**ACADEMIC MASTER**
**Ministry of Higher Education and Scientific Research**
**Kasdi Merbah Ouargla University**
**Faculty of New Information and Communication Technologies**
**Department of Electronics and Telecommunications**

# Master's Academic Thesis

**To obtain the Master's degree awarded by**

## Kasdi Merbah Ouargla University

### Speciality “Telecommunications Systems”

*Presented and publicly defended by*

**Lakehal Leila** And **AbdouAli Fatimazohra Dassine**

**Thesis title**

# Medical image watermarking applications

15 june 2023

**Jury**

| | | |
|---|---|---|
| Djalila Belkbir | MCA at Ouargla’s university | President |
| Nasri Nadjib | MAA at Ouargla’s university | Examiner |
| Moad Mohamed Sayah | MCB at Ouargla’s university | Advisor |

P
F
E

# Dedication

In the name of Allah the most compassionate the most merciful and peace be upon his Messenger.

Al hamdu li Allah who gave me enough energy to finish this work. I dedicate this to my parents who literally did everything they could to help me my brother my cousins especially Marwa and Mounir my uncle and everyone who supported me even with a small word of encouragement mat Allah bless them All. I'll always be grateful!

Leila Lakehal

Thanks Almighty God first and foremost for the great blessing bestowed on me,
Then I thank my beloved parents for supporting me from my birth until these blessed moments.
I thank my brothers and my fiancé and all my family and my friends.
To everyone who advised me, guided me, contributed with me,
Or directed me with me in preparing this research and linked me to Acknowledgements.

Abdouali fatimazohra dassine

# Acknowledgments

Thank Almighty God first and foremost for the great blessing Bestowed on us

Then we thank our beloved parents for supporting us

We would also like to thank the distinguished professor: Sayeh Moad, for helping us, supporting us, and guiding us with advice, education, and correction.

We are also pleased to thank the respected faculty administration: Kasdi Merbah Ouargla, the new Faculty of Information Technology and Communications, Department of Electronics and Communications.

And every other one who helped us with useful information

# Abstract:

With the increasing volume of medical digital images and the imperative to securely share them among specialists and hospitals for accurate diagnoses, safeguarding patient privacy has become a critical concern. Consequently, the demand for effective medical image watermarking techniques has emerged. However, the application of watermarking in this context necessitates meticulous attention for two primary reasons. Firstly, the integrity and quality of the image must remain uncompromised during the watermarking process. Secondly, the retrieval of confidential patient information embedded within the image after decompression should be error-free. Despite extensive research conducted in this field, a comprehensive method that meets all the requirements of medical image watermarking remains elusive. This study aims to fill this gap by providing a comprehensive survey of watermarking techniques, specifically focusing on the strengths and weaknesses of various existing methods, including DCT, SVD, and spread spectrum. By analysing these techniques, this research offers valuable insights and perspectives to interested researchers in the field of medical image watermarking. Ultimately, it strives to advance the understanding and implementation of secure and privacy-preserving practices in the sharing and analysis of medical digital images.

Key words: svd, dct, spread spectrum, watermarking

# Résumé:

Face à l'augmentation croissante du nombre d'images médicales numériques et à la nécessité de les partager entre spécialistes et hôpitaux pour des diagnostics plus précis et fiables, il est impératif de protéger la confidentialité des patients. C'est dans ce contexte qu'émerge le besoin de techniques de tatouage numérique spécifiquement adaptées aux images médicales. Cependant, leur application doit être réalisée avec une attention particulière pour deux raisons majeures. Tout d'abord, le processus de tatouage ne peut compromettre la qualité de l'image. Ensuite, les informations confidentielles des patients intégrées à l'image doivent pouvoir être récupérées sans risque d'erreur après la décompression de l'image. Malgré les nombreuses recherches menées dans ce domaine, aucune méthode ne remplit actuellement toutes les exigences du tatouage numérique pour les images médicales. Cette étude vise à combler cette lacune en proposant une enquête approfondie sur les techniques de tatouage numérique, en mettant particulièrement l'accent sur les forces et les faiblesses des différentes méthodes existantes, telles que la DCT, la SVD et l'Etalement de spectre. En analysant ces techniques, cette recherche offre des perspectives précieuses aux chercheurs intéressés par le tatouage numérique des images médicales. Elle contribue ainsi à promouvoir la compréhension et la mise en œuvre de pratiques sécurisées préservant la confidentialité dans le partage et l'analyse des images médicales numériques.

Mot clé: svd , dct , étalement de spectre , tatouage.

## ملخص:

مع زيادة أعداد الصور الرقمية الطبية والحاجة إلى مشاركتها بين الأخصائيين والمستشفيات لتشخيص أدق وأكثر دقة، فإن الحفاظ على خصوصية المرضى يتطلب اهتمامًا كبيرًا. ومن هذا المنطلق، ينشأ الحاجة إلى تقنيات تعتمد على وضع علامة مائية رقمية خاصة بالصور الطبية. ومع ذلك، يجب أن يتم هذا العمل بعناية خاصة لسببين رئيسيين. أولاً، يجب ألا يؤثر عملية وضع العلامة المائية على جودة الصورة. ثانيًا، يجب أن تكون المعلومات السرية للمرضى المضمنة في الصورة قابلة للاسترداد بدون خطر الخطأ بعد فك الضغط عن الصورة. على الرغم من البحوث الواسعة التي تم إجراؤها في هذا المجال، إلا أنه لا يزال لا يتوفر أي طريقة تستوفي جميع متطلبات وضع العلامة المائية للصور الطبية. تهدف هذه الدراسة إلى تقديم مسح مفيد حول تقنيات وضع العلامة المائية وتقديم وجهة نظر واضحة للباحثين المهتمين من خلال تحليل نقاط القوة والضعف للأساليب المختلفة المستخدمة مثلDCT, SVD وانتشار الطيف من خلال تحليل هذه التقنيات، تقدم هذه الدراسة رؤية مفيدة للباحثين المهتمين بوضع العلامة المائية للصور الطبية. وبذلك، تساهم في تعزيز الفهم وتنفيذ الممارسات الآمنة للحفاظ على الخصوصية في مشاركة وتحليل الصور الطبية الرقمية.

كلمات مفتاحية: SVD، DCT، انتشار الطيف، علامة مائية.

# Table of contents

# List of figures

# List of equations

# List of Abbreviation

**BER:** Bit Error Rate

**CT:** Computed Tomography

**DCT:** Discrete Cosine Transform

**DES:** Data Encryption Standard

**DICOM:** Digital Imaging and Communication in Medicine

**DSA:** Digital Signature Algorithm

**DFT:** Discrete Fourier Transform

**EPR:** Electronic Patient Record

**HIPAA:** Health Insurance Portability and Accountability Act

**HIS:** Hospital Information System

**ICT:** Information and Communication Technology

**ISCL:** Integrated Secure Communication Layer

**LBP:** Local Binary Pattern

**LSB:** Least Significant Bit

**MAC:** Message Authentication Code

**MSE:** Mean Square Error

**MRI:** Magnetic Resonance Imaging

**NC:** Normalized Correlation

**NVF:** Noise Visibility Function

**OFFIS:** Oldenburger Forschung und Entwicklungsinstitut Für Informatik

**PACS:** Picture Archiving and Communication System

**PSNR:** Peak Signal-to-Noise Ratio

**RIS:** Radiology Information System

**ROI:** Region of Interest

**RONI:** Region of Non-Interest

**SNR:** Signal-to-Noise Ratio

**SSL:** Secure Socket Layer

**SSIM:** Structural Similarity Index Measure

**SVD:** Singular Value Decomposition

**TAF:** Tamper Assessment Factor

**TLS:** Transport Security Layer

**WPSNR:** Weighted Peak Signal-to-Noise Ratio

# GENERAL INTRODUCTION

Medical imaging plays a critical role in healthcare, offering accurate diagnosis, treatment planning, and research. However, concerns regarding the authenticity, integrity, and ownership of medical images have prompted the development of various solutions, including steganography, watermarking, and cryptography.

Medical image watermarking has emerged as a valuable solution by embedding imperceptible yet robust information within the images. This watermark serves as a digital marker, verifying the image's authenticity, integrity, and protecting it from unauthorized use, tampering, or misinterpretation. Unlike general-purpose image watermarking, medical image watermarking addresses the specific requirements and challenges unique to medical images.

The primary objective of medical image watermarking is to ensure that the embedded information does not compromise the visual quality or diagnostic accuracy of the images. Imperceptibility is crucial in medical imaging, as even slight changes or artefacts introduced by watermarking can impact the interpretation by healthcare professionals. Another challenge is the robustness of the watermark against various image processing techniques, considering that medical images undergo transformations such as compression, resizing, and enhancement, which could potentially alter or remove the embedded watermark.

Ensuring the security and authentication of medical image watermarks requires robust encryption algorithms and secure key management techniques. Ethical and legal considerations, such as patient privacy and intellectual property rights, should also be addressed by watermarking techniques. The applications of medical image watermarking are diverse, contributing to patient data protection, research credibility, and clinical trials. By incorporating watermarking techniques, healthcare institutions, researchers, and imaging professionals can safeguard patient privacy, establish ownership, and maintain the trustworthiness of medical image data.

In Chapter 1, the significance of medical imaging is discussed, highlighting the need to protect patient privacy while sharing digital images among specialists and hospitals to enhance diagnostic precision.

Chapter 2 focuses on watermarking as a crucial technique in medical imaging. It emphasizes the importance of watermarking in safeguarding sensitive medical images and explores various applications and techniques. The chapter provides an in-depth analysis of different watermarking methodologies employed in medical imaging.

Chapter 3 introduces a novel watermarking technique that utilizes the Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and Spread Spectrum. This technique addresses challenges associated with preserving image quality and ensuring the accurate retrieval of confidential patient information after image decompression. The chapter presents a detailed explanation of the proposed watermarking technique, its implementation, and its potential advantages in protecting medical images.

.

# 1 Chapter 1: Medical Imaging

## 1.1 Introduction

Medical imaging plays a crucial role in modern healthcare, aiding in the diagnosis, treatment, and monitoring of various medical conditions. With the increasing adoption of digital systems for storing and transmitting medical images, the security of these sensitive data has become a significant concern. Protecting patient privacy, ensuring data integrity, and complying with regulatory standards such as DICOM (Digital Imaging and Communications in Medicine) and HIPAA (Health Insurance Portability and Accountability Act) are of utmost importance.

This chapter focuses on the security aspects of medical imaging, aiming to address the challenges faced in safeguarding medical image data. We will explore the potential vulnerabilities and risks associated with the digital management of medical images, including unauthorized access, data breaches, and the potential impact on patient confidentiality.

To mitigate these risks, various security measures are employed, including encryption, steganography, cryptography, and watermarking. Steganography involves hiding information within the medical image itself, while cryptography focuses on securing the communication channels and data storage. Watermarking, on the other hand, aims to embed imperceptible and tamper-resistant marks within the image for ownership verification and integrity protection.

Throughout this chapter, we will examine the principles and applications of these security techniques in the context of medical imaging. By understanding the challenges and available solutions, healthcare organizations can implement robust security measures to protect the privacy and integrity of medical images, ensuring the highest standards of patient care and data security.

## 1.2 Medical Imaging

Medical imaging is the medical field related to generating representative images of the internal structure of the human body, to diagnose, monitor or treat medical conditions these images help doctors with identifying abnormalities such as fractures, infections, and tumours, and plan an appropriate treatment.

## 1.3 Medical Imaging Types

There are many different modalities of medical imaging including X-rays, MRI resonance imaging), CT scan (computed tomography), ultrasound, and nuclear medicine scans. Each type uses different technology to create an image.

### 1.3.1 X-rays

Being one of the very first medical imaging modalities, X-rays has been commonly used soon after its discovery in 1895 in medical practices. Even though X-ray imaging is a projection technique and originally the image forms up on photosensitive film, direct digital X-ray imaging is becoming widely more used. The X-Rays are produced when electrons of high energy interact with the subject, we're studying converting the kinetic energy into electromagnetic radiation. While the surrounding tissues appear darker. X-rays can reveal very subtle features, they also are commonly used to detect bone fractures, infections, and tumours. However, they are not as effective at detecting soft tissue abnormalities, such as those in the brain or other organs this is due to the excellent contrast. The ionization of tissue along the beam path is an unwanted yet unavoidable side-effect of the photon-atom interaction. That last can lead to radiation damage repeated exposures therefore X-rays can be harmful, so they are generally only used when necessary and with proper precautions. The cost-effective equipment and the straightforward imaging procedure make the x-ray imaging quite popular [1][2].

### 1.3.2 CT scans computed tomography

In 1971, CT also called computed axial tomography became clinically available, and is the first medical imaging modality made possible by the computer. CT images are generated by passing X-rays through the body, at various angles, by rotating the X-ray tube around the body. Fractions of a second is the time that takes modern CT scans to generate a 2D cross-sectional image. Special microscopic CT scanners provide voxels of less than 10 µm while in-plane special resolution goes as low as 100µm. Using CT allows to detect small tumours, and structural detail in trabecular bone or the alveolar tissue in the lungs However, CT scans expose the patient to more radiation than a standard X-ray, so they are generally only used when necessary and with proper precautions. Due to it being costly clinical CT scans are not widely adopted like x-rays [1][2].

### 1.3.3 MRI Magnetic Resonance Imaging

Introduced in the late 1970s, Magnetic resonance imaging (MRI), is a type of volumetric imaging that shares some similarities with computed tomography (CT), but is based on fundamentally different physical principles. CT generates contrast by using high-energy photons and the interaction of photons with electrons of the atomic shell. In contrast, MRI is based on the orientation of protons inside a strong magnetic field. Resonant radiofrequency waves can manipulate this orientation, and the return of the protons to their equilibrium state can be measured. MRI is able to diagnose various pathologies due to their ability to discern different types of soft tissues with a better precision than CT making it the best choice to evaluate conditions such as herniated disks, ligament tears, and soft tissue tumours in the spine. However, MRI requires significantly more time for image acquisition than CT. Additionally, modern MRI scanners require a superconductive magnet with liquid helium cooling infrastructure, extremely sensitive radiofrequency amplifiers, and a complete room shielded against electromagnetic interference. As a result, MRI equipment is expensive, with costs of several million dollars for the scanner hardware and high recurring costs for maintenance. Nevertheless, MRI scanners provide images with a high diagnostic value, and MRI can be used to monitor some physiological processes (such as water diffusion and blood oxygenation) and therefore partly overlaps with nuclear imaging modalities. Since MRI is a radiation-free modality, it is often used in clinical studies with volunteers [2][3].

### 1.3.4 Ultrasound

Ultrasound imaging is a diagnostic imaging technique that utilizes the properties of sound waves in tissue. Low megahertz pressure waves travel through tissue at the speed of sound, undergoing refraction and partial reflection at interfaces. Ultrasound contrast is therefore dependent on echogenic in homogeneities in tissue. The travel time of the echo can determine the depth of an echogenic object. Emitting focused sound waves in different directions enables two-dimensional scans. Due to the complex relationship between inhomogeneous tissue and the echoes, ultrasound images are highly qualitative in nature. Differences in the speed of sound in different tissues and the weak signal and high amplification that result in a high noise component contribute to this complexity. While ultrasound images exhibit good soft tissue contrast, they are not effective in the presence of bone and air. Modern ultrasound devices use computerized image processing for image formation, enhancement, and visualization, although purely analogue circuitry can be used to generate ultrasound images. Ultrasound imaging is a popular diagnostic tool due to its low-cost instrumentation and ease of use. However, the presence of an experienced operator is necessary to adjust various parameters for optimum contrast, and an experienced radiologist is often required to interpret ultrasound images [2].

### 1.3.5 Nuclear medicine

Nuclear imaging employs radiation, similar to X-ray and CT imaging, but distinct in that it uses radioactive compounds that are injected into the body as radiation sources. These compounds, referred to as radiopharmaceuticals, are typically linked to pharmacologically active substances and accumulate in specific body sites, such as tumours. The spatial distribution of the radiopharmaceutical can be determined by projection techniques or volumetric computerized image reconstruction. This allows for imaging of metabolic processes and subsequent diagnosis. Single-photon emission computed tomography (SPECT) is a modality that uses three-dimensional reconstructions similar to CT imaging. Positron emission tomography (PET) is a parallel technology that uses positron emitters to cause coincident pairs of gamma photons to be emitted, with better detection sensitivity and signal-to-noise ratio than SPECT. However, both SPECT and PET have significantly lower resolution than CT imaging, with voxel sizes not much smaller than 1 cm. SPECT or PET images are often superimposed with CT or MR images to provide a spatial reference. The cost of nuclear imaging modalities is a limiting factor for their widespread use. Additionally, the radioactive labels are short-lived, with half-lives of mere hours, and most radiopharmaceuticals need to be produced on-site, requiring nuclear imaging centres to have some form of reactor for isotope generation [2].

## 1.4 Digital images

A digital image is an array of non-negative integer function in two dimensions (2-D), denoted as f(x, y), where x and y are positive integers representing coordinates of a small square (pixel) in the image. The pixel is located within the range of 1 to M for x and 1 to N for y [4].

## 1.5 Digital medical images

According to [4], the terms 'digitized' or 'digital' are used to refer to medical images that are obtained through a digitizer or generated digitally. The pixel or voxel value, also known as grey level value, can range from 0 to 255 (8-bit), 0 to 511 (9-bit), 0 to 1023 (10-bit), 0 to 2045 (11-bit), and 0 to 4095 (12-bit), depending on the digitization or image generation procedure used. These grey levels indicate the physical, chemical, and physiological properties of anatomical structures or physiological processes when the image was captured. For instance, in an x-ray film image, the grey level value of a pixel represents the optical density of the small square area of the film. In the case of XCT, the pixel value represents the relative linear attenuation coefficient of the tissue, while in MRI, it corresponds to the magnetic resonance signal response of the tissue. Ultrasound imaging utilizes the echoes produced by the ultrasound beam as it passes through tissues, while endoscopic images are created using pixel values that represent light signals.

## 1.6 Security Requirements of Medical image

The protection of patient privacy is a requirement of the Health Insurance Portability and Accountability Act (HIPAA) through the implementation of medical image security [5]. The DICOM standard provides an optional guide for producing medical images, but in telemedicine, medical images are transmitted via a network between the referring and expert sites. Therefore, security becomes a crucial issue just to store data in the medical system but also for transmitting data over the network in telemedicine to maintain patient confidentiality, authenticity, and integrity [6]. Confidentiality involves restricting access to patient information, while integrity refers to the safety of medical images transmitted from any tampering, modifying, or changing. Additionally, authenticity is used to verify the image source, confirming that it belongs to the right patient. To ensure the highest security levels for patient information and medical data, extensive work is being done in this area. The following section will examine the characteristics of medical images.

### 1.6.1 Safeguarding the Confidentiality of Medical Images and Patient Information

Preserving the confidentiality of patient information is necessary to maintain the sensitive data’s privacy and security. Confidentiality ensures that only the authorized individuals have the necessary access, modification, and processing rights while preventing unauthorized users from accessing or alternating any data. It serves is an initial step in safeguarding patient information and upholding their privacy [7].

Strict adherence to legal and ethical standards is essential to maintain the confidentiality of patient information. The information must possess a critical attribute: trustworthiness. During data transitions upholding confidentiality is particularly vital, where measures must be in place to ensure information remains confidential. Furthermore, maintaining the security of patient data within the responsible team, which may include physicians, lab workers, and other involved parties is crucial [8].

Breaking confidentiality may be legally permissible, under certain circumstances. For instance, if patients provide their consent to disclose their information or if it contributes to improving and benefiting the public health sector, confidentiality can be breached [9].

### 1.6.2 Ensuring the Integrity of Medical Images

Maintaining the accuracy and reliability of medical images requires upholding integrity as a fundamental aspect. This involves preventing any intentional or unintentional modifications by non-authorized individuals. The responsibility of detecting and mitigating any illegal attempts to compromise the integrity of medical information lies with those managing the data within telemedicine systems [10].

To ensure integrity, health informatics professionals adhere to a code of ethics that provides guidance and principles for safeguarding health information, including medical images. This ethical framework serves as a cornerstone for promoting responsible and secure handling of patient data [11].

### 1.6.3 Achieving Reliable Medical Image Authentication

The goal of medical image authentication is to establish the source and ownership of an image while preserving its originality during transmission. This process aims to prevent any falsification or unauthorized alterations during data exchange. Medical image authentication techniques play a crucial role in enhancing tamper detection and recovery mechanisms. Authentication and integrity are closely intertwined, as the verification of authenticity contributes to maintaining overall data integrity [12].

The process of medical image authentication involves inserting data from the source into a host image, which is then transmitted to the receiver. The embedded data is extracted by the receiver from the host image determining its authenticity. Authentication schemes of medical image can be classified into two main categories: those based on digital signatures (metadata) and those using watermarking techniques [13].

To verify the authenticity of medical images, header data or digital signatures are stored alongside the images. These additional measures serve as validation mechanisms and further contribute to maintaining the integrity and security of the data [14]. Watermarking, a widely adopted method, involves embedding invisible information within the host data, enabling subsequent extraction and verification of the image's authenticity [15].

## 1.7 Picture archiving and communication system (PACS)

PACS plays an indispensable role as a central server to manage medical images. It receives and stores images from various sources such as the Hospital Information System (HIS) and Radiology Information System (RIS). PACS encompasses a range of radiological imaging modalities and contains patient information along with case-related data. The core components of PACS are the database server and archiving system, which are essential for its functioning.

When the HIS and RIS transmit examination images to the PACS server, the system extracts descriptive data from the DICOM header. It then updates the database system, sets boundaries, and manages the newly generated data. In situations where the volume of information is substantial, PACS compresses and stores the data or updates the database accordingly.

PACS can be seamlessly integrated with Teleradiology systems in the medical field, enabling the exchange of vital patient data. As a server housing the hospital's medical image database, PACS can receive medical images from external imaging centres and distribute reports to the HIS and other medical expert systems within the hospital. Additionally, in a Teleradiology model, the image centre can transmit the images directly to the expert system [16].

## 1.8 Digital Imaging and Communication in Medicine (DICOM)

The need for a standardized format for medical images arose due to the incorporation of various digital products, modalities, archiving, and information within medical systems. In response to this, Digital Imaging and Communications in Medicine (DICOM) was established as the standard format for storing, transmitting, saving, and utilizing medical images. The collaboration between The American College of Radiology (ACR) and the National Electrical Manufactures Association (NEMA) led to the creation of DICOM in 1983, aiming to establish a standardized approach for data transfer. The initial ACR-NEMA standard versions were published in 1985, improving the storage and transfer of data in a non-proprietary form. Subsequent versions of DICOM, particularly version 3 released in 1993, introduced enhancements such as network protocol integration through TCP/IP. The data structure model of DICOM revolves around specific definitions for services and objects, including image objects and patient objects.

Within the DICOM header, essential components include patient information, physician details, and hospital information, collectively referred to as information object definitions (IODs). Each object within the header carries its own significance. The data is organized into different groups, with each group containing related data. For instance, group 10 encompasses patient data and unique identifiers (UIDs) pertaining to image technology details such as X-ray exposure.

Moving on to the DICOM body, it contains crucial information about the patient case. This data can be categorized into the region of interest (ROI), typically located at the centre, and the region of non-interest (RONI), representing the image's borders. Figures I.1 and I.2 in the mentioned resource illustrate the components of a medical image [17].

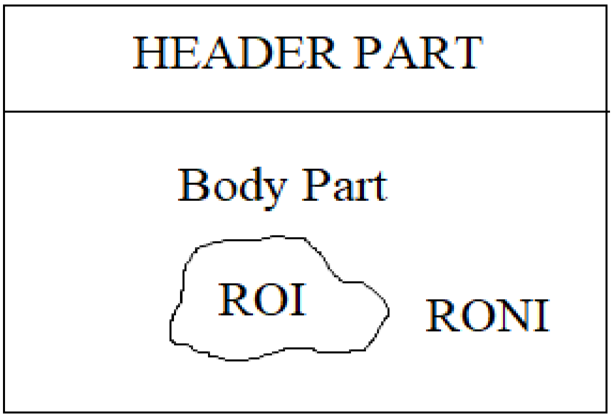


Figure 1-1 Medical Image components

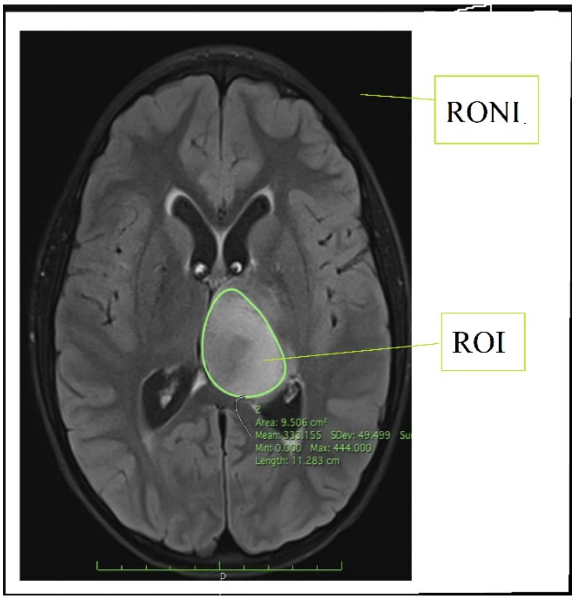


Figure 1-2 Medical image ROI & RONI

DICOM services continue to be developed and enhanced through research, and OFFIS (Oldenburger Forschung und Entwicklungsinstitut Für Informatik The Oldenburger Institute) serves as the main European partner for the DICOM team. OFFIS is a German institution founded in 1991 and located in Oldenburg.

OFFIS is actively involved in research and development across various domains, including energy, health, and transportation. They are dedicated to advancing knowledge and innovation in these areas, and their collaboration with the DICOM team is part of their broader research efforts [18].

## 1.9 DICOM Security Profiles: Enhancing Medical Image Security

DICOM, as a medical image standard, recognizes the importance of addressing security concerns [19]. In order to enhance security, four security profiles have been introduced to DICOM, namely secure use profiles, secure transport connection profiles, digital signature profiles, and media storage secure profiles [19]. These profiles focus on various attributes and employ measures such as association security, object authentication, and file security. Let's delve into each of these security profiles in detail.

### 1.9.1 Secure Use Profiles:

Secure use profiles provide guidelines for utilizing attributes and other security profiles in specific modes. These profiles encompass secure practices for online electronic storage, bit maintenance, and electronic signatures. By adhering to these profiles, healthcare professionals can ensure the secure handling of sensitive medical data.

### 1.9.2 Secure Transport Connection Profiles:

Secure transport connection profiles are designed to facilitate secure data exchange over networks and the internet within DICOM applications. They employ techniques similar to the secure socket layer (SSL) used in securing online websites. These profiles leverage asymmetric cryptography, allowing only the intended recipient to access and decode the transmitted message. Two options for implementing secure transport connection are transport layer security (TLS) and integrated secure communication layer (ISCL). These profiles mandate specific features that must be implemented within DICOM to establish a secure transport connection.

### 1.9.3 Digital Signature Profiles:

Digital signature profiles enable integrity checks for digital signatures in DICOM. A digital signature validates the identity and integrity of DICOM data that has been generated, approved, or modified. The process involves the digital signature generator identifying the DICOM data set, embedding the MAC (Message Authentication Code) and hash value, and subsequently embedding the MAC value within the digital signature. The receiver can verify the authenticity and integrity of the received data by recalculating the MAC value and comparing it to the embedded MAC value. The profiles offer three methods of digital signature implementation: base, creator, and authentication, depending on the content to be embedded in DICOM.

### 1.9.4 Media Storage Security Profiles:

To safeguard DICOM data against unauthorized access, media storage security profiles provide a secure mechanism. These profiles employ cryptographic techniques to compress data with a cryptographic wrapper, defining a structure for DICOM protection. Asymmetric cryptography techniques are applied, enabling image encryption using algorithms such as DES (Data Encryption Standard) and DSA (Digital Signature Algorithm). However, it is important to note that once the information is decrypted, its security is compromised. Therefore, verifying the authenticity and reliability of decrypted data becomes challenging [20]. In addition, the DICOM security standard does not fully address the confidentiality and integrity of medical image data. Malicious individuals can easily manipulate the header and create fake images. As a solution, watermarking can be considered to ensure data confidentiality and integrity during storage and transmission [21].

Furthermore, the field of medical data security employs watermarking and cryptography techniques to enhance image security. These techniques are used to improve the confidentiality, authenticity, and integrity of medical data.

Let's take a closer look at the sender and receiver sides of the encryption and embedding methods:

At the sender side:

1. Image pre-processing: This involves segmenting and extracting relevant patient information from the DICOM header.

2. Data encryption: Medical data is encrypted, generating a ciphered data form.

3. Data embedding: Secret information is embedded within the medical data.

At the receiver side:

1. Extraction of secret information: The secret information is extracted from the received medical data.

2. Decryption of medical data: The medical data is decrypted to its original form.

3. Ensuring integrity, authenticity, and confidentiality: The received data is validated to ensure its integrity, authenticity, and confidentiality.

## 1.10 Applications of Medical Image Security

Numerous studies have proposed various techniques for ensuring the security of medical images, including watermarking and cryptography methods. This section highlights the most significant and crucial approaches for watermarking and cryptography applications in the field of medicine. While many works have focused on the spatial domain, only a few have explored watermarking techniques in the frequency domain. Research findings suggest that the frequency domain surpasses the spatial domain in terms of security robustness. However, the spatial domain exhibits greater complexity. Given the real-time nature of the applications (such as Telemedicine), this study primarily concentrates on the spatial domain to achieve a lower complexity objective while also aiming to enhance the balance between robustness, capacity, and imperceptibility requirements. In the medical sector, security applications can be broadly categorized into two types. The first type encompasses pure watermarking techniques employed in both the frequency and spatial domains. The second category involves medical image applications that rely on a combination of cryptography and watermarking techniques. These applications are specifically geared towards safeguarding medical images.

### 1.10.1 Applications of Steganography in Security

Cryptography plays a vital role in ensuring the security and privacy of medical image data. It enables the encryption and decryption of sensitive information, protecting it from unauthorized access and ensuring secure transmission and storage. Cryptographic techniques such as symmetric and asymmetric encryption, digital signatures, and secure key exchange provide robust mechanisms for securing medical images and preventing tampering or unauthorized modifications. By employing cryptographic algorithms and protocols, healthcare providers can maintain the confidentiality and integrity of patient data, comply with privacy regulations, and mitigate the risks associated with data breaches and cyber threats in the context of medical imaging.

### 1.10.2 Applications of Steganography in Security

Steganography finds utility in various practical applications, serving purposes such as copyright control for materials, enhancing the resilience of image search engines, and embedding individuals' details in smart IDs (identity cards) along with their photographs. Furthermore, it facilitates video-audio synchronization, secure data transmission in business environments, TV broadcasting, embedding unique IDs into TCP/IP packets (e.g., to analyse network traffic of specific users) [22], and embedding checksums [23]. Petitcolas [24] illustrated several modern applications, including Medical Imaging Systems, where the need for confidentiality between patients' image data or DNA sequences and their corresponding captions (e.g., physician, patient's name, address, etc.) necessitates a separation. However, a connection must be maintained between the two, making the embedding of patient information within the image a valuable security measure for addressing such concerns. Steganography provides an unmatched assurance of authentication that other security tools cannot deliver.

### 1.10.3 Applications of Watermarking in Medical Images

Watermarking is a valuable technique used to enhance the security and authenticity of medical imaging. It involves embedding imperceptible but identifiable markers within the image to verify its integrity and origin. In the field of medical imaging, watermarking serves multiple purposes. It protects against unauthorized modifications, detects tampering, and ensures the traceability of images. By embedding unique identifiers or digital signatures, watermarking enables the authentication of medical images, preventing the use of counterfeit or manipulated images for diagnosis or research. Watermarking techniques have found various applications in the field of medical imaging. Some key applications of watermarking in medical images include:

**Ownership Protection**: Watermarking can be used to protect the ownership and intellectual property rights of medical images. By embedding a unique watermark into the images, it becomes possible to identify and trace the original source or owner of the images. This is particularly important in cases where medical images are shared, distributed, or used for research purposes.

**Authentication and Integrity Verification:** Watermarking can ensure the authenticity and integrity of medical images. By embedding a digital watermark into the images, any unauthorized modifications or tampering attempts can be detected. This is crucial for maintaining the trustworthiness and reliability of medical image data, especially in critical applications such as diagnosis, treatment planning, and research studies.

**Data Security and Patient Privacy**: Medical images often contain sensitive patient information. Watermarking can be used to protect patient privacy by embedding patient-specific watermarks or invisible digital signatures into the images. This enables the identification and tracking of images, ensuring that they are not disclosed or used without proper authorization.

**Content Identification and Tracking**: Watermarking can facilitate the identification and tracking of medical images throughout their lifecycle. Each image can be embedded with a unique watermark that carries information about the patient, healthcare provider, acquisition date, or other relevant metadata. This helps in organizing and managing large medical image databases, ensuring accurate retrieval and proper documentation.

**Research and Clinical Trials**: Watermarking can be applied to medical images used in research studies and clinical trials. By embedding watermarks, it becomes possible to identify and track specific image datasets, ensuring the integrity and traceability of the data. This is particularly important for maintaining research integrity, reproducibility, and adherence to regulatory requirements.

**Forensic Analysis**: Watermarking techniques can aid in forensic analysis and investigation of medical image tampering or unauthorized use. If a medical image is tampered with or used without proper authorization, the embedded watermarks can serve as evidence to identify the source and track the distribution of the image.

These are just a few examples of how watermarking can be applied in the context of medical images.

### 1.10.4 The Relationship between Watermarking, Cryptography, and Steganography

The concept of watermarking is closely related to the two fields: cryptography and steganography, all of which fall under the broader domain of data security systems (as depicted in Figure 1.3).

Cryptography is a method used to securely transmit an encrypted message that can only be decoded by the authorized recipient. However, once the message is decrypted, it is no longer protected. This is the primary distinction between cryptography and watermarking.

Steganography, on the other hand, involves hiding a message or information within another data such as an image, video, or audio file. [25] The objective of steganography is to make the hidden data undetectable. In other words, the presence of the hidden message should not be apparent to an observer. The goal of steganography is to achieve secrecy or confidentiality.

In contrast, watermarking serves a different purpose. The primary objective of watermarking is to embed a message or identifier into a digital object (such as an image or audio file) in a way that it cannot be easily removed or altered. Watermarks are often used for purposes such as copyright protection, content authentication, or ownership verification. Unlike cryptography or steganography, watermarking is not primarily concerned with concealing the presence of the embedded message but rather with ensuring its persistence and resilience.

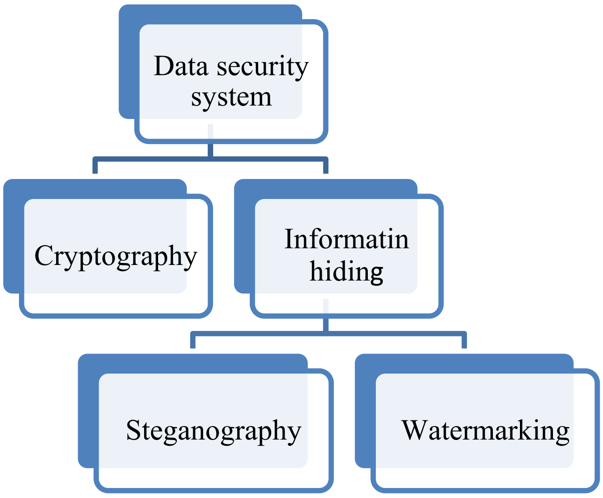


**Figure 1-3 data security system field[26]**

.

## Conclusion

In conclusion, medical imaging plays a pivotal role in the diagnosis, monitoring, and treatment of various medical conditions, employing diverse modalities and technologies. Digital medical images, represented as pixel or voxel arrays, provide valuable insights into the internal structures and physiological processes of the human body. It is imperative to ensure the security of these images to safeguard patient privacy and comply with regulatory requirements.

To protect the confidentiality and integrity of medical images, the implementation of robust security measures such as encryption, access controls, and adherence to legal and ethical standards is crucial. Additional authentication techniques, including digital signatures and watermarking, can further enhance the overall security posture.

The Picture Archiving and Communication System (PACS) acts as a centralized server for the management of medical images, facilitating storage, retrieval, and distribution. DICOM, the standardized format for medical images, incorporates patient and physician information, as well as technological details, thereby enabling efficient data transfer and interoperability.

Moving forward, our research focus will be centred on watermarking techniques in the context of medical imaging. Watermarking methodologies can effectively embed imperceptible marks within medical images, serving to establish ownership, authenticity, and integrity. Through our investigations, we aim to explore how watermarking can strengthen security measures, offering robust protection against unauthorized utilization or tampering of medical images.

# 2 Chapter 2: Watermarking

## 2.1 Introduction

In the past few years, the use of Information and Communication Technology (ICT) for distributing digital documents through open channels has become essential and cost-effective. However, ensuring copyright protection, ownership identification, and preventing identity theft remain significant challenges due to malicious attacks and hacking attempts on open channels. These attacks aim to tamper with or remove document watermarks to falsely claim ownership or hinder the intended information transfer. Consequently, researchers have been actively seeking solutions to address these critical challenges.

A well-known concept in invisible communication, called the prisoner's problem, was introduced by Simmons in 1984. This concept revolves around two prisoners attempting to devise an escape plan without alerting a warden. They must communicate covertly by hiding meaningful information within a cover message to avoid arousing suspicion from the warden [27][28].

The advancements in high-bandwidth digital communication technologies have revolutionized the transmission of medical data across various geographical boundaries, including remote and rural areas, using the internet, mobile networks, and other communication channels [29]. However, transmitting medical data over open channels poses risks to its authenticity, integrity, and confidentiality. This necessitates the development of effective medical image watermarking schemes to ensure the secure exchange of patient records. Embedding additional data within medical images must be done with care to avoid compromising image quality while preserving the confidentiality, reliability, and availability of electronic patient records exchanged through unsecured channels [29-32].

The field of digital watermarking has experienced significant growth in the last few decades, driven by advancements in multimedia data processing, digital signal processing, and computational platforms. Digital watermarking, closely associated with steganography, involves the insertion of data (watermark) into digital multimedia cover objects to establish their authenticity and originality. This technique finds applications in asserting ownership, establishing fingerprints, preventing unauthorized copying, facilitating secure telemedicine, enabling secure e-commerce, and more [33].

Furthermore, medical images have gained prominence in telemedicine services such as telemedicine, tele-ophthalmology, tele-diagnosis, and tele-consultancy. These images facilitate prompt diagnosis, improve understanding of critical diseases, and help prevent misdiagnosis. However, the rising concern of medical identity theft in the field of telemedicine emphasizes the crucial role of medical image watermarking in ensuring the authenticity, integrity, and confidentiality of transmitted medical data [34, 35].

## 2.2 Importance and necessity of watermarking

Although cryptography is a widely used technique for protecting digital content, it lacks the ability to monitor how the content is handled after decryption. This limitation can lead to illegal copying, distribution, or misuse of private information. Cryptographic techniques provide content protection during transit but offer no further safeguards after decryption. To address this limitation, watermarking techniques have emerged, which protect the content even after decryption. Watermarking involves embedding imperceptible watermark information into the main content, ensuring that the watermark remains intact during normal usage without causing inconvenience to users. Watermarks can withstand processes such as decryption, re-encryption, compression, and geometrical manipulations, providing enhanced content protection [36]. In the context of telemedicine applications, where digital imaging and communications in medicine (DICOM) standards are used to communicate electronic patient record (EPR) data, the protection of the accompanying header information during transmission and storage is crucial. Watermarking techniques can effectively address this issue, ensuring security and authenticity of the header information [37].

## 2.3 Watermarking framework

The watermarking system follows a framework that consists of two main processes: encoding and extraction. [38].

This framework is illustrated in Figure 2-1. In the encoding process (Figure 2-1 a), there are three inputs: a watermark, the original cover media, and an optional public or secret key. These inputs are used to generate a watermarked image.

The extraction process (Figure 2-1 b) takes as input the watermarked image or original data (cover), along with the secret or public key and test data. This process allows for the determination of the cover image and its ownership.

In general, a watermarked cover image (W) can be expressed as a function (F) of the watermark data (Wd), the cover data (Cd), and the secret key (K), as shown in equation 2-1

$$\mathbf{W} = \mathbf{f}(\mathbf{Wd}, \mathbf{Cd}, \mathbf{K}) \quad 2\text{-}1$$

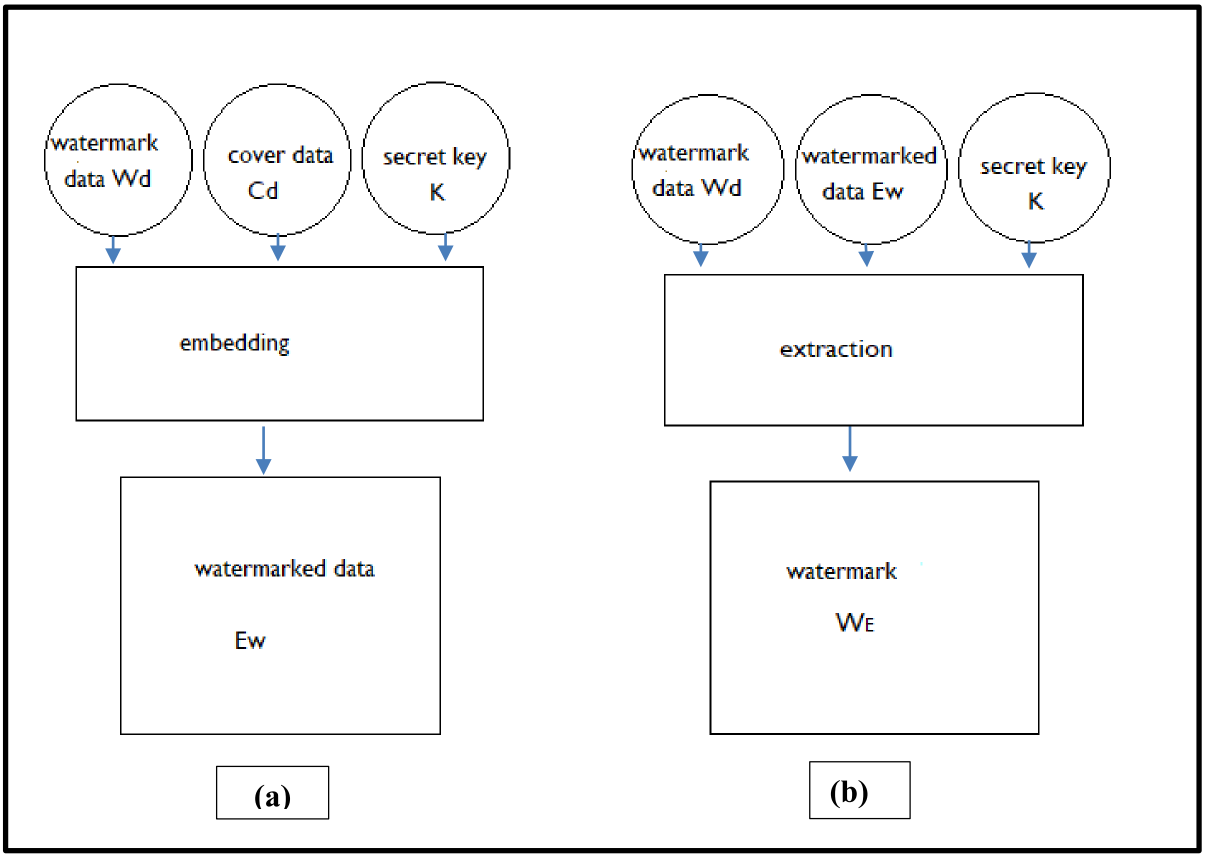


**Figure 2-1 the watermark process (a) the embedding (b) the extraction**

The watermark embedding process, denoted as E (W), can be defined as:

$$(\boldsymbol{Ew}) = \boldsymbol{f}(\boldsymbol{Wd}, \boldsymbol{Cd}, \boldsymbol{K}) \quad 2\text{-}2$$

Similarly, the watermark extraction process, denoted as W', can be defined as:

$$\boldsymbol{We} = \boldsymbol{f}(\boldsymbol{WorCd}, \boldsymbol{Ew}, \boldsymbol{K}) \quad 2\text{-}3$$

## 2.4 Digital Watermark Classifications

According to S.P. Mohanty [39] Watermarks can be classified into three main types:

**Visible Watermark**: A visible watermark is a secondary translucent overlay that is superimposed onto the primary image. This type of watermark is intentionally made visible to viewers and can be easily noticed upon careful inspection. Visible watermarks are commonly used for branding or indicating ownership of the image.

**Invisible-Robust Watermark**: An invisible-robust watermark is embedded in such a way that any alterations made to the pixel values of the image are not perceptually noticeable. This type of watermark is designed to be robust against common image processing operations, such as compression or cropping. Proper decoding mechanisms are required to extract the watermark from the watermarked image.

**Invisible-Fragile Watermark**: An invisible-fragile watermark is embedded in a manner that makes it sensitive to any modifications or tampering of the cover image. Even slight modifications or manipulations of the image can alter or destroy the watermark. This type of watermark is useful for ensuring the integrity and authenticity of the image content.

In addition to these types, there is a dual watermark which combines both visible and invisible watermarks. This approach provides both a visual indication of ownership and embedded information for authentication or tracking purposes.

Watermarking techniques can also be categorized based on the working domain, such as spatial domain or transform domain. Furthermore, from an application viewpoint, watermarks can be source-based or destination-based. Source-based watermarking embeds a unique watermark identifying the owner into all copies of the cover image being distributed, while destination-based watermarking assigns a unique watermark to each distributed copy to identify the specific buyer and trace illegal distribution or reselling.

Watermarking techniques can also be classified as reversible or irreversible. Reversible techniques aim to avoid irreversible distortions in the host cover image by allowing extraction of the watermark from the watermarked document. These techniques are preferred for medical image watermarking to minimize the risk of incorrect diagnosis.

Overall, the selection of a watermarking technique depends on the specific requirements and application scenarios, considering factors such as visibility, robustness, fragility, and reversibility.

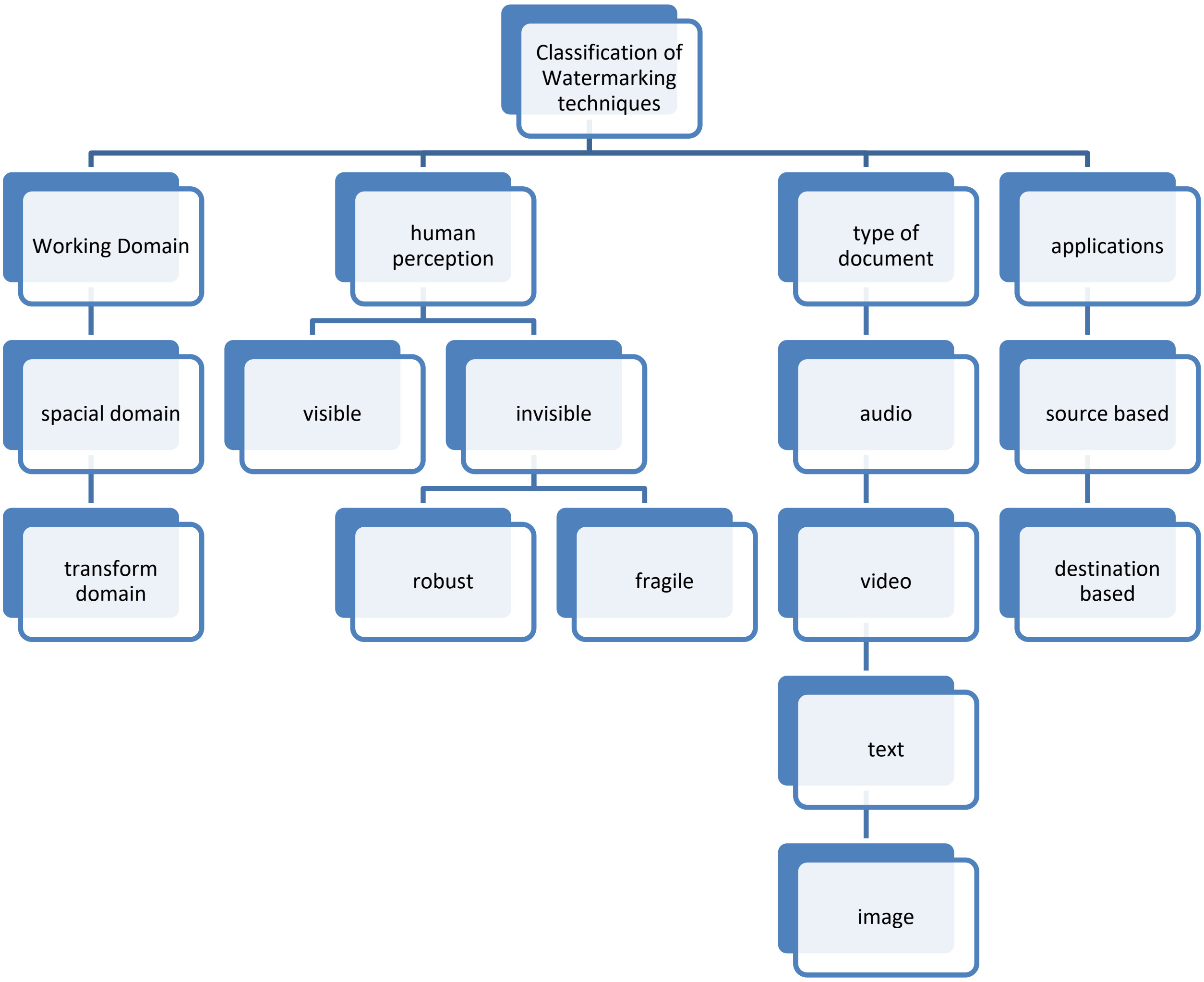


**Figure 2-2 Classification of Watermarking techniques**

## 2.5 Characteristics, applications and attacks related to watermarking

Figure 2-1sums up watermarking characteristics, the applications and the attacks that might occur to the watermark:

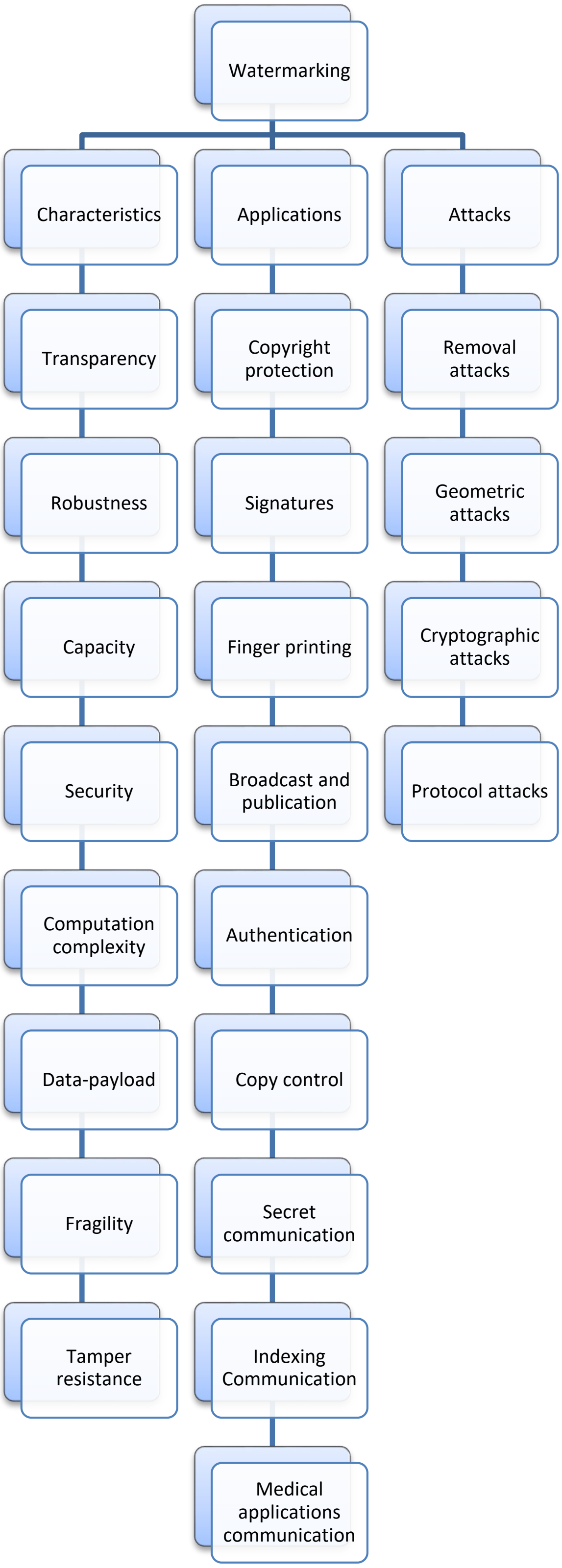


Figure 2-3 Watermarking: Characteristics Applications and Attacks

### 2.5.1 Potential Characteristics of Digital Watermarks

Digital watermarks should possess several key characteristics, as illustrated in Figure 2-1. These requirements ensure the effectiveness and functionality of watermarks. The following properties are desirable for an image watermark:

1. **Transparency**: When embedding a watermark in an image, it is crucial that the quality of the image and the conveyed message remain undistorted. The embedded watermark should be imperceptible to the viewer, maintaining perceptual similarity between the watermarked and original images. In certain cases, imperceptibility may be compromised to achieve a higher level of robustness or reduce costs.
2. **Robustness**: Watermarks should be resilient against various attacks, both geometric and non-geometric in nature [40]. It should be extremely difficult or impossible to eliminate or manipulate watermarks without adequate knowledge of the specific embedding process pertaining to the particular fields involved.
3. **Capacity**: Watermarked images should have the ability to carry a suitable amount of information, known as the data payload. The number of bits encoded [41] in the watermarking process and the image information should offer an adequate combination for the intended application.
4. **Security**: Watermarks should be protected using secret keys to prevent unauthorized alterations. Strong security measures should safeguard against unauthorized additions, deletions, or updates made by individuals without specific knowledge of the secret key.
5. **Computational Complexity**: The computational complexity of watermarking algorithms, involving encoding and decoding, is an important consideration. High computational complexity is often necessary to establish robust security measures and ensure the validity of watermarks. For real-time applications, efficiency and speed are crucial factors.
6. **Data Payload**: The data payload of a watermark refers to the amount of information it contains. A good watermark should be able to encapsulate all the required data within a small, arbitrary portion of the cover image, enabling efficient and compact representation.
7. **Fragility**: Fragile watermarks focus on content authentication. They are designed to detect even slight modifications in the watermarked content, differentiating them from digital signatures that require a 100% match.
8. **Tamper Resistance**: Tamper-detection mechanisms in watermarks are employed to verify the authenticity of digital photographs. Watermarks of this type are sensitive to any changes in the watermark data. By checking the integrity of the watermark, the system can determine whether the watermark has been modified or replaced.

### 2.5.2 Applications of Watermarking

Digital watermarking has a range of uses [42], as seen in Figure 2-1. Generally, applications of watermarking techniques can be divided into categories. These include a variety of potential applications, all of which serve to meet different needs and requirements. Some of the potential applications of watermarking include:

1**. Copyright Protection**: One of the primary applications of watermarking is to protect copyrighted content. By detecting the original owner of digital media, watermarks help prevent unauthorized alterations to the content. The goal is to ensure that no additional information can be attached or modified without significantly changing the digital media.

2**. Signatures**: Watermarks can be used to recognize the owner of the content, granting them control over legal rights for copying or publishing the data. This application enables the authentic owner to maintain authority over their content.

3**. Fingerprinting**: Watermarks serve as unique identifiers, allowing the identification of buyers of content. This application is particularly valuable in tracking the origin of illegal copies of digital media [43].

4**. Broadcast and Publication Monitoring**: Watermarking techniques, such as signatures, aid in detecting the owner of the content. In broadcast and publication monitoring, automated systems are employed to monitor possible computer networks, television and radio broadcasts, and other distribution channels. This application enables the tracking of when and where the content appears.

5**. Authentication**: Watermarks can encode information to verify the originality of the content. By examining the watermark, authenticity can be established.

6**. Copy Control**: Watermarks can contain information regarding usage and copying rules enforced by the content owner. These rules may range from simple restrictions like "no replication allowed" to more complex conditions, such as allowing copying but prohibiting subsequent replicas of the copy.

7**. Secret Communication**: Watermarks can be utilized for secret communication [44]. The signals are embedded within the transmission of confidential information from one location to another.

8**. Indexing**: Watermarking enables indexing in applications like video mail, where comments can be embedded within the video content. It also facilitates the insertion of markers and comments in movies and news items, which can be utilized by search engines for efficient retrieval.

9**. Medical Applications**: Watermarking plays a significant role in medical applications, offering both authentication and confidentiality without impacting the medical image. The secure transmission, storage, and sharing of Electronic Patient Record (EPR) data between hospitals or through open/unsecured channels are crucial concerns. Medical image watermarking must carefully embed additional data without compromising image quality. Confidentiality, authentication, integrity, and availability are vital security requirements for EPR data exchange.

Watermarking plays a crucial role in ensuring the confidentiality, authentication, integrity, and availability of Electronic Patient Record (EPR) data exchange in medical applications. It provides both authentication and confidentiality in a reversible manner without affecting the medical image. Watermarking techniques are particularly important in telemedicine, tele-ophthalmology, tele-diagnosis, tele-consultancy, tele-cardiology, and tele-radiology applications where the secure transmission, storage, and sharing of EPR data are essential. These applications highlight the diverse range of needs that watermarking can address, providing security and protection to various types of digital content.

### 2.5.3 Attacks

In the context of digital watermarking, attacks refer to attempts to modify or undermine the embedded watermark in the host signal. [45] These attacks can be categorized into four main groups:

1**. Removal Attacks:** These attacks are carried out with the intention of completely removing the watermarks from the host signal. Attackers may employ various techniques to eliminate or destroy the watermark, such as signal processing algorithms or modifications to the file format.

2**. Geometrical Attacks**: Geometrical attacks aim to disrupt or damage the embedded watermark without necessarily removing it. Common geometric attacks include rotation, cropping, and scaling of the host signal. These transformations can alter the watermark's spatial characteristics, making it more difficult to detect or extract.

3**. Cryptographic Attacks**: Cryptographic attacks focus on breaking the security methods employed in watermarking schemes. Attackers may attempt to decipher the encryption or cryptographic algorithms used to protect the watermark, with the goal of unauthorized extraction or manipulation.

4**. Protocol Attacks**: Protocol attacks target the entire scheme of watermarking, rather than specifically focusing on the watermark itself. These attacks exploit vulnerabilities in the communication protocols or system architecture used for embedding, transmitting, or extracting watermarks. By compromising the overall framework, attackers can undermine the effectiveness or integrity of the watermarking process.

It is important for watermarking techniques to be resilient against these various types of attacks to ensure the security and reliability of the embedded watermarks. Researchers and developers continuously work on improving the robustness of watermarking algorithms to withstand different attack scenarios.

## 2.6 Watermarking Techniques

Watermarking techniques are used to embed hidden information or digital watermarks into digital media such as images, audio, or video files. These watermarks are imperceptible to the human eye or ear but can be extracted or detected using specialized algorithms. The purpose of watermarking is to provide copyright protection, content authentication, or data integrity verification. There are two main types of watermarking techniques: spatial domain and transform domain.

### 2.6.1 Spatial domain techniques

Spatial domain techniques [46-50] involve modifying the pixel values of the cover media directly to embed data. One simple approach in this technique is to add a pseudorandom noise pattern to the luminance values of the image's pixels. Unlike transform domain techniques, spatial domain techniques do not transfer the protected images to another domain. This lack of transformation reduces the computation time for watermark embedding and extraction. However, spatial domain techniques are less resistant to signal processing attacks. Some essential spatial domain techniques are:

#### 2.6.1.1 The least significant bit (LSB)

The technique known as the least significant bit (LSB) [47] is a simple and straightforward method commonly used in watermarking. It involves the hiding of information within a sequence of binary numbers by replacing the least significant bit of each element with a bit from the secret message. In the case of floating-point arithmetic, the LSB of the mantissa can also be utilized. Typically, the size of the hidden message is much smaller than the available bits for information hiding, allowing the remaining LSBs to remain unchanged.

However, it's important to note that the LSB substitution technique has certain limitations. Although it may withstand certain transformations such as cropping, the presence of noise or lossy compression can often result in the watermark becoming undetectable. Additionally, once the algorithm is discovered, an intermediary party could easily modify the embedded watermark, undermining its integrity.

### 2.6.1.2 Correlation-based watermarking

The watermarking technique discussed in the statement utilizes the correlation properties of additive pseudo-random noise patterns for embedding watermarks into images [51][52]. This technique involves adding a pseudo-random noise pattern, denoted as W(x, y), to the original image I(x, y) using the equation:

$$\boldsymbol{I}_{\boldsymbol{w}(\boldsymbol{x},\boldsymbol{y})} = \boldsymbol{I}(\boldsymbol{x},\boldsymbol{y}) + \boldsymbol{\alpha} * \boldsymbol{W}(\boldsymbol{x},\boldsymbol{y}) \qquad 2\text{-}4$$

In the equation, I_w(x, y) represents the resulting watermarked image, I(x, y) is the original cover image, α is the gain factor that determines the strength of the watermark, and W(x, y) is the pseudo-random noise pattern.

By adjusting the value of α, the robustness of the watermark against attacks or modifications can be increased. However, a higher α value can introduce visible artefacts or degrade the image quality.

During the watermark retrieval process, the same pseudo-random noise generator algorithm is used along with the original key that was used during embedding. The correlation between the noise pattern and the potentially watermarked image is evaluated. If the correlation exceeds a predefined threshold value T, the presence of the watermark is detected, and a single bit is identified.

To accommodate multiple-bit watermarks, this correlation-based technique can be extended by partitioning the image into blocks or regions. The embedding and detection procedure is then applied independently to each block, allowing for the detection of multiple bits of information within the image.

### 2.6.1.3 Patchwork technique

The patchwork technique, initially proposed by Bender et al. [53] in 1995, is a statistical process that involves embedding a specific statistic imperceptibly into a cover image. This statistic follows a Gaussian distribution [46]. In the embedding process of the patchwork technique, the image owner randomly selects n-pixel pairs based on a secret key and modifies the luminance values of these pairs. If the original luminance values are denoted as xi and yi, the modified luminance values are determined by adding '1' to all xi values and subtracting '1' from all yi values (i.e. $\overline{xi} = xi + 1$ and $\overline{yi} = yi - 1$). The same secret key is used in the extraction process of the technique, which relies on statistical assumptions and calculates the sum of these modified luminance values. Furthermore, in the patchwork technique, the sum (S) is calculated as $S = \Sigma\ (xi - yi)$ for i = 1 to n. If the sum (S) equals 2n, it indicates that the cover image contains the watermark. Conversely, if the sum is close to zero, it suggests that the watermark is not present in the cover image. In [54,55], enhancements were made to the patchwork technique to improve its robustness, allowing the cover image to hide a watermark longer than a single bit.

### 2.6.1.4 Spread spectrum technique

The spread-spectrum technique offers a solution to the challenge of embedding a watermark into the perceptually significant regions of an image's spectrum while preserving its fidelity. This technique draws parallels to spread-spectrum communication, where the image's frequency domain acts as a communication channel, treating the watermark as a transmitted signal.

In spread-spectrum watermarking, the primary objective is to make the embedded signal resilient to attacks and unintentional distortions, treating them as noise. Similar to spread-spectrum communication, the sender transmits a narrowband signal across a much wider bandwidth, ensuring that the energy present in individual frequency bins remains undetectable. Similarly, the watermark is spread across multiple frequency bins, resulting in minimal energy in each bin, making it challenging to detect [56].

During the process of watermark verification, knowledge about the watermark's location and content enables the consolidation of multiple weak signals into a single output signal with a high signal-to-noise ratio (SNR). Removing such a watermark would require introducing high-amplitude noise across all frequency bins [57].

By spreading the watermark throughout the image's spectrum, this technique provides an elevated level of security against intentional or unintentional attacks. The variable location of the watermark and careful selection of frequency regions ensure that the energy present in any individual coefficient remains minimal. As a result, a well-placed watermark in the transformed domain of an image becomes practically imperceptible.

### 2.6.2 Transform domain techniques

The vulnerabilities of spatial domain techniques in embedding secret information are well-known [58]. Even minor modifications to the cover image can easily destroy the hidden data, and lossy compression systems often lead to complete information loss. In contrast, the use of transform domain techniques provides enhanced robustness for watermarked data. These techniques exploit significant areas within the cover image to conceal secret information, making them highly resistant to signal processing attacks compared to spatial domain techniques. In the following subsections, we will explore the key transform domain techniques that offer these advantages

#### 2.6.2.1 Discrete Fourier transform (DFT)

The discrete Fourier transform (DFT) quickly gained attention in the field of watermarking due to its ability to control the frequencies of the cover data. This allows for the selection of appropriate image areas to embed the watermark, achieving an optimal balance between imperceptibility and robustness. There are two main advantages of using DFT over spatial domain techniques [59]. Firstly, DFT is translation invariant and rotation resistant, providing strong resilience against geometric attacks. Secondly, the watermark information is spread throughout the entire image, enabling the implementation of stronger watermarks with minimal perceptual impact.

However, it's important to note that fast Fourier transform (FFT) methods introduce round-off errors, which can result in quality loss and errors during watermark extraction, as mentioned in [60]. Unfortunately, this limitation becomes more significant for hidden communication [59].

To compute the DFT of an image F(m, n) of size M × N, the result is G(k, l) and can be calculated as follows:

$$\boldsymbol{G(k,1) = \frac{1}{M \times N} \sum_{M-1}^{m=0} \sum_{N-1}^{n=0} F(m,n) e^{-j2\pi\left[\frac{km}{M}+\frac{nl}{N}\right]}} \qquad 2\text{-}5$$

The inverse DFT is defined as:

$$\boldsymbol{F(m,n)} = \sum_{M-1}^{k=0} \sum_{N-1}^{l=0} \boldsymbol{G\,(k,l)e^{j2\pi\left[\frac{mk}{M}+\frac{nl}{N}\right]}} \qquad 2\text{-}6$$

While the DFT is computationally efficient, its major disadvantages are its complexity and poor energy compaction properties.

The Discrete Wavelet Transform (DWT) is a frequency domain transform that has gained popularity in digital image watermarking due to its superior spatial localization and multi-resolution properties, which align with the characteristics of the human visual system. Compared to other frequency domain transforms like the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT), DWT has shown to be more effective in addressing the imperceptibility and robustness requirements of watermarking methods.

### 2.6.2.2 Discrete wavelet transform

The DWT is a transform used in numerical and functional analysis, where the wavelets are sampled with discrete values. Unlike the Fourier Transform, which captures only frequency information, the DWT captures both frequency and local information. This makes it well-suited for various image processing tasks, including watermarking.

In DWT-based watermarking approaches, the signal energy tends to concentrate on specific wavelet coefficients. This property is useful for image compression, as it allows for efficient representation of the image while preserving important details. The DWT separates the signal into different frequency sub-bands, including high-frequency and low-frequency components.

The LL (low-low) sub-band in the DWT one-level decomposition contains a significant amount of information from the original image. The LH (low-high), HL (high-low), and HH (high-high) sub-bands capture vertical, horizontal, and diagonal information, respectively. The high-frequency components, represented by the LH, HL, and HH bands, often describe edge components of the image. Since the human eye is less sensitive to fluctuations in edges, these high-frequency components can be selectively used in watermarking algorithms.

It is worth noting that the LL band is the only sub-band that can be used to reproduce the original image accurately, while the other sub-bands are typically ignored. By utilizing the multi-resolution representation provided by the DWT, it is possible to decode the image from a low resolution to a higher resolution gradually.

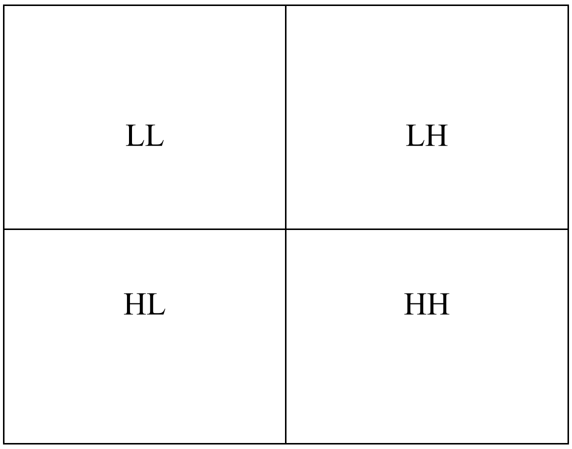


**Figure 2-4** DWT sub-bands

Increasing the degree of DWT in DWT-based digital image watermarking approaches can lead to even more computational speed gains. This makes DWT an attractive choice for watermarking applications where both imperceptibility and robustness are crucial considerations [61].

#### 2.6.2.3 Discrete cosine transform (DCT)

The discrete cosine transform (DCT) is a technique that partitions an image into different frequency components, such as low, high, and middle frequencies [62–64]. This partitioning makes it convenient to embed watermark information into the middle frequency band, which offers additional resistance to lossy compression techniques while minimizing significant modifications to the original image. The DCT exhibits excellent energy compaction properties, allowing for efficient representation of the image.

Figure 2.3 illustrates the various frequencies within an 8x8 DCT block. The lowest frequency components are denoted as FL, while the higher frequency components are denoted as FH. The embedding region, denoted as FM, is selected to provide resistance against lossy compression while maintaining the integrity of the cover image.

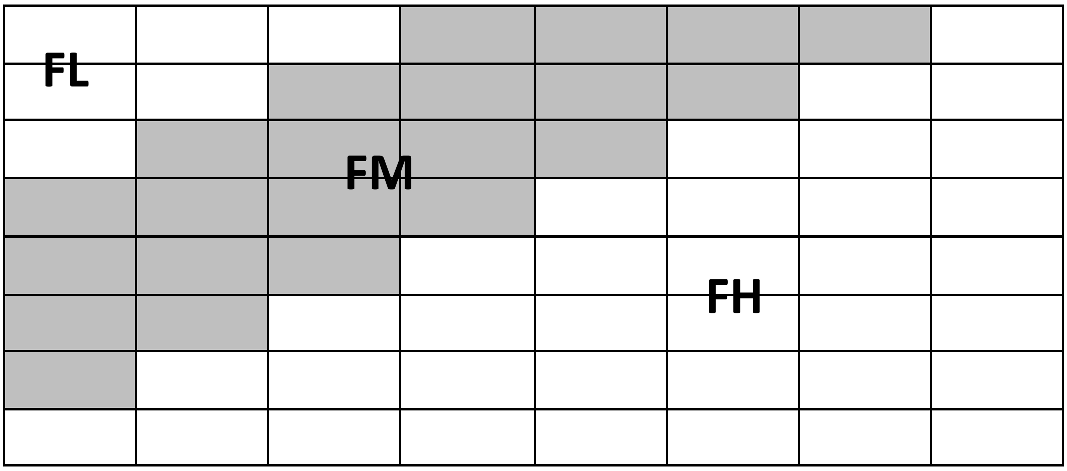


Figure 2-5 Definition of DCT regions [47]

For an input image, I, of size N x N, the DCT coefficients for the transformed output image, D, are calculated using Equation (2-4). In this equation, I(x, y) represents the intensity of the image pixel at row x and column y, while D(i, j) represents the DCT coefficient at row i and column j of the DCT matrix.

The equation for computing the DCT coefficients, as given in Equation (2-4), involves a sum over the image pixels and the cosine functions. The constants Ci and Cj represent scaling factors for normalization purposes.

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{N-1}^{x=0} \sum_{N-1}^{y=0} I(x,y) \cos\frac{(2x+1)i\pi}{2N} \cos\frac{(2y+1)i\pi}{2N} \qquad 2\text{-}7$$

With: $\mathbf{C(i), C(j)} = \frac{1}{\sqrt{2}}$ **for** $\mathbf{i, j = 0}$ **and** $\mathbf{C(i), C(j) = 1}$ **for** $\mathbf{i, j > 0}$.

The DCT matrix is defined using Equation (2-4), taking into account the relationship between the DCT coefficients and the image pixels.

#### 2.6.2.4 Singular value decomposition (SVD)

The singular value decomposition (SVD) is a mathematical operation that breaks down an image into three matrices: a diagonal matrix and two orthonormal matrices. When applied to a matrix A with dimensions M × N, the SVD can be represented as:

$$\boldsymbol{A = USV} \qquad 2\text{-}8$$

where 'S' is the singular value matrix with dimensions M × N, and 'U' and 'V' are orthonormal matrices of dimensions M × M and N × N, respectively. These matrices are commonly utilized in compression and watermarking applications due to their unique properties [65].

## 2.7 Performance measures

Performance measures play a crucial role in evaluating the effectiveness of medical image watermarking algorithms. The two main aspects of evaluation are imperceptibility and robustness. Several performance measures are commonly used to assess these aspects:

- **Mean Square Error (MSE):**

  MSE calculates the cumulative squared error between the original and watermarked images. A lower MSE value indicates that the watermarked image closely resembles the original, indicating better visual quality [666].

  $$\boldsymbol{MSE = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{i=1}^{Y} \left(I_{ij} - W_{ij}\right)^{2}} \qquad \textbf{2}\text{-9}$$

  $I_{ij}$ And $W_{ij}$ are respectively the pixel of the original image of size X×Y and water marked image of size X×Y.

- **Peak Signal-to-Noise Ratio (PSNR):**

  PSNR measures the imperceptibility of the watermark by quantifying the similarity between the watermarked image and the original image. A higher PSNR value signifies that the watermarked image closely resembles the original. A PSNR value greater than 28 dB is generally considered acceptable [67]. It is defined as:

  $$\boldsymbol{PSNR = 10 log \frac{(255)^{2}}{MSE}} \qquad \text{2-10}$$

- **Weighted Peak Signal-to-Noise Ratio (WPSNR):**

  WPSNR is a modified version of PSNR that incorporates a noise visibility function NVF. It takes into account the texture masking function and assigns weights accordingly [67]. WPSNR is defined as:

  $$\boldsymbol{PSNR = 10 log_{10} \frac{(255)^{2}}{MSE \times NVF}} \qquad \text{2-11}$$

- **Universal Image Quality Index:**

The universal image quality index evaluates image distortion in terms of loss of correlation, luminance distortion, and contrast distortion. It provides a comprehensive assessment of image quality and distortion, surpassing metrics like MSE. Let X represent the original image and Y represent a potentially distorted image. We can express X as a set of elements xi, where i ranges from 1 to N, and Y as a set of elements yi, also ranging from 1 to N [68]. The universal image quality index can be defined as follows:

$$\boldsymbol{Q} = \frac{\boldsymbol{4\sigma_{xy}\,\overline{xy}}}{\boldsymbol{(\sigma_x^2+\sigma_y^2)(\overline{x}^2+\overline{y}^2)}} \qquad \mathbf{2}\text{-}12$$

Where $\bar{x} = \frac{1}{N}\sum_{N=1}^{i=1} x_i$ and $\bar{y} = \frac{1}{N}\sum_{N}^{i=1} y_i$.

And $\sigma_x^2 = \frac{1}{N-1}\sum_{N}^{i=1}(x_{i-\bar{x}})^2\,, \sigma_y^2 = \frac{1}{N-1}\sum_{N}^{i=1}(y_i-\bar{y})^2, \sigma_{xy} = \frac{1}{N-1}\sum_{N}^{i=1}(x_i-\bar{x})(y_i-\bar{y})$.

The term ‘Q’ can also define the product of three components:

$$\mathbf{Q} = \left\{\begin{matrix} \boldsymbol{loss\ of\ correlation}\left[\frac{\sigma_{xy}}{\sigma_x\sigma_y}\right].\boldsymbol{luminance\ distortion}\left[\frac{\mathbf{2}\,\overline{\boldsymbol{xy}}}{(\boldsymbol{x})^2+\overline{(\boldsymbol{y})}^2}\right] \\ .\boldsymbol{contrastdistortion}\left[\frac{\mathbf{2}\sigma_x\sigma_y}{\sigma_x^2+\sigma_y^2}\right] \end{matrix}\right\} \qquad 2\text{-}13$$

The components can be described as follows:

1. The loss of correlation quantifies the linear correlation between x and y, ranging from -1 to 1.

2. The luminance distortion measures the similarity of mean luminance between x and y, ranging from 0 to 1.

3. The contrast distortion assesses the similarity of contrast between images, ranging from 0 to 1.

- **Structural Similarity Index Measure (SSIM):**

SSIM compares the luminance, contrast, and structure measurements between the original and watermarked images [67]. It provides a measure of similarity between the two images, with higher values indicating better preservation of image characteristics.

$$\boldsymbol{SSIM}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{f}\big(\boldsymbol{l}(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{c}(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{s}(\boldsymbol{x},\boldsymbol{y})\big) \qquad \mathbf{2}\text{-}14$$

Where $l(x,y)$ is luminance, $c(x,y)$ is contrast and $s(x,y)$ is structure mesurment.

- **Normalized Correlation (NC):**

  NC measures the differences and similarity between the extracted watermark and the original watermark. It quantifies the quality of watermark retrieval, with a value ideally close to 1 and a value of 0.7 considered acceptable [46].

$$\boldsymbol{NC} = \sum_{\boldsymbol{X}}^{\boldsymbol{i=1}}\sum_{\boldsymbol{Y}}^{\boldsymbol{j=1}}\left(\boldsymbol{W}_{\boldsymbol{Original}_{\boldsymbol{ij}}} \times \boldsymbol{W}_{\boldsymbol{recovered}_{\boldsymbol{ig}}}\right) / \sum_{\boldsymbol{X}}^{\boldsymbol{i=1}}\sum_{\boldsymbol{Y}}^{\boldsymbol{j=1}} \boldsymbol{W}^{\boldsymbol{2}}_{\boldsymbol{original}_{\boldsymbol{ij}}} \qquad \mathbf{2}\text{-}15$$

$W_{Original_{ij}}$ and $W_{recovered_{ig}}$are respectively pixel of original watermark and recovered watermark of size X×Y.

- **Bit Error Rate (BER)**

  BER is applicable to random binary sequence watermarks [42]. It calculates the ratio of incorrectly decoded bits to the total number of bits. A lower BER value indicates a more accurate retrieval of the watermark, and

  ideally, the BER value should be 0.

$$\boldsymbol{BER} = (\boldsymbol{Number\ of\ incorrectly\ decoded\ bits}\ ) \\ /\ (\boldsymbol{Total\ number\ of\ bits}\,) \quad \mathbf{2}\text{-}16$$

By utilizing these performance measures, researchers and practitioners can evaluate the imperceptibility and robustness of medical image watermarking algorithms and make informed decisions about their effectiveness for specific applications.

## 2.8 Essential Requirements for Secure Medical Image Watermarking

In recent years, medical images have become crucial for instant diagnosis, understanding critical diseases, and ensuring accurate telemedicine services. However, the security of medical images is a growing concern due to the risk of medical identity theft and potential attacks by hackers. Protecting the integrity and confidentiality of medical images is essential to maintain patient privacy and avoid misdiagnosis.

To address these challenges, secure medical data/image watermarking schemes have been developed. Medical image watermarking offers several advantages [70-73]:

1. Efficient Storage: By embedding patient records within the image, the need for separate storage of medical images and patient records is reduced, saving storage space.

2. Bandwidth Optimization: Watermarking allows for the transmission of medical data without the additional bandwidth required for separate metadata transmission. This optimizes bandwidth usage during image transmission.

3. Ownership Identification and Confidentiality: The hiding of patient data within the cover image helps preserve ownership identification and ensures the confidentiality of sensitive information.

4. Tamper Protection: Watermarked medical images provide protection against tampering, as any unauthorized changes can lead to incorrect diagnoses and potential harm to patients.

5. Archiving and Data Retrieval: Hidden watermarks can act as keywords, facilitating efficient archiving and data retrieval through querying mechanisms. This aids in medical data management and distribution.

While embedding additional data in medical images, it is crucial to ensure that image quality is not degraded. The exchange of electronic patient record (EPR) data over unsecured channels requires a high level of security. Three mandatory security requirements for EPR data exchange are [74]:

1. Confidentiality: Only authorized users should have access to the information, ensuring privacy and preventing unauthorized disclosure.

2. Reliability: This encompasses data integrity, which ensures that the information remains unaltered by unauthorized individuals, and authentication, providing proof of the information's origin. Traceability is also crucial for tracking information during distribution.

3. Availability: The information system should be available for authorized users under normal access conditions, ensuring uninterrupted access to medical data.

Addressing authentication, integrity, and confidentiality concerns is crucial when exchanging EPR data over unsecured channels. By employing suitable watermarking techniques, these security requirements can be fulfilled, safeguarding the integrity, privacy, and accessibility of medical images [40, 74].

## Conclusion

Digital watermarking is a valuable solution for addressing copyright protection, ownership identification, and secure data transmission. It involves embedding imperceptible information into digital media to ensure authenticity, integrity, and confidentiality. Watermarking techniques can be categorized based on visibility, working domain, and application focus. They should possess transparency, robustness, capacity, security, fragility, and tamper resistance. Spatial and transform domain techniques are commonly used for embedding watermarks. Watermarking finds applications in various domains such as copyright protection, authentication, secret communication, and medical applications. Ongoing research aims to enhance the robustness of algorithms and techniques to withstand new attack scenarios and ensure the security and reliability of embedded watermarks. In summary, digital watermarking plays a crucial role in protecting digital content and enabling secure communication in the digital age.

# 3 Chapter 3: Watermarking Simulation Analysis and Results

## 3.1 Introduction

In this chapter, we present the experimental results obtained from the implementation of watermarking techniques on medical images using Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and Spread Spectrum.

The main objectives of this chapter are to evaluate the performance of the watermarking algorithms based on DCT, SVD, and Spread Spectrum, and to analyse the robustness and imperceptibility of the embedded watermarks. To achieve these objectives, we conducted extensive experiments using various medical images and employed different performance metrics for evaluation.

## 3.2 Medical image Watermarking using SVD DCT spread spectrum

### 3.2.1 Watermark Embedding Algorithm

As shown in figure 3-1 the embedding algorithm process embeds a text watermark into a grayscale host image using the spread spectrum technique. It applies the discrete cosine transform (DCT) to the host image, extracts the low-frequency DCT coefficients, and performs singular value decomposition (SVD) on both the host and watermark images. It then generates a pseudo-random sequence and combines it with the watermark coefficients using spread spectrum embedding. Finally, it replaces the low-frequency DCT coefficients with the modified coefficients to obtain the watermarked image.

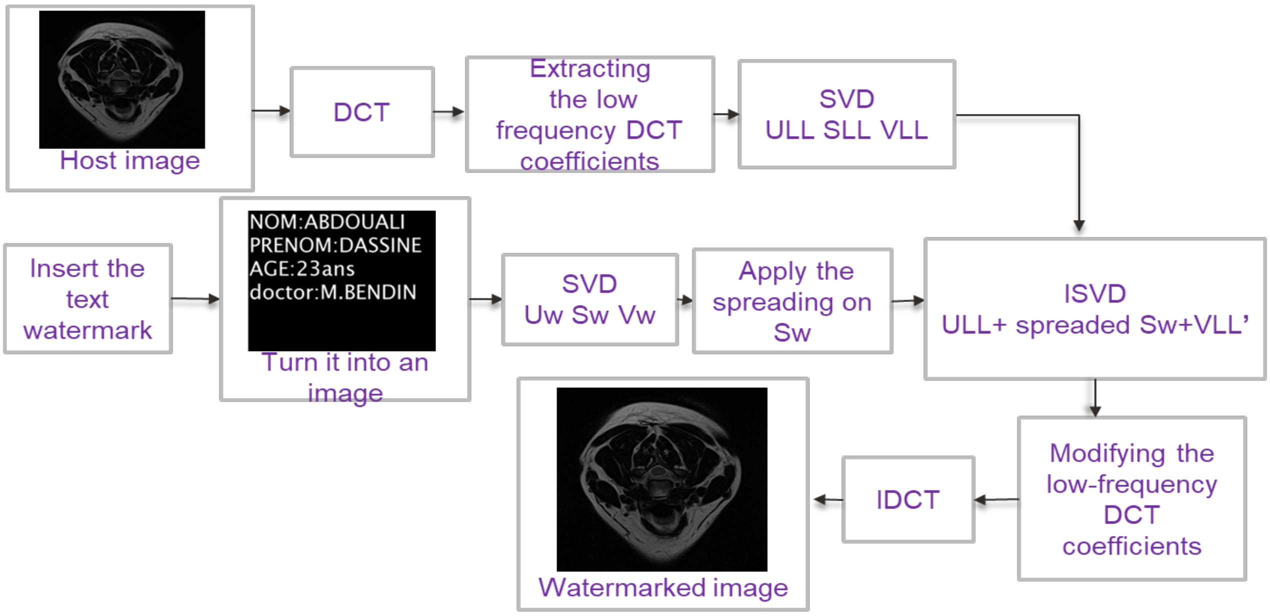


Figure 3-1 Embedding process

### 3.2.2 Watermark Extraction Algorithm

In the extraction algorithm (which is shown in the figure 3-2) to extract the watermark from the watermarked image which is shown in the figure 3-2. It performs the DCT on the watermarked image, extracts the low-frequency DCT coefficients, and applies SVD to these coefficients. It then calculates the extracted watermark coefficients by subtracting the original watermark coefficients (Sll) and dividing by the spread spectrum parameter (alpha). Finally, it removes the spread spectrum effect by subtracting the product of spread factor and pnSequence from the extracted coefficients. The extracted watermark is obtained by multiplying the extracted coefficients with the corresponding SVD matrices (Uw, S_extracted, Vw').

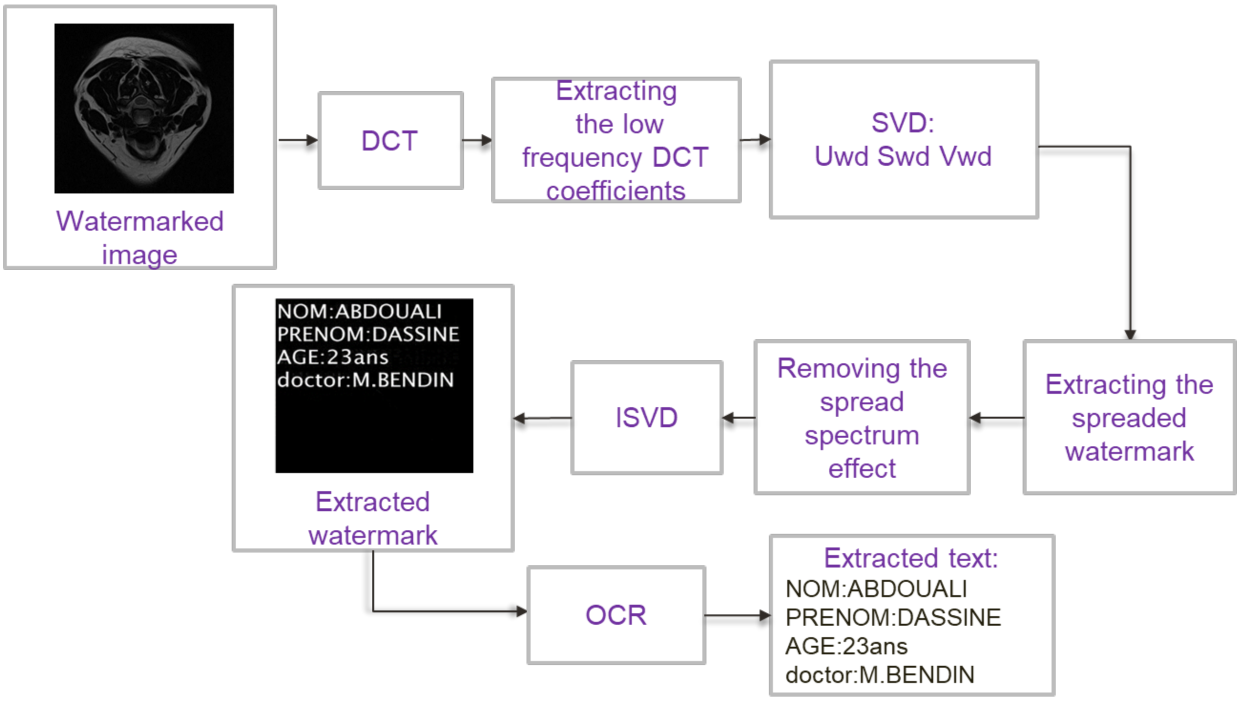


Figure 3-2 Extraction process

## 3.3 Simulation of Watermarking

The proposed watermarking technique utilizes a combination of DCT, SVD, and spread spectrum. The cover medical image used in the method has dimensions of 512x512, while the watermark image, which contains the text watermark, has dimensions of 256x265. The performance of the watermarking technique is evaluated based on two factors: robustness, measured by NC (correlation coefficient), and imperceptibility, measured by PSNR (peak signal-to-noise ratio). It is observed that the size of the watermark has an impact on the quality of the watermarked image. However, if the watermark size is small, the degradation in image quality is not noticeable. The cover and watermarked images are shown in Figure 3-3, while the original and extracted watermarks are displayed in Figure 3-4. Table 3-1 presents the PSNR, BER, SSIM and NC performance of the proposed method at different scale factors and spread factor.

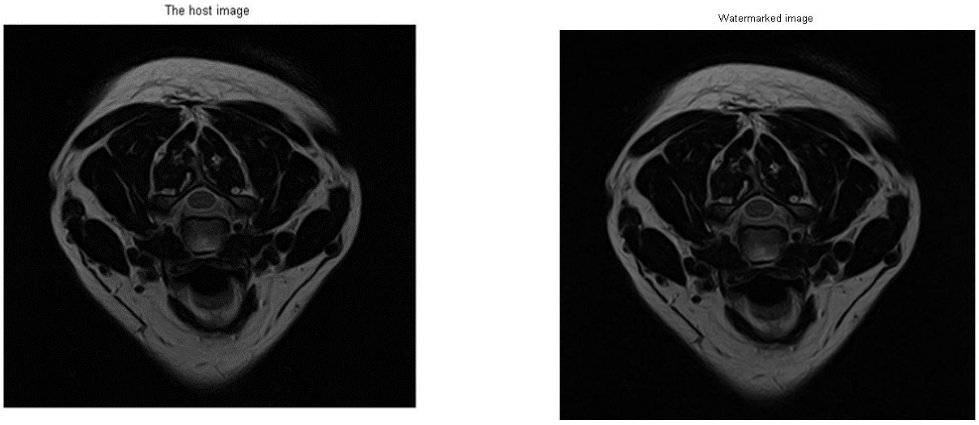
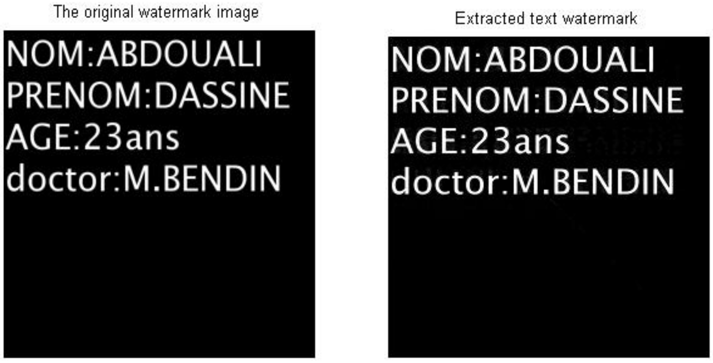


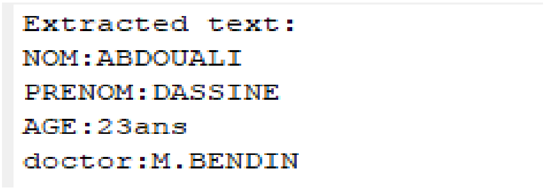
**Figure 3-3 host image and watermarked image**


The original watermark image
Extracted text watermark

NOM:ABDOUALI
PRENOM:DASSINE
AGE:23ans
doctor:M.BENDIN

NOM:ABDOUALI
PRENOM:DASSINE
AGE:23ans
doctor:M.BENDIN

**Figure 3-4 watermark and extracted watermark**



```
Extracted text:
NOM:ABDOUALI
PRENOM:DASSINE
AGE:23ans
doctor:M.BENDIN
```

**Figure 3-5 extracted text watermark output**

**Table 3-1 Measurements of PSNR NC & BER using different scaling /spreading factors and comparing it to a different method**

| | | used method | | | | A.K Singh et al DWT watermarking | | | |
|---|---|---|---|---|---|---|---|---|---|
| Alpha | Spread factor | BER | PSNR | NC | SSIM | BER | NC | PSNR | SSIM |
| 0.01 | | 0.01 | 55.9501 | 0.87748 | 0.94093 | 0 | 0.9043 | 39.22 | - |
| | 0.1 | 0.16522 | 55.9502 | 0.87759 | 0.941 | | | | |
| 0.03 | 0.01 | 0.25773 | 48.0619 | 0.95191 | 0.9736 | 0 | 0.992 | 37.55 | - |
| | 0.1 | 0.25773 | 48.0662 | 0.95184 | 0.97357 | | | | |
| 0.1 | 0.01 | 0.44938 | 37.6765 | 0.99894 | 0.99912 | 0 | 0.9933 | 29.69 | - |
| | 0.1 | 0.44932 | 37.6766 | 0. 99894 | 0.9911 | | | | |

## Discussion :

We aimed to evaluate the performance of watermarking techniques by analysing the Bit Error Rate (BER) and Peak Signal-to-Noise Ratio (PSNR) between the host and watermarked images. Additionally, we examined the Normalized Correlation (NC) and Structural Similarity Index (SSIM) between the watermark and the extracted watermark. Our investigation involved varying the scaling factor (alpha) and spreading factor to assess their impact on the results. And we also compared it to the Dwt method of A.K Singh et al [75].

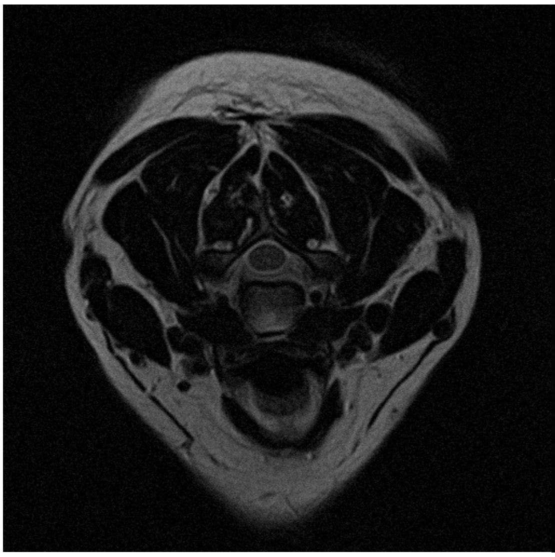
Regarding the BER and PSNR metrics, we observed that their values decreased as the scaling factor (alpha) increased. Specifically, the best performance was achieved at alpha = 0.01, indicating a higher fidelity of the watermarked image compared to the original host image. Moreover, we noted that slight modifications occurred when the spreading factor was augmented, suggesting a minor influence on the overall results.

Conversely, the NC and SSIM metrics exhibited a different behaviour. These metrics demonstrated improved performance as the scaling factor (alpha) increased. Notably, the optimal results were obtained at alpha = 0.1. Similarly, the spreading factor only introduced a marginal effect on the performance.

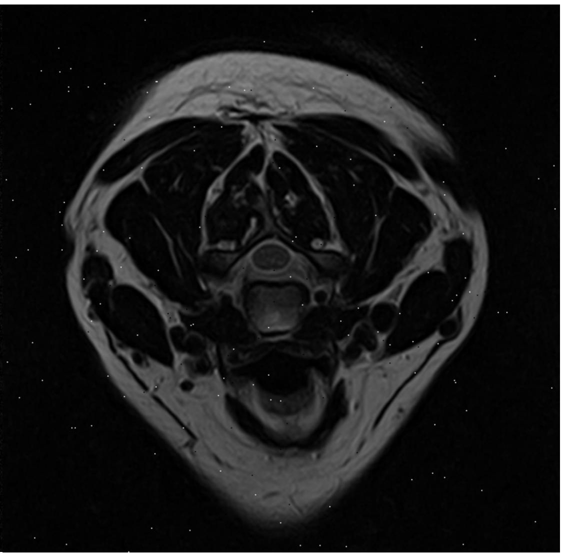
The used method has a remarkably better performances regarding the PSNR levels and as the alpha gets higher the performance of NC gets better too compared to the other method.

## 3.4 Discussion of Experimental Results after applying different Attacks

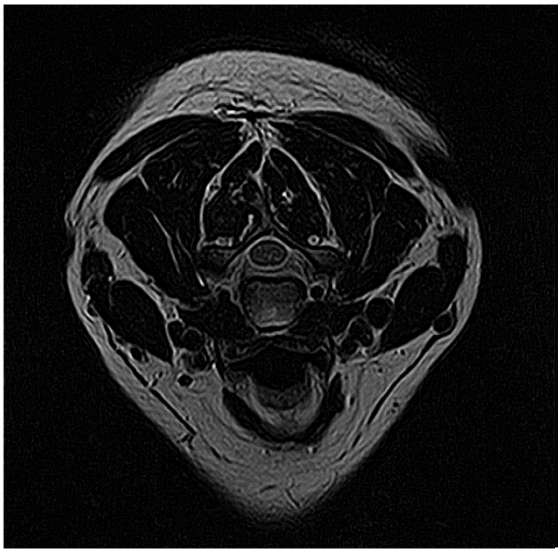
The concept of "attack" encompasses various techniques capable of inducing destruction, distortion, or alteration to the watermarked image. Robustness, in this context, refers to the inherent capability of a watermarking technique to withstand and endure such attacks without significant degradation. In order to assess the robustness of our proposed technique, we subjected the watermarked image to four distinct attacks: Gaussian attack, sharpening attack, salt & pepper attack, and blurring attack. These attacks were chosen to represent a range of potential threats that could potentially compromise the integrity and effectiveness of the watermarking process. The figure 3-6 shows the attacked watermarked MRI image:



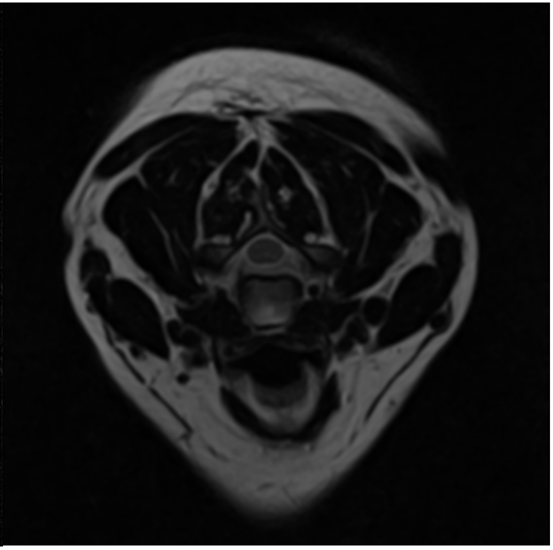
Gaussien noise attack



Salt  and Pepper attack



**Sharpening attack**

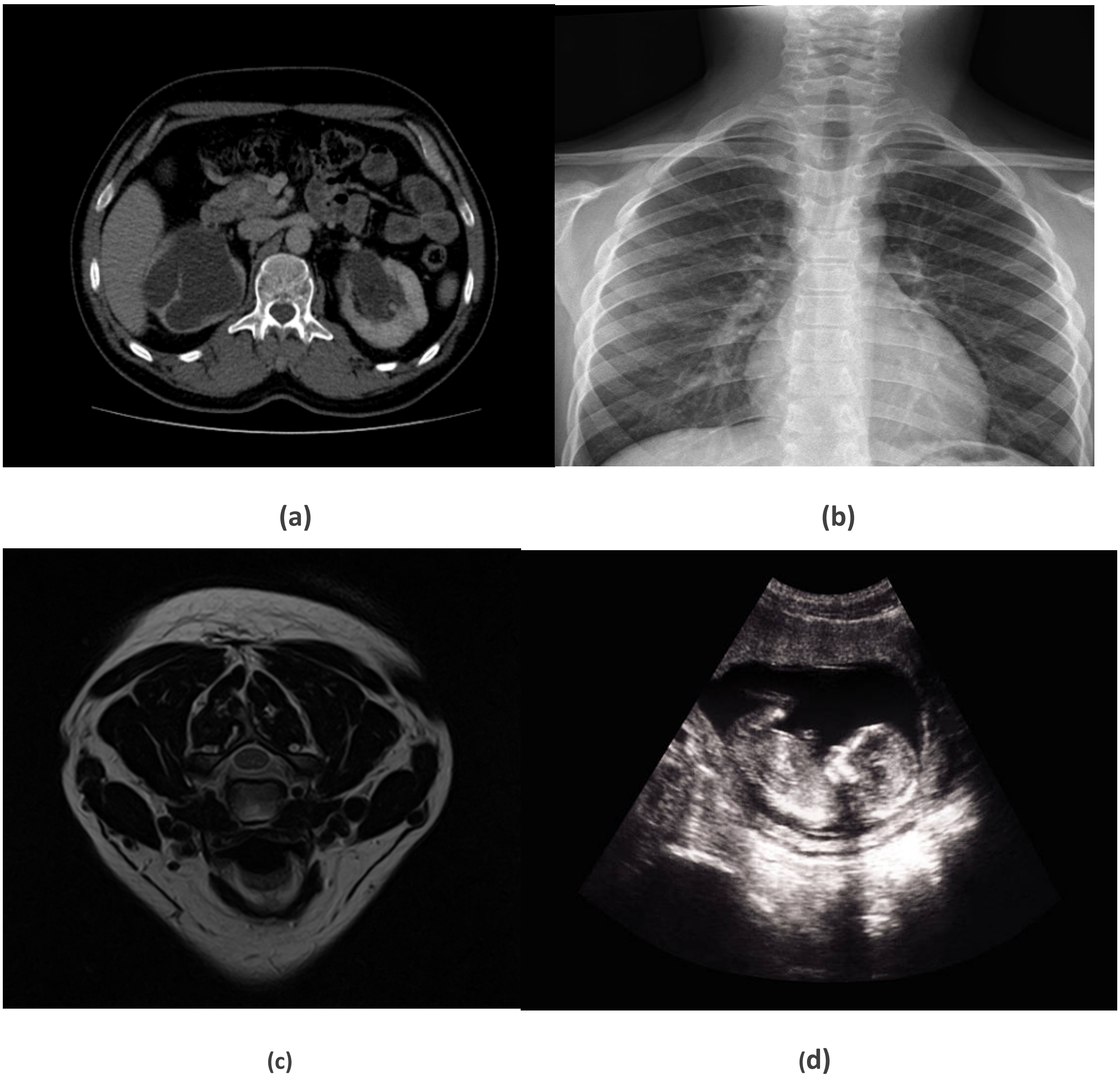


**Blurring attack**

**Figure 3-6 attacks applied to the watermarked image***

The robustness of the embedded watermark against applied attacks was assessed by extracting the watermark from the attacked watermarked images using the proposed extraction procedures. The resulting extracted watermarks were visually examined, revealing varying levels of quality. Some of the proposed method gives good quality extracted watermark image while the others don't. The quality of the extracted watermark can be quantified using objective metrics.

The examined images are shown in the following figure (figure 3-7):



(a) (b)

(c) (d)

**Figure 3-7 Medical test images : a : CT-scan ; b : X-ray ; c : MRI ; d : Ultrasound.**

To evaluate the resilience of the embedded watermark against attacks, we extracted the watermark from the affected images using the proposed extraction procedures. Figure 3-6 displays the extracted watermarks obtained from the attacked watermarked images.

**Table 3-1 extracted watermark after applying attacks to each modality**

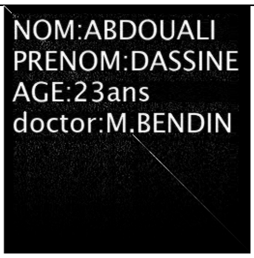
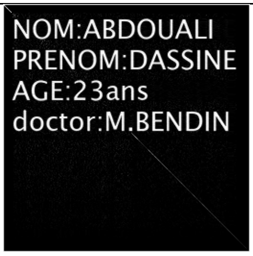
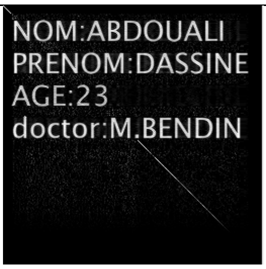
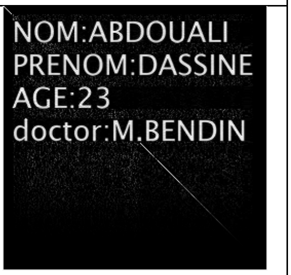
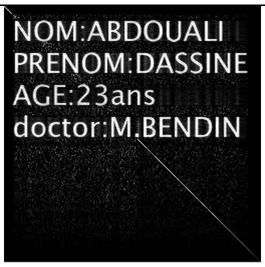
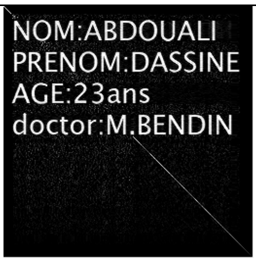
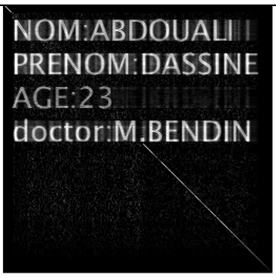
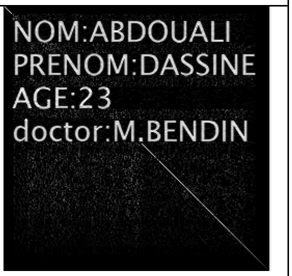
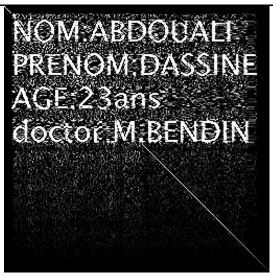
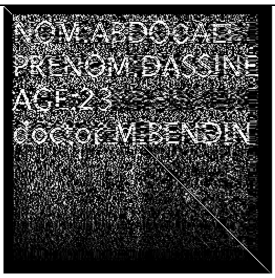
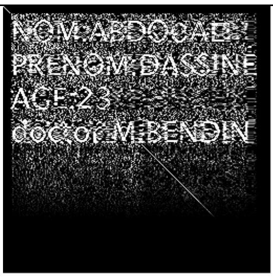
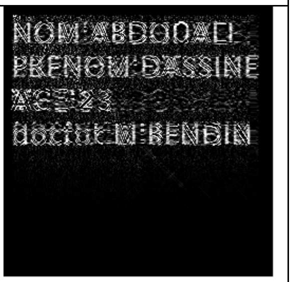
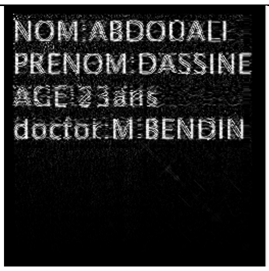
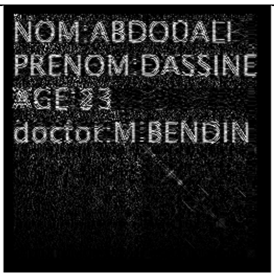
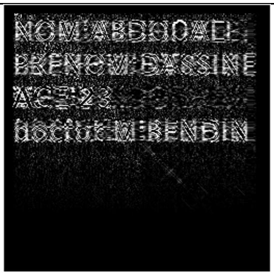
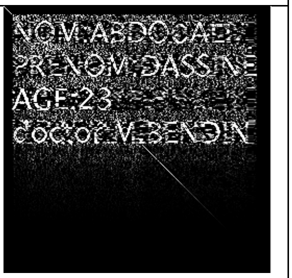
| Host Image<br>Attacks | Extracted watermark | | | |
|---|---|---|---|---|
| | **MRI** | **X-ray** | **CT-Scan** | **Ultrasound** |
| Salt and pepper |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23ans<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23ans<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |
| **Gaussian noise** |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23ans<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23ans<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |
| **Sharpening attack** |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23ans<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |
| **Blurring attack** |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23ans<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |  NOM:ABDOUALI<br>PRENOM:DASSINE<br>AGE:23<br>doctor:M.BENDIN |

Table 3-2 shows the PSNR,BER,NC and SSIM results after applying attacks on each watermarked image modality (scale factor=0.1 , spreading factor=0.01)

# Chapter 3: Watermarking Simulation Analysis and Results

Table 3-2 The results of measure performance after applying attacks for each modality

| | ultrasound | | | | MRI | | | | X-ray | | | | Ct-scan | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Attacks | BER | PSNR | NC | Ssim | BER | PSNR | NC | Ssim | BER | PSNR | NC | Ssim | BER | PSNR | NC | Ssim |
| Gaussien | 0.95081 | 30.6849 | 0.58382 | 0.48454 | 0.951558 | 30.4579 | 0.56322 | 0.45767 | 0.95279 | 29.4542 | 0.59949 | 0.50091 | 0.66869 | 30.9029 | 0.56546 | 0.43432 |
| Salt& Pep | 0.37554 | 32.1683 | 0.67236 | 0.62655 | 0.44995 | 32.2617 | 0.67232 | 0.59522 | 0.85904 | 33.0931 | 0.7651 | 0.68847 | 0.36896 | 32.2614 | 0.62375 | 0.57578 |
| Sharpenin | 0.50244 | 20.1638 | 0.4621 | 0.46422 | 0.94014 | 25.01972 | 0.47321 | 0.33038 | 0.96009 | 18.7491 | 0.40663 | 0.24408 | 0.39894 | 20.479 | 0.46268 | 0.40157 |
| Blurring | 0.44167 | 31.4506 | 0.53983 | 0.47064 | 0.72894 | 35.3818 | 0.61753 | 0.48849 | 0.89016 | 30.4768 | 0.538336 | 0.32289 | 0.44065 | 29.9084 | 0.47546 | 0.3613 |

## Observations:

From table 3-1, we can notice that the proposed method gives excellent to moderate quality with some attacks and low quality with others. The quality of the extracted watermark can be measured using many metrics.

We observe in the table 3-2 that the extracted watermarks  that, the Gaussian attack exhibited moderate performance across all modalities, with a relatively high Bit Error Rate (BER) and moderate Peak Signal-to-Noise Ratio (PSNR). The extracted watermark showed a moderate correlation with the original in terms of Normalized Correlation (NC) and Structural Similarity Index (SSIM).

The Salt & Pepper attack consistently outperformed other attacks, demonstrating better resistance to noise and distortion. It achieved lower BER, higher PSNR, and stronger correlation between the extracted watermark and the original in all modalities. The NC and SSIM values indicated a relatively strong correlation, highlighting the robustness of the Salt & Pepper attack in preserving the watermark's integrity.

The Sharpening attack resulted in significant distortion and reduced image quality. It produced higher BER values and lower PSNR values across all modalities, indicating a weaker correlation between the extracted watermark and the original. The NC and SSIM values also indicated a relatively weak correlation, suggesting that the Sharpening attack significantly affected the extracted watermark.

The Blurring attack caused moderate distortion and relatively good image quality. It resulted in moderate BER values and moderate PSNR values in most cases. The extracted watermark showed a moderate correlation with the original, as indicated by the NC and SSIM values.

## Conclusion

These findings underscore the importance of carefully selecting the scaling factor and considerate the spreading factor when employing watermarking techniques. The optimal values of these factors depend on the specific application and desired performance metrics. Therefore, a comprehensive understanding of the trade-offs between fidelity and robustness is essential for successful watermarking implementation in real-world scenarios. The watermarking technique displayed varying levels of robustness when applied to different modalities of medical images, with different attacks causing different degrees of distortion and correlation between the extracted watermark and the original.

# Summary

The main objective of this study is to assess the performance, robustness, and imperceptibility of watermarking techniques applied to medical images, specifically using the Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and Spread Spectrum methods.

The research methodology involves implementing and evaluating different watermarking techniques for medical images. The process includes pre-processing the host image, performing DCT computations, extracting low-frequency DCT coefficients, applying SVD to the watermark image, generating a pseudo-random sequence, incorporating spread spectrum watermarking, modifying DCT coefficients, and reconstructing the watermarked image. The watermark extraction algorithm involves applying DCT, extracting low-frequency coefficients, performing SVD on the coefficients, extracting the spread watermark, removing the spread spectrum effect, and retrieving the watermark image.

A diverse set of medical images from publicly available databases is utilized in this study. The sample size includes a wide range of medical images to ensure comprehensive evaluation.

The evaluation of the watermarking techniques revealed significant findings. Patterns, trends, and relationships were observed through data analysis, demonstrating the effectiveness and limitations of the DCT, SVD, and Spread Spectrum methods in medical image watermarking.

This research contributes to the existing knowledge and understanding of watermarking techniques applied to medical images. The study presents novel insights into the performance, robustness, and imperceptibility aspects of watermarking methods using DCT, SVD, and Spread Spectrum. The findings have both theoretical advancements and practical implications for enhancing the security and integrity of medical images.

Certain limitations were encountered, including the sample size and availability of data. These limitations provide opportunities for future research to further investigate and address these constraints.

Based on our findings, several recommendations can be made for future research. Further investigation should explore the application of other watermarking techniques and evaluate their performance on different types of medical images. Additionally, research efforts should focus on optimizing the watermarking process to enhance robustness and imperceptibility.

In conclusion, this study experimentally evaluated the performance, robustness, and imperceptibility of watermarking techniques using DCT, SVD, and Spread Spectrum on medical images. The findings contribute to the existing knowledge in the field, providing insights into the effectiveness and limitations of these methods. The research highlights the significance of watermarking techniques for enhancing the security and integrity of medical images, while also identifying areas for future exploration and improvement.

# REFERENCES

1. Jerrold T. Bushberg; J Anthony Seibert; Edwin M Leidholdt, Jr. & John.M Boone: The Essential Physics of Medical Imaging. Second edition. 2003
2. M. A. Haidekker, Medical Imaging Technology, Springer Briefs in Physics 2013
3. Harjit Singh ;Janet A Neutze & Jonathan R. Enterline MD : Radiology Fundamentals ; springer 2014 fourth edition
4. Huang, H. K. (2011). PACS and imaging informatics: basic principles and applications. John Wiley & Sons. pp. 33-6
5. Act, A. (1996). Health insurance portability and accountability act of 1996. Public Law, 104,191.
6. Bouslimi, D., Coatrieux, G., Cozic, M., & Roux, C. A joint encryption/watermarking system for verifying the reliability of medical images.Information Technology in Biomedicine, IEEE Transactions on, 16(5), 891-899. (2012).
7. Al-Haj, A. Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. Journal of digital imaging, 1-9. (2014).
8. Abbing, H. R. Medical Confidentiality and Patient Safety: Reporting Procedures. European journal of health law, 21(3), 245-259. (2014).
9. Klutas, Edna May, RN,M.P.H., C.O.H.N. “Confidentiality of medical information”. Occupational Health Nursing, 25(4), 14-17. (1977).
10. Schneider, M., & Chang, S. F. A robust content-based digital signature for image authentication. In Image Processing, 1996. Proceedings. International Conference on (Vol. 3, pp. 227-230). IEEE. (1996). [
11. http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf
12. Umamageswari, A., & R Suresh, G. “A New Cryptographic Digital Signature for Secure Medical Image Communication in Telemedicine”. International Journal of Computer Applications, 86(11), 4-9. (2014).
13. Lo, C. C., & Hu, Y. C. “A novel reversible image authentication scheme for digital images”. Signal Processing, 98, 174-185. (2014).
14. Vellaisamy, S., & Ramesh, V. (2014). Inversion attack resilient zero-watermarking scheme for medical image authentication. IET Image Processing, 8(12), 718-727.

15. Memon, N. A., Keerio, Z. A., & Abbasi, F. “Dual Watermarking of CT Scan Medical Images for Content Authentication and Copyright Protection”. In Communication Technologies, Information Security and Sustainable Development (pp. 173-183). Springer International Publishing. (2014).

16. Huang, H. K. (2011). Picture Archiving and Communication System Components and Workflow. In PACS and Imaging Informatics: Basic Principles and Applications, Second Edition, 217-235.

17. Bairagi, V. K., & Sapkal, A. M. "ROI based DICOM Image Compression for Telemedicine". Digital Image Processing, 3(11), 662-666. (2011).

18. http://www.offis.de/en/start.html

19. McAuliffe, M. J., Lalonde, F. M., McGarry, D., Gandler, W., Csaky, K., & Trus, B. L. (2001). Medical image processing, analysis and visualization in clinical research. In Computer Based Medical Systems, 2001. CBMS 2001. Proceedings. 14th IEEE Symposium on (pp. 381-386). IEEE.

20. Bouslimi, D., Coatrieux, G., & Roux, C. (2012). A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images. Computer methods and programs in biomedicine, 106(1), 47-54.

21. Huang, H. K. (2011). PACS and imaging informatics: Basic principles and applications. Chapter 17: Image/Data Security. John Wiley & Sons, pp. 519-558.

22. N.F. Johnson, S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, 31(2), 1998, 26-34.

23. W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, "Applications for data hiding," IBM Systems Journal, 39(3&4), 2000, 547-568.

24. F.A.P. Petitcolas, "Introduction to information hiding," in: S. Katzenbeisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

25. Cavaro-Ménard, C., Lu, Z. G., & Le Callet, P. ” QoE for telemedicine: challenges and trends”. In SPIE Optical Engineering+ Applications (pp. 88561A-88561A). International Society for Optics and Photonics.. (2013)

26. Allaf, Abdelhay & M'hamed, Aït Kbir. (2020). Watermarking Image Scheme Based on Image Content and Corners Decomposition Method. 10.1007/978-3-030-37629-1_50..

27. G.J. Simmons, "The prisoners problem and the subliminal channel," in Advances in Cryptology, Proceedings of CRYPTO 83, Plenum Press, New York, 1984, pp. 51–67.

28. W. Bender, D. Gruhl, N. Morimoto, A. Lou, "Techniques for data hiding," IBM Syst. J., vol. 35, no. 3&4, pp. 313–336, 1996.

29. A.K. Singh, B. Kumar, M. Dave, A. Mohan, "Robust and imperceptible spread-spectrum watermarking for telemedicine applications," Proc. Natl. Acad. Sci., India Sect. A: Phys. Sci., vol. 85, no. 2, pp. 295–301, 2015.

30. S.A.K. Mostafa, N. El-sheimy, A.S. Tolba, F.M. Abdelkader, H.M. Elhindy, "Wavelet packets-based blind watermarking for medical image management," Open Biomed. Eng. J., vol. 4, pp. 93–98, 2010.

31. G. Coatrieux, L. Lecornu, Ch. Roux, B. Sankur, "A review of image watermarking applications in healthcare," in Proceedings of IEEE-EMBC Conference, New York, USA, pp. 4691–4694, 2006.

32. B. Kumar, H.V. Singh, S.P. Singh, A. Mohan, "Secure spread spectrum watermarking for telemedicine applications," J. Inf. Secur., vol. 2, pp. 91–98, 2011.

33. S. Katzenbeisser, F.A.P. Petitcolas, "Information hiding techniques for steganography and digital watermarking," Artech House, London, 2000.

34. M. Terry, Medical identity theft and telemedicine security. Telemed. e-Health 15(10), 928–932 (2009)

35. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Multiple watermarking on medical images using selective DWT coefficients. J. Med. Imaging Health Inf. 5(3), 607–614 (2015)

36. Irany, B.M. "A high capacity reversible multiple watermarking scheme – applications to images, medical data, and biometrics." Master Thesis, Department of Electrical and Computer Engineering, University of Toronto, 2011.

37. Mostafa, S.A.K., El-sheimy, N., Tolba, A.S., Abdelkader, F.M., Elhindy, H.M. "Wavelet packets based blind watermarking for medical image management." Open Biomedical Engineering Journal, vol. 4, pp. 93–98, 2010

38. . Katzenbeisser, F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking (Artech House, London, 2000)

39. S.P. Mohanty, "Watermarking of digital images," M.S. Thesis, Indian Institute of Science, India, 1999.

40. I.J. Image, Graphics and Signal Processing, 2017, 4, 56-66 Published Online April 2017 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijigsp.2017.04.07

41. Tang Wenliang, "A Feature-Based Digital Image Watermarking Algorithm Resisting to Geometrical Attacks," Second International Symposium on Electronic Commerce and Security, IEEE, 2009. DOI: https://doi.org/10.1109/isecs.2009.94

42. 14. N. Deshpande, A. Rajarkar, R.R. Muthalkar, "Robust Dual Watermarking Scheme for Video Derived from Strategy Fusion," International Journal of Image, Graphics and Signal Processing, vol. 6, no. 5, pp. 19-27, 2013. DOI: https://doi.org/10.5815/ijigsp.2014.05.03
43. 15. C. Lu and H. Yuan M. Liao, "Multipurpose Watermarking for Image Authentication and Protection," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579–1592, October 2001. DOI: https://doi.org/10.1109/83.951542
44. 16. M. Miller, I. J. Cox, J. P. Linnartz, and T. Kalker, "A review of watermarking principles and practices," In Digital Signal Processing in Multimedia Systems, pp. 461-485, 1999.
45. A Review of Digital Watermarking Applications for Medical Image Exchange Security, Chapter • January 2019. Authors: Aït Kbir M'hamed and Abdelmalek Essaâdi University. DOI: 10.1007/978-3-030-11196-0_40
46. D. Arya, A survey of frequency and wavelet domain digital watermarking techniques. Int. J. Sci. Eng. Res. 1(2), 1–4 (2010)
47. C. Shoemaker, Hidden Bits: A Survey of Techniques for Digital Watermarking, Independent Study (Spring, 2002)
48. O. Bruyndonckx, J.J. Quisquater, B. Macq, Spatial method for copyright labeling of digital images, in Proceeding of IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, pp. 456–459, 1995
49. N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain. Signal Process. 66(3), 385–403 (1998)
50. A.K. Singh, N. Sharma, M. Dave, A. Mohan, A novel technique for digital image watermarking in spatial domain, in Proceeding of 2nd International Conference on Parallel Distributed and Grid Computing, Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India, pp. 497–501, 201
51. G. Langelaar, I. Setyawan, R. Lagendijk, Watermarking digital image and video data: a state of-art overview. IEEE Signal Process. Mag. 17(5), 20–46 (2000)
52. A.K. Parthasarathy, S. Kak, An improved method of content based image watermarking. IEEE Trans. Broadcast. 53(2), 468–479 (2007)
53. W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding, in Proceedings of the SPIE 2420, Storage and Retrieval for Image and Video Databases III, pp. 164–173, 1995

54. G.C. Langelaar, J.C.A. Van der Lubbe, R.L. Lagendijk, Robust labeling methods for copy protection of images, in Proceedings of SPIE 3022, Storage and Retrieval for Image and Video Databases V, pp. 298–309, 1997 12.

55. I. Pitas, T.H. Kaskalis, Applying signatures on digital images, in IEEE Workshop on Nonlinear Signal and Image Processing, Thessaloniki, Greece, pp. 460–463, 1995

56. .I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. 6(12), 1673–1687 (1997)

57. B. Kumar, H.V. Singh, S.P. Singh, A. Mohan, Secure spread-spectrum watermarking for telemedicine applications. J. Inf. Secur. 2(2), 91–98 (2011)

58. K.T. Lin, Digital image hiding in an image using n-graylevel encoding, in Proceeding of 1st International Conference on Information Science and Engineering, IEEE Computer Society, Washington, DC, USA, pp. 1720–1724, 2009

59. A. Poljicak, L. Mandic, D. Agic, Discrete Fourier transform–based watermarking method with an optimal implementation radius. J. Electron. Imaging 20(3), 033008 (2011)

60. A. Cheddad, J. Condell, K. Curran, M. Kevitt, Digital image steganography: survey and analysis of current methods. Signal Process. 90, 727–752 (2010)

61. Dubolia, Rakhi & Singh, Roop & Bhadauria, Sarita & Gupta, Rekha. (2011). Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR. Proceedings - 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011. 10.1109/CSNT.2011.127.

62. A. Al-Haj, Combined DWT–DCT digital image watermarking. J. Comput. Sci. 3(9), 740–746 (2007)

63. J.R. Hernandez, M. Amado, F. Perez-Gonzalez, DCT-Domain watermarking techniques for still images: detector performance analysis and a new structure. IEEE Trans. Image Process. 9(1), 55–68 (2000)

64. K. Viswanath, J. Mukherjee, P.K. Biswas, Image filtering in the block DCT domain using symmetric convolution. J. Vis. Commun. Image Represen t. 22(2), 141–152 (2011).

65. Lai CC, Tsai CC (2007) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE T Instrum Meas 59(11):3060-3063. doi:10.1109/TIM.2010.2066770

66. Z. Wang, A.C. Bovik, Mean squared error: love it or leave it? A new look at signal fidelity measures. IEEE Signal Process. Mag. 26, 98–117 (2009)

67. A.K. Singh, B. Kumar, M. Dave, S.P. Ghrera, A. Mohan, Digital image watermarking: techniques and emerging applications, in Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, (IGI Global, Hershey, 2016), pp. 246–272

68. Z. Wang, A.C. Bovik, A universal image quality index. IEEE Signal Process. Lett. 9(3), 81–84 (2002)

69. A.K. Singh, Improved hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools Appl. 76(6), 8881–8900 (2017)

70. A.K. Singh, M. Dave, A. Mohan, Robust and secure multiple watermarking in wavelet domain, a special issue on advanced signal processing technologies and systems for healthcare applications (ASPTSHA). J. Med. Imaging Health Inf. 5(2), 406–414 (2015)

71. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible dual watermarking for telemedicine applications. Wirel. Pers. Commun. 80(4), 1415–1433 (2014)

72. A. Sharma, A.K. Singh, S.P. Ghrera, Robust and secure multiple watermarking technique for medical images. Wirel. Pers. Commun. 92(4), 1611–1624 (2017)

73. A.K. Singh, M. Dave, A. Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images. J. Multimedia Tools Appl. 75(14), 8381–8401 (2015

74. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, Relevance of watermarking in medical imaging, in Proceedings of the IEEE EMBS Conference on Information Technology Applications in Biomedicine, Arlington, USA, pp. 250–255, 2000.

75. Singh, A.K., Kumar, B., Singh, G., Mohan, A. (2017). Robust and Secure Multiple Watermarking for Medical Images. In: Singh, A., Kumar, B., Singh, G., Mohan, A. (eds) Medical Image Watermarking. Multimedia Systems and Applications. Springer, Cham. https://doi.org/10.1007/978-3-319-57699-2_5