedded the encryption QR code of the medical information by Arnold transformation in the singular value component created by the SVD technique. The suggested method strongly resists geometric and common attacks, such as rotation, scaling, cropping, translation, JPEG compression, common noise, and filtering, surpassing alternative approaches. Additionally, the live code extracted from this scheme can be successfully decoded using mobile devices and other scanners. while PRIYANKA SINGH et al. [53] use the QR code to represent the hospital logo and embed it in singular value of the RONI of the medical image with the EPR and the vector of the ROI bits after applying the DWT-SVD technique. the scheme achieved imperceptibility, security, robustness, and temper detection.

A medical image watermarking study based on a QR code proposed by C. Kavitha and S. Sakthivel [78] introduces two zero watermarking algorithms for authenticating medical images. One method employs singular-value decomposition, while the other utilizes

the composite CT-SVD domain, where the watermark image is the QR code of the admit discharge transfer—admit patient message. Experimental evaluations with medical images demonstrate the proposed model's suitability for healthcare institutions. The scheme proves highly resilient against diverse attacks, ensuring robust authentication of medical images. Furthermore, it enables remote radiologists to access additional clinical information. The scheme proposed by Jian Li et al. [79] is a medical image watermarking scheme based on the visible encrypted watermark by using Arnold map, this watermark represents the patient information in the QR code form.

The application of the QR Code in many approaches can achieve many advantages points as empowers the storage and transmission of medical image data in open network environments, ensuring the secure handling of such data. Enables the secure transmission and storage of medical image data while supporting the full recovery of encrypted sensitive regions within the image. Features a substantial storage capacity, rapid identification speed, and robust resistance to tampering. Delivers encryption and anti-counterfeiting capabilities, adding significant value to the process.

3.5 Conclusion

Several image watermarking approaches are presented in this chapter. These approaches are presented through four categories; the first presents a medical image watermarking approach based on spatial and transform domains. The second category presents a set of medical image watermarking approaches combined with encryption techniques, the third category presents a set of medical image watermarking approaches that use the QR code in the generation watermark process.

The majority of the proposed methods primarily utilize spatial domain techniques, such as the LSB technique or the LBP, where the watermark is generated from the extracted features. These approaches are known for their simplicity in implementation and rapid processing. Conversely, methods based on the transform domain often integrate techniques like DWT with SVD or DCT with SVD, sometimes in combination, to bolster security and meet robustness requirements.

The primary aim of integrating encryption into medical image watermarking is to elevate the security level of the embedded Electronic Patient Record (EPR) within the image. By encrypting this information, it becomes challenging for unauthorized individuals to decipher, even if detected. this refers to the challenge of knowing and identifying the encryption key.

In the third category discussed in this chapter, which revolves around Quick Response codes, many of these methods involve converting hospital logos or small data sets into QR codes to reduce the capacity of the data, thereby enhancing their efficacy.

CHAPTER 4

WATERMARKING APPROACH FOR SECURE EPR TRANSMISSION APPLIED TO E-HEALTH

Summary

This chapter constitutes our first contribution to medical image watermarking. The publication discussed in the last chapter has presented different methods of medical image watermarking based on domain application, combination with encryption technique and QR code. But they don't benefit from the power and the advantage of the QR code, which is applied to represent a hospital logo or a small amount of patient data, where it's possible to covert a high-capacity document to a small binary image is a QR code and solve the first part of the watermarking trade-off requirement which is the capacity, and automatically its effect of the image imperceptibility. This chapter presents two proposed solutions; one of them is based on the LSB technique and the second is addressed to solve the problem of imperceptibility and payload capacity using QR code with the presentation of results obtained and the evaluation of its performance..

4.1 Introduction

The advancement of telemedicine and e-health technologies has facilitated the exchange of patient images, EPR, and MITR among doctors and hospitals to enhance patient diagnoses. However, this data transmission is susceptible to attacks where patient information may be misused or altered [3]. To secure such transmitted data within the Internet of Medical Things (IoMT), various watermarking techniques have been devised [80]. Digital watermarking involves the embedding of confidential information (EPR, Patient ID, doctor's information, MITR) into the cover medical image [53, 81]. However, when this additional data has a high loading capacity, it may compromise the visual quality of the medical image, potentially distorting critical medical information. In response, researchers have explored and devised new methods to increase payload capacity without compromising visual quality. Additionally, digital watermarking finds applications in copyright protection [82], patient data authentication [83], integrity verification, and security enhancement [84].

The suggested approaches for medical image watermarking rely on two domains: the spatial domain utilizes the LSB technique due to its simplicity and quick implementation, while transform domain techniques prioritize security and robustness by transforming data into different coefficients depending on the technique employed [85].

The integration of image watermarking and encryption techniques in the proposed scheme enhances its robustness, ensuring the safety of Electronic Patient Records (EPR) [86]. A widely employed technique in the medical field is Quick Response (QR code), a two-dimensional barcode representing specific items. This technique augments the payload capacity of the watermark by reducing its bits and fortifies the security of the EPR [87]. While the literature commonly uses this technique for transforming hospital logos or basic patient information into QR codes, its potential extends to addressing the high payload capacity of medical image report documents by encoding them into smaller images.

4.2 Medical Image Watermarking using DWT and LSB techniques

One of the earliest techniques utilized in digital image watermarking, and still widely applied today, is the LSB (Least Significant Bit) technique. It is preferred due to its simplicity of implementation and computational efficiency [88], It relies on substituting the least significant bit within the image pixel with the corresponding watermark bit, which could encompass text, images, audio, or other data. In medical imaging, the watermark typically represents Electronic Patient Records (EPR). However, this technique lacks robustness against attacks

and is susceptible to simple decryption. To bolster its resilience, it is often combined with transformative techniques like DWT, DCT, and SVD.

4.2.1 The Proposed Method

The proposed method is on the embedding of the EPR like a watermark in the frequency domain of the RONI. For the embedding algorithm section; the original medical image is processed and filtered to enhance, before the separation of the two regions. The application of DWT in level 2 can decompose the RONI into 4 sub-bands and use the LL2 sub-band to limit the location of the watermark. On the other hand, the EPR character is converted to the ASCII code than binary. The LL2 band is the band that contains the approximation coefficient, we will treat this part as an image and we will add the bits of the EPR bit by bit in it, it is an application of the LSB algorithm in the frequency domain. After the embedding of the watermark is done, apply the DWT inverse to get RONI watermarked then the medical image is watermarked by combining the two regions of the image (see block diagram in Figure 4.1). The steps of the watermark embedding are represented as follows:

Algorithm 1 Embedding Algorithm

Require: Patient's Information, Cover Medical image
Ensure: Watermarked medical image

1: Read the medical image and apply the sharpen filter to enhance it.
2: Apply the Snack segmentation to the image and separate the RON and RONI.
3: Rpply the second level of DWT on RONI to obtain LL2 sub bond. Then, Read the EPR character and convert it to ASCII code then to binary .
4: Calculates the LSB of each pixel of the LL2 sub-bond and replaces it with each bit of EPR one by one.
5: Applies the inverse of DWT on the RONI by replacing the LL2 with the LL2 obtained in step 4.
6: Gets the watermarked image by combining the two image areas ROI and RONI obtained in step 5.

For the extraction algorithm section, get the watermarked image and separate the two regions, apply the DWT in the second level to obtain the LL2 sub-band which the watermark is excited and extracted and converted to the ASCII code then to the character mentioned in (fig. 3b). The steps of the watermark extraction are represented as follows:

4.2.2 Measurements and results analysis

For performance evaluation, the proposed approach is examined on grayscale medical images in different modalities like IRM (images 1, 2, and 3), PET (image 4), and OCT (image 5) images of various sizes, then we resize the small size image to be 512× 512 pixels for more evaluation and comparison. The watermark tested has 12 characters, and the results are

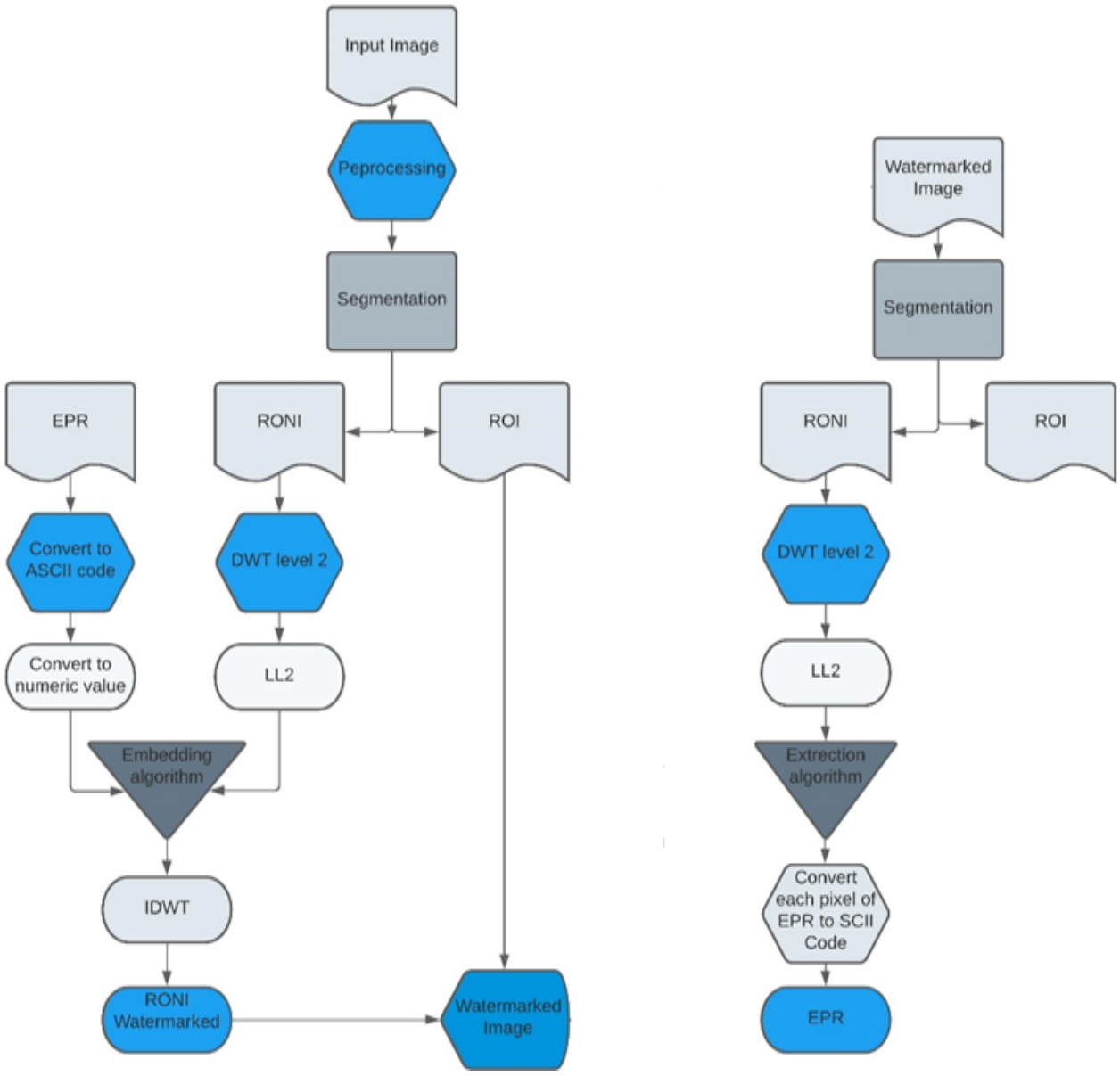

Figure 4.1: Block diagram of the proposed medical image watermarking based on DWT and LSB techniques, embedding, and extraction algorithm

Algorithm 2 Extracted Algorithm

Require: Watermarked medical image
Ensure: Patient's information
1: Read the watermarked image then separate the ROI and RONI.
2: Apply the second level of DWT on RONI to obtain LL2 sub bond.
3: Calculate the LSB of each pixel of LL2 sub-bond.
4: Retrieve bits and convert each 8 pixels into a character and obtain the EPR.

performed on the platform of Core i3, 1.70GHz CPU, 4 GB RAM, MATLAB R2020a. For evaluating the watermarked image perceptibility, we use some quality metrics like PNSR, MSE, and NC.

Table 4.1: The PSNR, SNR, and NC of the proposed approach

Images	Image sie	PSNR	SNR	NC
Image 1	287x230	40.4146	36.1154	0.9986
	512x512	46.4039	42.0824	0.9997
Image 2	512x512	46.4039	37.0435	0.9999
Image 3	283x211	39.9792	33.1776	0.9996
	512x512	46.4039	39.4427	0.9999
Image 4	287x230	40.4146	34.0898	0.9992
	512x512	46.4039	40.0675	0.9998
Image 5	512x512	46.4039	35.3562	0.9999

Table 4.1 shows the 3 parameters values PNSR, SNR, and NC for the 5 medical images with different modalities and sizes, the images (1, 3, and 4) are evaluated first in the average size, and their PSNR value is between 39.9792 and 40.4146, for better comparison, we resize this images to will be in 512*512 size like other, their PSNR value reaches to 46.4039 with the same number of bit of EPR.

The human visual system (HVS) will struggle to detect changes between the original image and the watermarked one if the PSNR value is more than 30. So the imperceptibility of the watermark will be better and make it more secure against attackers that are clearly verified in the PSNR value of the proposed method.

The SNR values are used in image watermarking to evaluate the performance of the method and compare the quality of images and distortion between the original and watermarked images. When the value of SNR is more than 32dB it means that the watermarked image has an excellent quality. In the **Table 4.1** the last value of SNR is equal to 33.1776dB and the highest value is equal to 42.0824Db, that's means that the quality of the medical image watermark excellent and the necessary information about the patient's illness is not changed.

The NC values of the proposed method are between 0.9986 and 0.9999, and they are reaching 1, this means that the EPR hiding in the medical image is the same extracted data from the watermarked one, which means that the hiding data are authenticated.

Figure 4.2 represents the histogram analysis of both the medical image and the watermarked one, it shows the similarity between them for each image and explains the value of the SNR and PSNR. And **Table 4.2** shows the comparison of 4 existing schemes [89, 90, 91, 92] when no attack is applied with the proposed method, its PSNS value reaches 46.4039 dB, and it is higher than the PSNR values of other schemes.

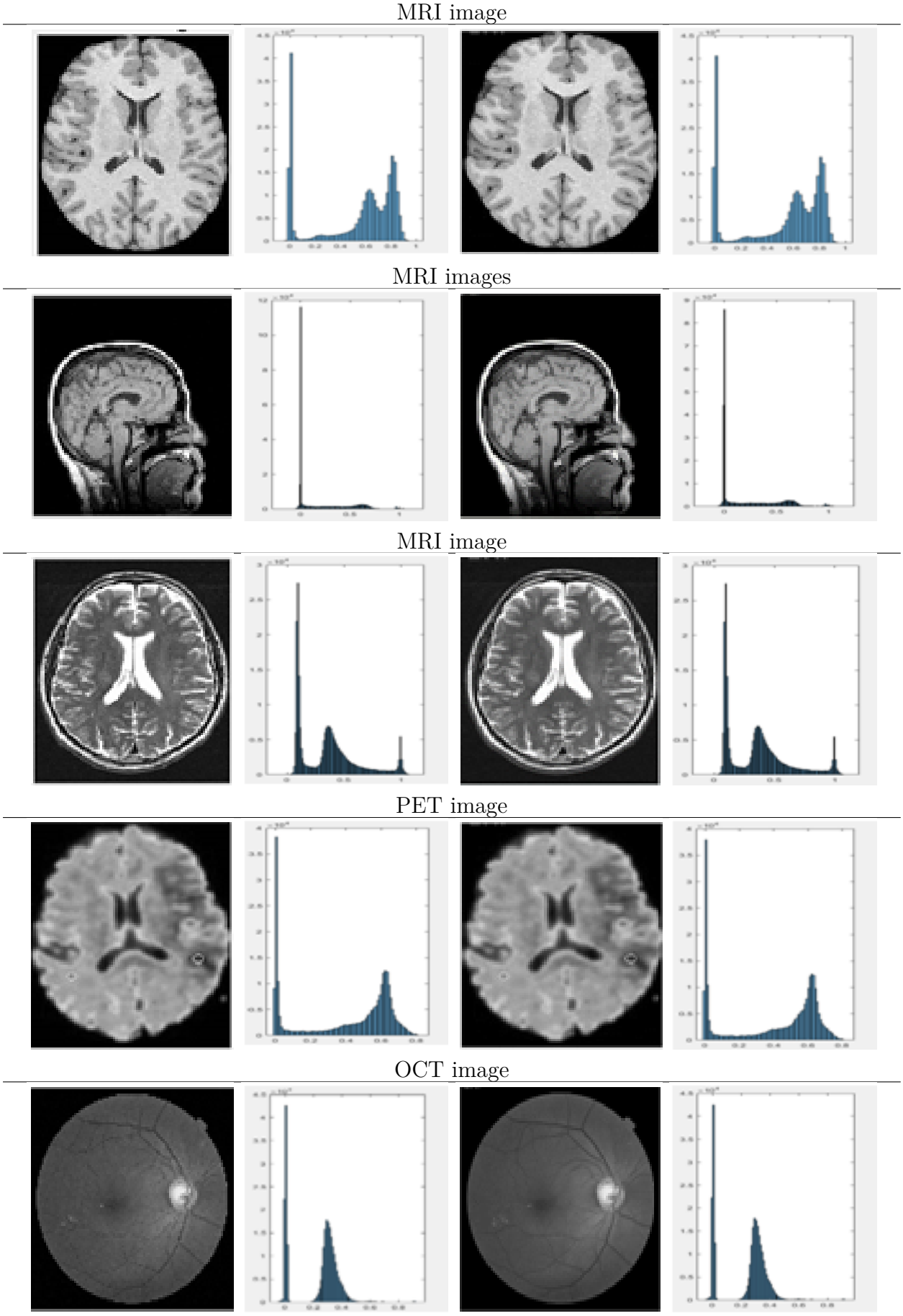

Figure 4.2: Histogram analysis of the original and watermarked image, first column: Original medical image, second column: Original medical image Histogram, third column: Watermarked medical image, and last column: Watermarked medical image Histogram

Table 4.2: Imperceptibility results in comparison with literature methods

work	Technique used	Application domain	PNSR value (dB)
[89]	RC4 for encryption DFT	Medical image	PSNR = 44
[90]	Human visual system (HVS) Model Image processing operations	Medica image	PSNR = 38.01
[91]	DWT Elephant Herding-Monarch Butterfly (EH-MB) Optimization algorithm	Medical image, Non medical image	max PSNR=42.1776, for medical image. maxPSNR=38.01444, for Lena
[92]	DWT-SVD, ECC, Chaotic-LZW	Mdica image, Non medical image	PSNR = 44.1944
Proposed method	Snake segmentation DWT, LSB Algorithm	Medical image	PSNR = 46.4039

4.2.3 Discussion

The LSB algorithm is a technique used in the spatial domain for hiding data bits in the last signification bit of the cover image, to make the embedding data more robust, we apply it in the frequency domain. The approach is based on the Haar wavelet to transform the RONI to the frequency domain, trait the LL2 band like the new cover image, and hide the EPR in it by the LSB algorithm. For the watermarked original medical image we apply the IDWT and combine the ROI with RONI watermarked. The experimental results show that the proposed method has good values in SNR, PSNR, and NC. That represents the impeccability and security of the EPR embedding, and good image quality without destroying the necessary health information which is exciting in ROI.

4.3 Rigion-based medical image watermarking approach for e-health application

The combination of the spatial and transform domain technique in the first proposed method by applying the LSB and DWT techniques is efficient, and it gives good results in terms of the imperceptibility present in the PSNR value that is attending to 46.4039dB, which means that the watermark hiding in the medical image is not detectable by the human visual systems. However, the problem with this method is that the watermark is only 12 characters. If we require incorporating high-capacity patient information, the image quality will decrease, and the perceptibility of the medical image will be altered as the PSNR value decreases.

So the novel watermarking algorithm introduced in this contribution operates in the frequency domain, utilizing the second level of the discrete wavelet transform (DWT) and singular value decomposition (SVD) on the LL2 sub-band. The QR code image of the medical imaging test report is incorporated into the S component. One distinctive feature of this method is maintaining a fixed size for the watermark image, irrespective of the size of the generated test report document after the examination. Thus, the key contributions of this work include:

- Ensuring the security of patient information within medical images during segmentation by exclusively adding the watermark image to the RONI, preserving all illness-related information in the ROI without distortion. Another critical aspect is the security of the MITR information when transformed into the QR code, which remains non-readable without a QR reader.
- Facilitating a substantial payload capacity to accommodate all Medical Imaging Test Report (MITR) documents.
- Attaining imperceptibility of the embedded watermark within medical images while safeguarding the security of patient information.
- The objective of this approach is to increase the payload capacity of medical images while maintaining the integrity of the important medical data.

4.3.1 Examination Report

This is an official document prepared by a certified radiologist to interpret and analyze the MRI images obtained during the examination. It is a comprehensive and confidential report that contains important details about the patient's condition, medical history, and personal information. Unfortunately, this document lacks the advanced data protection measures found in current health information watermarking techniques. Despite its vulnerability, the report is transmitted at a high rate since healthcare providers can make decisions without waiting for the radiologist's analysis, allowing prompt treatment by the appropriate specialists.

4.3.2 Quick response code

A Quick Response code (QR code) is a binary pattern of white and black pixels, forming a two-dimensional barcode. Functioning as an optical label, QR codes can be recognized by devices to retrieve information related to the associated object or item. Noteworthy characteristics of QR codes include their compact size, swift readability from multiple angles, language support, error correction capabilities, and increased storage capacity. QR codes

Patient medical imaging test report

Patient : xxxxxx xxxxxx
Id_ patient :11111111
Téléphone : 00000000

Indications :
Clinique = *TR : nodule palpable ? : T1 ou T2 ; doute sur extension : T3 ?*
Taux de PSA = ng/ml
Résultats des biopsies (date) = nombre de sextans envahis, pourcentage d'atteinte des carottes, score de Gleason.

Technique :
Séquences axiale T2, frontale T2, axiale T1, axiale T1 dynamiques avec injection intraveineuse de gadolinium.

Conditions d'examens :
Bonnes, moyennes, mauvaises.
Artéfacts : *oui/non*, type
Séquelles biopsiques en pondération T1 : *oui/non.*

Résultats :
Volume prostatique (hauteur x largeur x épaisseur en cm / 2) = cm soit cm3.

Analyse du signal :
=> De la zone périphérique :
- Plage suspecte : *oui/non*
  - Nombre, signal T2 et après gado, localisations : *sextants*
  - pour chaque lésion : mensurations, volume, forme, contact capsulaire ,zone transitionnelle
- Extension capsulaire : *non/possible/probable*
  - contact
  - déformation régulière
  - déformation irrégulière
  - comblement d'un angle prostato-rectal
  - comblement d'une bandelette neuro-vasculaire
- Extension aux vésicules séminales : *non/possible/probable*
  - localisation par rapport aux canaux éjaculateurs
  - anomalie de signal vésiculaires : *uni-bilatéral ; focal-diffus*

=> De la zone transitionnelle :
- Hyperplasie bénigne : *oui/non*
  - volume
  - lobe médian
- Plage suspecte : *oui/non*
  - forme
  - signal T2, PDC sur la séquence dynamique
  - Atteinte un ou deux lobes
  - Atteinte du stroma fibro-musculaire antérieur

=> Atteinte ganglionnaire : *non/possible/probable* : Ganglion de grand axe > 8 mm, localisation

=> Vessie, rectum, uretère : *non/possible/probable.*

Conclusion :

Compte tenu du contexte de risque d'extension (clinique, PSA, Gleason) :
Faible : PSA ≤ 10 ng/ml ; Gleason ≤ 6
Intermédiaire : PSA 10 – 20 ng/ml ; Gleason ≤ 7
Elevé : PSA > 20 ng/ml ; Gleason > 7

Visibilité d'une lésion évocatrice d'une néoplasie *postérieure/antérieure/mixte* occupant *sextans/lobes* avec envahissement *absent/possible/probable* de la capsule, *absent/possible/probable* de une/deux vésicules séminales, avec envahissement *absent/possible/probable* de une/deux deux bandelettes neurovasculaires.
Adénomégalie associée : *oui/non*
Autres : *oui/non*

Staging TNM IRM :

Figure 4.3: Patient's medical imaging report and his QR code image

efficiently encode data in a binary image format, facilitating rapid and precise scanning while accommodating the storage of substantial amounts of information.[93, 30]

4.3.3 Proposed approach of region-based watermarking for EPR transmission

4.3.4 QR Code of the Patient's Medical Imaging Test Report

The medical imaging test report, authored by a radiologist on behalf of the ordering doctor, is a comprehensive document containing the radiologist's analysis of collected medical images. Sent to the healthcare professional who requested the test, the report transforms to be embedded in the Region of Non-Interest (RONI) of the cover. This process involves reducing the medical image size without data loss and converting the report into a QR code—a two-

dimensional barcode with black-and-white pixel patterns. Figure 4.3 illustrates the imaging test report and its corresponding QR code, while Algorithm 3 outlines the necessary image processing steps before embedding and extraction (Figure 4.4).

Algorithm 3 Require preparation

Require: Patient's Medical Imaging Test Report, Cover Medical image
Ensure: RONI, QR code
1: Processing the medical image and filtering it.
2: Use a segmentation algorithm to separate the ROI and the RONI.
3: Get the QR code image of the patient's medical imaging test report.

4.3.4.1 Embedding watermark process

The watermark embedding process is shown in Figure 4.4, and the corresponding steps are detailed in Algorithm 4. In the case of the Region of Non-Interest (RONI) image, a two-level discrete wavelet transform (DWT) is employed. This results in four sub-bands—LL1, LH1, HL1, and HH1—obtained through DWT, representing the approximation, horizontal, vertical, and diagonal components. In scenarios involving multi-level wavelet decomposition, the process includes dividing the approximation coefficient or one of the level 1 sub-bands. The sub-bands LL2, LH2, HL2, and HH2 are derived from LL1 in the second level of the discrete wavelet transform (DWT) applied to the Region of Non-Interest (RONI), as illustrated in Figure 4.6. Since the HH sub-band carries crucial image data, any modifications to it can lead to distortions in the cover image. To mitigate this, the LL2 approximate sub-band is utilized to constrain the watermark.

The analysis of square and rectangular matrices is a mathematical procedure commonly employed in image security applications to determine the Singular Value Decomposition (SVD) matrix of the image. When watermarking is implemented, it is typically done by computing the SVD matrix of the LL2 sub-band and subsequently working with the three matrices U, S, and V obtained from the SVD process. This process is represented by the following equation:

$$M_{LL2} = U_{LL2} \times S_{LL2} \times V_{LL2}^{T}. \tag{4.1}$$

The embedding phase of this step concludes by scaling the QR code of the imaging test report with a specified scaling factor, as expressed in the following equation:

$$S = S_{LL2} + \alpha \times QR \tag{4.2}$$

The watermarked RONI' image is produced by reversing the SVD to obtain the watermarked LL2' using equation 4.3 and subsequently applying a 2-level DWT to create the

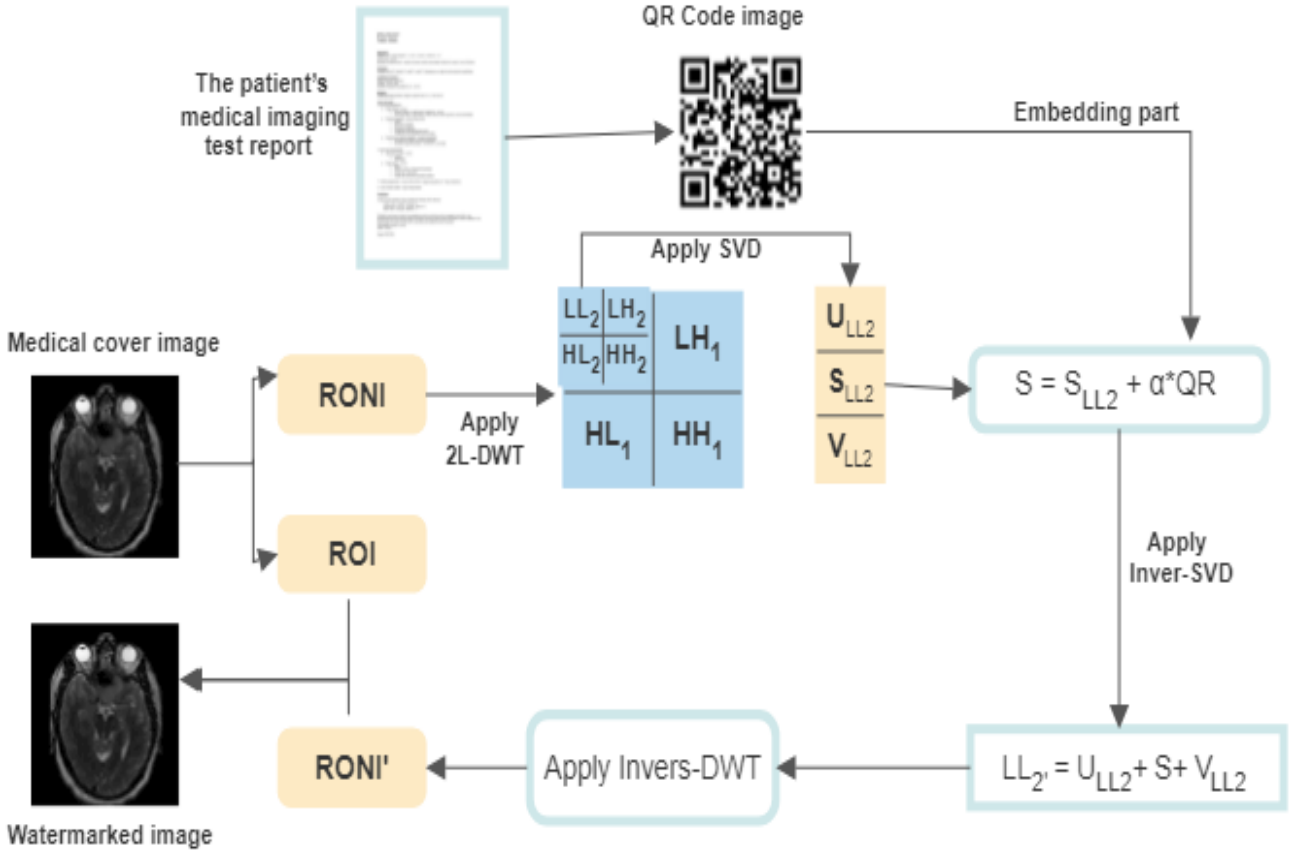

Figure 4.4: Watermarking embedding process

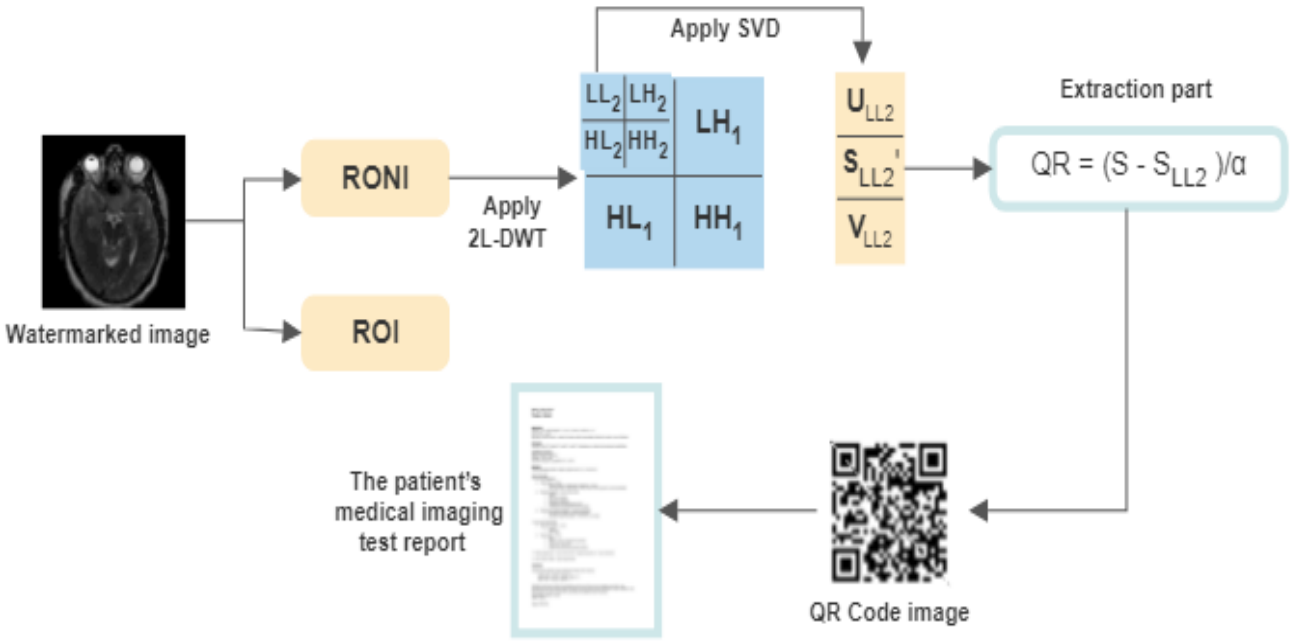

Figure 4.5: Watermarking extracting process

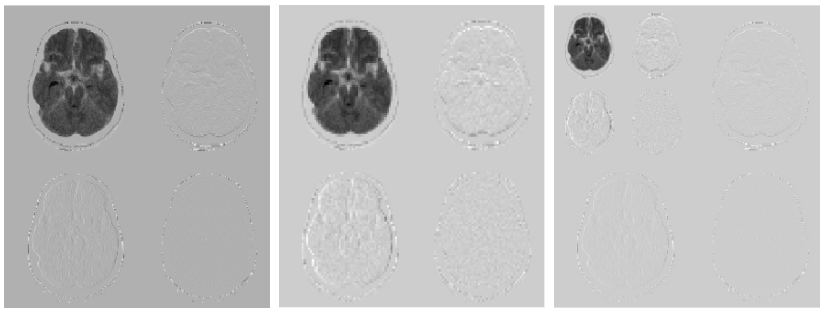

Figure 4.6: 2-level DWT decomposition of medical image

watermarked image (RONI'). The integration of RONI' and ROI results in the watermarked medical image.

$$M_{LL_2'} = U_{LL2} \times V_{LL_2'} \tag{4.3}$$

Algorithm 4 Embedding Process

Require: RONI, QR code
Ensure: Watermarked RONI
Apply the second level of DWT on RONI to obtain the LL2 sub-bond.
2: Apply the SVD algorithm on LL2 and get the three components U LL2, S LL2 , V LL2.
Embedding watermark by the following equation: S' = S + QR code.
4: Apply inverse SVD then inverse 2-level DWT and get the watermarked RONI.
Get the medical image watermarked MIW by combining the two regions ROI and RONI' Watermarked

4.3.4.2 Extraction watermark process

In the watermark extraction process illustrated in Figure 4.5, the watermarked MIW is decomposed into LL2', LH2', HL2', and HH2' by applying a 2-level DWT. The secure watermark resides in the watermarked LL2' sub-band, particularly in its singular matrix S LL2' generated through the SVD algorithm. Algorithm 5 outlines all the steps, and Equation 4.4 is employed to extract the QR code, followed by the utilization of a QR code reader to retrieve the medical imaging test report document.

$$QR - code = (S - S_{LL_2'})/\alpha \tag{4.4}$$

The recipient uses the inverse process of the embedding phase to extract the watermark image, depicted by the QR code, from the watermarked medical image. Through a QR code reader, the recipient then accesses the entire medical image test report document.

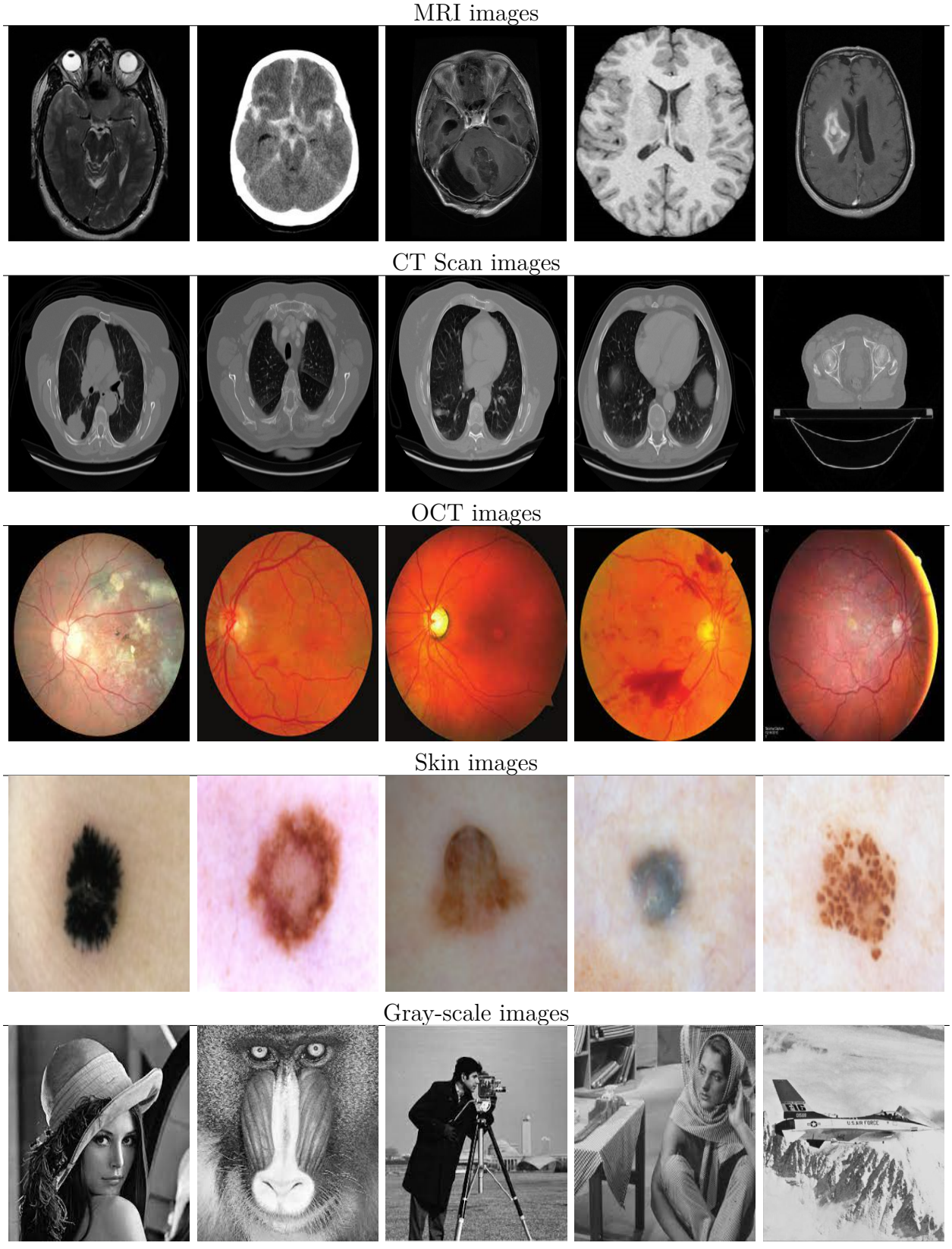

Figure 4.7: Medical and gray-scale cover images tested

Algorithm 5 Extraction Process

Require: MIW
Ensure: QR code of the patient's medical imaging test report
Separate the two regions of the MIW to get RONI'.
Apply the 2 levels of DWT on RONI' and get the LL2'.
3: Apply the SVD algorithm and get the U, S', and V components.
Extraction of the QR image by the following equation: QR code = (S – S')/ α.
Read the QR code image by QR code reader and get all patient's medical imaging test reports as a PDF document.

4.3.5 Experiment Analysis

The proposed method has been tested on a dataset comprising 20 medical images from various modalities, including IRM, CT Scan, OCT, and Skin images. Additionally, 5 grayscale images of dimensions 512x512 pixels are depicted in Figure 4.7. The watermark image utilized is a QR code of the MITR, presented as a black-and-white pattern of 64x64 pixels. The testing was conducted on a platform equipped with a Core i3, 1.70GHz Processor, 4 GB of Memory, and MATLAB R2020a.

4.3.5.1 Imperceptibility analysis

Enhancing the imperceptibility of a medical image is crucial for accurate diagnosis. In this approach, the evaluation of imperceptibility was conducted using metrics such as Peak Signal Noise Ratio (PSNR) and Structural Similarity Index Metric (SSIM).

The quality of medical images is crucial for clinicians to discern organ and tissue activities, especially in e-health and telemedicine applications where transmitted images must maintain high visual quality. This work introduces a proposed watermarking method that embeds report documents in medical images without distortion, ensuring EPR security and high imperceptibility. Table 4.3 presents metric values, including PSNR, SSIM, and NC, for 20 medical images across various modalities and five grayscale images, measured at two different scaling values (0.01 and 0.05).

When α is set to 0.01, the PSNR value for all images is 55.2132 dB, and for $\alpha = 0.05$, it decreases to 41.2338 dB. This indicates that the suggested method significantly enhances the watermark imperceptibility, making it more resistant to attackers. The PSNR values exceeding 30 dB suggest that the watermark becomes challenging for the HVS to distinguish from the original image. This enhancement is visually evident in Figure 4.8. And Table 4.3 includes the SSIM values, which were 0.9980 for a scaling factor of 0.01 and 0.9951 for a scaling factor of 0.05. These values demonstrate the similarity between the original cover medical image and the watermarked version. Table 4.4 presents SSIM values, revealing the

Table 4.3: PSNR, NC, SSIM for gray-scale and medical images ($\alpha = 0.01, \alpha = 0.05$)

Images		$\alpha = 0.01$			$\alpha = 0.05$		
		PSNR	NC	SSIM	PSNR	NC	SSIM
MRI	Image1	55.2132	0.9999	0.9976	41.2338	0.9987	0.9509
	Image2	55.2132	1.0000	0.9973	41.2338	0.9997	0.9453
	Image3	55.2132	0.9999	0.9972	41.2338	0.9986	0.9427
	Image4	55.2132	1.0000	0.9985	41.2338	0.9996	0.9694
	Image5	55.2132	1.0000	0.9973	41.2338	0.9995	0.9497
CT-Scan	Image1	55.2132	1.0000	0.9979	41.2338	0.9991	0.9558
	Image2	55.2132	1.0000	0.9976	41.2338	0.9990	0.9507
	Image3	55.2132	1.0000	0.9981	41.2338	0.9993	0.9608
	Image4	55.2132	1.0000	0.9978	41.2338	0.9993	0.9549
	Image5	55.2132	1.0000	0.9967	41.2338	0.9993	0.9368
OCT	Image1	55.2132	1.0000	0.9977	41.2338	0.9996	0.9540
	Image2	55.2132	1.0000	0.9978	41.2338	0.9988	0.9530
	Image3	55.2132	0.9999	0.9978	41.2338	0.9984	0.9528
	Image4	55.2132	1.0000	0.9978	41.2338	0.9992	0.9522
	Image5	55.2132	1.0000	0.9979	41.2338	0.9992	0.9553
Skin	Image1	55.2132	1.0000	0.9977	41.2338	0.9992	0.9512
	Image2	55.2132	1.0000	0.9978	41.2338	0.9989	0.9525
	Image3	55.2132	0.9998	0.9972	41.2338	0.9941	0.9415
	Image4	55.2132	0.9998	0.9975	41.2338	0.9954	0.9470
	Image5	55.2132	0.9999	0.9977	41.2338	0.9978	0.9509
Lena		55.2132	1.0000	0.9991	41.2338	0.9994	0.9798
Baboon		55.2132	1.0000	0.9997	41.2338	0.9993	0.9919
Cameramen		55.2132	1.0000	0.9985	41.2338	0.9994	0.9684
Barbara		55.2132	1.0000	0.9994	41.2338	0.9991	0.9869
Plane		55.2132	1.0000	0.9987	41.2338	0.9990	0.9720

similarity between the embedded watermark and the extracted one. Notably, the extracted watermark exhibits higher similarity when the scaling factor is 0.05.

4.3.5.2 Robustness analysis

The robustness of an approach depends on its capability to resist various attacks. Table 4.3 reveals that Normalized Correlation (NC) values range from 0.9999 to 1 for a scaling factor of 0.01 and from 0.9984 to 0.9997 (up to 1) for a scaling factor of 0.05, indicating a nearly identical match between watermarks and original images. The high visual quality of the proposed system for medical images from various modalities is evident.

Furthermore, a comprehensive evaluation was conducted to assess the robustness of the proposed watermarking method against noise attacks. Various noise attacks were applied to the watermarked image, and the extracted watermark quality was analyzed after each attack, as illustrated in Figure 4.9. Quantitative assessment, using Structural Similarity

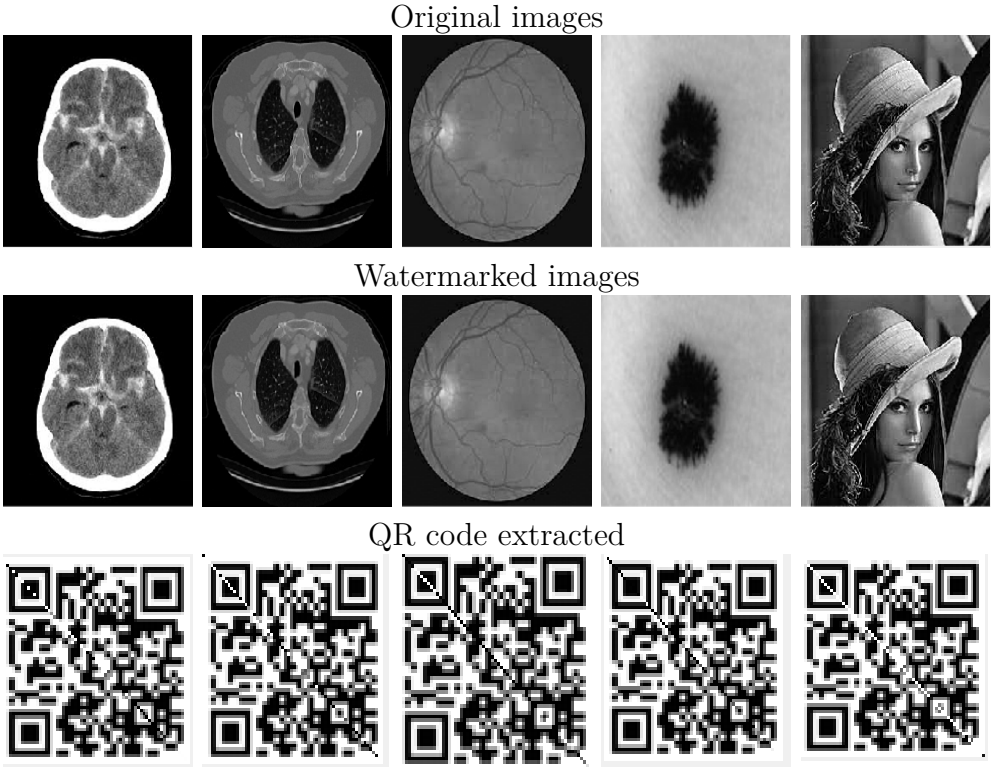

Figure 4.8: Original and watermarked images with QR code extracted

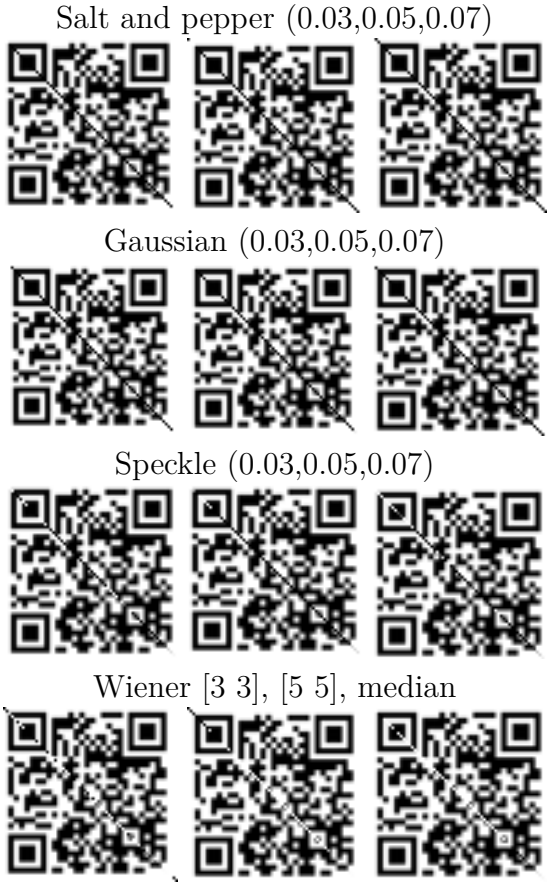

Figure 4.9: QR code extracted after attacks

Table 4.4: SSIM values of the embedding and extracted watermark ($\alpha = 0.01, \alpha = 0.05$)

Images		$\alpha = 0.01$	$\alpha = 0.05$
MRI	Image1	0.9011	0.9437
	Image2	0.9241	0.9643
	Image3	0.9191	0.9647
	Image4	0.9018	0.9679
	Image5	0.8988	0.9567
CT-Scan	Image1	0.9253	0.9766
	Image2	0.9093	0.9681
	Image3	0.8743	0.9729
	Image4	0.8853	0.9677
	Image5	0.9273	0.9597
OCT	Image1	0.9069	0.9565
	Image2	0.9143	0.9678
	Image3	0.9135	0.9246
	Image4	0.9295	0.9583
	Image5	0.9068	0.9454
Skin	Image1	0.9338	0.9296
	Image2	0.9362	0.9208
	Image3	0.8627	0.8473
	Image4	0.8897	0.8843
	Image5	0.9289	0.9406
Lena		0.9091	0.9450
Baboon		0.8733	0.9525
Cameramen		0.8775	0.9465
Barbara		0.8931	0.9586
Plane		0.8788	0.9311

Index (SSIM) and Mean Squared Error (MSE) metrics, is presented in Tables 4.5 and 4.6. Notably, the extracted watermark maintained a similarity higher than 0.7000 after the noise attacks, highlighting the remarkable robustness of the proposed method against such attacks.

4.3.6 Comparison

To evaluate the effectiveness of our proposed method in comparison to existing approaches, we conducted experiments using both non-medical images (Lina, baboon, plane, and cameramen) and medical images from diverse modalities (MRI, CT scan, OCT, and skin images). The techniques referenced in [50, 94, 51, 52, 54, 95, 55], which are grounded in the DWT-SVD image watermarking technique, utilized cover images with dimensions of 512x512 pixels.

The outcomes presented in Table 4.7 showcase the enhanced imperceptibility and similarity achieved by our method, as measured by the PSNR and SSIM parameters when compared to the techniques introduced in [50, 52, 95, 55]. With a PSNR value of 55.2132 dB

Table 4.5: Robustness of the proposed method for all images modality against different attacks (α=0.01)

Image	MRI		CT Scan		OCT image		Skin image		Lena	
	SSIM	MSE	SSIM	MSE	SSIM	MSE	SSIM	MSE	SSIM	MSE
SP(0.03)	0.7703	24.320	0.7689	29.851	0.7730	26.438	0.7456	362.74	0.8407	1.0581
SP(0.05)	0.7613	48.477	0.7619	62.400	0.7655	46.887	0.7415	548.59	0.8006	4.5904
SP(0.07)	0.7554	74.531	0.7572	85.353	0.7588	80.680	0.7369	753.44	0.7924	12.498
Gaussian(0.03)	0.7594	68.499	0.7709	29.660	0.7710	27.514	0.7490	244.03	0.8429	0.9592
Gaussian(0.05)	0.7594	65.523	0.7663	41.248	0.7707	31.085	0.7518	195.28	0.8322	2.1881
Gaussian(0.07)	0.7594	62.153	0.7684	36.725	0.7688	33.059	0.7538	173.43	0.8330	1.7560
Speckle(0.03)	0.8683	1.2754	0.8416	1.8514	0.7954	6.8899	0.7355	1107.0	0.8320	5.3358
Speckle(0.05)	0.8477	3.1994	0.8264	3.6828	0.7834	15.701	0.7349	1304.4	0.8489	1.1033
Speckle(0.07)	0.8750	3.7576	0.8230	4.7751	0.7805	18.699	0.7352	1410.1	0.8317	4.1522
Wiener(3×3)	0.8904	0.6482	0.8762	1.1138	0.9062	0.2984	0.9324	0.3013	0.7827	39.850
Wiener(5×5)	0.8548	4.1622	0.8516	1.5554	0.8657	2.1750	0.8879	1.1149	0.7712	55.249
Median	0.8597	1.6370	0.8894	1.0001	0.8859	1.0767	0.9317	0.6549	0.7727	49.282

Table 4.6: Robustness of the proposed method for all images modality against different attacks (α=0.05)

Image	MRI		CT Scan		OCT image		Skin image		Lena	
	SSIM	MSE	SSIM	MSE	SSIM	MSE	SSIM	MSE	SSIM	MSE
SP(0.03)	0.8256	1.0707	0.8240	1.3279	0.8277	1.3131	0.7957	12.628	0.9164	0.1953
SP(0.05)	0.8143	1.8634	0.8117	2.8058	0.8177	2.1736	0.7868	22.806	0.8775	0.2774
SP(0.07)	0.8061	2.9913	0.8049	3.9767	0.8106	3.4827	0.7820	30.803	0.8414	1.0689
Gaussian(0.03)	0.8121	2.5999	0.8208	1.8910	0.8290	1.3152	0.7959	10.540	0.9285	0.0657
Gaussian(0.05)	0.8111	2.8485	0.8231	1.6175	0.8291	1.2949	0.7979	10.676	0.9107	0.1143
Gaussian(0.07)	0.8104	2.6693	0.8218	1.6371	0.8274	1.2135	0.8038	6.6563	0.9306	0.1574
Speckle(0.03)	0.9236	0.0894	0.9170	0.0991	0.8624	0.3476	0.7771	44.341	0.9243	0.0998
Speckle(0.05)	0.9231	0.1056	0.8919	0.2145	0.8464	0.6312	0.7766	51.239	0.9250	0.1364
Speckle(0.07)	0.9175	0.1587	0.8807	0.3229	0.8359	0.9660	0.7736	60.209	0.9255	0.1620
Wiener(3×3)	0.9583	0.0308	0.9558	0.0439	0.9746	0.0482	0.9712	0.0226	0.8536	1.3296
Wiener(5×5)	0.9308	0.1879	0.9333	0.0726	0.9593	0.0839	0.9668	0.0746	0.8431	1.9359
Median	0.9452	0.0620	0.9717	0.0345	0.9661	0.0351	0.9541	0.0734	0.8413	1.6028

and an SSIM value of 0.9997, our method exhibits superior fidelity and similarity between the original and watermarked images, outperforming the mentioned methods.

Moreover, Table 4.8 furnishes an exhaustive analysis of imperceptibility and similarity in medical images across diverse modalities, juxtaposed with methodologies from the literature [50, 94, 51, 54, 95, 55]. Our proposed method consistently attains elevated PSNR values and exhibits commendable SSIM outcomes. These results underscore the efficacy of our suggested approach when employed across different image categories.

4.4 Conclusion

In numerous instances, physicians need access to medical images along with the accompanying radiologist's reports for precise patient diagnoses and tailored treatments. Nevertheless, the transmission of this sensitive data over the Internet introduces concerns about potential security breaches. In response to this challenge, We have proposed in this chapter, the first

Table 4.7: comparison of the proposed method with the literature in the non-medical image

Image	Method	PSNR	SSIM
Lena	**Proposed**	**55.2132**	**0.9991**
	Hussan et al. [95]	44.15	/
	Alquhayz et al. [55]	51.6293	0.9998
	Anand et al. [50]	47.5768	0.999785
	Mokashi et al. [52]	39.4843	0.9964
Baboon	**Proposed**	**55.2132**	**0.9997**
	Hussan et al. [95]	44.17	/
	Alquhayz et al.[55]	51.5029	0.9997
	Mokashi et al.[52]	39.4837	0.9967
Plan	**Proposed**	**55.2132**	**0.9987**
	Alquhayz et al [55]	51.6293	0.9974
Barbara	**Proposed**	**55.2132**	**0.9994**
	Hussan et al.[95]	44.13	/
	Alquhayz et al.[23]	53.4976	0.9996
	Anand et al.[50]	47.5719	0.999822
Cameramen	**Proposed**	**55.2132**	**0.9985**
	Hussan et al [95]	44.15	/
	Anand et al. [50]	47.7453	0.999869

Table 4.8: comparison of the proposed method with the literature in the medical image

Image	Method	PSNR	SSIM
MRI	**Proposed**	**55.2132**	**0.9985**
	Hussan et al. [95]	44.36	0.9832
	Anand et al. [50]	47.5648	0.999737
	Arumugham et al. [54]	47.486796	0.956391
	Sing et al. [51]	44.986	0.997
CT Scan	**Proposed**	**55.2132**	**0.997**
	Hussan et al. [95]	43.98	0.9450
	Alquhayz et al.[55]	51.5029	0.9997
	Anand et al.[50]	49.9552	0.999916
OCT image	**Proposed**	**55.2132**	**0.9979**
	Amine et al. [94]	43.28	0.9864

one based on the combination of the transform and spatial domain by using the DWT and LSB techniques. The method is efficient, simple to implement, and gives good results in terms of the low-capacity patient information hiding in the medical image. But to solve the problem of the high payload capacity, we have proposed a second innovative medical image watermarking method based on DWT-SVD. Our approach entails the incorporation of a QR code image containing comprehensive medical imaging test reports generated by radiologists. Notably, we have ensured that the size of the watermark image remains fixed, irrespective of the size of the test report document. This solution effectively addresses the challenge of accommodating the high uploading capacities associated with medical cover images.

The presented method provides notable advantages, including heightened security against diverse attacks, imperceptibility, and data authentication. These attributes were assessed through metrics such as PSNR, SSIM, and NC. The outcomes affirm the robustness and

dependability of our approach in safeguarding the integrity and confidentiality of medical imaging data.

CHAPTER 5

SECURITY AND AUTHENTICATION OF THE MEDICAL IMAGE TEST REPORT TRANSMISSION

Summary

In this chapter, we address the third requirement of medical image watermarking, focusing on the robustness of the approach. By transforming the Medical Imaging Test Report (MITR) into a QR code, we enhance both the payload capacity and the imperceptibility of the medical image compared to existing literature. The robustness of the watermarking method, crucial for resisting various attacks while maintaining manageable complexity and execution time, is thoroughly explored. Our proposed solution, as detailed in Chapter 4, aims to provide a comprehensive resolution to the watermarking trade-off dilemma by securely embedding a large amount of MITR data via QR code, prioritizing robustness, and also the authentication of the data by the verification of the hospital's logo (sender and receiver) and patient photo. The chapter concludes with a presentation and discussion of the results obtained.

5.1 Introduction

Building upon our previous work presented in the preceding chapter, we propose a further developed scheme aimed at bolstering robustness and ensuring image authentication during transmission. This involves embedding the QR code of the Medical Image Transmission Record (MITR) along with the logos of both the sending and receiving hospitals, as well as the patient's photograph.

5.1.1 Motivation

Although the conduct of medical imaging watermarking ensures the security of medical data transfer, it is still important to improve image watermarking, particularly when the trade-off between imperceptibility, capacity, and robustness is not fully resolved. This drives us to suggest robust medical image watermarking to protect the medical image report test (MIRT) that includes patient photographs and the hospital's label using the frequency watermarking technique DWT-SVD. Consequently, the work's contribution is as follows:

- The high payload and security of the MIRT report, It's encrypted and transformed into a QR code image with a small size whatever the medical report size, this feature augments the payload capacity, and encrypted patient information enhances the security.
- The high imperceptibility of the watermarked medical image, even if the watermark capacity is high, the imperceptibility is higher with a PSNR value of more than 67 dB.
- The approach has been shown robust against a variety of attacks, and the hospital's logo has acquired the authenticity watermark scheme.
- Ensuring the authenticity of medical data through incorporating hospital logos and patient. By including these visual identifiers, we aim to provide an additional layer of validation to medical records, thereby increasing their reliability and trustworthiness.

5.2 Medical image test report transmission approach

5.2.1 Data extraction process

The data collection process initiates with the patient undergoing an MRI examination. Utilizing precise imaging techniques, the MRI equipment captures detailed pictures of the patient's brain structure, offering a comprehensive view of the internal brain anatomy. This imaging procedure serves to identify potential abnormalities or disorders within the patient's

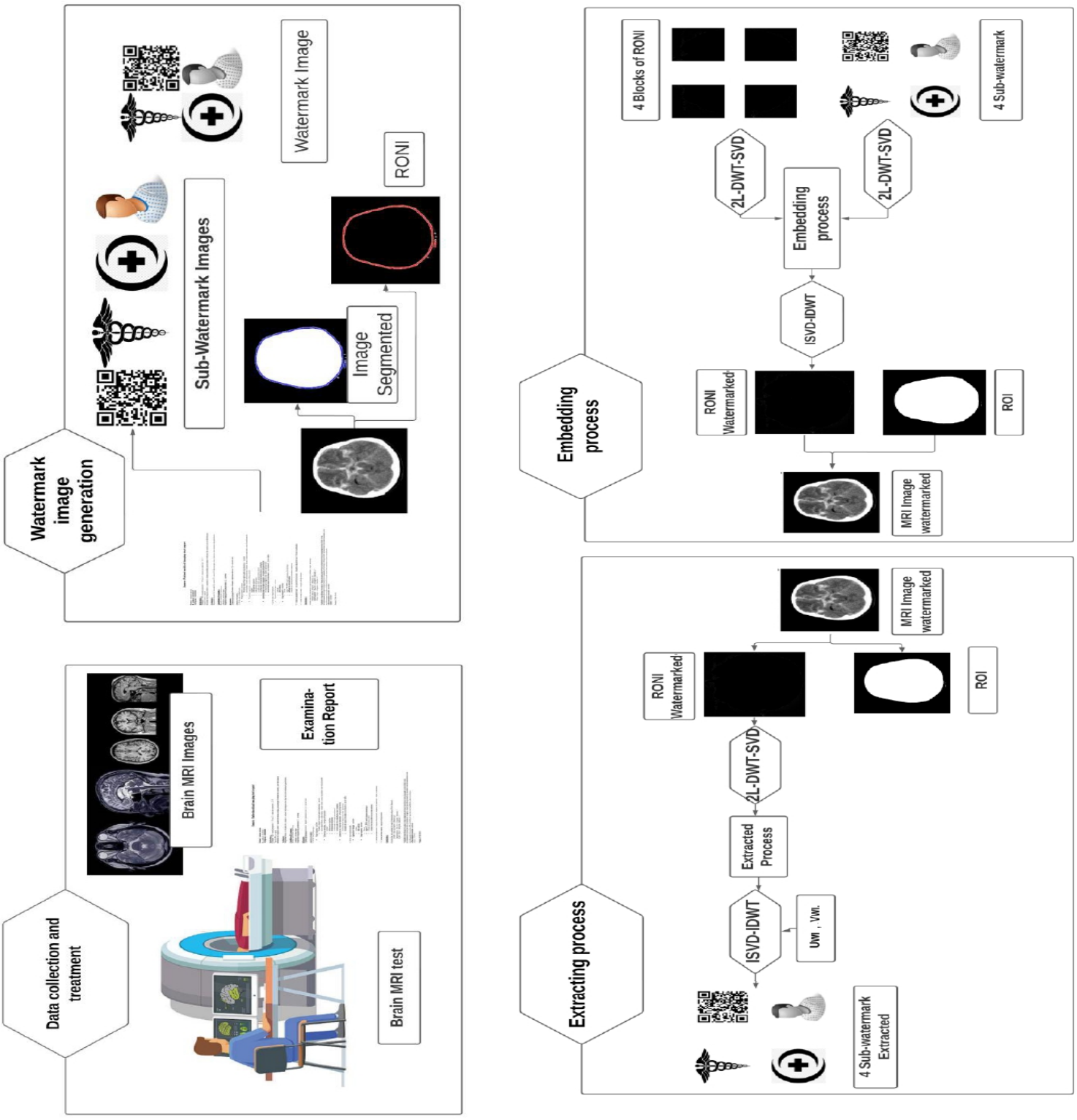

Figure 5.1: Proposed watermark diagram

brain. The gathered MRI images, along with the interpretation by healthcare professionals, provide valuable insights into the patient's condition. These insights are essential for generating the examination report, as illustrated in Figure 5.1 (Data Collection and Treatment section). Consequently, the medical data encompass the brain MRI image and the radiologist's report, elucidating the results and image information.

5.2.2 Watermark generation process

The watermark generation is a crucial aspect of the watermarking technique, especially when embedding information needs to be secure and organized. This step is divided into two parts: generating and encrypting the medical image test report (MITR) and collecting the four sub-watermark images to form the final watermark image. The second part involves medical image segmentation to prepare the Region of Non-Interest (RONI) of the cover image. This process is outlined in Algorithm 6 and illustrated in Figure 5.1 (Watermark Image Generation).

5.2.2.1 QR code generation

Incorporating QR codes in this watermarking method serves dual purposes. Firstly, it entails encrypting the MITR document and transforming it into a compact QR code image. Secondly, and more significantly, it generates a condensed encrypted image of a consistent size, irrespective of the original size of the MITR document. This step effectively addresses the challenge of high payload capacity, which typically impacts the imperceptibility of the watermarked image. Embedding patient information, such as name, age, ID, and others, bit by bit in the image using the LSB technique in the spatial domain [26], can affect imperceptibility despite the low capacity. The proposed approach of converting the document to a QR code and concealing it in the Region of Non-Interest (RONI) image in the transform domain resolves the issues of payload capacity and imperceptibility. The QR code image in Fig. 5 represents the MITR report.

In this approach, generation is accomplished using the application described in [51]. The watermark image is constructed by assembling sub-watermark images, each with a size of 6464, forming a larger image of 128 $\times$ 128, as illustrated in Figure 5.2.

5.2.2.2 Medical image segmentation

Following a simple preprocessing and filtering of the medical image, a segmentation technique is employed to separate the two regions within the image. This segmentation is crucial for safeguarding vital medical information related to the patient's condition, such as tumors, hemorrhages, inflammation, Alzheimer's, or any other details aiding expert diagnosis and analysis.

Figure 5.2: The 4 sub-watermark image

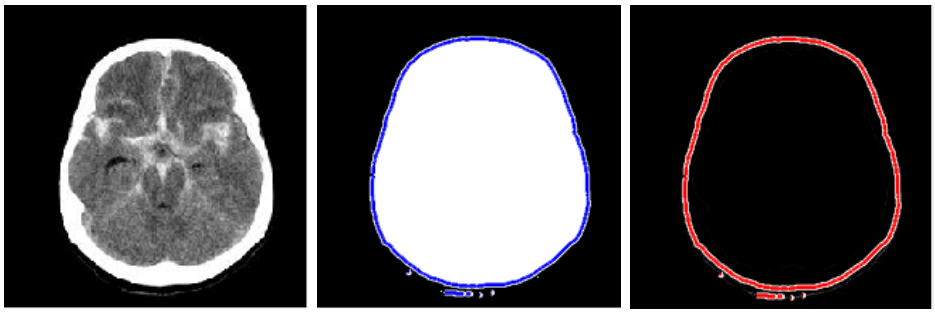

Figure 5.3: Medical image with ROI and RONI respectively

- Active contour method

Active Contour Models (ACMs) represent a widely utilized technique for fitting curves within an image. Active contouring involves the iterative expansion of a curve towards the borders of an object. The curve is initially placed in the image and is subsequently evolved through iterations until accurately outlines the object boundaries [96]. While this method typically selects the Region of Interest (ROI) in the image, the Region Outside the Region of Interest (RONI) image pertains to the medical image without the ROI. Figure 5.3 illustrates the segmented ROI medical image and the RONI.

Algorithm 6 Require preparation

Require: MRI image, Patient image, sender hospital logo, receiver hospital logo, and medical image test report

Ensure: RONI, QR code image of MITR then watermark image

1: • RONI
Read the medical image, resize it to (512*512), and process it by sharpening the filter. Separation of the two regions by active contour technique to select the ROI. Extract the RONI of the MRI image.

2: • Watermark generation
Create the QR code image of the MITR. Read the patient and hospital logo images, transform to grayscale images then resize them to (128*128). Collect the four images in one watermark image named 'WI' of 256*256 image size.

5.2.3 Watermark embedding process

In this phase, the systematic embedding of watermark images, including the sender hospital logo, QR code of the MITR, patient photo, and the received hospital logo, into the Region Outside the Region of Interest (RONI) image is outlined. The procedures are visualized in Figure 5.1 (Embedding process) and detailed in Algorithm 7.

The embedding process in this approach operates in the transform domain. The RONI image, sized at 512 ×512 pixels, is partitioned into four non-overlapping blocks of 256×256 pixels each. Simultaneously, the watermark image is decomposed into four sub-watermark images, representing the QR code, patient photo, and two hospital logos, each having a size of 128×128 pixels. The embedding technique employs the second-level Discrete Wavelet Transform (DWT) on the RONI sub-blocks, producing approximate, vertical, horizontal, and diagonal sub-bands of size 64×64 pixels (LL2, LH2, HL2, HH2). Additionally, the first-level DWT is implemented on the sub-watermark, resulting in LL, LH, HL, and HH sub-bands, each sized at 64*64 pixels in the first level.

The LL sub-band on each level captures the low-frequency components of the image, making it imperceptible to the human eye if any embedding data is introduced. The subsequent phase involves decomposing this sub-band into three matrices using the Singular Value Decomposition (SVD) technique. These matrices consist of two square matrices with orthonormal basis columns, denoted as U and V, and a diagonal matrix represented by S, containing non-zero values exclusively along its diagonal. This decomposition is expressed by the following equation:

$$LL_2 = U_{LL2} \times S_{LL2} \times V_{LL2}^T \tag{5.1}$$

$$LL = U_{WI} \times S_{WI} \times V_{WI}^T \tag{5.2}$$

The application of SVD occurs twice in the process: initially on the LL2 sub-band of each block within the RONI (as per Equation 5.1, and subsequently on the LL sub-band of each sub-watermark image (as per Equation 5.2. For each block, this results in three matrices: the singular value S, and the right and left singular vectors U and V.

The embedding stage in this procedure involves concatenating the two matrices, SLL2 and SWI, from each RONI block with its respective watermark image (A for the sender hospital, B for the QR code, C for the patient photo, and D for the receiver hospital logo). This concatenation is accomplished using the following equation:

$$S0 = S_{LL2} + \alpha \times S_{WI} \tag{5.3}$$

Algorithm 7 Embedding Process

Require: RONI, QR code image, patient photo, sender hospital logos, receiver hospital logo
Ensure: RONI' watermarked the MRI' image watermarked

- RONI processing

  Decompose the RONI image to 4 blocks (A, B,C,D) of 256*256 images. Apply the second level of DWT on each of the four blocks and obtain the LL2, LH2, HL2, HH2 sub-bands. Apply the SVD technique on the LL2 of each block (A, B, C, D) to get the U LL2, SLL2, VLL2 components.

- WI processing

  Decompose the WI image to 4 blocks which are already QR, Patient, and Hospital logos images. Apply on each of the 4 blocks level 1 of the DWT and decompose them to four sub-bands LLWI, LHWI, HLWI, HHWI. Apply the SVD technique on LLWI sub-band and get the three matrices UWI, SWI, VWI.

- Embedding part

Chose a scaling factor value α
Index =1
For i=1: number of block horizontally
J=1: number of blocks vertically
S0 = SLL2 + α × SWI; (Additional of SWI of the 4 blocks of the WI to the SLL2 of each of the 4 blocks of RONI (A, B, C, D) respectively.
End Apply the inverse of the SVD technique of the RONI with adding U and V components. Apply the inverse of 2-level of DWT of RONI to create the RONI' image watermarked. The medical image watermarked (MIW or MRI' image) is the combination of the two region ROI and RONI.

where α represents the scaling factor for the additional watermark data. In this method, it will be tested with three different values (0.001, 0.01, and 0.05).

To embed the watermark in the LL2 sub-band, the SVD technique is inverted. This process generates the watermarked RONI' through the inverse DWT. The ultimate watermarked image, referred to as the Medical Image Watermarked (MIW), is achieved by combining the watermarked RONI' with the unchanged ROI.

5.2.4 Watermark extraction process

The extraction of the embedded watermark is depicted in Figure 5.1 (Extracting process) and systematically outlined in Algorithm 8. This procedure essentially reverses the steps conducted during the embedding process.

Initially, the MIW is segmented using the ACM segmentation technique. Subsequently, the RONI' Watermarked is decomposed into four non-overlapping blocks, each carrying the singular value of a corresponding sub-watermark image (SWI). Extraction of the S0 from each block is accomplished through the application of DWT and SVD techniques.

Algorithm 8 Extraction process

Require: MIW

Ensure: WI (QR code for obtaining the MITR, patient photo, and the sender and receiver hospital logos)

1: Separation of the two regions ROI and RONI' of MRI image by active contour segmentation technique.
2: Decompose the RONI' to four blocks of 256*256 size (A, B, C, D).
3: Apply the 2-level of DwT technique of each block and get the LL'2, LH'2, HL'2, HH'2 sub-bands, to extract the U, S0, and V component of the LL2 (the watermark existence) and apply SVD technique.

- Extraction part

Chose a scaling factor value α Index =1 For i=1: number of blocks horizontally J=1: number of blocks vertically SWI = S0 - SLL2 $\times$ α * SWI; (Subtraction of SWI of the 4 blocks of the WI from SLL'2 of each of the 4 blocks of RONI' watermarked (A, B, C, D) respectively.

4: End
5: Apply the inverse of the SVD technique on the extracted SWI by adding UWI and VWI components to get the LLW sub-band.
6: Apply the inverse of 2-level of DWT on LLW with LHWI, HLWI, and HHWI to create the watermark image (QR code, patient photo, hospital logos).
7: In this step, we can extract all the documents of the MITR from the QR code.

$$S_{WI} = S0 - S_{LL2} \times \alpha \tag{5.4}$$

Equation 5.4 is utilized to extract the singular value from each sub-watermark, followed by the application of inverse DWT-SVD techniques. This involves adding the corresponding matrices U and V, resulting in the three sub-bands LH, HL, and HH of the sub-watermark images.

5.3 Simulation results and analysis

Simulation has been conducted to assess and validate the proposed method's behavior and performance, focusing on watermarking requirements, imperceptibility, security, and robustness. The testing platform features a Core i3, 1.70GHz Processor, and 4 GB of Memory. This section includes details about the dataset used, along with results from imperceptibility and robustness tests, including a comparison with state-of-the-art approaches, followed by a discussion.

5.3.1 Dataset tested

The dataset employed for evaluating the proposed method in this study is referred to as 'SAMAH-HAFSA,' sourced from Kaggle. It encompasses diverse sets of brain MRI images

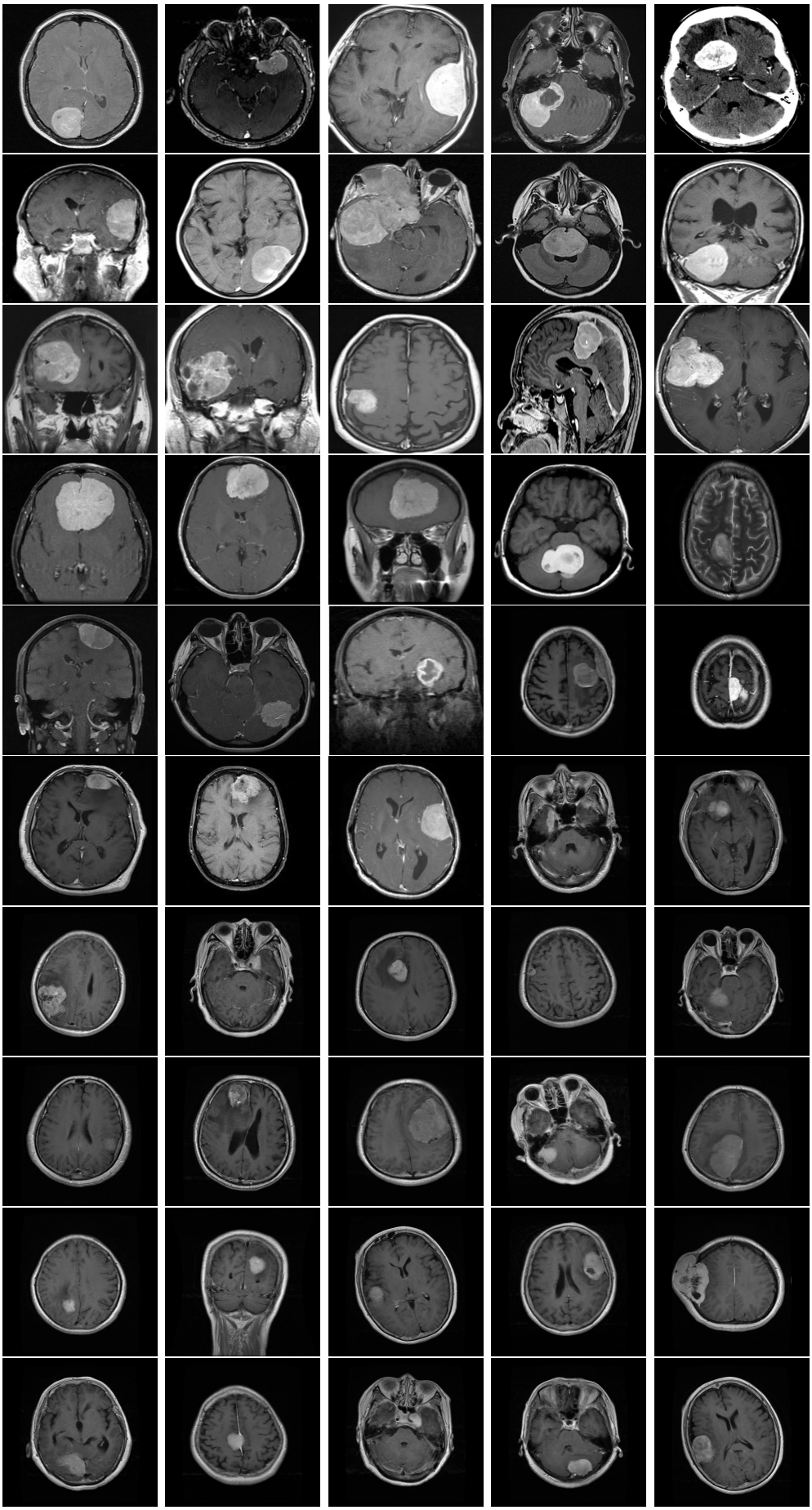

Figure 5.4: Medical images tested (Brain MRI Images)

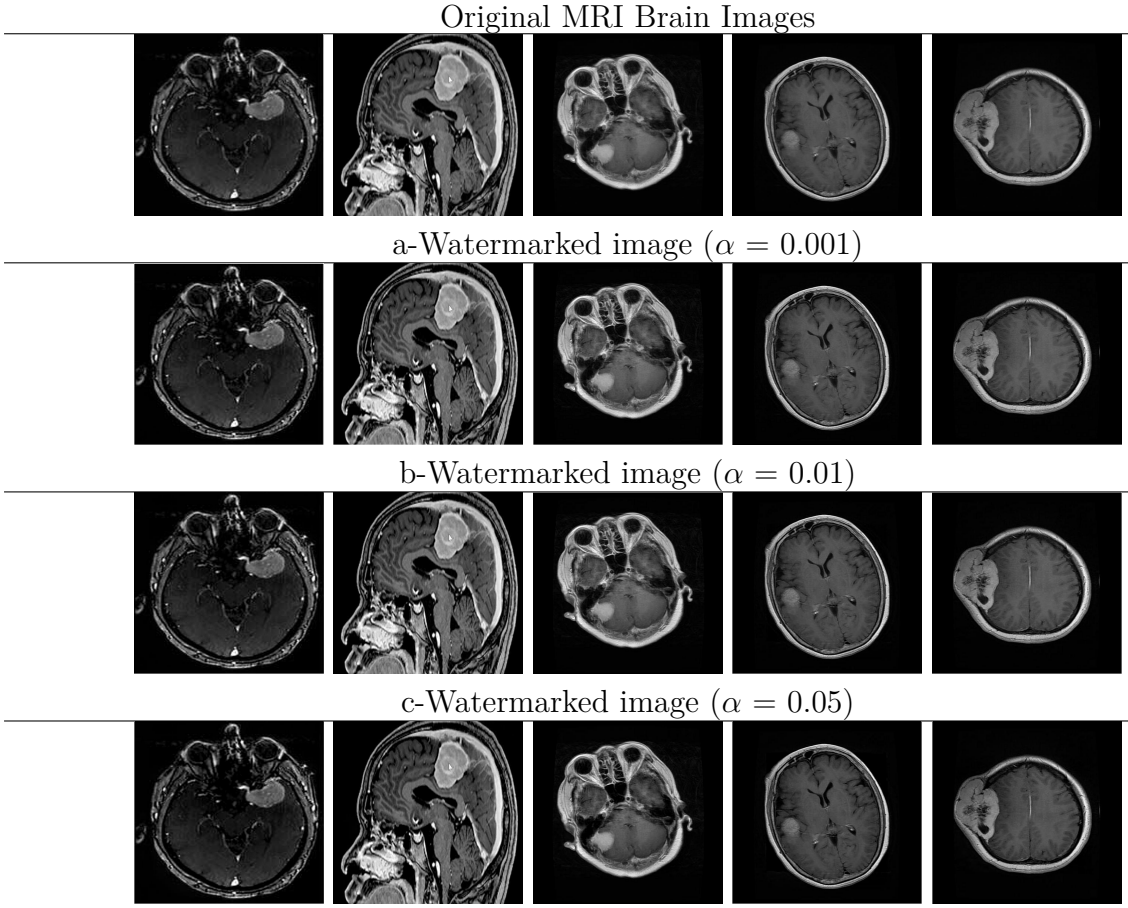

Figure 5.5: Watermarked images in different scaling factors

categorized into non-tumor and tumor (glioma, meningioma, and pituitary). Since the images exhibit varied sizes, the 50 test images have been resized to dimensions of 512x512 pixels, as illustrated in Figure 5.4.

5.3.2 Imperceptibility

Within the medical domain and e-health sector, the visual quality of medical images holds paramount significance due to the presence of sensitive information. Even minor distortions can impact a doctor's diagnosis. Whether the medical image is transmitted or received from another hospital, ensuring visual quality and imperceptibility is crucial. Imperceptibility entails that the original and watermarked images closely resemble each other, making it difficult for the human eye to discern any differences. This similarity is quantified using metrics such as PSNR and SSIM.

The imperceptibility of the proposed medical image watermarking method is assessed using 50 brain MRI images (Figure 5.4) and tested with various scaling factors, denoted as α (0.001, 0.01, and 0.05). Selected watermarked images are displayed in Figure 5.5, where (a) represents the original image, and (b), (c), and (d) present the watermarked images with

Table 5.1: PSNR, MSE, and SSIM between original and watermarked Brain MRI images

Image	α=0.001			α=0.01			α=0.05		
	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM
001	67.9025	0.0000	1.0000	47.9025	0.0000	0.9997	33.9231	0.0004	0.9914
002	67.9025	0.0000	0.9999	47.9025	0.0000	0.9925	33.9231	0.0004	0.8867
003	67.9025	0.0000	1.0000	47.9025	0.0000	0.9999	33.9231	0.0004	0.9970
004	67.9025	0.0000	1.0000	47.9025	0.0000	0.9996	33.9231	0.0004	0.9892
005	67.9025	0.0000	0.9999	47.9025	0.0000	0.9891	33.9231	0.0004	0.9573
006	67.9025	0.0000	1.0000	47.9025	0.0000	0.9988	33.9231	0.0004	0.9752
007	67.9025	0.0000	1.0000	47.9025	0.0000	0.9980	33.9231	0.0004	0.9671
008	67.9025	0.0000	1.0000	47.9025	0.0000	0.9998	33.9231	0.0004	0.9937
009	67.9025	0.0000	1.0000	47.9025	0.0000	0.9991	33.9231	0.0004	0.9680
010	67.9025	0.0000	1.0000	47.9025	0.0000	0.9993	33.9231	0.0004	0.9820
011	67.9025	0.0000	1.0000	47.9025	0.0000	0.9997	33.9231	0.0004	0.9911
012	67.9025	0.0000	1.0000	47.9025	0.0000	0.9998	33.9231	0.0004	0.9939
013	67.9025	0.0000	1.0000	47.9025	0.0000	0.9998	33.9231	0.0004	0.9961
014	67.9025	0.0000	0.9999	47.9025	0.0000	0.9913	33.9231	0.0004	0.9270
015	67.9025	0.0000	1.0000	47.9025	0.0000	0.9998	33.9231	0.0004	0.9935
016	67.9025	0.0000	1.0000	47.9025	0.0000	0.9992	33.9231	0.0004	0.9770
017	67.9025	0.0000	1.0000	47.9025	0.0000	0.9986	33.9231	0.0004	0.9726
018	67.9025	0.0000	1.0000	47.9025	0.0000	0.9980	33.9231	0.0004	0.9500
019	67.9025	0.0000	0.9999	47.9025	0.0000	0.9886	33.9231	0.0004	0.9002
020	67.9025	0.0000	1.0000	47.9025	0.0000	0.9983	33.9231	0.0004	0.9680
021	67.9025	0.0000	1.0000	47.9025	0.0000	0.9994	33.9231	0.0004	0.9793
022	67.9025	0.0000	1.0000	47.9025	0.0000	0.9977	33.9231	0.0004	0.9290
023	67.9025	0.0000	1.0000	47.9025	0.0000	0.9997	33.9231	0.0004	0.9903
024	67.9025	0.0000	1.0000	47.9025	0.0000	0.9986	33.9231	0.0004	0.9666
025	67.9025	0.0000	1.0000	47.9025	0.0000	0.9984	33.9231	0.0004	0.9680
026	67.9025	0.0000	1.0000	47.9025	0.0000	0.9990	33.9231	0.0004	0.9780
027	67.9025	0.0000	1.0000	47.9025	0.0000	0.9966	33.9231	0.0004	0.9448
028	67.9025	0.0000	1.0000	47.9025	0.0000	0.9991	33.9231	0.0004	0.9801
029	67.9025	0.0000	1.0000	47.9025	0.0000	0.9979	33.9231	0.0004	0.9466
030	67.9025	0.0000	1.0000	47.9025	0.0000	0.9958	33.9231	0.0004	0.9481
031	67.9025	0.0000	1.0000	47.9025	0.0000	0.9996	33.9231	0.0004	0.9897
032	67.9025	0.0000	1.0000	47.9025	0.0000	0.9991	33.9231	0.0004	0.9759
033	67.9025	0.0000	1.0000	47.9025	0.0000	0.9992	33.9231	0.0004	0.9787
034	67.9025	0.0000	1.0000	47.9025	0.0000	0.9995	33.9231	0.0004	0.9882
035	67.9025	0.0000	1.0000	47.9025	0.0000	0.9985	33.9231	0.0004	0.9674
036	67.9025	0.0000	1.0000	47.9025	0.0000	0.9993	33.9231	0.0004	0.9834
037	67.9025	0.0000	1.0000	47.9025	0.0000	0.9994	33.9231	0.0004	0.9820
038	67.9025	0.0000	1.0000	47.9025	0.0000	0.9995	33.9231	0.0004	0.9874
039	67.9025	0.0000	1.0000	47.9025	0.0000	0.9992	33.9231	0.0004	0.9742
040	67.9025	0.0000	1.0000	47.9025	0.0000	0.9992	33.9231	0.0004	0.9836
041	67.9025	0.0000	1.0000	47.9025	0.0000	0.9996	33.9231	0.0004	0.9898
042	67.9025	0.0000	1.0000	47.9025	0.0000	0.9994	33.9231	0.0004	0.9849
043	67.9025	0.0000	1.0000	47.9025	0.0000	0.9941	33.9231	0.0004	0.9296
044	67.9025	0.0000	1.0000	47.9025	0.0000	0.9994	33.9231	0.0004	0.9851
045	67.9025	0.0000	1.0000	47.9025	0.0000	0.9993	33.9231	0.0004	0.9815
046	67.9025	0.0000	1.0000	47.9025	0.0000	0.9944	33.9231	0.0004	0.9457
047	67.9025	0.0000	1.0000	47.9025	0.0000	0.9991	33.9231	0.0004	0.9826
048	67.9025	0.0000	1.0000	47.9025	0.0000	0.9983	33.9231	0.0004	0.9611
049	67.9025	0.0000	1.0000	47.9025	0.0000	0.9991	33.9231	0.0004	0.9763
050	67.9025	0.0000	1.0000	47.9025	0.0000	0.9955	33.9231	0.0004	0.9385
Average	67.9025	0.0000	1.0000	47.9025	0.0000	0.994312	33.9231	0.0004	0.98461

scaling factors of 0.001, 0.01, and 0.05, respectively. Notably, Figure 5.5 illustrates the striking similarity between the watermarked MRI images and the original one. The PSNR values consistently exhibit high quality, reaching 67.9025 dB with a scaling factor α of 0.001. Even with α set to 0.01, the PSNR value remains excellent at 47.9025 dB. However, with a further increase in the scaling factor, the PSNR value decreases to 33.9231 dB. The overall visual quality of the watermarked images is excellent, surpassing the human visual system's ability to detect the watermark, particularly when the PSNR value exceeds 30 dB, as confirmed by the tabulated PSNR and SSIM values in Table 5.1.

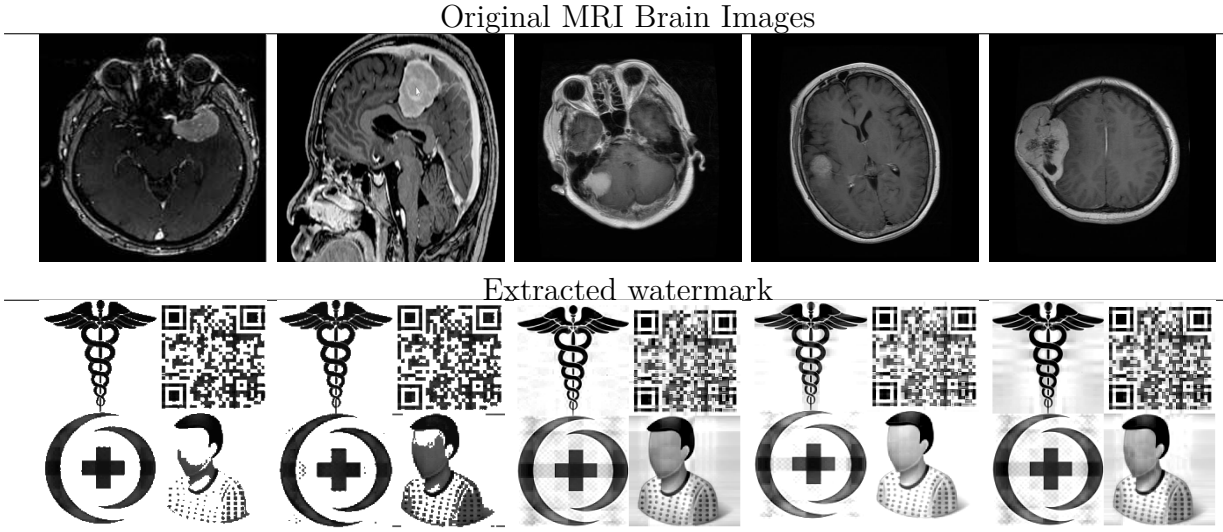

Figure 5.6: Extracted watermark under no attacks

The Structural Similarity Index (SSIM) serves as a crucial parameter for assessing the imperceptibility of the proposed watermarking method. The average SSIM values, depicted in the table 5.1, are 1.0000, 0.994312, and 0.98461 across the three scaling factors. These consistently high average values underscore the method's excellent imperceptibility. An anticipated SSIM value nearing 1 signifies exceptional imperceptibility, a criterion successfully met by this method.

5.3.3 Robustness

The robustness of a watermarking system denotes its ability to withstand various types of attacks during the transmission of the watermarked image over the internet. It ensures that, regardless of the attack type, the system can resist it, and the receiver is capable of successfully extracting the concealed information. In assessing the proposed watermarking technique for brain MRI images, additional noise attacks—such as salt and pepper, Gaussian, and speckle noise—along with image processing attacks like sharpening, Wiener, and median filters, are applied. The Normalization Coefficient (NC) is employed to evaluate the similarity between embedded and extracted watermarks under these attacks.

The proposed method's robustness has been rigorously assessed through various attacks. The Normalization Coefficient (NC) values, representing the similarity between embedded and extracted watermarks without any attack, are provided in Table 5.2 for the 50 brain MRI images tested under different scaling factors ($\alpha = 0.03, 0.05, 0.07$). Table 5.3 showcases the method's resilience against additional noise attacks, including salt and pepper, Gaussian noise, and speckle noise. Furthermore, Table 5.4 demonstrates its robustness against image processing attacks. The consistently high NC values, ranging between 0.9156 and 0.9436,

Table 5.2: NC value between original and recovered watermark

Image	α=0.001	α=0.01	α=0.05	Image	α=0.001	α=0.01	α=0.05
001	0.9162	0.9174	0.9224	026	0.9076	0.9078	0.9085
002	0.9430	0.9433	0.9430	027	0.9100	0.9115	0.9169
003	0.8215	0.8235	0.8302	028	0.9169	0.9182	0.9234
004	0.9017	0.9007	0.8947	029	0.9054	0.9069	0.9127
005	0.8167	0.8718	0.8796	030	0.9038	0.9044	0.9081
006	0.8593	0.7910	0.7904	031	0.8875	0.8886	0.8947
007	0.8500	0.8522	0.8623	032	0.8804	0.8820	0.8892
008	0.8609	0.8627	0.8711	033	0.8895	0.8907	0.8948
009	0.8990	0.9002	0.9102	034	0.9000	0.9015	0.9069
010	0.9008	0.9012	0.9014	035	0.8933	0.8949	0.9008
011	0.8150	0.8156	0.8162	036	0.8768	0.8783	0.8850
012	0.8435	0.8459	0.8606	037	0.8922	0.8937	0.8998
013	0.8652	0.8658	0.8660	038	0.9041	0.9046	0.9084
014	0.9226	0.9226	0.9211	039	0.9124	0.9137	0.9215
015	0.8526	0.8507	0.8410	040	0.8628	0.8647	0.8721
016	0.8101	0.8084	0.8700	041	0.8985	0.9000	0.9049
017	0.9048	0.9060	0.9109	042	0.8457	0.8468	0.8519
018	0.8950	0.8962	0.8944	043	0.9134	0.9139	0.9159
019	0.8942	0.8942	0.8957	044	0.8852	0.8871	0.8940
020	0.9114	0.9105	0.9081	045	0.9143	0.9154	0.9198
021	0.9263	0.9259	0.9210	046	0.9039	0.9044	0.9067
022	0.9240	0.9245	0.9260	047	0.9018	0.9033	0.9074
023	0.8578	0.8506	0.8258	048	0.8986	0.9001	0.9060
024	0.8871	0.8878	0.8917	049	0.9043	0.9058	0.9122
025	0.8622	0.8635	0.8688	050	0.9184	0.9193	0.9226

affirm the method's robust performance. The extracted watermark images for randomly selected samples are visualized in the accompanying figure.

5.3.4 Computational complexity

A highly effective medical image watermarking method must exhibit robustness and imperceptibility while maintaining efficiency and swift execution in real-time applications, especially considering the high capacity of medical images, whether in DICOM or electronic patient records (EPR). As depicted in Table 5, the proposed method demonstrates efficient performance in terms of embedding and extracting watermarking times under different scaling factors (α). The embedding process is completed within a short time frame, ranging from 0.29688 to 0.32024 seconds, indicating a rapid execution. Similarly, the extraction time falls within the range of 1.9023 to 2.213 seconds. This efficient performance suggests that the proposed method is well-suited for practical applications where speed is crucial.

Several factors influence watermarking speed, with two notable considerations. Firstly

Table 5.3: Robustness against various additional noise attacks

Attack	Noise density	α=0.001	α=0.01	α=0.05
Salt and pepper	0.03	0.9248	0.9206	0.9156
	0.05	0.9253	0.9246	0.9174
	0.07	0.9270	0.9264	0.9219
Gaussian	0.03	0.9338	0.9344	0.9286
	0.05	0.9375	0.9363	0.9318
	0.07	0.9426	0.9392	0.9194
Speckle	0.03	0.9428	0.9428	0.9431
	0.05	0.9428	0.9426	0.9432
	0.07	0.9426	0.9419	0.9435

Table 5.4: Robustness against various image processing attacks

Attack	Noise density	α=0.001	α=0.01	α=0.05
Winner	[3 3]	0.9429	0.9433	0.9435
	[5 5]	0.9432	0.9431	0.9435
Median	[3 3]	0.9430	0.9433	0.9436
	[5 5]	0.9433	0.9435	0.9432
Histogram equalization		0.7745	0.7613	0.7498
Sharpening		0.9427	0.9428	0.9434

(i), the technique employed in the watermarking method impacts speed. In our method, each step in the embedding process is executed four times, corresponding to the hiding of each watermark image (QR code, patient photo, sender hospital logo, or received hospital logo) in the corresponding RONI blocks. This four-time embedding process contributes to overall efficiency. Secondly (ii), hardware characteristics also play a role in execution speed, and in our case, the machine specifications include a Core i3 processor with a clock speed of 1.70GHz and 4 GB of memory.

5.4 Comparison

This section involves a comparative analysis of the proposed region-based image watermarking method with existing techniques found in the literature. In Table 5.6, a performance overview of the compared works is presented, covering various aspects such as objectives, datasets, embedding regions, employed techniques, and the strengths of each method. Addi-

Table 5.5: Time analysis of the proposed method

Time (second)	α=0.001	α=0.01	α=0.05
Embedding time	0.32024	0.29688	0.3037
Extracting time	2.0066	2.2133	1.9023

Table 5.6: Comparison with state-of-the-art existing watermarking techniques

Scheme	Years	Description	Dataset	Segmentation	Region based	Technique used	Reversible or not	Strengths
[97]	2017	Robust and secure watermarking technique	MRI and CT scan images	No	Whole image	DWT, DCT	Yes	Security, Robustness
[98]	2019	robust reversible watermarking method	MRI, CT scan, Ultrasound and founded images	Yes	Whole image	IWT, BTC, SVD	Yes	authenticity, integrity
[99]	2020	reversible medical image watermarking	CT Scan	yes	ROI, RONI	Prediction error expanding , LSB	Yes	Authentication, copyright protection
[100]	2021	Multiple watermarking for health record security	MRI image	No	Whole image	DTCWT, SVD	yes	security
[101]	2022	dual robust watermarking	CT scan	Yes	Whole image	DCT, QIM-DM	Yes	Robustness, Imperceptibility
[53]	2022	region-based hybrid watermark method	MRI, CT scan, Ultrasound, Doppler, X-Ray, Mammographic images	yes	ROI, RONI	DWT, SVD	Yes	imperceptibility, robustness, security, payload, tamper detection, and recovery accuracy
[102]	2023	Robust blind watermarking method	MRI, CT scan, Ultrasound and X-Ray images	No	Whole image	DWT	Yes	Imperceptibility, Robustness
proposed	–	region-based reversible watermarking method	MRI images	yes	RONI	DWT, SVD	Yes	Authenticity, Imperceptibility, robustness, capacity

Table 5.7: Performance comparison of the proposed scheme with related work

Scheme	PSNR	SSIM	NC	BER
[97]	51.8332	-	1	0
[98]	41.2995	0.9607	0.9592	0.0456
[99]	56.33612	-	-	-
[100]	46.6291	0.9974	0.9942	0
[101]	54.91	-	1	0
[53]	43.30	0.99	0.9999	0
[102]	49.48	-	-	
Proposed	67.9025	1.0000	0.901956	0.1120

tionally, Table 5.7 provides a tabulation of parameter values, where our method achieves the highest PSNR (67.9025 dB) and SSIM (1.000) values. These outcomes signify a remarkable level of imperceptibility for our method, making it challenging for the human visual system to discern differences between the original and watermarked brain MRI images. The Normalization Coefficient (NC) and Bit Error Rate (BER) values further highlight the strength of our method, assessing the similarity and accuracy of the hidden and extracted watermark.

5.5 Discussion

Our proposed watermarking method exhibits several noteworthy advantages based on a comprehensive evaluation. **Firstly**, the PSNR consistently exceeds 67 dB, and SSIM attains a value of 1 for most tested MRI brain images at a scaling factor of 0.001, as detailed in Table 5.1. This underscores the method's high imperceptibility, ensuring a remarkable similarity between watermarked and original images.

Secondly, the robustness of the proposed approach is rigorously examined through image processing and additional noise attacks, with the NC metric used for evaluation. Extracted watermark images are displayed in Figure 5.6 and detailed in Table 2.

Thirdly, our watermark image comprises four distinct watermarks representing the QR code of the MITR report containing comprehensive patient medical information. This high-capacity document is fortified by the inclusion of two hospital logos and patient photos to authenticate its origin. This approach effectively navigates the trade-off challenges inherent in capacity, imperceptibility, and robustness. By encrypting a substantial volume of data as a QR code into a medical image, our method succeeds in maintaining both visual quality and imperceptibility while demonstrating resilience against various attacks.

Fourth, Computational speed is a pivotal factor in determining the efficiency of image watermarking techniques, especially in the medical domain where embedding and extraction

processes are of paramount importance. A shorter processing time directly correlates with faster computational speed. The assessment of speed for the proposed method is detailed in **Table 5.5**, encompassing the embedding and extraction stages across three scaling factors. It's worth noting that the complexity of the algorithm implementation and the specifications of the testing machine can influence the speed of the watermarking technique, as outlined in the proviso section.

Fifth, the EPR embedded in the medical image is an MRI test report, a document containing all patient information. Embedding this report onto the medical image bit by bit as text can distort illness information and degrade image quality due to the high information capacity. Encrypting this report document as a QR code achieves (i) the security of the EPR and (ii) can map an arbitrarily large ratio document to a small binary image, effectively addressing capacity, imperceptibility, and security concerns.

Finally, based on the comparison of the proposed method with existing ones in the literature as depicted in **Table 5.6**, highlighting distinctions in techniques, datasets, and strengths, **Table 5.7** tabulates differences in the evaluation metric values for each. The region-based medical image watermarking, employing QR code encryption in this work, attains a high level of imperceptibility with substantial payload capacity. It achieves this without distorting information in MRI brain images and ensures robust security against various attacks. The proposed method proves to be efficient for medical image transmission and e-health applications, particularly enhancing Electronic Patient Record (EPR) security.

5.6 Conclusion

The capacity to accommodate a high payload of data in the cover image can impact the imperceptibility and security of the embedded watermark. In our approach, we introduce a region-based MRI image watermarking technique to enhance the security of transmitting the medical image test report document, containing comprehensive patient information, along with a patient photo and two hospital logos (sender and receiver). The MITR document is encrypted into a QR code image to ensure security and standardize the size of the watermark, irrespective of the test report document's size. This approach effectively resolves the trade-off dilemma between capacity, imperceptibility, and robustness. It becomes feasible to embed extensive data in the medical image by encrypting it into a QR code without compromising the visual quality or imperceptibility of the watermarked image. Our method achieves this goal without distorting the patient's illness information in the ROI of their brain MRI image. This proposed approach can be extended to other medical image modalities.

CHAPTER 6

GENERAL CONCLUSION

Summary

In this chapter, we revisit the essence of this thesis, highlighting our contributions and main findings. We then explore potential avenues for further research and discuss future perspectives in the field.

6.1 Summary of the main results

The work presented in this thesis has delved into the critical realm of biomedical security, particularly focusing on safeguarding Electronic Patient Records (EPR) from unauthorized manipulation or exploitation for malicious purposes such as identity theft or financial fraud. To mitigate these risks, various security techniques including encryption, steganography, and watermarking have been explored. Throughout this research endeavor, our primary objective has been to enhance the capacity, imperceptibility, and robustness of medical image watermarking to ensure the security and authenticity of medical data. Chapters 4 and 5 have outlined innovative methods aimed at achieving these goals. Leveraging the advantages of Quick Response (QR) codes, our approach addresses the challenge of capacity and imperceptibility, especially when embedding watermarks in the Region of Non-Interest (RONI) of medical images. This strategy is particularly pertinent as doctors rely on these images to make critical decisions regarding patient care, often requiring additional data to inform their judgments.

In the first contribution, We introduced a novel region-based medical image watermarking approach aimed at securing patient Medical Imaging Test Reports (MITR). This method involves embedding a QR code image representing the MITR into the non-interest region of the medical image in the frequency domain, employing techniques such as Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Evaluation of the proposed method was conducted using parameters including PSNR, SSIM, and NC, demonstrating its high payload capacity, imperceptibility, and resilience against various attacks.

In the second contribution, We introduce a region-based MRI brain image watermarking technique to enhance the security of medical image test reports (MITRs). Each medical image test contains specific information that needs to be securely transmitted. We proposed a method that involves encrypting the MITR using Quick Response (QR code) encryption and embedding it into the non-interest region of the MRI image with the patient photo and sender and receiving the hospital's logo to enhance the authentication of the method. The technique employs watermarking techniques in the frequency domain, utilizing the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) methods. Our work demonstrates excellent imperceptibility, authenticity, security, and robustness compared with other schemes in the literature.

6.2 Perspectives and Future Work

The exploration conducted in this study has unveiled numerous biomedical security techniques centered around digital watermarking. Moving forward, the following areas can be

identified as potential avenues for future research:

- We might delve into the issue of QR code creation security for our initial and second contributions to the QR code application. In this study, QR codes are generated online to assess their efficacy in watermarking to enhance payload capacity. However, ensuring the security of the QR code generation process is imperative.
- After an in-depth review of the literature, it is evident that the combination of encryption techniques with watermarking methods can yield promising results. However, certain techniques like Elliptic Curve Cryptography (ECC), which offers various advantages are seldom utilized in biomedical security applications.
- Ultimately, there are two emerging areas of importance within the biomedical field: biomedical security and artificial intelligence models for segmentation and classification methods. Both aspects carry significant impact and are essential. It is imperative to ensure the reliability of developed models, as well as to integrate artificial intelligence with robust security schemes.

BIBLIOGRAPHY

[1] Stefano Omboni. Connected health: in the right place at the right time. *Conn Health*, 1:1–6, 2021.

[2] Rumi Chunara, Yuan Zhao, Ji Chen, Katharine Lawrence, Paul A Testa, Oded Nov, and Devin M Mann. Telemedicine and healthcare disparities: a cohort study in a large healthcare system in new york city during covid-19. *Journal of the American Medical Informatics Association*, 28(1):33–41, 2021.

[3] Abid Haleem, Mohd Javaid, Ravi Pratap Singh, and Rajiv Suman. Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors international*, 2:100117, 2021.

[4] https://www.hipaajournal.com/hacking-incidents-reported-by-retinal-consultants-medical-group-three-rivers-regional-commission-ace-surgical-supply/.

[5] Clemens Scott Kruse, Brenna Smith, Hannah Vanderlinden, and Alexandra Nealand. Security techniques for the electronic health records. *Journal of medical systems*, 41:1–9, 2017.

[6] Ge Wang, Jong Chul Ye, and Bruno De Man. Deep learning for tomographic image reconstruction. *Nature Machine Intelligence*, 2(12):737–748, 2020.

[7] Mohammad H Bagheri, Mark A Ahlman, Liza Lindenberg, Baris Turkbey, Jeffrey Lin, Ali Cahid Civelek, Ashkan A Malayeri, Piyush K Agarwal, Peter L Choyke, Les R Folio, et al. Advances in medical imaging for the diagnosis and management of common genitourinary cancers. In *Urologic Oncology: Seminars and Original Investigations*, volume 35, pages 473–491. Elsevier, 2017.

[8] Hannah Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104:333–339, 2019.

[9] Hassan Goodarzi, Seyed-Masoud Khatami, Hammidreza Javadzadeh, Sadrollah Mahmoudi, Hojjatollah Khajehpour, Soleiman Heidari, Morteza Khodaparast, Ali Ebrahimi, Hamidreza Rasouli, Mohammadreza Ghane, et al. User acceptance of picture archiving and communication system in the emergency department. *Iranian Journal of Radiology*, 13(2), 2016.

[10] Reza Abbasi, Monireh Sadeqi Jabali, Reza Khajouei, and Hamidreza Tadayon. Investigating the satisfaction level of physicians in regards to implementing medical picture archiving and communication system (pacs). *BMC medical informatics and decision making*, 20:1–8, 2020.

[11] Najmeh Hasani, AghaFatemeh Hosseini, and Abbas Sheikhtaheri. Effect of implementation of picture archiving and communication system on radiologist reporting time and utilization of radiology services: a case study in iran. *Journal of Digital Imaging*, 33:595–601, 2020.

[12] Mohammadhiwa Abdekhoda and Kawa Mirza Salih. Determinant factors in applying picture archiving and communication systems (pacs) in healthcare. *Perspectives in health information management*, 14(Summer), 2017.

[13] Sahar Haddad. *Protection of encrypted and/or compressed medical images by means of watermarking*. PhD thesis, Ecole nationale supérieure Mines-Télécom Atlantique, 2020.

[14] David A Clunie. Dicom format and protocol standardization—a core requirement for digital pathology success. *Toxicologic Pathology*, 49(4):738–749, 2021.

[15] Rishi Saripalle, Christopher Runyan, and Mitchell Russell. Using hl7 fhir to achieve interoperability in patient health record. *Journal of biomedical informatics*, 94:103188, 2019.

[16] Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, and BN Chatterji. Digital image steganography: A literature survey. *Information sciences*, 2022.

[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] Lalan Kumar, Kamred Udham Singh, and Indrajeet Kumar. A compreshensive review on digital image watermarking techniques. In *2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, pages 737–743. IEEE, 2023.

[19] Muhammad Aamir Qureshi and Ran Tao. Technical challenges for digital watermarking. In *The Proceedings of the Multiconference on" Computational Engineering in Systems Applications"*, volume 1, pages 444–447. IEEE, 2006.

[20] Musab Qassem Al-Ghadi. *Watermarking approaches for images authentication in applications with time constraints*. PhD thesis, Université de Bretagne occidentale-Brest, 2018.

[21] Mohamed Meselhy Eltoukhy, Ayman E Khedr, Mostafa M Abdel-Aziz, and Khalid M Hosny. Robust watermarking method for securing color medical images using slant-svd-qft transforms and otp encryption. *Alexandria Engineering Journal*, 78:517–529, 2023.

[22] Aberna Palani and Agilandeeswari Loganathan. Semi-blind watermarking using convolutional attention-based turtle shell matrix for tamper detection and recovery of medical images. *Expert Systems with Applications*, 238:121903, 2024.

[23] Zongwei Tang, Xiuli Chai, Yang Lu, Binjie Wang, and Yong Tan. An end-to-end screen shooting resilient blind watermarking scheme for medical images. *Journal of Information Security and Applications*, 76:103547, 2023.

[24] Wendan Li, Changgen Peng, Weijie Tan, Yi Xu, and Kun Niu. A reversible and lossless secret image sharing scheme with authentication for color images. *Journal of King Saud University-Computer and Information Sciences*, page 101854, 2023.

[25] Yi Zhang, Xiangyang Luo, Jinwei Wang, Yanqing Guo, and Fenlin Liu. Image robust adaptive steganography adapted to lossy channels in open social networks. *Information Sciences*, 564:306–326, 2021.

[26] Aicha Benyoucef and M'Hamed Hamadouche. Roni-based medical image watermarking using dwt and lsb algorithms. In *International Conference on Artificial Intelligence and its Applications*, pages 468–478. Springer, 2021.

[27] Pabitra Pal, Biswapati Jana, and Jaydeb Bhaumik. A secure reversible color image watermarking scheme based on lbp, lagrange interpolation polynomial and weighted matrix. *Multimedia Tools and Applications*, 80:21651–21678, 2021.

[28] Zhang Wenyin and Frank Y Shih. Semi-fragile spatial watermarking based on local binary pattern operators. *Optics Communications*, 284(16-17):3904–3912, 2011.

[29] Jide Kehinde Adeniyi, Tinuke Omolewa Oladele, Noah Oluwatobi Akande, Roseline Oluwaseun Ogundokun, and Tunde Taiwo Adeniyi. A multiple algorithm approach to textural features extraction in offline signature recognition. In *Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020,*

Dubai, United Arab Emirates, November 25–26, 2020, Proceedings 17, pages 541–552. Springer, 2020.

[30] Aicha Benyoucef and M'Hamed Hamaouche. Region-based medical image watermarking approach for secure epr transmission applied to e-health. *Arabian Journal for Science and Engineering*, pages 1–13, 2023.

[31] Saradha Rani Sabbavarapu, Sasibhushans Rao Gottapu, and Prabhakara Rao Bhima. A discrete wavelet transform and recurrent neural network based medical image compression for mri and ct images. *Journal of Ambient Intelligence and Humanized Computing*, 12:6333–6345, 2021.

[32] Qingtang Su and Beijing Chen. Robust color image watermarking technique in the spatial domain. *Soft Computing*, 22:91–106, 2018.

[33] Simone Venturi and Tiernan Casey. Svd perspectives for augmenting deeponet flexibility and interpretability. *Computer Methods in Applied Mechanics and Engineering*, 403:115718, 2023.

[34] Bilal Hassan, Ramsha Ahmed, Bo Li, and Omar Hassan. An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an ehealth arrangement. *IEEE Access*, 7:69758–69775, 2019.

[35] Chih-Chin Lai. An improved svd-based watermarking scheme using human visual characteristics. *Optics Communications*, 284(4):938–944, 2011.

[36] Christof Kauba and Andreas Uhl. Robustness evaluation of hand vein recognition systems. In *2015 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–5. IEEE, 2015.

[37] Asim Naveed, Yasir Saleem, Nisar Ahmed, and Aasia Rafiq. Performance evaluation and watermark security assessment of digital watermarking techniques. *Science International*, 27(2), 2015.

[38] Mykola Ponomarenko, Karen Egiazarian, Vladimir Lukin, and Victoriya Abramova. Structural similarity index with predictability of image blocks. In *2018 IEEE 17th International Conference on Mathematical Methods in Electromagnetic Theory (MMET)*, pages 115–118. IEEE, 2018.

[39] Dimitrios K Tsolis, Spyros Sioutas, and Theodore S Papatheodorou. A multimedia application for watermarking digital images based on a content based image retrieval technique. *Multimedia Tools and Applications*, 47:581–597, 2010.

[40] Sawsan D Mahmood, Fadoua Drira, Hussain Falih Mahdi, Yassine Aribi, and Adel M Alimi. Chaotic model-based blind watermarking with lsb technique for digital fundus image authentication. In *2023 International Conference on Cyberworlds (CW)*, pages 395–402. IEEE, 2023.

[41] Gaurav Kumar Soni, Akash Rawat, Smriti Jain, and Saurabh Kumar Sharma. A pixel-based digital medical images protection using genetic algorithm with lsb watermark technique. In *Smart Systems and IoT: Innovations in Computing: Proceeding of SSIC 2019*, pages 483–492. Springer, 2020.

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

[43] Lamri Laouamer. New informed non-blind medical image watermarking based on local binary pattern. 2022.

[44] Wenyi Liu, Jingbing Li, Chunyan Shao, Jixin Ma, Mengxing Huang, and Uzair Aslam Bhatti. Robust zero watermarking algorithm for medical images using local binary pattern and discrete cosine transform. In *International Conference on Artificial Intelligence and Security*, pages 350–362. Springer, 2022.

[45] Ali Alzahrani and Nisar Ahmed Memon. Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images. *IEEE Access*, 9:113714–113734, 2021.

[46] Narima Zermi, Amine Khaldi, Redouane Kafi, Fares Kahlessenane, and Salah Euschi. A dwt-svd based robust digital watermarking for medical image security. *Forensic science international*, 320:110691, 2021.

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

[48] Ranjana Dwivedi, Divyanshu Awasthi, and Vinay Kumar Srivastava. An optimized dual image watermarking scheme based on redundant dwt and randomized svd with henon mapping encryption. *Circuits, Systems, and Signal Processing*, pages 1–49, 2023.

[49] M Sajeer and Ashutosh Mishra. A robust and secured fusion based hybrid medical image watermarking approach using rdwt-dwt-msvd with hyperchaotic system-fibonacci q matrix encryption. *Multimedia Tools and Applications*, pages 1–23, 2023.

[50] Ashima Anand and Amit Kumar Singh. Dual watermarking for security of covid-19 patient record. *IEEE Transactions on Dependable and Secure Computing*, 20(1):859–866, 2022.

[51] Kumari Suniti Singh, Pushpanjali Singh, and Harsh Vikram Singh. Security of e-healthcare data using dwt-svd based hybrid watermarking. In *2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22)*, pages 1–6. IEEE, 2022.

[52] Bhargavi Mokashi, Vandana S Bhat, Jagadeesh D Pujari, S Roopashree, TR Mahesh, and D Stalin Alex. Efficient hybrid blind watermarking in dwt-dct-svd with dual biometric features for images. *Contrast Media & Molecular Imaging*, 2022, 2022.

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

[54] Sridevi Arumugham, Sundararaman Rajagopalan, John Bosco Balaguru Rayappan, and Rengarajan Amirtharajan. Tamper-resistant secure medical image carrier: an iwt–svd–chaos–fpga combination. *Arabian Journal for Science and Engineering*, 44(11):9561–9580, 2019.

[55] Hani Alquhayz and Basit Raza. Watermarking techniques for the security of medical images and image sequences. *Arabian Journal for Science and Engineering*, 47(8):9471–9488, 2022.

[56] George Klington, K Ramesh, and Seifedine Kadry. Cost-effective watermarking scheme for authentication of digital fundus images in healthcare data management. *Information Technology and Control*, 50(4):645–655, 2021.

[57] Yang Yang, Xingxing Xiao, Xue Cai, and Weiming Zhang. A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. *IEEE Access*, 7:96900–96911, 2019.

[58] Xueyan Wu. An algorithm for reversible information hiding of encrypted medical images in homomorphic encrypted domain. *Discrete and Continuous Dynamical Systems-S*, 12(4&5):1441–1455, 2019.

[59] B Karthikeyan, Jagannathan Chakravarthy, and V Vaithiyanathan. An enhanced hill cipher approach for image encryption in steganography. *International Journal of Electronic Security and Digital Forensics*, 5(3-4):178–187, 2013.

[60] Kandala Sree Rama Murthy and VM Manikandan. A reversible data hiding through encryption scheme for medical image transmission using aes encryption with key scrambling. *Journal of Advances in Information Technology Vol*, 13(5), 2022.

[61] Bowen Meng, Xiaochen Yuan, Qiyuan Zhang, Chan-Tong Lam, and Guoheng Huang. Encryption-then-embedding-based hybrid data hiding scheme for medical images. *Journal of King Saud University-Computer and Information Sciences*, page 101932, 2024.

[62] Puvvadi Aparna and Polurie Venkata Vijay Kishore. A blind medical image watermarking for secure e-healthcare application using crypto-watermarking system. *Journal of Intelligent Systems*, 29(1):1558–1575, 2019.

[63] Abhilasha Sharma, Amit Kumar Singh, and SP Ghrera. Secure hybrid robust watermarking technique for medical images. *Procedia Computer Science*, 70:778–784, 2015.

[64] Jaishree Jain, Arpit Jain, Saurabh Kumar Srivastava, Chaman Verma, Maria Simona Raboaca, and Zoltán Illés. Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with rsa. *Mathematics*, 10(7):1071, 2022.

[65] JR Aparna and Sonal Ayyappan. Image watermarking using diffie hellman key exchange algorithm. *Procedia Computer Science*, 46:1684–1691, 2015.

[66] Priyanka Priyadarshini and Kshiramani Naik. Dual image watermarking technique using iwt-svd and diffie hellman key exchange algorithm. In *International Conference on Computing, Communication and Learning*, pages 172–183. Springer, 2022.

[67] Fepslin AthishMon and K Suthendran. Combined cryptography and digital watermarking for secure transmission of medical images in ehr systems. *Int J Pure Appl Math*, 118(8):265–269, 2018.

[68] Amira K Jabbar, Ashwaq T Hashim, and Qussay F Hassan. Medical image authentication by combining hash signature and watermarking based on frequency domains. In *Journal of Physics: Conference Series*, volume 1963, page 012039. IOP Publishing, 2021.

[69] Hui Shi, Shouquan Zhou, Meihan Chen, and Mingchu Li. A novel zero-watermarking algorithm based on multi-feature and dna encryption for medical images. *Multimedia Tools and Applications*, pages 1–46, 2023.

[70] Zhiqiu Xia, Xingyuan Wang, Wenjie Zhou, Rui Li, Chunpeng Wang, and Chuan Zhang. Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms. *Signal Processing*, 157:108–118, 2019.

[71] Sriti Thakur, Amit Kumar Singh, Satya Prakash Ghrera, and Anand Mohan. Chaotic based secure watermarking approach for medical images. *Multimedia Tools and Applications*, 79:4263–4276, 2020.

[72] K Balasamy and D Shamia. Feature extraction-based medical image watermarking using fuzzy-based median filter. *IETE Journal of Research*, 69(1):83–91, 2023.

[73] KN Madhusudhan and P Sakthivel. Combining digital signature with local binary pattern-least significant bit steganography techniques for securing medical images. *Journal of Medical Imaging and Health Informatics*, 10(6):1288–1293, 2020.

[74] D Shamia, K Balasamy, and S Suganyadevi. A secure framework for medical image by integrating watermarking and encryption through fuzzy based roi selection. *Journal of Intelligent & Fuzzy Systems*, (Preprint):1–9, 2023.

[75] Ashutosh Tripathi and Amit Verma. An intelligence system for visual cryptography technique relying on qr codes: A review.

[76] Muhammad Usama and Ulas Yaman. Embedding information into or onto additively manufactured parts: A review of qr codes, steganography and watermarking methods. *Materials*, 15(7):2596, 2022.

[77] Weixia Chen, Qin Li, Xiaoyan Tang, and Qiyong Pan. A digital watermarking method for medical images resistant to print-scan based on qr code. *Multimedia Tools and Applications*, pages 1–22, 2023.

[78] C Kavitha and S Sakthivel. An effective mechanism for medical images authentication using quick response code. *Cluster Computing*, 22:4375–4382, 2019.

[79] Jian Li, Zelin Zhang, Shengyu Li, Ryan Benton, Yulong Huang, Mohan Vamsi Kasukurthi, Dongqi Li, Jingwei Lin, Glen M Borchert, Shaobo Tan, et al. A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology. *BMC Medical Informatics and Decision Making*, 20:1–16, 2020.

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

[81] Rishi Sinhal, Sachin Sharma, Irshad Ahmad Ansari, and Varun Bajaj. Multipurpose medical image watermarking for effective security solutions. *Multimedia Tools and Applications*, 81(10):14045–14063, 2022.

[82] Jullius Kumar and Amit Kumar Singh. Copyright protection of medical images: A view of the state-of-the-art research and current developments. *Multimedia Tools and Applications*, pages 1–31, 2023.

[83] K Balasamy, N Krishnaraj, and K Vijayalakshmi. An adaptive neuro-fuzzy based region selection and authenticating medical image through watermarking for secure communication. *Wireless Personal Communications*, 122(3):2817–2837, 2022.

[84] Med Sayah Moad, Med Redouane Kafi, and Amine Khaldi. A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. *Microprocessors and Microsystems*, 90:104490, 2022.

[85] Rania A Ghazy, Alaa M Abbas, Nayel Al-Zubi, Emad S Hassan, Nawal A El-Fishawy, Mohiy M Hadhoud, Moawad I Dessouky, El-Sayed M El-Rabaie, Saleh A Alshebeili, and Fathi E Abd El-Samie. Block-based svd image watermarking in spatial and transform domains. *International Journal of Electronics*, 102(7):1091–1113, 2015.

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

[87] Muhammad Khoiruddin Harahap and Nurul Khairina. Copyright protection of scientific works using digital watermarking by embedding doi qr code. *Journal of Computer Networks, Architecture and High Performance Computing*, 3(2):234–240, 2021.

[88] Mohammed Abdul Majeed and Rossilawati Sulaiman. An improved lsb image steganography technique using bit-inverse in 24 bit colour image. *Journal of Theoretical & Applied Information Technology*, 80(2), 2015.

[89] MI Khalil. Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain. *International Journal of Computer Network and Information Security*, 9(2):22, 2017.

[90] Rohit Thanki, Surekha Borra, Vedvyas Dwivedi, and Komal Borisagar. A roni based visible watermarking approach for medical image authentication. *Journal of medical systems*, 41:1–11, 2017.

[91] Ambika and Rajkumar L Biradar. Secure medical image steganography through optimal pixel selection by eh-mb pipelined optimization technique. *Health and Technology*, 10(1):231–247, 2020.

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

[93] Lijing Ren and Denghui Zhang. A qr code-based user-friendly visual cryptography scheme. *Scientific Reports*, 12(1):7667, 2022.

[94] Khaldi Amine, Kafi Redouane, and Maghni Bilel. A redundant wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. *Multimedia Tools and Applications*, 82(5):7901–7915, 2023.

[95] Muzamil Hussan, Shabir A Parah, Solihah Gull, and GJ Qureshi. Tamper detection and self-recovery of medical imagery for smart health. *Arabian Journal for Science and Engineering*, 46:3465–3481, 2021.

[96] Soumen Biswas and Ranjay Hazra. State-of-the-art level set models and their performances in image segmentation: a decade review. *Archives of Computational Methods in Engineering*, 29(4):2019–2042, 2022.

[97] Abhilasha Sharma, Amit Kumar Singh, and Satya Prakash Ghrera. Robust and secure multiple watermarking for medical images. *Wireless Personal Communications*, 92:1611–1624, 2017.

[98] Xiyao Liu, Jieting Lou, Hui Fang, Yan Chen, Pingbo Ouyang, Yifan Wang, Beiji Zou, and Lei Wang. A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. *Ieee Access*, 7:76580–76598, 2019.

[99] Nisar Ahmed Memon and Ali Alzahrani. Prediction-based reversible watermarking of ct scan images for content authentication and copyright protection. *Ieee Access*, 8:75448–75462, 2020.

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

[101] David Mata-Mendoza, Manuel Cedillo-Hernandez, Francisco Garcia-Ugalde, Antonio Cedillo-Hernandez, Mariko Nakano-Miyatake, and Hector Perez-Meana. Secured telemedicine of medical imaging based on dual robust watermarking. *The Visual Computer*, 38(6):2073–2090, 2022.

[102] Hidangmayum Saxena Devi and Hitesh Mohapatra. A novel robust blind medical image watermarking using rank-based dwt. *International Journal of Information Technology*, 15(4):1901–1909, 2023.