KASDI MERBAH UNIVERSITY OUARGLA

Faculty of new Information and Telecommunication Technologies

Department of Electronic and Telecommunication

ACADEMIC MASTER

Domain: Telecommunication

Field: Telecommunication System

Submitted by:

NAIMI Aziza

BADAOUI Rabab

Theme:

Watermarking security in IWT transform domain

Evaluation Date: 06/2024

Before the Jury:

Dr. Berrak Oulaya	**Chairman**	**MAB**	**UKMO**
Mr. Sayeh Moad	**Supervisor**	**MCA**	**UKMO**
Dr. Bettayeb Nadjla	**Examiner**	**MCB**	**UKMO**

Academic Year: 2023/2024

Dedication

Praise be to God, who gave us success and stability. He gave us steadfastness and steadfastness Help us get this work done.

I humbly dedicate this modest achievement to: Dear Father Ahmed, to the one who taught me to give without expectation My father planted in my soul the love of ambition and perseverance for a friend The kind heart, my hero, whose name I carry with pride.

"My dear mother is the best" to the one who gives me Love, compassion and devotion, you filled me with your tenderness and tenderness Throughout my life, you have been the support of life, its smile, and the secret of existence.“My dear brothers and sisters,” to those who shared my childhood with me and carried me with it The burden of life in my youth, to those who paved the path to success with me, To my dear brothers Abdullah, Mustafa, Somaya, Saadia, Doaa. To my husband and my two sons, Zakaria and Ihab, God gave them to me. For everyone who contributed to the completion of this work, from near or far.

Rabab.

In the name of my Creator and the facilitator of my affairs, to you, praise and gratitude, I dedicate this success to myself first, then to everyone who worked with me to complete this journey, to my “dear father” and “mother”, my first and eternal supporter, to” my brothers”, my best support, to those who accompanied me and supported me and were the best companion, “Bouthaina” is grateful to you.

Aziza.

Acknowledgements

We thank God who helped us and gave us patience necessary to overcome the difficulties we encountered in completing our work.

I also want to thank our teachers who helped us throughout our preparation for the algorithm Especially the two teachers, Sherif Fela and Tijani Sayhia, who provided us with several guidelines to improve our work, and our supervisor, Dr. Sayeh Maad, and all Professors and workers in the electronics department and Telecommunications. Special thanks go to the jury members Dr. Berrak Oulaya and Dr Bettayeb Nadjla who provided more suggestions and constructive criticism to ameliorate our work.

Finally, we thank everyone who helped us from near, far and especially Naimi Samiha and Melody Tariq.

ملخص:

نظرًا للتقدم في تقنيات نقل المعلومات عبر الوسائط المتعددة والإنترنت، أصبح الوصول غير المصرح به لهذه المعلومات ونسخها ممكنًا، مما أدى إلى انتهاكات لأمن الوسائط الرقمية. وبالتالي، أصبح من الضروري وضع علامة مائية على الصور الطبية. ومع ذلك، يجب تنفيذ عملية وضع العلامة المائية بعناية لضمان إمكانية استرداد معلومات المريض السرية الموجودة في الصورة بالكامل دون أخطاء بعد فك الضغط. على الرغم من أهمية العلامة المائية، إلا أنه لا توجد طريقة تلبي جميع متطلباتها حاليًا. تهدف هذه الدراسة إلى تقديم مسح شامل لمختلف الأساليب، بما في ذلك تحويل المويجات الصحيحة مع تحليل القيمة المفردة والطيف المنتشر. تم تقييم كفاءة هذه الطرق من خلال حساب قيم ذروة نسبة الإشارة إلى الضوضاء، ومعامل الارتباط الطبيعي، ومؤشر التشابه الهيكلي، إلى جانب اختبار مرونة العلامة المائية في مواجهة الهجمات المختلفة.

Abstract:

Due to advancements in technologies for transmitting information via multimedia and the Internet, unauthorized access and copying of this information have become possible, resulting in breaches of digital media security. Consequently, it has become essential to watermark medical images. The watermarking process, however, must be executed with care to ensure that confidential patient information in the image can be fully recovered without error after decompression. Despite the significance of watermarking, no method currently meets all its requirements. This study aims to provide a comprehensive survey of various methods, including integer wavelet transform (IWT) with singular value decomposition (SVD) and spread spectrum. The efficiency of these methods was assessed by calculating peak signal-to-noise ratio (PSNR) values, the normalized correlation coefficient (NCC), and the structural similarity index measure (SSIM), along with testing the watermark's resilience to various attacks.

Keyword:

IWT, SVD, Securer Telemedicine Watermarking. PSNR, NCC and SSIM measurement performance

Résume :

Grâce aux progrès des technologies de transmission d'informations via le multimédia et Internet, l'accès non autorisé et la copie de ces informations sont devenus possibles, entraînant des violations de la sécurité des médias numériques. Il est donc devenu indispensable de filigraner les images médicales. Le processus de tatouage doit cependant être exécuté avec soin pour garantir que les informations confidentielles du patient dans l'image puissent être entièrement récupérées sans erreur après la décompression. Malgré l'importance du tatouage, aucune méthode ne répond actuellement à toutes ses exigences. Cette étude vise à fournir une étude complète de diverses méthodes, y compris la transformation en ondelettes entières (IWT) avec analyse de valeurs singulières (SVD) et spectre étalé. L'efficacité de ces méthodes a été évaluée en calculant les valeurs maximales du rapport signal/bruit (PSNR), le coefficient de corrélation normalisé (SSIM) et l'indice de similarité structurelle (SSIM), ainsi qu'en testant la résilience du filigrane à diverses attaques.

Mots-clés : IWT, SVD, Tatouage de télémédecine sécurisé. PSNR, NCC and SSIM performance de mesure

List of Contents

CHAPTER II : WATERMARKING TECHNIQUES

CHAPTER III : Watermarking Experimental Analysis and Results

List of figures

List of Tables

List of Abbreviation

BER: Bit Error Rate.

CT: Computed tomography.

CWT: Continuous Wavelet Transform.

DCT: Discrete Cosine Transform.

DFT: Discrete Fourier Transform.

DICOM: Digital Imaging and Communications in Medicine.

DWT: Discrete Wavelet Transform.

EPR: Electronic Patient Record.

IEEE: Institute of Electrical and Electronics Engineers.

ISO: International Organization for Standardization.

IWT: Integer Wavelet Transform.

LSB: Least Significant Bit.

LBP: Local binary pattern.

MRI: Magnetic resonance imaging.

MSE: Mean Square Error.

NC: Normalized Correlation.

NEMA: National Electrical Manufacturers Association.

PET: positron-emission tomography.

PACS: Picture Archiving and Communication System.

PSNR: Peak Signal-to-Noise Ratio.

SVD: Singular Value Decomposition.

SSIM: Structural Similarity Index Measure.

US: Ultrasonography.

General Introduction

In today's world, with the rapid advancement of the Internet, data exchange takes only seconds, making the protection of digital copyright content crucial. Digital watermarking is a method to achieve this by revealing or extracting the watermark to verify ownership in case of copyright disputes. For digital content, watermarking methods must meet essential requirements such as robustness and imperceptibility. Robustness is critical as it ensures that the methods can withstand various types of attacks. Additionally, the watermarked image must maintain good transparency. This document is organized into three chapters:

- The first chapter covers medical imaging, its types, and the functioning of digital communication systems in healthcare institutions.
- The second chapter discusses watermarking techniques for medical images, detailing their characteristics and requirements, the watermarking framework, and the tools used for measuring performance.
- The third chapter presents the proposed watermarking techniques, experimental simulations, and results.

I.1. Introduction

Medical imaging encompasses various techniques used to visualize the internal structures of the human body for diagnostic, monitoring, and treatment purposes, making it a vital field in medical engineering. Regardless of the specific method used, all imaging techniques share the common goal of identifying and examining significant features such as tumors under the guidance of skilled imaging professionals. Despite the diversity in imaging technologies, they all adhere to fundamental principles of interpretation as systems and involve mathematical processing. The image itself is treated as a multi-dimensional signal, and the processes involved in its formation can be conceptualized as a linear system, enabling straightforward mathematical treatment. This chapter also covers topics such as types of medical imaging, digital imaging, archival systems, and communication systems used in medical contexts.

I.2. Medical Imaging

Medical imaging, also referred to as radiology, encompasses the field of medicine where healthcare professionals create images of different parts of the body for diagnostic or treatment purposes. These imaging procedures are typically non-invasive, meaning they do not require surgery or any invasive measures, yet they enable doctors to diagnose injuries and diseases effectively. [1]

I.3. Medical Imaging Types

According to [2, 3] Medical imaging is a central part of the improved outcomes of modern medicine. Different types of medical imaging procedures include:

I.3.1. X-rays imaging

- **Types:** Standard X-ray, fluoroscopy
- **Uses:** X-rays are commonly used to examine bones, lungs, and the digestive system. Fluoroscopy, a real-time form of X-ray, is used for procedures like barium enemas and joint injections.
- **Procedure:** Patients are exposed to a controlled dose of ionizing radiation, and an image is captured on film or electronically. It's a quick and painless procedure.

I.3.2. Magnetic resonance imaging (MRI)

- **Types:** MRI with contrast, functional MRI (fMRI)
- **Uses:** MRI is excellent for visualizing soft tissues like the brain, muscles, and organs. It's used for diagnosing conditions such as tumors, joint problems, and neurological disorders.
- **Procedure:** Patients lie inside a large magnet, and radio waves create detailed images based on the body's response to magnetic fields. It's non-invasive and doesn't involve radiation.

I.3.3. Ultrasounds imaging

- **Types :** 2D ultrasound, Doppler ultrasound
- **Uses:** Ultrasound is widely used for imaging fetuses during pregnancy, assessing blood flow, and examining various organs.
- **Procedure:** A transducer is placed on the skin, and high-frequency sound waves create images of the body's internal structures. It's painless and radiation-free.

I.3.4. Computerized tomography (CT) imaging

- **Types:** Conventional CT, CT angiography
- **Uses:** CT scans provide detailed cross-sectional images of the body, making them useful for diagnosing various conditions, including cancer, trauma, and vascular disorders.
- **Procedure:** The patient lies on a table that moves through a doughnut-shaped CT scanner. Multiple X-ray beams create detailed cross-sectional images.

I.3.5. Nuclear imaging

- **Types:** Single-photon emission computed tomography (SPECT), positron emission tomography (PET).
- **Uses:** Nuclear medicine involves the use of radioactive materials to diagnose and treat various diseases, including cancer and heart conditions.
- **Procedure:** Patients receive a small amount of a radioactive substance, and a gamma camera or PET scanner is used to capture images of the distribution of the radioactive material in the body.

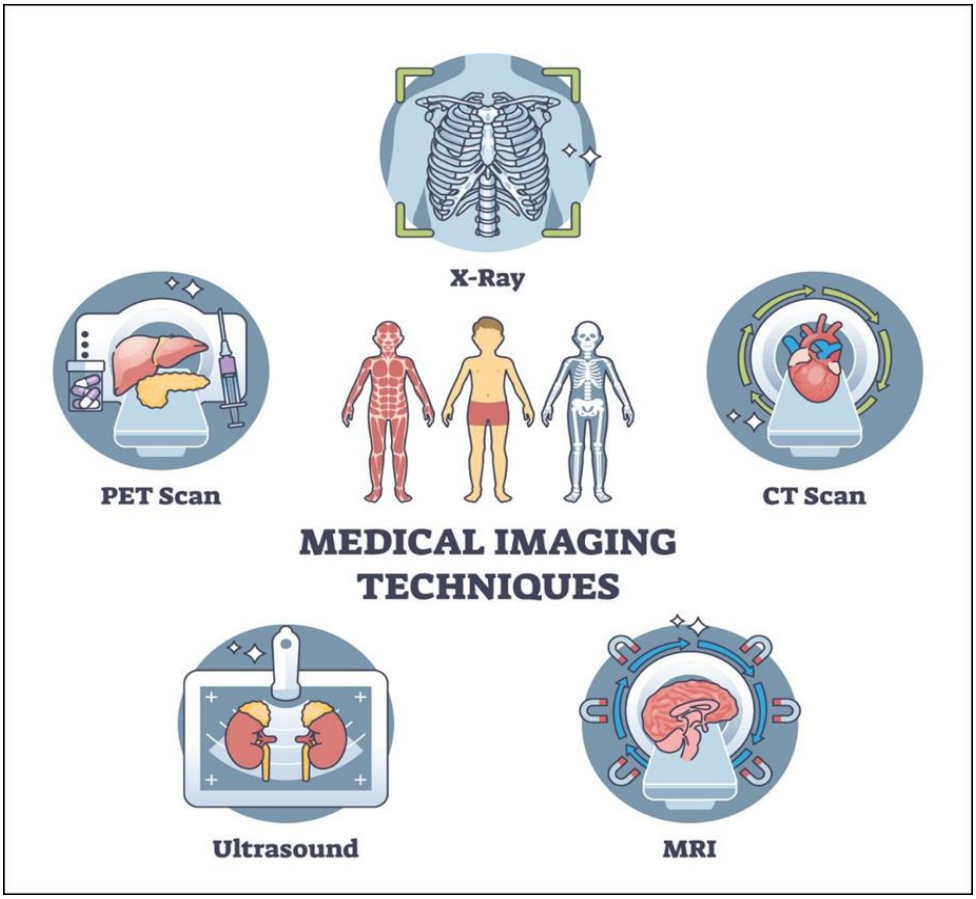


Figure I.1 Common Diagnostic Radiology Procedures [2]

I.4. Importance of medical imaging

Medical imaging [3] plays a vital role in modern healthcare by diagnosing and treating a diverse array of medical conditions ranging from cancer and cardiovascular disease to neurological disorders. Despite some limitations and associated risks, ongoing research and advancements by healthcare professionals aim to develop safer, faster, and more accurate imaging technologies. As these technologies evolve, they are expected to significantly enhance the diagnosis and treatment of medical conditions, thereby improving the overall quality of healthcare.

I.5. Digital image

A digital image is a representation of a two-dimensional image on a computer electronic device and is composed of a grid of pixels. These pixels are generally displayed as small squares of color, each containing a color value, which, when properly arranged by the computer,

produces a coherent image. We obtain a digital image using a digital camera, a scanner, or by creating an image in a graphics program. The image is saved in a digital file such as JPEG, PNG, or GIF, which can be displayed on a computer screen. The digital image has many applications, including photography, art, design, advertising, and medical photography.

I.6. Digital medical image

A digital medical image is an image that has been captured using medical imaging equipment, such as X-rays, CT scans, MRI, or ultrasound, and is stored in a digital format. These images can be viewed, analysed, and shared electronically,allowing medical professionals to make more accurate diagnoses and treatment plans. [4]

I.7. Medical image security requirements

Securing medical images and data is of paramount importance when they are stored or transmitted over communication networks between doctors or hospitals. This process, known as telemedicine, necessitates stringent measures to protect patient information, as mandated by the Health Insurance Portability and Accountability Act (HIPAA). The DICOM standard offers guidelines for producing medical images in telemedicine, yet ensuring the security of these images during transmission over networks remains a critical concern. This security is essential not only for data storage within medical systems but also for the safe transmission of data in telemedicine applications.

I.7.1. Medical image confidentiality

Medical image confidentiality is essential to ensure patient privacy and protect sensitive medical information. Medical images often contain personal and health-related information

that must be kept confidential to avoid misuse, discrimination or stigmatization.

To protect patient confidentiality, medical facilities, and practitioners must implement security measures that comply with legal and ethical standards. The same measures include [5]:

1. **Access control:** Access to medical images should be restricted to authorized personnel only. Access should be granted based on a need-to-know basis, and any access should be monitored and logged.
2. **Encryption:** Medical images should be encrypted during storage and transmission to prevent unauthorized access or interception.
3. **De-identification:** Before sharing medical images for research or other purposes, personal and identifiable information should be removed or anonymized.
4. **Secure storage:** Medical images should be stored in a secure location, with restricted access and regular backups to prevent loss or damage.
5. **Staff training:** All staff handling medical images should be trained on the importance of patient confidentiality and the security measures in place.

I.7.2. Medical image integrity

Medical image integrity refers to the accuracy and reliability of medical images, which is essential to ensure accurate diagnosis and treatment. Medical images must be free from any alteration, manipulation, or corruption that could lead to incorrect diagnoses, inappropriate treatments, or harm to patients. To maintain medical image integrity, healthcare facilities and practitioners should implement several measures, such as [6]:

1. **Quality control:** Regular quality control checks should be performed on the medical imaging equipment to ensure they are functioning correctly and producing accurate images.
2. **Verification:** Medical images should be checked for accuracy and consistency before and after the acquisition, and any discrepancies should be corrected.
3. **Storage and transmission:** Medical images should be stored and transmitted using secure and reliable methods to prevent corruption or loss of data.
4. **Metadata:** Metadata, such as the date, time, and patient information, should be recorded and preserved along with the medical image to ensure its integrity.
5. **Staff training:** All staff handling medical images should be trained on the importance of maintaining medical image integrity and the methods used to do so.

I.7.3. Medical image authentication

Medical image authentication is the process of verifying the authenticity and integrity of medical images to ensure that they have not been tampered with or altered in any way. Authentication methods can include digital signatures, watermarking, and encryption [7].

I.8. Picture Archiving and Communication System (PACS)

A Picture Archiving and Communication System (PACS) [8,9] is a medical imaging technology employed by healthcare organizations to securely store and electronically transmit electronic images and relevant clinical reports. It replaces traditional methods of manual filing, retrieval, and transportation of X-ray films. PACS facilitates the storage, retrieval, presentation, and sharing of images generated by various medical imaging devices such as X-ray machines, CT scans, MRI scans, and ultrasound machines. The system consists of four primary components: imaging devices, a secure network for image distribution, workstations for image viewing, and an electronic archive for storing images and associated documentation.

I.9. Digital Imaging and Communications in Medicine (DICOM)

DICOM (Digital Imaging and Communications in Medicine) is a standardized framework used for managing, storing, printing, and transmitting medical imaging information. It encompasses both a file format specification and a network communication protocol. The communication protocol operates as an application layer protocol utilizing TCP/IP for inter-system communication. DICOM files can be exchanged between entities capable of receiving image and patient data in DICOM format.

The standard is copyrighted by the National Electrical Manufacturers Association (NEMA) and was developed by the DICOM Standards Committee, which includes members affiliated with NEMA. DICOM facilitates the integration of scanners, servers, workstations, printers, and network hardware from various manufacturers into a cohesive Picture Archiving and Communication System (PACS). Each device is accompanied by DICOM conformance statements that specify the DICOM classes they support. DICOM has been widely adopted by hospitals and is increasingly utilized in smaller healthcare settings such as dentists' and doctors' offices. It serves as a universal standard for securely communicating medical images over networks. [10]

I.10 DICOM security profiles

DICOM (Digital Imaging and Communications in Medicine) security profiles encompass various aspects aimed at securing DICOM files and ensuring secure data exchange within healthcare communication systems. These profiles are specifically defined within the DICOM

standard to guarantee the confidentiality, integrity, and authenticity of medical imaging and related information. There are four primary DICOM security profiles [11]:

- Secure use profiles.
- Secure transport connection profiles.
- Digital signature profiles.
- Media storage security profiles.

Each of these security profiles plays a crucial role in safeguarding sensitive medical imaging data, adhering to the stringent privacy and security requirements mandated in healthcare settings.

I.11 Medical image security applications

In the medical field, current security measures can be categorized into two types. The first type comprises pure watermarking techniques applied in both frequency and spatial domains. The second category encompasses medical image applications that utilize cryptography alongside watermarking techniques. Watermarking is a technique that involves embedding a digital signature or other digital information into a digital object, such as a medical image. Watermarking is commonly used in medical imaging for a variety of purposes, including image authentication, copyright protection, and patient identification. One of the main applications of watermarking in medical images is to prevent unauthorized use or distribution of the images. By embedding a digital signature or a unique identifier into the image, it becomes difficult to tamper with or copy the image without authorization. This helps prevent medical image theft, which can lead to misdiagnosis or harm to patients. Watermarking can also be used to provide a clear and definitive way of identifying the owner of the image. Watermarking can also be used to provide additional information about the image. For example, by embedding the name of the patient, the date and time of image acquisition, or the type of examination, medical professionals can easily identify and track images. This can improve patient care and workflow efficiency, especially in large medical facilities where there may be many medical images being generated every day. Another application of watermarking in medical images is to protect the copyrights of medical images. Medical images are often copyrighted, and watermarking can help prevent the unauthorized use or distribution of these images. By embedding a copyright

notice or a logo into the image, it is possible to identify the owner of the image and deter unauthorized use. [12]

Figure I.2 Data security system field

I.12 Conclusion

Medical imaging plays a crucial role in diagnosing various diseases and health conditions non-invasively. Technological advancements in this field have significantly enhanced the accuracy and efficacy of diagnoses and surgical procedures by analyzing high-quality images obtained from medical imaging devices. Ensuring the security of medical images, integral to telemedicine, against deliberate or accidental alterations involves maintaining confidentiality, authenticity, and integrity.

Based on recent research, two primary methods ensure the security of medical images: watermarking and metadata (digital signatures). Encryption technology also plays a role in enhancing security levels. Despite available encryption methods provided by DICOM security profiles, decrypted data may not be fully protected. Therefore, watermarking emerges as a critical solution to safeguard medical images during storage and transmission, offering a standardized assurance of data confidentiality and integrity.

II.1 Introduction

Digital watermarking technology involves embedding a message within a multimedia entity, such as an image, text, or other digital content. This technique serves various critical applications, with digital copyright protection being one of the most significant. Like other data hiding methods, digital watermarking systems must meet specific requirements to ensure their strength and effectiveness.

Digital watermarking technologies are typically categorized based on their domain: spatial domain, frequency domain (transform), and wavelet domain. However, these methods are vulnerable to various attacks, including modern watermark attacks and watermark estimation attacks. To assess the resilience of watermarks against such attacks, several parameters are considered, including PSNR (Peak Signal-to-Noise Ratio), SSIM (Structural Similarity Index), and NC (Normalized Correlation).

Recovering from these attacks necessitates robust detection techniques. The Digital Watermark Proxy offers a professional solution to counter these challenges effectively. This proxy system is designed to enhance the security and reliability of digital watermarking applications by providing robust detection and mitigation strategies against potential attacks.

II.2 Importance and Necessity of Watermarking

While cryptography is widely used to safeguard digital content, it lacks the capability for owners to monitor how their content is handled post-decryption. This limitation can potentially lead to unauthorized copying, distribution, or misuse of private information. Cryptographic techniques effectively protect content during transmission but offer no further protection once the content is decrypted. Addressing this significant drawback, watermarking technology ensures continued protection of content even after decryption. Watermarking involves embedding imperceptible information into the main content, ensuring the watermark remains intact during normal usage without inconveniencing users. This embedded watermark can survive various processes such as decryption, reencryption, compression, and geometric manipulations [13]. In recent years, telemedicine applications have become pivotal in advancing technology within the medical field. Digital Imaging and Communications in Medicine (DICOM) serves as a fundamental standard for transmitting electronic patient record

(EPR) data DICOM files include a header containing crucial patient information, necessitating protection during transmission and storage. Watermarking offers a robust solution to ensure the security and authenticity of DICOM files, thereby addressing these critical concerns effectively. [14]

II.3 Classifications of Digital Watermarks

Watermarking techniques can be classified into several categories based on different parameters such as insertion field, human perception or detection method as shown in the following figure II.1 [15–17]:

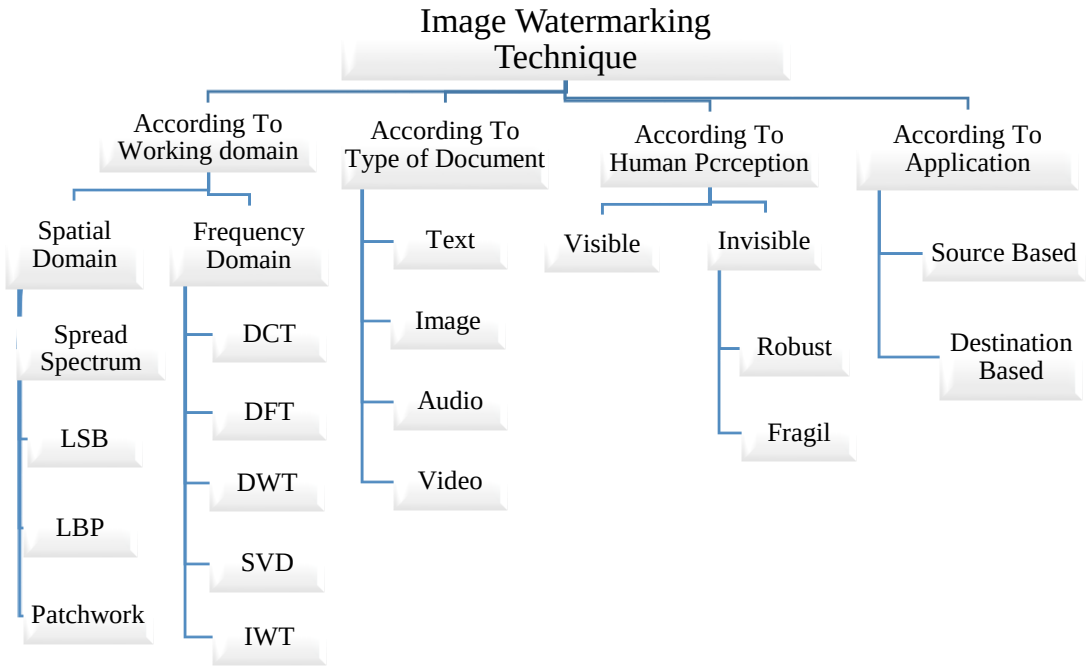


Figure II.1 Classification of watermarking techniques.

1. Classification based on domain of insertion

Most watermarking techniques can be categorized into two main approaches: those in the spatial domain, where the watermark is inserted at the pixel level, and those in the frequency domain, which involve transformed domains such as Discrete Wavelet Transform (DWT), and Integer Wavelet Transform (IWT).

2. Classification based on human perception

There are two types of watermarks in this classification: visible watermarks, such as logos or text, clearly identify the owner of an image or video. The second type is invisible watermarks that are not perceptible to the human sensory system. Invisible watermarks can be fragile, semi-fragile, or robust against various attacks.

3. Classification based on method of detection

There are three methods that can be used to detect embedded data: blind, semi-blind, and non-blind. The first method does not use the original signal to detect the marker, the second method only uses some information, and the third method requires the original signal to detect the marker. Compared with the blind method, the non-blind method is the most robust to attacks. [16]

4. Classification based on type of document

The type of host signal which can be an image, audio, video, text, script, or any other digital data can be used to categorize watermarking techniques.

II.4 Possible Features of Digital Watermarks

The key characteristics of digital watermarks [18, 19] are:

1. Robustness: A digital watermark is considered robust if it can withstand a specific class of transformations and is hence appropriate for use as a copyright safeguard. The robustness criterion is concerned with two things: (1) can the watermark be identified by the watermark detector, and (2) does it remain present after the data has been distorted.

***2. Imperceptibility*:** This relates to the degree of similarity between the original and watermarked images and can be viewed as a gauge of the watermark's perceptual transparency.

3. Capacity: The quantity of data that can be contained in a cover is known as its capacity. Since the information to be embedded may be a logo picture, a number, etc., the amount of information required greatly depends on the applications, such as copyright protection, fingerprinting, authentication, and secrecy of medical data.

4. Security: The security of a watermark implies that altering or removing it should be difficult without damaging the original image. The necessary level of watermark security will depend on its intended use.

5. Data-payload *:* The data payload of a watermark can be defined as the amount of information that it contains e.g. if a watermark contains 'n' bits, then there are 2^n possible watermarks with actually $2^n + 1$ possibilities as one possibility can be that no watermark is present. A good watermark should contain all the required data within any arbitrary and small portion of the cover.

6. Fragility : The content authentication is the main goal of the fragile watermark. This is the robustness requirement in reverse. Because of the distortions in the media content, the watermarks can be made to tolerate different levels of permissible alterations. Here, watermarks are not the same as digital signatures, which demand a perfect match.

7. Computational cost : The price associated with inserting the watermark into a cover and removing it from the digital cover is referred to as the computational cost. In certain applications, it's crucial that the embedding procedure be as quick and easy as feasible, but the extraction procedure may take longer. For some applications, extraction speed is vitally important.

8. Tamper resistance: Digital photo authenticity is verified using watermark tamper-detection. These kinds of watermarks are susceptible to any alteration to the watermark data, therefore the system can ascertain whether the watermark has ever been changed or replaced by verifying the integrity of the watermark.

II.5 Framework for Watermarking

The watermarking framework typically involves two main processes: encoding and extraction [20]. This framework is illustrated in Figure II.2. In Figure II.2a, three inputs are required: a watermark, the original cover media, and an optional public or secret key for generating a watermarked image. Figure II.2b represents the extraction process, which takes as input the watermarked image or original data (cover), along with the secret or public key and test data. These inputs are utilized to determine the cover image and its ownership [21, 22]. Thus, based on Figure II.2, a general watermarked cover image (W) is expressed as a function (F) of the watermark data (W_d), cover data (C_d), and a secret key (K), as shown in equation (II.1):

$$W = F(W_d, C_d, K) \quad \text{(II.1)}$$

The definition of the watermark embedding procedure is:

$$\text{Watermark Embedding: } (E_w) = F(W_d, C_d, K) \quad \text{(II.2)}$$

Additionally, the method of extracting a watermark is described as:

$$\text{Watermark Extraction : } (W_e) = F(\text{W } or\ C_d, E_w, K) \quad \text{(II.3)}$$

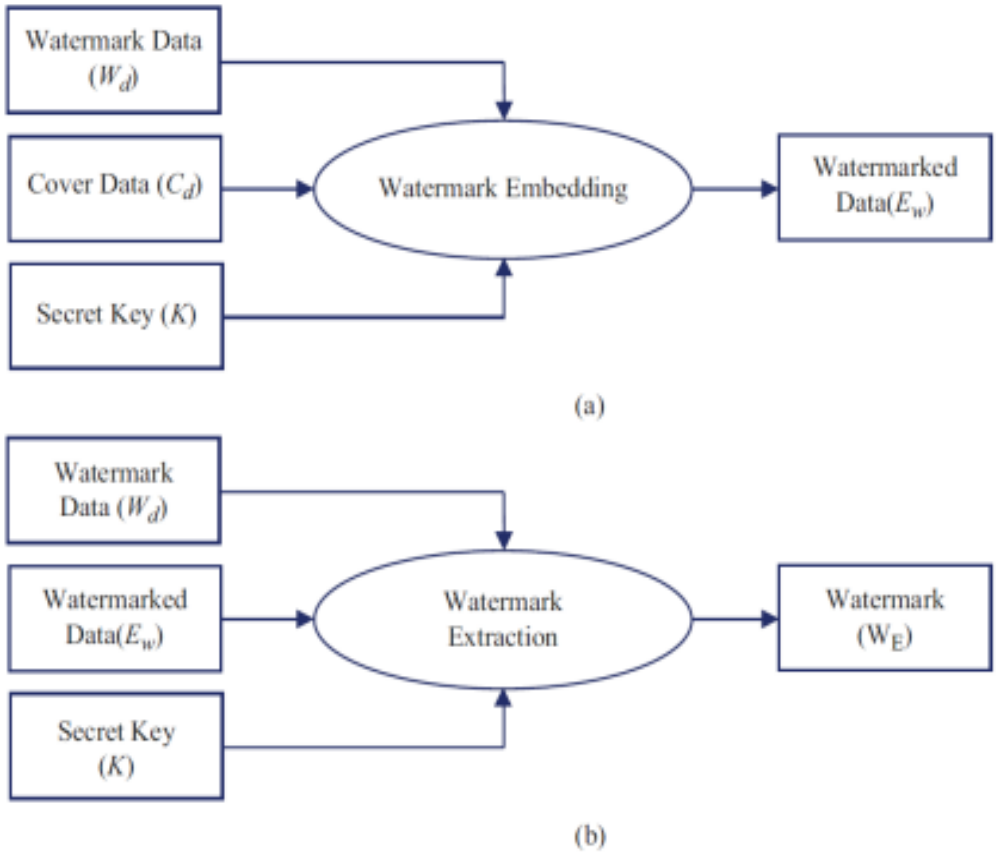


Figure II.2 The watermark process (a) embedding and (b) extraction [21]

II.6 Recent Applications of Digital Watermark

Digital watermarking has found various recent applications, as illustrated in Figure II.3. Some important and emerging applications include [18, 23, 24, 25]:

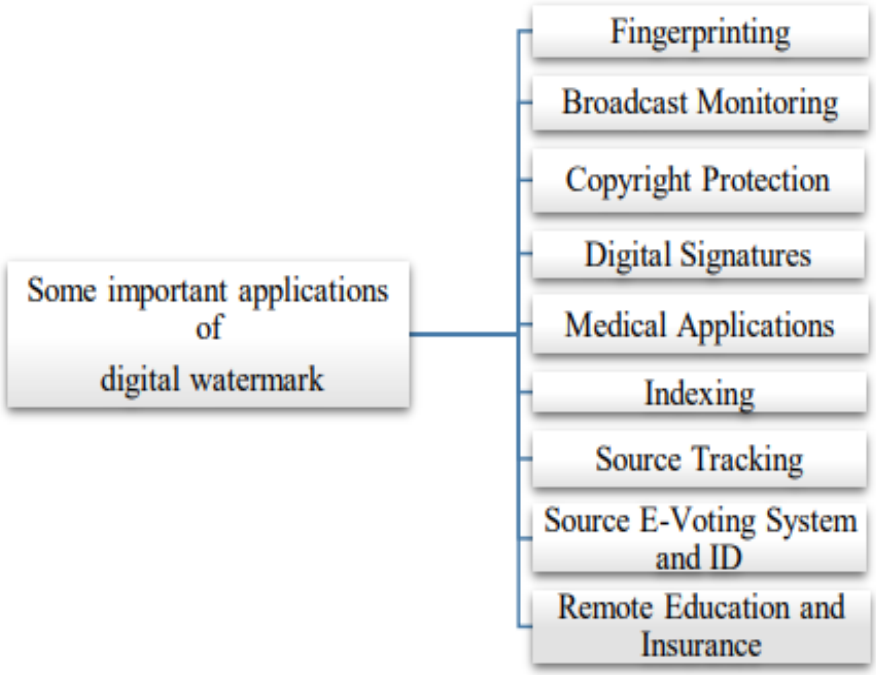


Figure II.3 Potential applications of watermarking

1. **Fingerprinting:** This application involves embedding identification information in watermarked content to trace the source of illegal distribution.
2. **Broadcast monitoring:** Watermarking allows content owners to automatically confirm broadcasting parameters on terrestrial, cable, or satellite television, including time, place, and duration. In addition, watermarking is essential for copy control, media identification, e-commerce, e-governance, and monitoring intellectual property.
3. **Copyright protection:** By concealing confidential information, digital watermarking helps to safeguard digital material against infringement. To communicate and protect picture copyrights, many content owners include watermarks in their photos. This helps to ensure that guidelines are followed and makes enforcement of copyright more efficient.
4. **Digital signature :** Watermarking is employed in public-key cryptosystems to generate signatures that provide proof of the authenticity of the originator of an information object.
5. **Medical applications:** Watermarking in the medical field serves both authentication and confidentiality purposes without affecting the medical image. Applications such as

telemedicine, teleophthalmology, telediagnosis, tele-consultancy, telecardiology, and teleradiology rely on watermarking for secure transmission, storage, and sharing of electronic patient record (EPR) data. It ensures confidentiality, authentication, integrity, and availability of EPR data exchange.

6. **Indexing:** Watermarking allows the indexing of video mail by embedding comments within the video content. It can also be used for movies and news items, where markers and comments aid search engines.
7. **Source tracking:** Watermarks embedded at each distribution point enable the retrieval of the watermark from a copied work, allowing the source of distribution to be identified.
8. **Secured e-voting systems:** Watermarking contributes to building highly secure e-voting systems, ensuring the accuracy, speed, and privacy of online voting processes. Additionally, digital watermarks are used to protect state driver licenses, providing a covert and machine-readable layer of security against digital counterfeiting, fraud, and identity theft [25].
9. **Remote education:** Remote education and insurance companies are two additional areas where digital watermarking finds applications. Secured data transmission is crucial in distance learning, and digital watermarking offers a potential solution to address these challenges.

II.7 Domains of image watermarking

II.7.1 Spatial Domain Techniques

In order to integrate the data, spatial domain approaches [26–30] need explicitly altering the cover media's pixel values. The most basic method in spatial domain approaches is to supplement an image's brightness values with a pseudorandom noise pattern [31]. These methods reduce the amount of time that must be spent computing watermark extraction and embedding because they do not need moving the protected images to the transform domain.

Spatial domain methods, however, are less resistant to attacks using signal processing. The following is a description of some key spatial domain approaches.

II.7.1.1 Spread-Spectrum Technique

The spread spectrum approach is used in watermarking to incorporate a watermark signal into a host signal. The watermark signal is typical of modest amplitude and is distributed across a wide frequency range by a pseudorandom sequence known as the spreading code. Only the watermark embedder and extractor have access to this propagating code.

The spread spectrum approach is used for watermarking in two stages:

- **Embedding:** The watermark signal is first turned into a series of bits, which are then modulated onto a carrier signal using the spreading code. To make a watermarked signal, the resulting spread signal is applied to the original host signal.
- **Extraction:** The watermarked signal is received and processed at this stage to extract the embedded watermark signal. Correlating the received signal with the same spreading code used in the embedding step is part of the extraction process. The correlation signal that results is then demodulated to obtain the original watermark signal.

Watermarking benefits from the spread spectrum approach in various ways. The spread watermark signal has the advantage of being resistant to signal processing attacks such as compression, filtering, or cropping. Another benefit is that the disseminated watermark signal is resistant to hostile attempts such as intentional watermark change or removal.

Furthermore, spread spectrum watermarking allows for the embedding of many watermarks into a single host signal. Watermarking with spread spectrum is widely utilized in a variety of applications such as copyright protection, content authentication, and tamper detection [32].

II.7.1.2 Least Substitution Bit (LSB)

The least substitution bit (LSB) is the most straightforward and easy-to-use watermarking approach among all of them [28]. This technique replaces each element's LSB with one bit of the secret message in order to conceal information in a series of binary numbers. Alternatively, the least significant bit of the mantissa can be employed in floating point arithmetic. The remainder of the LSB can be left untouched because, in most cases, the size of the hidden message is significantly smaller than the number of bits available to conceal the information. LSB substitution is straightforward, but it has a lot of disadvantages. The watermark is likely to be defeated by any addition of noise or lossy compression, even though it might withstand changes like cropping.

Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party.

II.7.1.3 Local binary pattern (LBP)

Local Binary Pattern (LBP) in Figure II.4 is a texture descriptor used in image processing and computer vision for analyzing textures. It is commonly employed in tasks such as texture classification, facial recognition, and object detection. In the context of watermarking, LBP can be utilized as a feature extraction method to embed or detect watermarks within images.

LBP technique in digital image watermarking [33]:

1. **Feature Extraction:** LBP calculates a binary code for each pixel in an image based on the intensity values of its neighbouring pixels. This binary representation encodes texture information, which can be used as features for watermark embedding or detection.
2. **Watermark Embedding:** In watermarking applications, the extracted LBP features can be modified to embed a watermark into the image. The watermark information is typically encoded into the LBP patterns by altering specific bits according to the watermark data.
3. **Watermark Detection:** To detect a watermark embedded using LBP, the same feature extraction process is applied to the watermarked image. By comparing the extracted features with the original unwatermarked image or reference features, it is possible to identify the presence of a watermark.
4. **Robustness and Security:** The use of LBP in watermarking offers advantages such as robustness against common image processing operations (e.g., compression, noise addition) and security against unauthorized removal or tampering of watermarks.
5. **Applications:** LBP-based watermarking techniques find applications in copyright protection, content authentication, and digital rights management where ensuring the integrity and ownership of digital media is crucial.

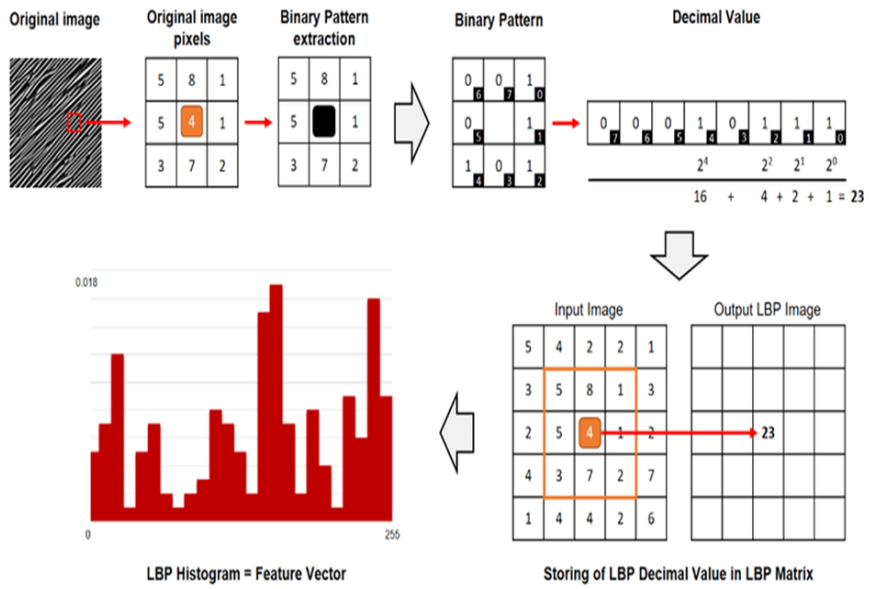


Figure II.4 Local binary pattern (LBP) technique example [34]

II.7.1.4 Patchwork Technique

The patchwork method was first put forth in 1995 by Bender et al [35] . This method uses patchwork to subtly incorporate a particular statistic with a Gaussian distribution in a cover image. It is based on a pseudorandom statistical procedure [27]. The owner selects n-pixel pairs pseudorandomly using a secret key during the patchwork technique's embedding phase, then changes the brightness values of the n-pairs of pixels. If the luminance values are xi and yi, the modified luminance values are determined by adding '1' to all values of xi and subtract '1' to all values of yi i.e. $\bar{xi} = xi + 1$ and $\bar{yi} = yi - 1$. The same secret key will be used in the extraction process of the technique (which is based on statistical assumption) and determine the sum (S) $=\sum_{n}^{i=1} \bar{xi} - \bar{y}ii = 1n$. If the sum (S) = 2n ; the cover image contained the watermark, otherwise it should be near/approximately zero. In [36, 37], the robustness performance of the patchwork technique is improved in that the cover image hides a watermark longer than one bit.

II.7.2 Transform Domain Techniques

Although it is simple to incorporate hidden information using the spatial domain techniques, these methods are extremely susceptible to even minor cover alterations [38]. Anybody can easily destroy all secret information by using signal processing techniques. Many times, even minor adjustments brought about by loss compression techniques result in the complete loss of information. Nonetheless, the data that has been watermarked is more robust due to the

information being embedded in the transform domain. Compared to spatial domain techniques, transform domain techniques are more resistant to signal processing attacks since they conceal sensitive information in key regions of the cover image. The upcoming subsections contain a presentation of the key transform domain techniques.

II.7.2.1 Discrete Cosine Transform (DCT)

By splitting an image into regions with different frequencies—low, high, and middle frequency coefficients—the discrete cosine transform (DCT) facilitates the embedding of watermark information into the middle frequency band, which offers additional resistance to lossy compression techniques without causing a significant alteration to the cover image [39–41]. The energy compression property of the DCT is excellent. An eight by eight DCT block's various frequencies are displayed in Figure II.5.

The block's lowest frequency components are shown by the FL, and its higher frequency components are indicated by the FH. In order to give more resistance to lossy compression methods without drastically altering the cover image, FM is selected as the embedding zone. The DCT coefficients for the converted output image, D, are calculated for the N x N input image, I.

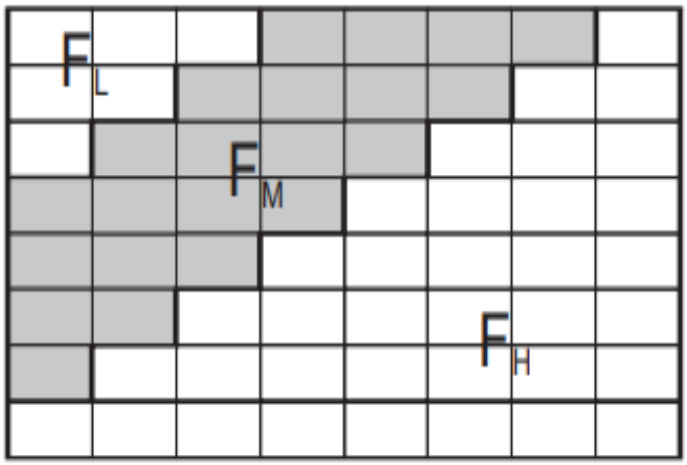


Figure II.5: Definition of DCT regions [28]

using Eq (II.4). The intensity of image is denoted as I (x, y), where the pixel in row x and column y of the image. The DCT coefficient is denoted as D (i, j) where i and j represent the row and column of the DCT matrix.

The DCT matrix can be define by using Eq. (II.4):

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{N-1}^{x=0} \sum_{N-1}^{y=0} I(x,y) \cos\left(\frac{(2x+1)\, i\pi}{2N}\right) \cos\left(\frac{(2y+1)\, i\pi}{2N}\right) \quad (II.4)$$

$$C(i), C(j) = \frac{1}{\sqrt{2}} \text{ for i,j = 0}$$

$$C(i), C(j) = 1 \text{ for i,j > 0}$$

II.7.2.2: Discrete Fourier Transform (DFT)

In the subject of watermarking, the discrete Fourier transform (DFT) was instantly taken into consideration because it provided the ability to adjust the frequencies of the cover data.To achieve the best trade-off between robustness and imperceptibility, it is useful to choose the appropriate areas of the image to insert the watermark in. DFT has two significant benefits over spatial domain approaches [42]: Strong resistance against geometric attacks is provided by two factors: (1) the watermark is translation invariant and rotation resistant; and (2) the watermark information is distributed throughout the entire image, allowing for the creation of stronger watermarks with minimal perceptual impact. However, roundoff errors are introduced by fast Fourier transform (FFT) methods, which might result in quality loss and watermark extraction mistakes. As reported in [43]. Unfortunately, this limitation is more important for hidden communication [42]. To determine the DFT of an image F (m, n) of size M × N image is G (k, l) whereas:

$$G(K,L) = \frac{1}{M.N} \sum_{M-1}^{m=0} \sum_{N-1}^{n=0} F(m,n) e^{-j2\pi\left[\frac{km}{M} + \frac{nl}{N}\right]} \quad (II.5)$$

The definition of DFT's inverse is:

$$F(m,n) = \sum_{M-1}^{k=0} \sum_{N-1}^{l=0} G(K,L)\, e^{2j\pi\left[\frac{mk}{M} + \frac{nl}{N}\right]} \quad (II.6)$$

The DFT is computationally efficient however, the complexity and poor energy compaction properties is the major disadvantages of the DFT.

II.7.2.3 Discrete Wavelet Transform (DWT)

The wavelet is a finite energy function i.e. $\psi \epsilon L^2$ (finite energy function) with zero means and is normalized ($\|\psi\| = 1$) [44]. A family of wavelets can be obtained by scaling ψ by s and translating it by u.

$$\psi_{u,s}(t) = S^{-1/2}\, \psi\left(\frac{t-u}{s}\right) \quad (II.7)$$

The continuous wavelet transform (CWT) of finite energy which is the sum over all time of scaled and shifted versions of the mother wavelet ψ for a 1-D signal $f(t)$ is given by:

$$f(u,s) = \int_{\infty}^{-\infty}(t)\, S^{\frac{-1}{2}}\, \psi'\left(\frac{t-u}{s}\right) dt \qquad (II.8)$$

where $\psi'(.)$ is the complex conjugate of $\psi(.)$. Equation (II.8) can be viewed as the convolution of the signal with dilated band-pass filters.

A continuous signal can be sampled so that a value is recorded after a discrete time interval. If the sampling of the signal is carried out at the Nyquist rate, no information would be lost. After sampling the discrete wavelet series could be used. However, this can still be very slow to compute. The reason is that the information available through the evaluation of wavelet series is still highly redundant and the solution requires a large amount of computation time. To make the wavelet computationally simple, a discrete algorithm is needed. The main idea behind DWT results from the multiresolution analysis, which involves the decomposition of an image in frequency channels of constant bandwidth on a logarithmic scale [45].

If x and y are the integer values, the DWT is defined as [46]:

$$S_{x,y} = \int_{\infty}^{-\infty} \psi' x, y(t)\, S(t)\, dt \qquad (II.9)$$

The inverse of the DWT is defined as:

$$S(t) = C_{\psi}\ \sum_x \sum_y S_{x,y}\ \psi_{x,y}(t) \qquad (II.10)$$

where s(t) is the original signal, and C_{ψ} is a constant value for normalization. ψ_x,(it) provides sampling points on the scale-time plane—linear and logarithmic sampling in the time and scale direction, respectively.

Using DWT, an image is divided into four non-overlapping multi-resolution sub-bands, which are referred to as horizontal (HH), vertical (LH), and lower resolution approximation image (LL) detail components [47]. One may then compute multiplescale wavelet decomposition by repeating the method. To retain superior image quality, the watermark can be integrated into the other three sub-bands (HL, LH, and HH sub-band) because human eyes are considerably more sensitive to the lowfrequency component (LL sub-band). demonstrates the three-level DWT sub-band pyramid structure. An image's energy is concentrated in the high decomposition levels that match the low-frequency coefficients that have perceptual significance. The low

decomposition levels accumulate a minor energy proportion, thus being vulnerable to image alterations. Therefore, the watermarks containing crucial medical information such as doctor's reference, patient identification code, image codes, etc., and requiring significantly excellent robustness are embedded in higher-level sub-bands [48].

Figure II.6 shows Pyramid structure of three levels DWT .

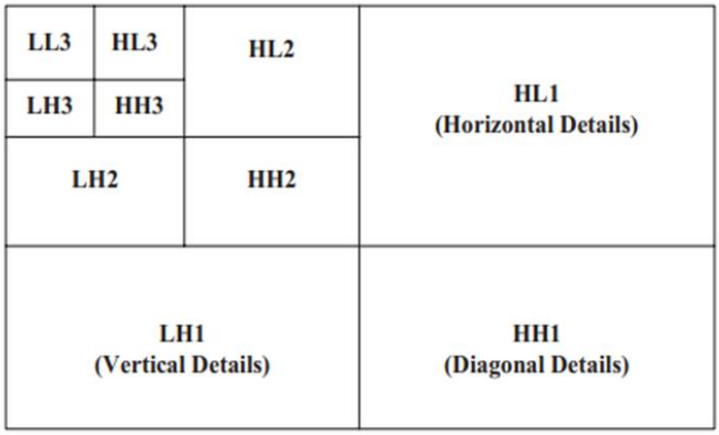


Figure II.6 Pyramid structure of three levels DWT.

II.7.2.4 Singular Value Decomposition (SVD)

SVD transform is a linear algebra transform which is used for factorization of a real or complex matrix with various applications in image processing [49]. A digital image can be represented in a matrix, with its entries giving the intensity value of each pixel in the image, SVD has an matrix A which has singular value decomposition into product of an orthogonal matrix U, an diagonal matrix of singular values S and transpose of anorthogonal square matrix V. Let A be a square matrix of order n. then according to SVD it can be represented mathematically as:

$$A = U\ S\ V^T \qquad (II.11)$$

$$U \times U^T = I$$

$$V \times V^T = I$$

Where, I represent an Identity matrix and S is the diagonal matrix of order m x n having elements Si (i=1, 2, 3, n). The singular values of A are represented by the diagonal elements of S. The columns of U matrix are known as the left singular values of A, and the columns of V are known as the right singular values of A. Factorization is called the singular value

decomposition of A. In recent years, lot of work has been carried out in transform domain watermarking using DCT, DWT, SVD and DWT-SVD and it is still going on.

II.7.2.5: Integer Wavelet Transform (IWT)

IWT is an integer-to-integer wavelet decomposition algorithm. For integer encoded signals, the integer wavelet transform (IWT) can be particularly effective for integer encoded signals. You can use IWT in applications that want to produce integer coefficients for integer encoded signals [50]. Compared with continuous wavelet transform (CWT) and discrete wavelet transform (DWT), IWT is not only computationally faster and more memory efficient but also more suitable for lossless data compression applications. IWT enables the perfect reconstruction of a scalar signal from the coefficients of the integers.

Figure II.7 shows Pyramid structure of two levels IWT .

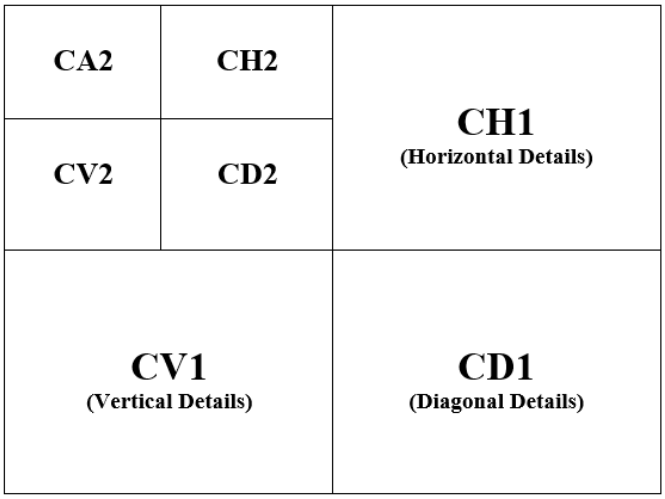


Figure II.7 Pyramid structure of two levels IWT.

II.7.3 Difference between the Spatial domain and Frequency domain

The choice of domain depends on the specific task at hand. The spatial domain is best suited for operations that require direct manipulation of pixel values or local features, such as image enhancement or object detection. On the other hand, the frequency domain is useful when analyzing the frequency components, identifying patterns, or performing operations based on the spectral characteristics of the signal, such as noise removal, compression, or spectrum analysis.

In summary, the spatial domain provides a direct representation of the signal or image, while the frequency domain reveals the underlying frequency components. Both domains have their

strengths and are used in different applications depending on the desired analysis or processing goals.

II.8 Digital Watermarking Attacks

In recent years, digital image watermarking has become a widely adopted technique to prevent copyright infringement, identify ownership, and protect against identity theft. However, the robustness and security of watermarks in medical applications face significant challenges due to malicious attacks and hacking of open channel information [52]. The objective of these attacks is often to alter or remove the watermark from its cover data, either to falsely claim ownership or to illegally block information transfer to the intended recipients.

II.8.1 Watermarking Attacks

A more sophisticated watermarking technique is required when one of the many malicious attack types causes the embed identifying key to be destroyed whole or partially [52, 53–56]. The possible assaults on watermarking systems are shown in Figure II.8. The principal attacks are as follows:

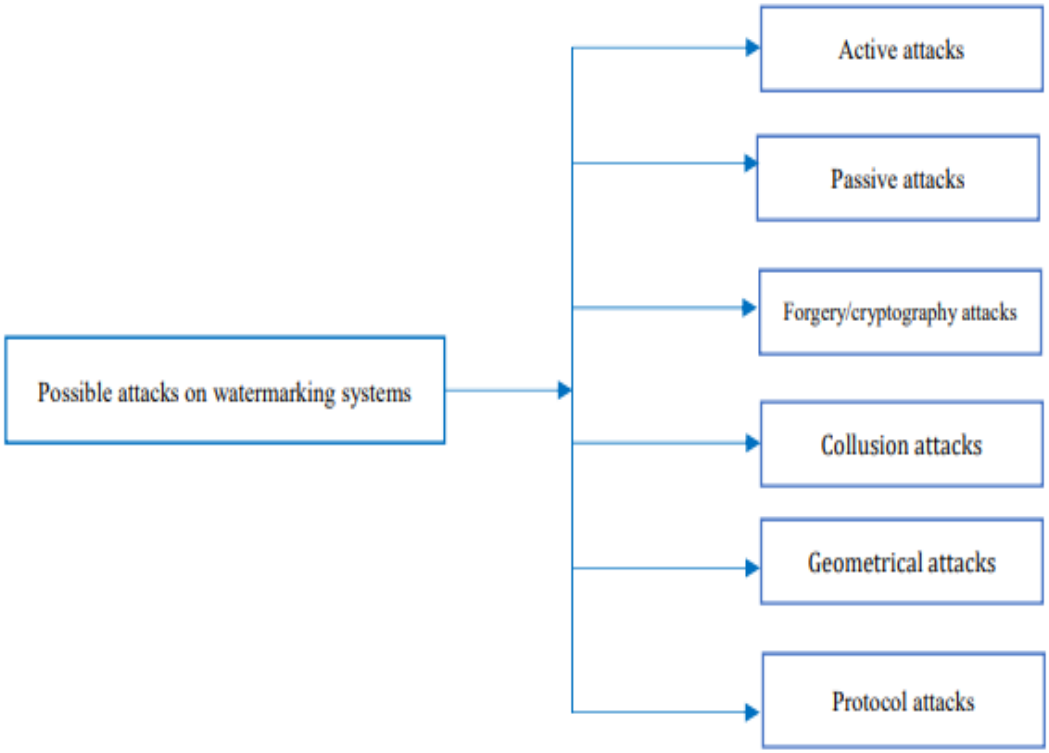


Figure II.8 Classification of possible attacks in digital watermarking.

1. **Active/Removal Attacks:** In this type of attack, the hacker tries deliberately to remove the watermark or simply make it undetectable. They are aimed at distorting a hidden watermark beyond recognition. The active attacks include Analytical de-noising, lossy compression, quantization, re-modulation, collusion and averaging attacks. This is a big issue in copyright protection, fingerprinting or copy control for example.
2. **Passive Attacks:** Hacker tries to determine whether there is a watermark and identify it. However, no damage or removal is done. As the reader should understand, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one wants to grant.
3. **Forgery/Cryptography Attacks**: This is another type of active attacks. In such attacks, the hacker embeds a new, valid watermark rather than removing one. This will help him to manipulate the protected data as he wants and then, re-implant a new given key to replace the destructed one, thus making the corrupted image seems genuine. One of the similar techniques in this category brute force attacks used in cryptography which aim to finds hidden information through an exhaustive search. For these types of attacks, it is very important to use a key of secure length as reported in [53]. The Oracle attack is the same category of the cryptographic attacks in which a non-watermarked image is created when a watermark detector device is available.
4. **Collusion Attacks:** In such attacks, the intention of the hacker is the same as for the active attacks but the approach is slightly different. The attacker uses many instances of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in finger printing applications but is not widely spread because the attacker should be able to access several copies of the same data and that the number needed can be very important. Collusion Attacks should be considered because if the attacker has access to more than one copy of watermarked image, the user can predict/remove the watermarked data by colluding them given key to replace the destructed one, thus making the corrupted image seem genuine.
5. **Geometrical Attacks:** The goal of geometrical attacks is to change/distort the hidden watermark by modifying the stego data spatially or temporally. The watermark detector loses synchronization with the hidden watermark as a result of this type of active attack. The popular integrated software for geometrical attacks is Unzign and Stirmark.
6. **Protocol Attacks:** Rather than eradicating or impairing the ability to identify the concealed watermark through local or global data alteration, the objective of these kinds

of passive attacks is to target the idea behind the watermarking application. The original protocol attack concept was dropped. The other kind of protocol assault is called a copy attack; the idea behind it is to generate doubt about who really owns the data by copying a watermark from one image to another without knowing the key that was used to embed the watermark.

II.9 Essential requirements for medical image watermarking

when embedding additional data within medical images, extreme caution is required because the additional information must not degrade image quality. The exchange of electronic patient record (EPR) data over unsecured channels demanded a high level of security.

As shown in Figure. II.9 it consists of three mandatory security requirements [57]:

- Confidentiality i.e. only the authorized users have to access the information.
- Reliability has two important outcomes: (a) integrity—the information has not been tampered with by unauthorized individuals; and (b) authentication—proof that the information does indeed belong to the correct source. Further, the traceability is an important component of the reliability and use to trace the information along its distribution.
- The availability of an information system refers to its ability to be used by authorized users under normal scheduled conditions of access and exercise. The most important issues concerning EPR data exchange via unsecured channels are authentication, integration, and confidentiality. [57, 58]. If a suitable watermark is used, all these requirements will be fulfilled.

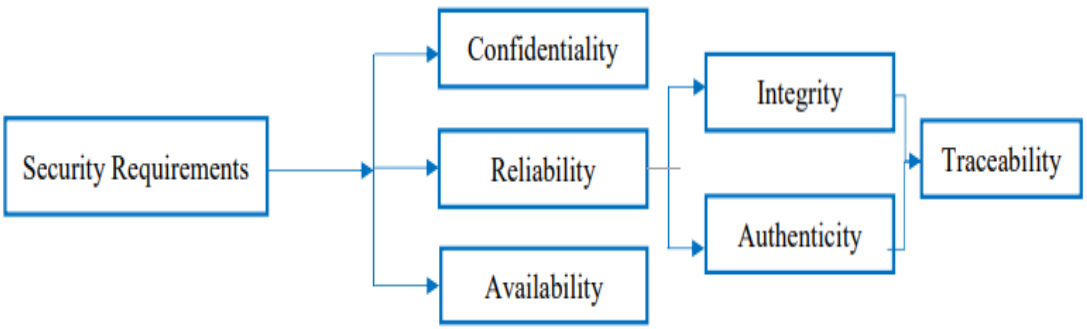


Figure II.9 Major security requirements for EPR data [57]

II.10 Performance Measures:

The primary criteria used to assess the efficacy of a medical picture watermarking algorithm are its robustness and imperceptibility.

II.10.1 Mean Square Error (MSE)

The MSE contains the cumulative squared error between the original and watermarked image [59]. A lower value of MSE indicates that the visual quality of the image will be near to the original one. The MSE can be defined as:

$$MSE = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{i=1}^{Y} (I_{ij} - W_{ij})^2 \quad \text{(II.12)}$$

where I_{ij} is a pixel of the original image of size X × Y and W_{ij} is a pixel of the watermarked image of size X × Y.

II.10.2 Peak Signal-to-Noise Ratio (PSNR)

If we want to find the watermarked image's quality loss in comparison to the original image. The PSNR of an image affects its imperceptibility [60]. It assesses the distortion generated by the watermarked image on the original image. After the watermark has been inserted, The PSNR is calculated as follows.

$$PSNR = 10log_{10} (\frac{L \times L}{MSE}) \quad \text{(II.13)}$$

Where L is the image's highest value. For an 8-bit image, L=255. In multimedia applications, any image with a brightness of greater than 30 DB is acceptable. However, with medical imaging, data quality is paramount, and PSNR of around 50Db indicates that the image is of high quality and that there has been no significant degradation in the image compared to the original.

II.10.3 Universal Image Quality Index

Wang and Bovik [57] define a universal image quality index which is a significant performance parameter to determine image distortion as a function of loss of correlation, luminance, and contrast distortion. The Universal image quality index parameter determines the image distortion significantly better than the other image distortion metrics like MSE. Suppose X is the original image and Y is possibly a distorted image whereas, $X = \{xi, i = 1,2,3, \dots \dots, N\}$ and $Y = \{yi, i = 1,2,3, \dots \dots, N\}$. The universal image quality index is defined as:

$$Q = \frac{4\,\sigma\, xy\, \overline{x}\,\overline{y}}{(\sigma_x^2 + \sigma_y^2)(\bar{x}^2 + y^2)} \qquad \text{(II.14)}$$

$$\bar{x} = \frac{1}{N}\sum_{N}^{i=1} x_I \quad \text{and} \quad \bar{y} = \frac{1}{N}\sum_{N}^{i=1} y_i$$

$$\sigma_x^2 = \frac{1}{N-1}\sum_{N}^{i=1}(x_I - \bar{x})^2)$$

$$\sigma_y^2 = \frac{1}{N-1}\sum_{N}^{i=1}(y_i - \overline{y})^2$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{N}^{i=1}(x_i - \bar{x})^2(y_i - \overline{y})^2$$

The term '$\boldsymbol{Q}$' can also define the product of three components:

$$Q = \left\{ loss\ of\ correlation\ \left(\frac{\sigma_{xy}}{\sigma_x \sigma_y}\right).\ luminance\ distortion\ \left(\frac{2\overline{x}\,\overline{y}}{(\bar{x})^2 + (\bar{y})^2}\right).\ contrast\ distortion\ \left(\frac{2\sigma_x.\sigma_y}{\sigma_x^2 + \sigma_y^2}\right) \right\}$$

These components define as:

1. The loss of correlation defines the linear correlation between x and y with dynamic range [−1, 1].
2. The luminance distortion is to determine how close the mean luminance is between x and y with a range of [0, 1].
3. The contrast distortion is to determine the contrast similarities between images with a range of [0, 1].

II.10.4 Structural Similarity Index Measure (SSIM)

The SSIM [60] can be defined as:

$$SSIM\ (x, y) = ((x, y), (x, y), (x, y)) \qquad \text{(II.15)}$$

where l(x, y), c(x, y), and s(x, y) are luminance measurement, contrast measurement, and structure measurement respectively are the important property of an image.

II.10.5 Normalized Correlation (NC)

The robustness of a watermarking algorithm is measured in terms of Normalized Correlation (NC) and bit error rate (BER). NC value measures the similarity and differences between the original watermark and extracted watermark. Its value is generally 0–1.

Though 1 is the optimal value, 0.7 is also acceptable [59].

$$NC = \sum_{i=1}^{x} \sum_{j=1}^{y} \left(W_{original\ ij} \times W_{recovered\ ij}\right) / \sum_{x}^{i=1} \sum_{y}^{j=1} W_{original\ ij}^{2} \qquad (II.16)$$

where $W_{original\ ij}$ is a pixel of the original/hidden watermark of size X × Y and $W_{recovered\ ij}$ is a pixel of the recovered watermark of size X × Y.

II.10.6 Bit Error Rate (BER)

The BER is defined as the ratio of the number of incorrectly decoded bits and the total number of bits [59]. Ideally, the BER value should be equal to 0.

$$BER = (Number\ of\ incorrectly\ decoded\ bits)/(Total\ number\ of\ bits) \qquad (II.17)$$

II.11 Conclusion

This chapter covers fundamental spatial techniques and conversion fields, as well as key performance parameters for medical and digital image watermarking, including Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC), and Broadcast Error Rate (BER). Additionally, we discuss various types of attacks, main performance measurement tools, and compare their performance against digital attacks. It is important to note that the type of attack affects the performance of robust watermarking algorithms. However, enhancements to measurement tools with more comprehensive features are necessary, as current measurement procedures are inadequate.

III.1 Introduction

Depending on the characteristics of the image, the watermark can be applied to the image in both spatial and transformational domains. Transformation domain techniques include data embedding by manipulating various transformation parameters such as integer wavelet transform (IWT), discrete wavelet transform (DWT), and singular value decomposition (SVD). The techniques can be computationally complex except they provide improved flexibility for watermarked data systems. In this chapter we propose a method for watermarking a medical image. The method uses, first, a two-level IWT subdomain of the original image and then singular value decomposition (SVD). Secondly, SVD Decomposition and spread spectrum techniques are performed on a text image watermark. We present experimental simulation results to evaluate the effectiveness of the proposed method.

III.2 Medical image Watermarking using two levels of IWT, SVD and spread spectrum

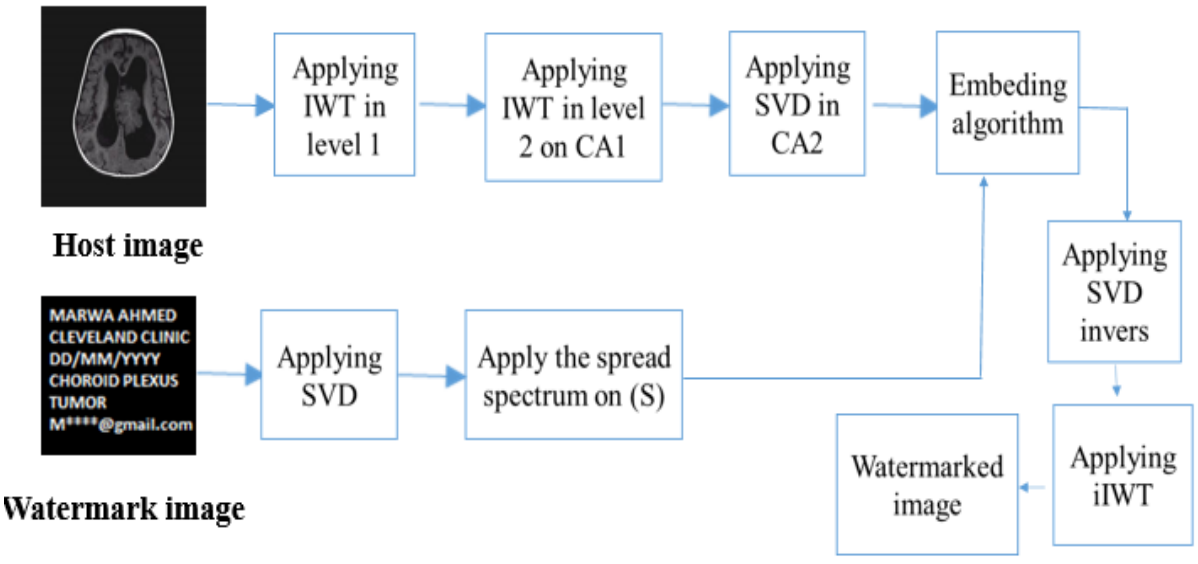


Figure III.1 Watermark embedding scheme.

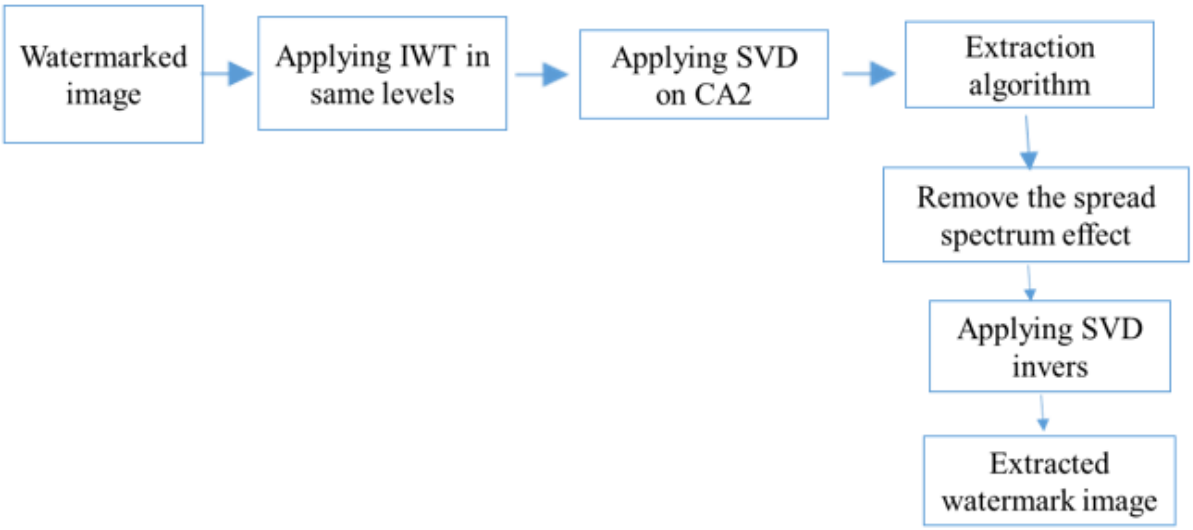


Figure III.2 Watermark extraction scheme.

III.2.1 Watermark Algorithm

- **Embedding algorithm:** In this algorithm, the studied cover image is transformed at two IWT levels, where the low frequency subband is decomposed by SVD. As for the watermark image, it is processed by SVD singular value analysis. The single value of the watermark information is spreaded, with several spread factor, and embedded in the SVD values of the host image according to the scaling factor (alpha).
- **Extraction algorithm:** The watermark extraction algorithm is just a reverse process of the steps of the embedding algorithm.

To program our proposed method, we used MATLAB version 16

The details of the medical image watermark embedding and extraction algorithm are formulated as Table III.1 follows :

.

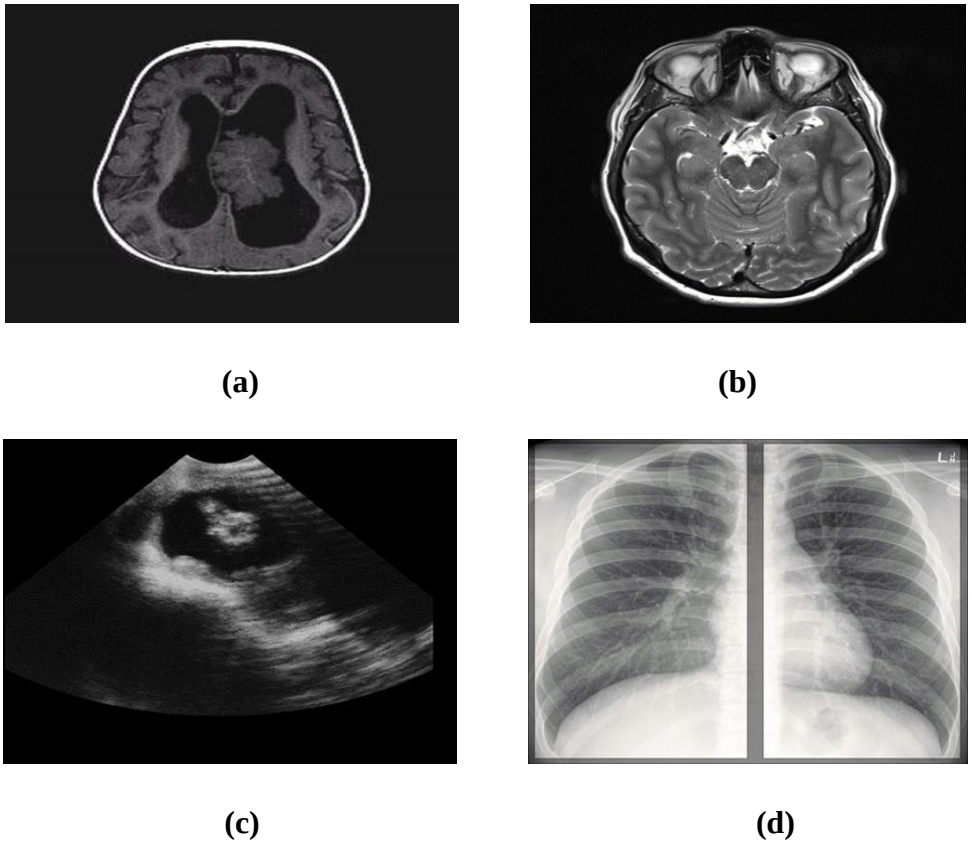
Table III.1 Embedding and extraction algorithm.

Embedding	Extraction
STEP 1: Variable Declaration Set the embedding strength (scale factor) **"alpha"** and spread spectrum factor **"spreadFactor"** for watermarking: **alpha = 0.01;** % Hint: Try with different scaling factor values (ex: 0.03,0.05,0.1,1). **spreadFactor = 0.5;** **STEP 2: Reading images** Reading and Resizing cover image: **host_image = imread('CT.jpg');** **host_image= imresize(host_image,[380 380]);** **STEP 3: Applying IWT** Applying First level IWT coefficients for cover image: **[CA1,CH1,CV1,CD1]= Iwt2(host_image,'haar');** Applying Second level IWT coefficients for cover image: **[CA2, CH2, CV2, CD2] = Iwt2(CA1,'haar');** **STEP 4: Choice of sub-bands in Cover and apply SVD on the selected sub-bands** Applying SVD on CA2: [**Uy,Sy,Vy] = svd(CA2);** **q=size(Sy);** **STEP5: Reading watermark image:**	**STEP 1:** Perform two levels of IWT on Watermarked image (possibly distorted) **[CA1_w,CH1_w,CV1_w,CD1_w]= Iwt2(watermarked_image,'haar');** **[CA2_w,CH2_w,CV2_w,CD2_w] = Iwt2(CA1_w, 'haar');** **STEP 2:** Applying SVD on the selected sub-bands **[Uy_w, Sy_w, Vy_w] = svd(CA2_w);** Extract the spreaded watermark: **extractedspreadedSw = (Sy_w- Sy) / alpha;** Remove the spread spectrum effect: **extractedSw = extractedspreadedSw - spreadFactor * pns ;** **Extracted_watermark= Uw* extractedSw * Vw';**

Reading watermark image**: I = imresize((imread('watermark')), [95 95]);** Resizing watermark image: **I = I(:,:,1);** **I1 = imresize(I, p);** Applying SVD on watermark image: **[Uw,Sw,Vw]= svd(double(I1_w));** **STEP6: Embed watermark with spread spectrum:** Spread the watermark**:** **pns =diag(diag(randn(size(Sw))));** **spreadedSw = Sw + spreadFactor * pns ;** Embedding watermark: **smark=Sy+alpha* spreadedSw;** Rebuild the sub-bands using SVD: **CA2_1= Uy*smark*Vy';** Applying the invers IWT to get watermarked image: **CA1_1 = iIwt2(CA2_1, CH2, CV2, CD2, 'haar');** **watermarked_image = iIwt2(CA1_1, CH1, CV1, CD1, 'haar');**	

III.2.2 Simulation of Watermarking Algorithms

The performance of the watermark technology depends on IWT, SVD, and spread spectrum. In the proposed method, the medical cover image (CT image) is 380 x 380 and the watermark image is 95 x 95. Figure III.3 shows the different types of medical images used as a cover image.



(a) **(b)**

(c) **(d)**

Figure III.3 shows test images CT brain-cancer (a) MRI (b) Ultrasound (c) Hand X-ray (d)

The strength of the watermark of the image is evaluated by determining the NC values. The imperceptibility of the image with the watermark is also evaluated by PSNR and SSIM. It is quite clear that the size of the watermark affects the quality of the image bearing the watermark. However, the deterioration in image quality due to the watermark will not be noticeable if the size of the watermark is small. Figure III.4 shows the original image of the cover and the image after the embedding process and after the extraction process. Figure III.5 shows the original watermark image and the extracted version. Table III.2 shows the PSNR performance, SSIM and NC for the proposed method with a different scale factor.

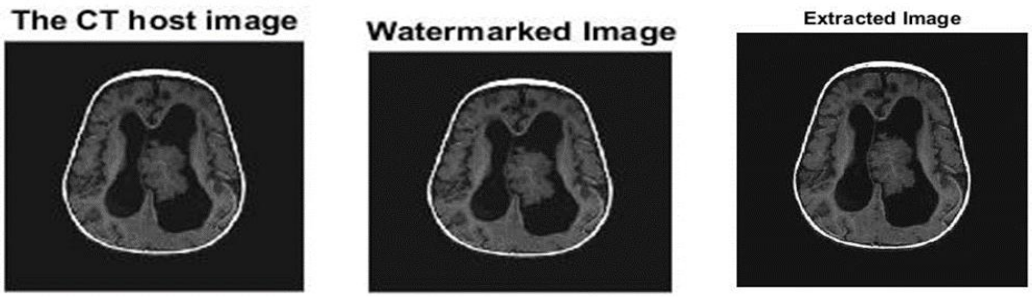


Figure III.4 The cover image and the watermarked image and the extracted cover image.

(a) **(b)**

Figure III.5 The original watermark (a) and the extracted watermark (b).

Table III.2 The PSNR, SSIM and NC performance at different scale factor.

Type of cover image	Scale Factor	PSNR	SSIM	NC
CT	0.01	48.0411	1	0.9845
	0.03	40.5447	0.9991	0.9845
	0.05	36.6353	0.9959	0.9845
	0.09	31.4616	0.9875	0.9845
	0.1	30.6338	0.9851	0.9845
MRI	0.01	47.9516	1	0.9845
	0.03	42.5380	0.9996	0.9845
	0.05	38.4907	0.9971	0.9845
	0.09	33.5313	0.9921	0.9845
	0.1	32.6227	0.9903	0.9845
Ultrasound	0.01	45.5493	1	0.9845
	0.03	38.4713	0.999	0.9845
	0.05	34.4526	0.9916	0.9845
	0.09	29.9642	0.9746	0.9845
	0.1	29.2111	0.9698	0.9845
X-ray	0.01	40.3041	0.9998	0.9845
	0.03	38.5772	0.9984	0.9845
	0.05	36.1234	0.9967	0.9845
	0.09	32.0512	0.9909	0.9845
	0.1	31.2356	0.9889	0.9845

Table III.3 Visual quality of the watermarked image at different scale factor.

Scale Factor	Quality of the watermarked image
0.01	stellar quality
0.05	Very good quality
0.1	Good quality
0.5	Average quality
1	pauper quality

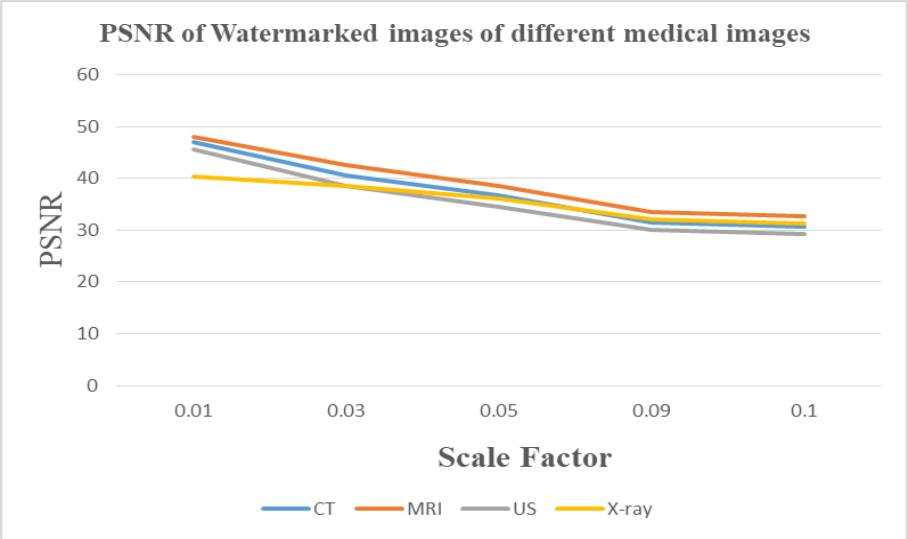


Figure III.6 The PSNR performance at different scale factor.

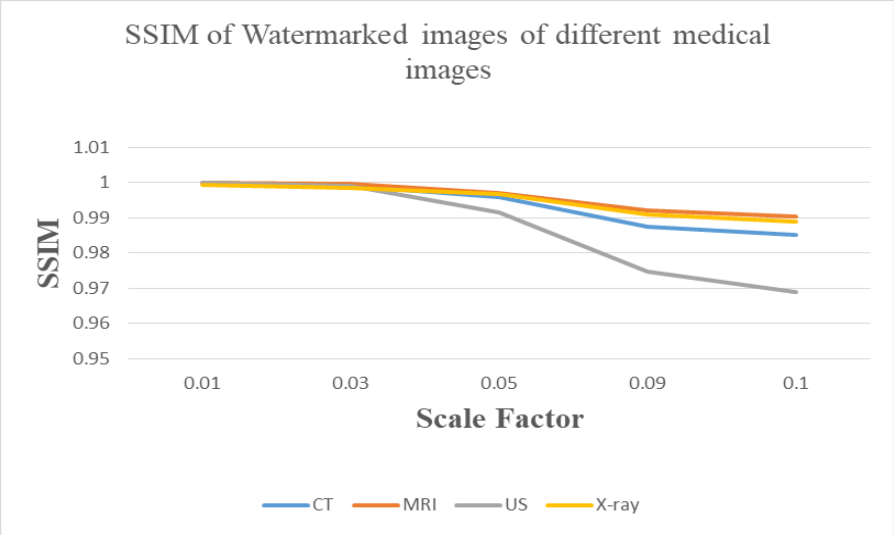


Figure III.7 The SSIM performance at different scale factor.

Discussion :

The watermarked image quality performance is measured by evaluating some of performance metrics and measurement tools, such as PSNR and SSIM. The performance of the quality of the extracted watermark image is measured by Normalized Correlation (NC). These standardized tools are commonly used to evaluate the performance of watermarking systems. The quality of a watermarked image is determined by its imperceptibility, which can be evaluated using peak signal-to-noise ratio (PSNR), and SSIM with different scale factor values. A higher PSNR value indicates better quality. Table III.2 show PSNR and SSIM values at different scale factors and the visual quality of Watermarked image. The image displays the clearest quality when the PSNR value is higher.

A low signal-to-noise ratio (PSNR) corresponds to poor watermark image quality. For example, the size factor 0.01 and a PSNR of 48.0411 dB result in excellent image quality, while a scaling factor of 0.1 a PSNR of 29.2111 dB indicates lower quality compared to the first value.

For NC, according to the data Table III.2, it is fixed as it indicates (0.9845), meaning that the quality of the extracted watermark image is excellent, not affected by either changing the scaling factor or changing the type of the host image.

III.3 Experimental Results and Discussion after applying different Attacks

In this part of the chapter, we tested the robustness of the proposed method as we applied different types of attacks on the watermarked image obtained from the method discussed above (two levels of IWT with SVD and spread spectrum). The attacks are salt and pepper noise attack, midian filter and Gaussian filter.

III.3.1 Applying attacks

Figure III.8 illustrates the watermarked CT images that have been subjected to various attacks. To assess the resilience of the embedded watermark, we employ our proposed extraction procedures to extract the watermark from the affected images. The extracted watermarks from the attacked watermarked images are displayed in the table III.4. Upon examination of these figures, it is evident that our proposed method successfully produces high-quality extracted watermark images in most cases. We evaluate the performance of the proposed technique, specifically the PSNR and NC, on

the image watermark using a uniform scale factor of alpha=0.1. Our method utilizes four different types of medical images and subjects each image to three distinct attacks. The PSNR and NC performance of all attacks are detailed in table III.5.

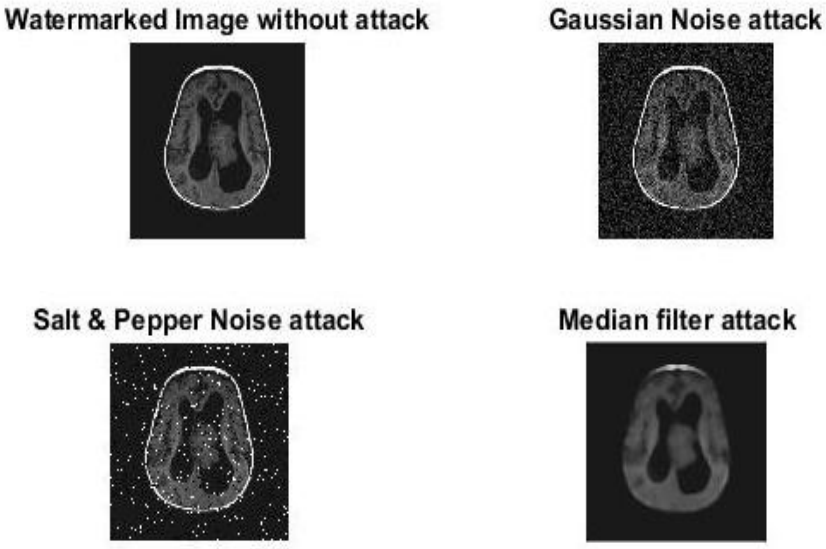
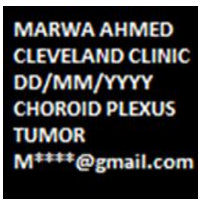
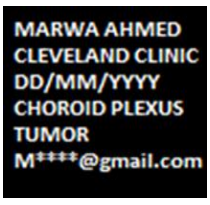
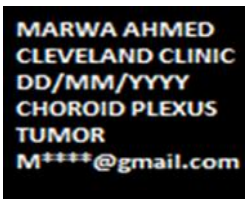


Figure III.8 attacked watermarked CT images using different attacks.

Table III.4 Extracted watermarks from Attacked watermarked images

Attacks Extractd watermk from cover image	Extracted watermark from cover image			
	CT	**MRI**	**Ultrasound**	**Hand X-ray**
Attack free				
Gaussian Noise attack				

Salt & pepper noise attack				
Median filter attack				

Table III.5 PSNR and NC result obtained from simulations using same watermark image.

Performed attacks	CT		MRI		Ultrasound		Hand x-ray	
	PSNR	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
Attack free	30.6338	0.9845	32.6227	0.9845	29.2111	0.9845	31.2356	0.9845
Gaussian Noise attack (GNA)	20.3810	0.7444	20.8050	0.7799	17.9924	0.9269	20.1815	0.8254
Salt & pepper noise attack	16.4359	0.8208	17.0488	0.8584	16.3674	0.8311	17.1383	0.7634
Median filter attack (MFA)	29.2209	0.8099	29.2669	0.8853	28.1395	0.7974	28.4446	0.8746

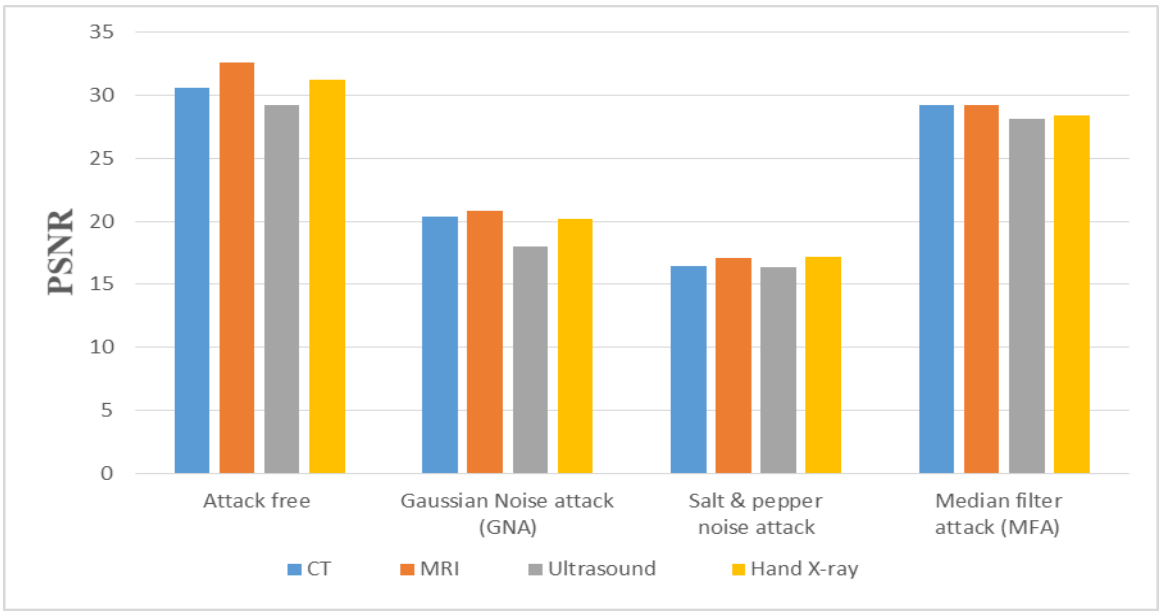


Figure III.9 PSNR result obtained from simulations using same watermark image.

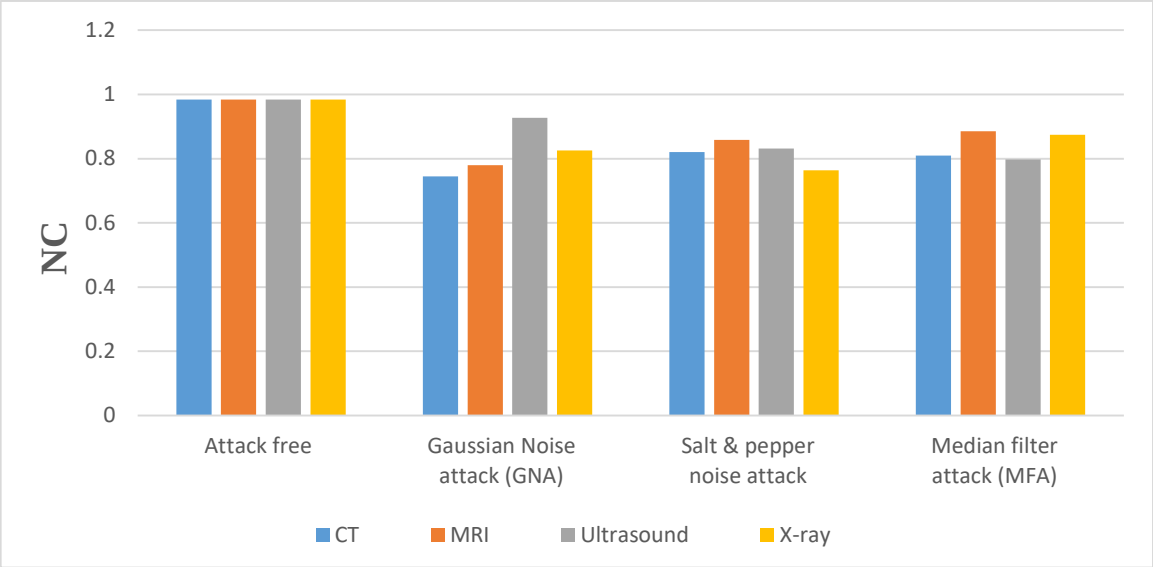


Figure III.10 NC result obtained from simulations using same watermark image.

Discussion:

From the above figures, Figure III.9, Figure III.10, we note that it is clear that we have the proposed method successfully produces high-quality extracted watermark images most of the time.

Cases except salt and pepper attack we found that salt and pepper are greatly affected PSNR values, as for NC values. We found that they are close depending on the type of attack, meaning that the extracted watermark can be recognized in all cases.

III.4 Experimental Results Comparing proposed method with other reported method

Table III.6 Comparison of PSNR and NC values with other reported method

Gain factor	Singh et al [61]		DWT [62]		Proposed method	
	PSNR (db)	NC	PSNR (db)	NC	PSNR (db)	NC
0.01	28.17	0.5247	35.75	0.6921	48.0411	0.9845
0.05	28.02	0.9288	33.07	0.9814	36.6353	0.9845
0.9	21.70	0.9668	29.73	0.9905	31.4616	0.9845
0.1	26.85	0.9697	28.96	0.9912	30.6338	0.9845

Discussion:

As we can see, this proposed method provides higher imperceptibility strength compared to the other methods described above.

Referring to Table III.6, the maximum NC value was obtained by the proposed method 0.9845 versus 0.9697 and 0.9912 obtained by Singh et al [61], and DWT [62] methods at gain factor = 0.1. However, the minimum value of NC was 0.5247 and 0.6921 obtained by Singh et al. DWT Methods at gain factor = 0.01 compared with the proposed method which was fixed at the same value.

We also see that the maximum PSNR value is obtained with Singh et al, it is 28.17 dB 35.75dB, DWT Methods. While the maximum PSNR value was obtained With the proposed method, it is 48.0411 dB at gain factor = 0.01.

On the other hand, the minimum PSNR value was obtained using Singh et al, it is 26.85 dB and 28.96 dB DWT methods. While the minimum PSNR value obtained by the proposed method is 30.6338 dB at gain factor = 0.1.

Overall, the performance of the proposed method is better than other reported technique Singh et al. In methods [61], DWT [62] in terms of inability to perceive.

Finally, the total the PSNR and NC performance of the proposed method is highly dependent on the size Watermarks, gain factor and noise contrast.

III.5 Conclusion

This chapter discusses a method for watermarking medical images. The approach utilizes a two-level IWT transform domain sub-band, where SVD decomposition is performed using spread spectrum techniques with a text watermark image. This method has shown potential for enhancing the robustness of the watermark, making it effectively extractable in medical and other applications. Additionally, it provides an optimal balance between robustness and perceptual quality (imperceptibility) of the cover image. The combined use of IWT, SVD, and spread spectrum techniques results in improved performance regarding imperceptibility.

GENERAL CONCLUSION

General conclusion

This document proposes a secure transmission method using watermarking techniques tailored for medical images. Experimental results were obtained by varying the scale factor, and the performance of the developed scheme was tested against various attacks, such as Median and Gaussian attacks. The imperceptibility and robustness of the proposed method were assessed through extensive experiments. The results indicate that the method offers good imperceptibility for watermarked images, evaluated by PSNR. The method's performance against different attacks on the watermarked image was evaluated using correlation coefficients of extracted watermark logos and subjective image tests. The experimental results demonstrate that the proposed method effectively withstands various attacks.

The integration of multiple techniques aimed to enhance the robustness of the watermarks and the quality of the watermarked image, which is the primary objective of the research. However, this may have increased the application's complexity, which needs to be examined separately. Further studies are necessary to explore approaches that simultaneously improve performance in terms of robustness, imperceptibility, security, and capacity. Additionally, we aim to conduct more research on lossless data hiding techniques, especially for medical applications, which will be reported in future communications.

References

[1] Kate Brush, *medical imaging (radiology)*, https://www.techtarget.com. December (2019)

[2] DR RUJU DOSH, *What are the Common radiology procedures?*, https://www.continentalhospitals.com, 07 Nov (2023).

[3] Tan Teck Jack, Department of Medical Imaging, TeleMedC Group, *The Importance of Medical Imaging in Modern Healthcare*, 03-Jul (2023)

[4] Kahn Jr, C. E. (2018). *Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide*. Springer.

[5] World Health Organization. (2016). WHO guideline: recommendations on digital interventions for health system strengthening.

[6] Kossoff, G., &Dorfman, R. (2018). Medical Image Integrity. Journal of Digital Imaging, 31(5), 637–644. https://doi.org/10.1007/s10278-018-0086-x

[7] Zhang, Y., & Zhang, J. (2016). Medical Image Authentication: A Review. Journal of Healthcare Engineering, 2016, 1–12. https://doi.org/10.1155/2016/1438761

[8] Estefanía García Gallardo, *What Is PACS (Picture Archiving and Communications System)?*, 04, (2023). https://builtin.com

[9] Arch Dis Child. *PACS (picture archiving and communication systems): filmless radiology*, 2000 Jul; 83(1): 82–86.

[10] S. Prabhakaran and P. Arumugam, *ENSURING SECURITY OF DICOM CONTENT USING TRANSPOSITION BASED AES*, August (2014). http://www.researchgate.net

[11] dcm4che DICOM Archive 5 supports the Basic TLS Secure Transport Connection Profile and the AES TLS Secure Transport Connection Profile as specified in DICOM Standard, Part 15

[12] 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.

REFERENCES

[13] B.M. Irany, 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

[14] S.A.K. Mostafa, N. El-sheimy, A.S. Tolba, F.M. Abdelkader, H.M. Elhindy, Wavelet packetsbased blind watermarking for medical image management. Open Biomed. Eng. J. 4, 93–98 (2010)

[15] Boreiry, M., Keyvanpour, M.-R.: Classification of watermarking methods based on watermarking approaches. pp. 73–76 (2017)

[16] Chawla, G., Saini, R., Yadav, R.: Classification of watermarking based upon various parameters. Int. J. Comput. Appl. 4 (2012)

[17] Song, C., Sudirman, S., Merabti, M.: Recent Advances And Classification of Watermarking Techniques in Digital Images, p. 6

[18] H.C. Huang, W.C. Fang, Techniques and application of intelligent multimedia data hiding. Telecommun. Syst. 44(3-4), 241–251 (2010)

[19] A.K. Singh, B. Kumar, M. Dave, S.P. Ghrera, A. Mohan, Digital image watermarking: techniques and emerging applications, handbook of research on modern cryptographic solutions for computer and cyber security, IGI Global, USA, pp. 246–272, 2016

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

[21] F. Cayre, C. Fontaine and T. Furon, Watermarking security: theory and practice, IEEE Trans. Signal Process., 53 (10), 3976–3987 (2005)

[22] L.P. Freire, P. Comesana, J.R. Troncoso-Pastoriza, F. Perez-Gonzalez, Watermarking security: a survey, in Transactions on Data Hiding and Multimedia Security, ed. by Y. Q. Shi (Ed), vol. 4300, (LNCS Springer, Berlin, 2006), pp. 41–72

[23] F. Hartung, F. Ramme, Digital rights management and watermarking of multimedia content for m-commerce applications. IEEE Commun. Mag. 38((11), 78–84 (2000)

[24] B.L. Gunjal, S.N. Mali, Applications of digital image watermarking in industries, pp. 5–7, CSI Communications, 2012

REFERENCES

[25] A.K. Singh, M. Dave, A. Mohan, Wavelet based image watermarking: futuristic concepts in information security. Proc. Natl. Acad. Sci., India Sect. A: Phys. Sci. 84(3), 345–359 (2014)

[26] D. Arya, A survey of frequency and wavelet domain digital watermarking techniques. Int. J. Sci. Eng. Res. 1(2), 1–4 (2010)

[27] C. Shoemaker, Hidden Bits: A Survey of Techniques for Digital Watermarking, Independent Study (Spring, 2002)

[28] 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

[29] N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain. Signal Process. 66(3), 385–403 (1998)

[30] 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, 2012

[31] Jian, Q., Huang, J., & Liu, Y. (2012). A robust spread spectrum image watermarking scheme using chaotic sequences. Signal Processing, 92(4), 1034-1045.

[32] G. Langelaar, I. Setyawan, R. Lagendijk, Watermarking digital image and video data: a stateof-art overview. IEEE Signal Process. Mag. 17(5), 20–46 (2000)

[33] S. R. Chalamala and K. R. Kakkirala, "Local Binary Patterns for Digital Image Watermarking," 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS), Kota Kinabalu, Malaysia, 2015, pp. 159-162, doi: 10.1109/AIMS.2015.34.

[34] M. Müller and D. Britz, Classification of Bainitic Structures Using Textural Parameters and Machine Learning Techniques, Department of Materials Science, Chair of Functional Materials, Saarland University, Saarbrücken 66123, Germany; d.britz@mx.uni-saarland.de (D.B.); lauraulrich@gmx.net (L.U.); muecke@matsci.uni-sb.de (F.M.) ,12 May 2020.

REFERENCES

[35] 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

[36] 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

[37] 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

[38] 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

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

[40] 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)

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

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

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

[44] R. Chellappa, S. Theodoridis, Academic Press Library in Signal Processing: Signal Processing Theory and Machine Learning, vol 1 (Elsevier, 2014)

[45] 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). doi:10.1007/s11042-015-2754-7

[46] D.T.L. Lee, A. Yamamoto, Wavelet analysis: theory and applications. Hewlett-Packard J. 5, 44–52 (1994)

REFERENCES

[47] M.K. Gupta, S. Tiwari, Performance evaluation of conventional and wavelet based OFDM system. AEU—Int. J. Electron. Commun. 67(4), 348–354 (2013)

[48] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Secure and efficient health data management through multiple watermarking on medical images. Med. Biol. Eng. Comput. 44(8), 619–631 (2006)

[49] Manjunath. M, Prof. Siddappaji, "*A New Robust Semi blind Watermarking Using Block DCT and SVD*", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 193-197, 2012

[50] N. Srinivasu, V Veeramani,CNN based "Text in Image" Steganography using Slice Encryption Algorithm and LWT Author links open overlay panelLingamallu , *September2022,* https://doi.org/10.1016/j.ijleo.2022.169398

[51] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun, Attack modelling: towards a second generation watermarking benchmark. Signal Process. 81(6), 1177–1214 (2001)

[52] M. Do, M. Vetterli, The contourlet transform: an efficient directional multiresolution image representation. IEEE Trans. Image Process. 14(12), 2091–2106 (2005)

[53] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun, Attack modelling: towards a second generation watermarking benchmark. Signal Process. 81(6), 1177–1214 (2001)

[54] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers, J.K. Su, Attacks on digital watermarks: classification, estimation-based attacks and benchmarks. IEEE Commun. Mag. 39, 118–126 (2001)

[55] C. Song, S. Sudirman, M. Merabti, D. Llewellyn-Jones, Analysis of digital image watermark attacks, in 7th IEEE Consumer Communications and Networking Conference, Las Vegas, Nevada, USA, pp. 941–945, January 09–12, 2010

[56] H. Nyeem, W. Boles, C. Boyd, Digital image watermarking: its formal model, fundamental properties and possible attacks. EURASIP J. Adv. Signal Process. 135, 1–22 (2014)

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

REFERENCES

[59] 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)

[60] 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

[61] A.K. Singh, M. Dave, A. Mohan, Robust and secure multiple watermarking in waveletdomain. A special issue on advanced signal processing technologies and systems for healthcare applications (ASPTSHA). J. Med. Imaging Health Inf. 5(2), 606–614 (2015)

[62] Amit,K.S and Basant. K, Medical Image Watermarking,133. (2017).