KASDI MERBAH UNIVERSITY OF OUARGLA

Faculty of new Information and Telecommunication Technologies

Department Of:

Electronic and Telecommunications

ACADEMIC MASTER

Domain: Telecommunication

Field: Telecommunication Systems

Submitted by:

KAIROUANI ISRA

AZZOUZI FATIMA EZAHRA

Theme:

Secure Transmission in Telemedicine

Evaluation Date: 06/2023

Before the Jury:

Mrs. Louazen Hassiba	Chairman	MCB	UKMO
Mr. Sayeh Mouad	Supervisor	MCB	UKMO
Mrs. Benkrinah Sabra	Examiner	MCB	UKMO

Academic Year: 2022/2023

Dedication

I express my deepest gratitude to the Almighty **God** for granting me the strength and determination to successfully complete this endeavor.

I humbly dedicate this modest achievement: In loving memory of my late father, **ABD EL-KADER**, whose unwavering support and encouragement propelled me forward. His absence is deeply felt, yet his influence remains with me always. I hope to make him proud as his beloved daughter, Isra.

To my dear mother, **HOURIA**, who has been my constant companion throughout this journey. Her unwavering love, guidance, and endless support have been my pillars of strength.

To my cherished sister, **Djihane**, and my dear brother, **Mouhamed Azzouz** your presence in my life has been a constant source of love and encouragement. Thank you for standing by me.

I also extend my gratitude to the entire **Kairouani** and **Boukhttala** family for their unwavering support and encouragement. To my best friends **Ayoub**, **Ilham**, **Fatima Ezahra**, **Nihad**, **Ines**, **Belkais** and **Anfal**, thank you for being a source of strength and inspiration. To my colleagues, including **Uncle Omar**, **Hanane**, **Abd Al-Majeed**, **Ramzi**, and **Mohammed Al-Amin**, your assistance has been invaluable.

Lastly, I am thankful for the support of everyone near and far.

ISRA.

Dedication

Thank God for giving us success and repayment .and giving us fortitude and helping us to complete this work .I humbly dedicate this modest achievement to :

" Dear Father **BELKACEM** " To those who taught me giving without waiting and that instilled in my soul the love of ambition and perseverance, to the owner of the good heart, my hero and To whom I carry his name with pride.

"My dear mother **AICHA** " To those who taught me giving without waiting, to feel love, compassion and dedication, filled me with your tenderness and affection throughout my life, you were the bond and smile of life and the secret of existence.

" My dear brothers and sister " To those who shared my childhood and carried with me the burden of life in my youth, to those who paved the path of success with me, to my dear brothers **Charaf eddine** , **Oussama**, **Abdel Fatah** and **Chima**. Your advices and encouragement to me is the indispensable support,

your prayers and support have always been helpful to me thank you from the heart. May Allah bless you . and may God clothe you with health, wellness, happiness and peace of mind, and may God keep you for me.

I also extend my gratitude to the entire **Azzouzi** and **Zakhrouf** family for their unwavering support and encouragement. To my best friends , **Ilham** ,**Wissal** , **Soundous** , **Hanan** , **Nihade** , **Mariam** and **Anfal**. To my colleagues and all my teachers throughout my school career.

" **Isra** " To my sister and classmate, I had the happiest moments and the most wonderful memories .For all who have contributed, far or near, to the realization of this work.

FATIMA EZAHRA.

Acknowledgements

We are grateful to **God** for helping us and for giving us the patience we needed to overcome the difficulties we faced in completing our work.

Also want to thank our teachers who have helped us throughout our education as well as the jury members **LOUAZEN HASSIBA** and **BENKRINAH SABRA** who provided more suggestions and constructive criticism to ameliorate our work, and our supervisor **SAYEH MOUAD** and all the professors and workers in the Department of Electronics and Telecommunications.

At last, we thank all those who have helped us from near and far, especially the students **GHOUAR BRAHIM** and **MILOUDI Tarek** .

ISRA.
FATIMA EZAHRA.

Abstract :

The growing number of medical digital images necessitates their secure sharing among specialists and hospitals while protecting patient privacy. To achieve this, medical image watermarking is essential. However, the watermarking process must be carefully executed for two key reasons. Firstly, it should not compromise image quality. Secondly, confidential patient information embedded in the image should be reliably retrievable even after decompression. Despite extensive research in this area, no existing method fulfills all requirements of medical image watermarking. This study aims to address this gap by providing a comprehensive survey of different methods, including DWT with SVD and spread spectrum, analyzing their strengths and weaknesses, and offering valuable insights to researchers.

Keywords: Medical digital images, Medical image watermarking, DWT, SVD, Spread spectrum.

Résume :

Le nombre croissant d'images médicales numériques nécessite leur partage sécurisé entre les spécialistes et les hôpitaux tout en protégeant la vie privée des patients. Pour ce faire, le filigrane d'image médicale est essentiel. Cependant, le processus de filigrane doit être soigneusement exécuté pour deux raisons principales. Premièrement, cela ne devrait pas compromettre la qualité de l'image. Deuxièmement, les informations confidentielles du patient intégrées dans l'image doivent pouvoir être récupérées de manière fiable même après la décompression. Malgré des recherches approfondies dans ce domaine, aucune méthode existante ne satisfait à toutes les exigences du filigrane d'image médicale. Cette étude vise à combler cette lacune en fournissant une étude complète des différentes méthodes, y compris DWT avec SVD et l'étalement du spectre, l'analyse de leurs forces et faiblesses, et offrant des perspectives précieuses aux chercheurs.

Mots-clés : Images numériques médicales, Filigrane d'images médicales, DWT, SVD, étalement du spectre.

ملخص:

يتطلب العدد المتزايد من الصور الرقمية الطبية مشاركتها الآمنة بين المتخصصين والمستشفيات مع حماية خصوصية المرضى. لتحقيق ذلك، يعد وضع العلامات المائية على الصورة الطبية أمرًا ضروريًا. ومع ذلك، يجب تنفيذ عملية وضع العلامات المائية بعناية لسببين رئيسيين. أولاً، لا ينبغي أن يضر بجودة الصورة. ثانيًا، يجب أن تكون معلومات المريض السرية المضمنة في الصورة قابلة للاسترداد بشكل موثوق حتى بعد تخفيف الضغط. على الرغم من البحث المكثف في هذا المجال، لا توجد طريقة موجودة تلبي جميع متطلبات وضع العلامات المائية على الصور الطبية. تهدف هذه الدراسة إلى معالجة هذه الفجوة من خلال تقديم مسح شامل للطرق المختلفة، بما في ذلك DWT مع SVD ونشر الطيف، وتحليل نقاط قوتها وضعفها، وتقديم رؤى قيمة للباحثين.

الكلمات الرئيسية: الصور الرقمية الطبية، العلامة المائية للصور الطبية، DWT، SVD، انتشار الطيف.

List of Contents

CHAPTER I

CHAPTER II

CHAPTER III

List of Figures

List of Tables

List of Abbreviation

ACR: American College of Radiology.

AHA: American Hospital Association.

BER :Bit Error Rate.

CT: Computed tomography.

CWT: Continuous Wavelet Transform.

DICOM: Digital Imaging and Communications in Medicine.

DWT: Discrete Wavelet Transform.

EHRs: Electronic Health Records.

EPR: Electronic Patient Record.

GUI: Graphical User Interface.

ICT: Information and Communication Technology.

IEEE :Institute of Electrical and Electronics Engineers.

ISO :International Organization for Standardization.

LSB: Least Significant Bit.

MRI: Magnetic resonance imaging.

MSB: Most Significant Bit.

MSE: Mean Square Error.

NC : Normalized Correlation.

NEMA: National Electrical Manufacturers Association.

PACS: Picture Archiving and Communication System.

PET: positron-emission tomography.

PSNR: Peak Signal-to-Noise Ratio.

RISs: Radiology Information Systems.

SSIM: Structural Similarity Index Measure.

SVD: Singular Value Decomposition.

US: Ultrasonography.

VPN: Virtual Private Network.

General Introduction

We are currently living in an age based on digital communication, the Internet, and technology, where data exchange has become incredibly easy and fast. It only takes a few seconds to share a personal image with the world. As a result of this digital advancement, tools for manipulating digital images have emerged. It becomes easier to claim false ownership and illegally reproduce shared images, making them accessible online and susceptible to tampering or alteration.

There are several ways to protect legal ownership of images. One of the most common methods is the use of digital watermarks, which are powerful tools for ownership verification and tamper detection. These methods must meet certain key requirements, such as Robustness and imperceptibility. Robustness is very important, which means that the proposed method should be able to withstand different types of attacks. Images with watermarks should be imperceptible or transparent. Finally, the watermark extraction process can be blind, i.e. the extraction does not require the original image.

This document contains three chapters structured in the following manners:

Chapter one focused on medical imaging and its types, as how archiving and digital communication systems work in health care organizations or hospitals.

Chapter Two dealt with different medical image watermarking techniques and their importance. Watermarking framework, watermarking requirement, watermarking advantages, and benchmark tools are also presented. Watermarking performance measurements are explained.

Chapter three presents a proposed watermarking techniques. Simulation and experimental results are shown.

I.1. Introduction

Medical imaging is a group of diverse technologies used to map the human body to diagnose, monitor and treat medical conditions. All imaging methods have one thing in common: Medical conditions are visualized as changes, so desired features (such as tumors) can be identified in photos and examined by qualified imaging physicians. This image can be viewed as a model of graphical tissue, such as muscle, nerve, epithelial tissue, and connectivity.

The images used in this document are digital images, meaning that there is a specific accuracy with pixels as the smallest element. In addition, any means of image capture will result in some image degradation compared to the original subject. Degradation usually consists of blurring (loss of detail) and noise (undesirable variation). There are some basic principles common to all means of image processing, including the interpretation and mathematical processing of images as a system. The image itself can be considered a multidimensional signal. In many cases, the steps of photo formation can be considered as a linear system, allowing for simplified mathematical processing.

Each technology provides different information about the area of the body being studied or treated in relation to potential diseases, injuries, or effects of treatment. Finally, this chapter deals with medical imaging and its types, digital imaging, archiving systems, and communication systems in healthcare institutions.

I.2. Medical Imaging

Due to recent developments in modern medical sciences, health-related information in terms of images is playing a significant role in providing solutions to health-related problems. The developments of various types of medical imaging techniques are aiding doctors to see the interior organs of the body. The history of different medical imaging techniques is given in Figure I.1 [1]. X-ray, ultrasonography, computed tomography (CT), and magnetic resonance imaging (MRI) are widely used worldwide. Recently some new imaging techniques are developed particularly for the treatment of diseases such as cancer and tumors. They are positron-emission tomography (PET), endoscopy, and the combination of PET with CT or MRI images.

I.3. Medical Imaging Types

In this section, various types of medical imaging techniques are described. There are mainly four types of medical imaging techniques: X-ray, MRI, CT, and US. The details of these techniques are given below:

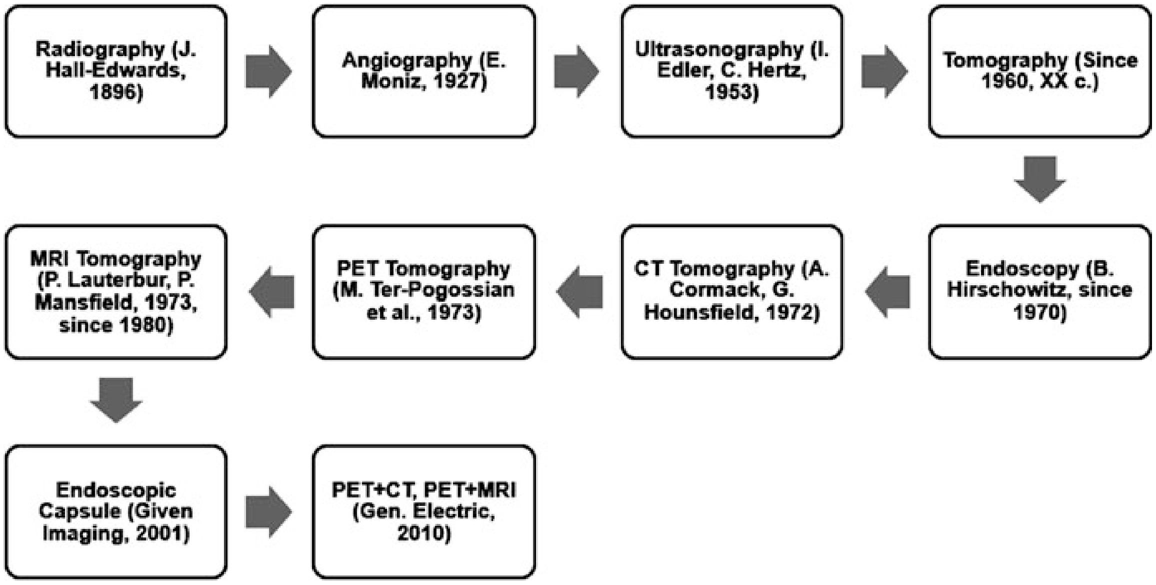

Radiography (J. Hall-Edwards, 1896)
Angiography (E. Moniz, 1927)
Ultrasonography (I. Edler, C. Hertz, 1953)
Tomography (Since 1960, XX c.)
Endoscopy (B. Hirschowitz, since 1970)
CT Tomography (A. Cormack, G. Hounsfield, 1972)
PET Tomography (M. Ter-Pogossian et al., 1973)
MRI Tomography (P. Lauterbur, P. Mansfield, 1973, since 1980)
Endoscopic Capsule (Given Imaging, 2001)
PET+CT, PET+MRI (Gen. Electric, 2010)

Figure I.1 Development in medical imaging techniques

• **X-ray imaging:** The first medical imaging technique is invented by Hall-Edwards for the observation of the internal organs of human bodies. This technique is known as X-ray imaging. Here, X-rays are passed through the disease-affected organ of the patient's body, and the result is acquired on the X-ray film. The images generated using these imaging techniques are less expensive and easy to be carried from one place to another place. But, the image generated using this technique has low quality, and sometimes, it is difficult to get information from it.

• **Ultrasonography (US) imaging:** The second major medical imaging technique is invented by I. Edler and C. Hertz in 1953. This technique is known as ultrasonography (US) imaging. In this technique, the ultrasonic signals are passed through the human skin by a transducer, and the same transducer receives echoes which are generated due to impedance differences in the tissue of humans. These echoes are amplified, processed, and displayed on the monitor as digital signals. Dr. Rao [2] has beautifully explained how this imaging technique works. The US images have low perceptual quality and are difficult to interpret.

• **Computed tomography (CT) imaging:** The third major medical imaging technique is inverted by A. Cormack and G. Hounsfield in 1972. This technique is known as computed tomography or computer tomography (CT). This image is generated by passing X-rays in multiple directions through the disease-affected organ of the patient's body. Recently, images generated using this technique is widely used in the treatment of health problems related to neurology, cardiology, and gastroenterology.

• **Magnetic resonance imaging (MRI):** The fourth major medical imaging technique is invented by P. Lauterbur and P. Mansfield in 1973. This technique is known as magnetic resonance imaging (MRI). In this technique, a liquid helium-cooled magnetic field is used for the generation of images. This imaging technique generates 3D medical images and is widely used in health problems related to neurology, gastroenterology, and angiography.

Some recent new medical imaging techniques arrived in the markets due to enhancements in basic sciences such as nuclear and lighting. This technique is known as positron emission tomography (PET) and endoscopy. These techniques are used for better diagnosis and treatment of the patient. PET images are used for the diagnosis of different types of tumor detection and treatments related to cancer. The invention of endoscopy has taken place around 2001 and is used to get optical images of the internal body. In 2010, Gen. Electronics introduced new medical imaging techniques with the combination of CT and/or MRI images with PET images for better health-related treatment.

I.4. Digital image

A digital image is a representation of a two-dimensional image in a computer or electronic device. It is composed of a grid of pixels (picture elements), each of which has a color value that determines the overall appearance of the image.

Digital images are created by using a digital camera or scanner to capture an analog image, or by creating an image in a graphics software program. The image is then saved as a digital file, such as a JPEG, PNG, or GIF, which can be viewed on a computer screen, printed out, or shared online.

Digital images have many applications, including in photography, art, design, advertising, and medical imaging. They can be edited and manipulated in various ways using graphics software, allowing for creative expression and the creation of new images. [3]

I.5. 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, analyzed, and shared electronically, allowing medical professionals to make more accurate diagnoses and treatment plans. [4]

I.6. Medical image security requirements

For a better treatment of patients, the medical images which contain patient health-related information need to be transferred from one doctor to another doctor or from one hospital to another hospital using various open communication networks. The transfer of medical images is known as telemedicine and is defined by the American Hospital Association (AHA) as "the use of medical data exchanged from one site to another via electronic communications to improve a patient's clinical health status, including an increasing variety of applications and services using two-way video, email, smartphones, wireless tools and other forms of telecommunications technology". [5]

In the last 20 years, many agencies, institutes, and researchers are working on developing various security parameters and standards for the security and integrity of medical images in telemedicine applications. The first standard for the security of medical images was developed by ISO around 2008 and is known as ISO 27799:2008. This standard is recently revised in 2016, and now it is known as ISO 27799:2016 [6]. Also, various countries developed their standards for the security of medical images [7].

Table I.1 Basic requirements of the telemedicine model

Basic requirement	Vulnerabilities	Security measures
Confidentiality	Image corruption at storage or during transmission of it.	Image encryption; storage time for an image; user access control services; user authentication.
Reliability	Modified image creation and distorted image at system storage.	Image encryption; authentication verification of image; access control services.
Availability	Modified image at system storage and distorted storage.	Access control services, and usage of antivirus software.

For the security of medical images, various telemedicine or teleradiology models are developed by researchers. One of the standard models for the security and privacy of medical images in telemedicine applications is given in Figure I.2. This model was developed by Ruotsalainen in 2010 [8]. The model describes security threats of medical images when it is transmitted online/offline. While developing a model for telemedicine applications, the following points must be fulfilled [8]: (1) all points must have the same security level, and (2) user authentication must be performed at every point of the model.

The basic requirements of the telemedicine model are confidentiality, reliability, and availability [8]. The basic requirements of telemedicine models against different vulnerabilities are summarized in Table I.1.

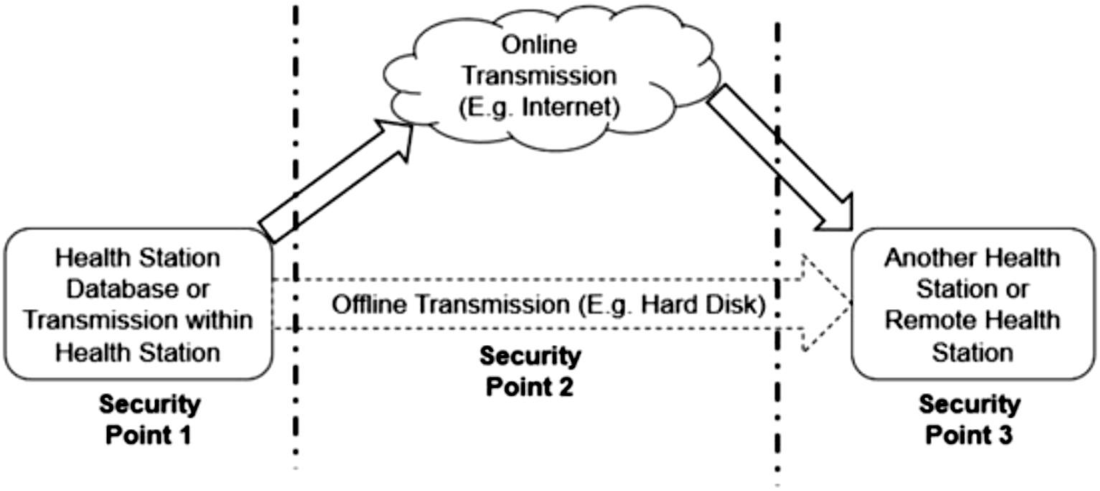

Online Transmission (E.g. Internet)
Health Station Database or Transmission within Health Station
Offline Transmission (E.g. Hard Disk)
Another Health Station or Remote Health Station
Security Point 1
Security Point 2
Security Point 3

Figure I.2 Standard telemedicine model

I.6.1. 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[9]:

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.6.2. 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[10]:

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.6.3. 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 [11].

I.7. Picture Archiving and Communication System (PACS)

Picture Archiving and Communication System (PACS) is a medical imaging technology that is used to store, retrieve, manage, and distribute medical images and associated patient data. PACS is used in various medical specialties including radiology, cardiology, dermatology, and dentistry.

PACS allows healthcare providers to view and share medical images electronically, eliminating the need for traditional film-based systems. PACS consists of four main components: image acquisition devices such as X-ray, CT, or MRI scanners, a secure network for image transmission, storage servers for storing the images, and workstations for image review and analysis.

PACS enables clinicians to access patient images and related data from any location, facilitating remote consultations and improving patient care. It also allows for faster and more accurate diagnosis and treatment planning, reduces costs associated with film-based systems, and increases workflow efficiency.

PACS can also integrate with other hospital information systems such as Electronic Health Records (EHRs) and Radiology Information Systems (RISs) to provide a comprehensive view of patient information. With the continued growth of medical imaging, PACS is becoming an essential tool for healthcare providers in improving patient care and outcomes. [12]

I.8. Digital Imaging and Communications in Medicine (DICOM)

Digital Imaging and Communications in Medicine (DICOM) is a standard for the exchange and management of medical images and related data. DICOM is widely used in medical imaging applications such as radiology, cardiology, pathology, and dentistry, among others. It was developed by the National Electrical Manufacturers Association (NEMA) and the American College of Radiology (ACR) to ensure interoperability and compatibility between different medical imaging equipment and systems.

DICOM allows medical images to be stored in a standardized format that can be easily exchanged and viewed by different medical imaging systems. It also provides a framework for storing and transmitting other patient-related information such as patient demographics, medical history, and examination protocols. DICOM is designed to be vendor-neutral, meaning it can be used with any medical imaging equipment from any manufacturer that supports the DICOM standard.

DICOM has several benefits, including improved interoperability and reduced data redundancy. It also enables remote access to medical images and data, facilitating collaboration among healthcare providers and improving patient care. Additionally, DICOM supports security and privacy features such as encryption and access control to protect patient data.

In summary, DICOM is a crucial standard for the efficient and effective management of medical images and data, promoting interoperability and collaboration among healthcare providers. [13]

I.9. DICOM security profiles

DICOM (Digital Imaging and Communications in Medicine) is a standard for storing and transmitting medical images and related data. DICOM security profiles are guidelines that outline the minimum security measures that should be implemented to protect patient data in DICOM systems[14].

There are several DICOM security profiles, including:

1) **Basic DICOM Security Profile:** This profile defines the basic security requirements for DICOM systems. It includes measures such as access control, authentication, encryption, and audit logging.
2) **DICOM Application Hosting Security Profile:** This profile defines the security requirements for hosting DICOM applications in a cloud environment. It includes measures such as secure data transfer, identity and access management, and secure storage.
3) **DICOM Network Connection Security Profile:** This profile defines the security requirements for DICOM network connections. It includes measures such as secure transmission protocols, encryption, and access control.

4) **DICOM Storage Security Profile:** This profile defines the security requirements for storing DICOM data. It includes measures such as access control, encryption, and backup and recovery procedures.
5) **DICOM Media Security Profile:** This profile defines the security requirements for physical media used to store DICOM data, such as CDs and DVDs. It includes measures such as encryption and secure disposal of media.

Implementing these DICOM security profiles can help ensure the confidentiality, integrity, and availability of patient data in DICOM systems. Healthcare organizations need to assess their own security needs and choose the appropriate security profiles to implement [14].

I.10. Medical image security applications

I.10.1. Techniques for Security of Medical Imaging

Recently, researchers have designed different types of security approaches for the protection of medical data based on computer security algorithms and network security algorithms [15]. These approaches like virtual private network (VPN), cryptographic-based techniques, and hashing-based techniques were used for the protection and authentication of medical data [16]. These existing techniques have various limitations such as the following: (1) these techniques only provide internal security or provide security within a network, (2) these techniques were less secure once a secret key is created by someone, and (3) these techniques don't recognize corruption in the medical data.

To overcome the limitation of these existing techniques, research on information hiding techniques for security and integrity verification of medical data has become a very hot research topic. Coatrieux and his team have given suggestions about the application of data-hiding techniques for the security and integrity verification of medical data. The basic comparison of data hiding technique with various existing techniques shows that data hiding technique provides a better security option for medical data in telemedicine applications [17].

I.10.2. Data Hiding Techniques for Security of Medical Imaging

Two types of data hiding techniques, steganography, and watermarking, are mainly used for the security of medical imaging [17]. These techniques insert some important information about the patient or user into the medical image to generate a secure medical image. Watermarking is mainly used for copyright protection and ownership authentication of multimedia data in various applications including telemedicine [18]. In general, watermarking has two stages: watermark embedding and watermark extraction [19]. The watermark information is inserted into the cover image using a watermark embedding procedure based on the watermarking key (which is optional in some cases), whereas a watermark extraction procedure is responsible for the extraction of watermark information from the watermarked image.

When any data hiding technique is designed for medical imaging, it must meet mainly two requirements: security or integrity (e.g., copyright protection and ownership authentication, etc.) and system requirements (e.g., size of memory, channel bandwidth, etc.) [16]. Some other requirements such as indexing of embedding keys and non-repudiation must be fulfilled by the data hiding technique when it is used as a security technique in telemedicine applications [20].

I.10.3. Watermarking applications in the medical image

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.

Overall, watermarking is a useful technique for identifying the owner or providing additional information in medical images, as well as preventing unauthorized use or distribution of these images. By using watermarking, medical professionals can ensure that their images remain secure and that patient care is optimized. [21]

I.10.4. Steganography security applications

Steganography is a technique that involves hiding a secret message within a digital medium, such as an image or audio file, in a way that is undetectable to the human eye or ear. Steganography can be used for a variety of security applications, including:

1) **Confidential Communication:** Steganography can be used to communicate sensitive information without detection. By hiding the message within a digital medium, the message can be sent without raising suspicion.
2) **Data protection:** Steganography can be used to protect data from unauthorized access. By hiding sensitive data within an image or audio file, it can be protected from being accessed by unauthorized individuals.
3) **Copyright protection:** Steganography can be used to protect copyrighted material, such as images or music, from being stolen or copied. By embedding a watermark or other hidden information, the owner of the material can prove ownership and deter unauthorized use.
4) **Covert operations:** Steganography can be used for covert operations, such as espionage or intelligence gathering. By hiding messages within seemingly innocuous digital media, covert agents can communicate without being detected.
5) **Digital forensics:** Steganography can be used in digital forensics to detect and recover hidden information in digital media. Forensic analysts can use steganalysis as a tool to detect the presence of hidden messages and recover the original data.

Overall, steganography is a powerful technique for securing digital communications and protecting sensitive data. While it is not foolproof, it can provide an additional layer of security and protection for individuals and organizations. [22]

I.10.5. Watermarking, Steganography and Cryptography

The watermarking concept is related to two fields: cryptography and steganography, and the three concepts are classified under the data security system field (Figure I.3). Cryptography is a method of sending an encrypted message that only authorized persons can decode, and when the message is decrypted it is not protected anymore and this is the main difference between cryptography and watermarking. Steganography is used to hide the existence of a message within another object (image, video, audio) known as data [23] To be undetectable, while the goal of watermarking is to embed a message in a way that it cannot be removed.

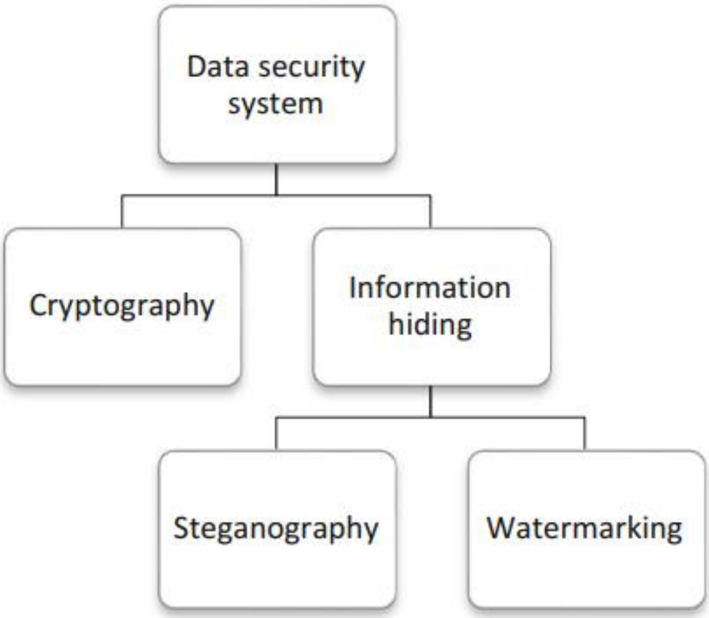


Figure I.3 Data security system field

I.11. CONCLUTION

Medical imaging plays a critical role in healthcare by enabling healthcare professionals to obtain valuable insights into the human anatomy without the need for invasive procedures. The continuous advancements in medical imaging technology have significantly enhanced the process of diagnosis, treatment, and surgical procedures through the utilization of high-resolution analysis and noise reduction techniques. To maintain the integrity and accuracy of medical images, it is essential to secure them against both intentional and unintentional distortions. Image security encompasses various interconnected aspects, including confidentiality, authenticity, and integrity. This literature review aims to explore two distinct approaches for achieving image security: watermarking and metadata (digital signature). Additionally, encryption techniques are also employed to further enhance the overall security of medical images.

Although encryption methods are offered by DICOM security profiles, they often lack sufficient measures to ensure data integrity, authenticity, and confidentiality comprehensively. Watermarking emerges as a viable solution for ensuring the security of medical images during storage and transmission, providing standardized guarantees. However, existing watermarking techniques often fall short in adequately addressing the requirements of robustness, imperceptibility, and capacity, particularly in real-time applications like telemedicine.

The primary objective of this study is to address these limitations and enhance the security of medical images during transmission and storage. This is achieved by proposing watermarking solutions that strike a better balance between the requirements of watermarking techniques and cryptographic methods, offering symmetric key security with reduced complexity. By adopting this approach, it is expected that medical image security can be significantly improved, thereby safeguarding the integrity, authenticity, and confidentiality of medical images in various healthcare applications.

II.1 Introduction

In recent years, digital document distribution over the open channel using information and communication technology (ICT) has proved an indispensable and cost-effective technique for the dissemination and distribution of digital media files. However, the prevention of copyright violation, ownership identification, and identity theft is still a challenging issue due to attempts of malicious attacks/hacking of open-channel information.

The prime motive behind this attack/hacking is to alter, modify, or even cross out the document watermark to illegally claim ownership or prevent the information transfer to intended recipients. Therefore, to address these critical challenges is an interesting problem for researchers in the field.

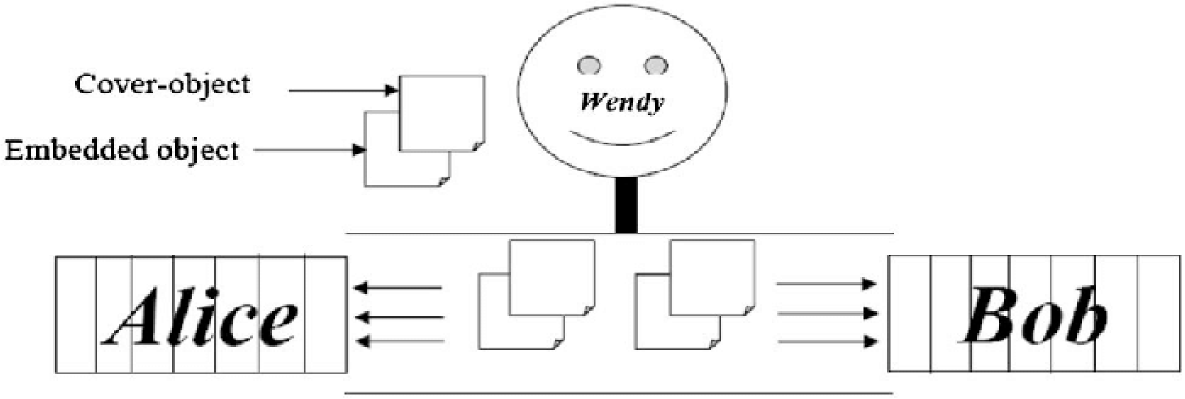


Figure II.1 The prisoner's problem [24]

data hiding is a technique to hide data in a cover message without creating any perceptual distortion of the cover for identification, annotation, and copyright. So you have to Must be respected, the constraints that affect the data hiding process [25] and are the quantity of data to be hidden, the need for invariance of these data under conditions where a cover (host) media is subjected to distortions like loss compression and the degree to which the data must be immune to interception, modification, or removal by a third party. Fundamentally, the data-hiding techniques can be classified into two categories: (1) digital watermarking and (2) steganography [26]. Digital watermarking is a process of embedding data (called a watermark) into digital multimedia cover objects in such a way that the watermark can be detected or extracted later to assert the authenticity and/or originality of the object [27]. The basic concept of digital watermarking is closely related to steganography (also known as covered writing) which emphasizes the bandwidth of the hidden message while concealing a message, image, or file within another message, image, or file, however, in the case of watermarking, the watermark robustness is the key performance parameter.

The watermarking technique has been in use for several centuries however the field of digital watermarking and its wide applications have exponentially grown over the last 30 years due to modern developments in multimedia data processing, advancements in digital signal processing, and availability of high-speed computational platforms. The watermarking is being potentially used for ownership assertion, fingerprinting, copy prevention/control, secure telemedicine, e-commerce, e-governance, media forensics, digital libraries, web publishing, media file archiving, artificial intelligence [30], and digital cinema [31] wherein a watermark can be embedded in every frame. Because of these interesting applications of watermarking, it has drawn focused attention in the present work and is thus discussed in detail.

II.2 Importance and Necessity of Watermarking

The significance and necessity of watermarking cannot be understated. While cryptography is commonly used to safeguard digital content, it lacks the ability for owners to monitor how the content is handled once decrypted. This limitation exposes the content to risks such as illegal copying, distribution, and misuse of private information. Cryptographic techniques protect during transmission, but once content is decrypted, it becomes vulnerable.

To overcome this major limitation, watermarking has emerged as a solution that ensures content protection even after decryption. Watermarking techniques involve embedding imperceptible information into the main content, which remains intact during normal usage and does not inconvenience users. These watermarks can withstand various processes, including decryption, re-encryption, compression, and geometrical manipulations [32].

In recent times, telemedicine applications have gained prominence in the medical field's technological advancements. The Digital Imaging and Communications in Medicine (DICOM) standard serves as a fundamental framework for communicating electronic patient record (EPR) data. Within DICOM, a header containing vital patient information is attached to the medical image file. Safeguarding this header during transmission and storage is a critical concern that can be effectively addressed through watermarking, ensuring security and authenticity [33].

II.3 Classifications of Digital Watermarks

The classification of watermarking techniques is illustrated in Figure II.2 . Watermarking methods can be categorized into four main types based on the data to be watermarked: text, image, audio, and video watermarking. However, this work primarily focuses on image watermarking due to its higher data embedding capacity. Based on human perception, watermarks can be further classified into visible, invisible-robust, invisible-fragile, and dual watermarks. A visible watermark is a translucent overlay that is noticeable upon careful inspection. An invisible-robust watermark is embedded in a way that changes to pixel values are imperceptible, and the watermark can only be recovered with the appropriate decoding mechanism. An invisible-fragile watermark is designed to be altered or destroyed if any manipulation or modification occurs on the cover. A dual watermark combines a visible and an invisible watermark, where the invisible watermark serves as a backup for the visible one [28].

Watermarks can also be applied in different domains, namely the spatial and transform domains, depending on the working domain. From an application perspective, watermarks can be source-based or destination-based. Source-based watermarking involves embedding a unique watermark in all copies of the distributed cover image, primarily for ownership identification or authentication. On the other hand, destination-based watermarking assigns a unique watermark to each distributed copy, enabling the identification of specific buyers and facilitating tracing in the case of illegal distribution or reselling. Additionally, watermarking techniques can be classified as reversible or irreversible [35]. Reversible watermarking techniques aim to avoid irreversible distortions in the host cover image and allow for the extraction of the watermark from the watermarked document. These techniques are particularly preferred in medical image watermarking to minimize the risk of incorrect diagnosis.

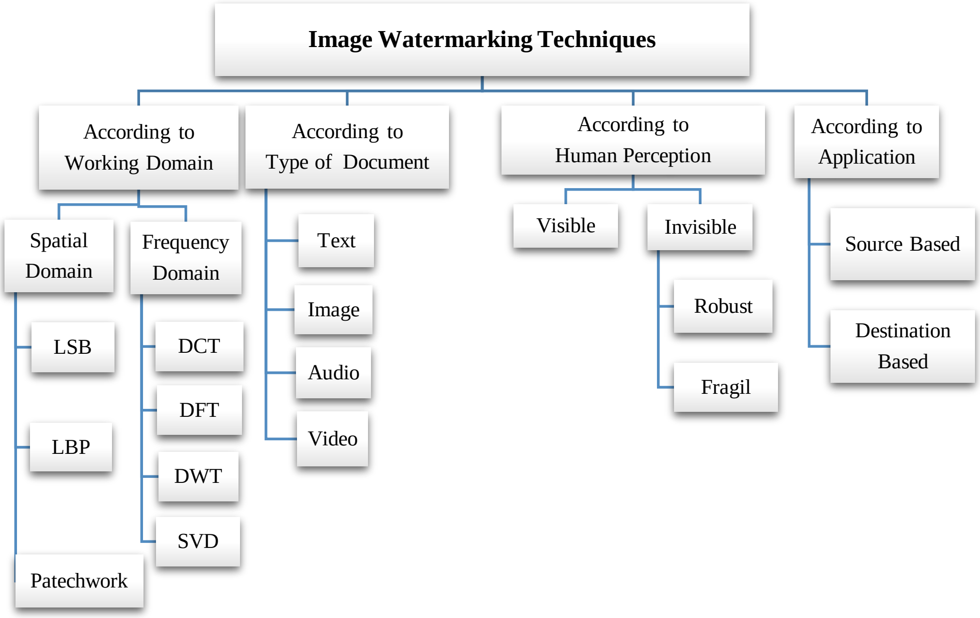


Figure II.2 Classification of watermarking techniques.

II.4 Potential Characteristics of Digital Watermarks

Digital watermarks possess several key characteristics [35, 36]:

1. Robustness: A digital watermark is considered robust if it can withstand a specified set of transformations, making it suitable for copyright protection. This criterion evaluates whether the watermark remains present after data distortion and if it can be detected by the watermark detector.

2. Imperceptibility: Imperceptibility measures the level of perceptual transparency of the watermark, indicating the similarity between the original and watermarked images.

3. Capacity: Capacity refers to the amount of information that can be embedded within a cover. The specific amount depends on the application, such as copyright protection, fingerprinting, authentication, or the confidentiality of medical data. The embedded information can be a logo image, a number, or other relevant data.

4. Security: The security of a watermark implies that it should be difficult to remove or alter without damaging the cover image. The level of watermark security required can vary based on the specific application.

5. Data payload: The data payload of a watermark refers to the amount of information it contains. For example, if a watermark contains 'n' bits, there are 2^(n+1) possibilities, including the possibility of no watermark being present. An effective watermark should accommodate all necessary data within any arbitrary and small portion of the cover.

6. Fragility: A fragile watermark aims at content authentication, serving as the reverse of the robustness criterion. Fragile watermarks are designed to withstand only acceptable modifications in the media content. This distinguishes them from digital signatures, which require a 100% match.

7. Computational cost: Computational cost refers to the expense of embedding the watermark into a cover and extracting it from the digital cover. In certain applications, the embedding process must be quick and straightforward, while extraction may be more time-consuming. In other applications, the speed of extraction is crucial.

8. Tamper resistance: Watermark tamper detection is utilized to verify the authenticity of digital photographs. These watermarks are sensitive to any changes in the watermark data. By examining the integrity of the watermark, the system can determine if the watermark has been modified or replaced at any point**.**

II.5 Framework for Watermarking

The watermarking framework typically involves two main processes: encoding and extraction [26]. This framework is illustrated in Figure II.3. In Figure II.3a, three inputs are required: a watermark, the original cover media, and an optional public or secret key for generating a watermarked image. Figure II.3 a 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 [37]. Thus, based on Figure II.3, 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):

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

The watermark embedding process is defined as:

Watermark Embedding $(E_W) = f(W_d, C_d, K)$

Further, the watermark extraction process is defined as:

Watermark Extraction $(W_E) = f(W\ or\ C_d, E_W, K)$

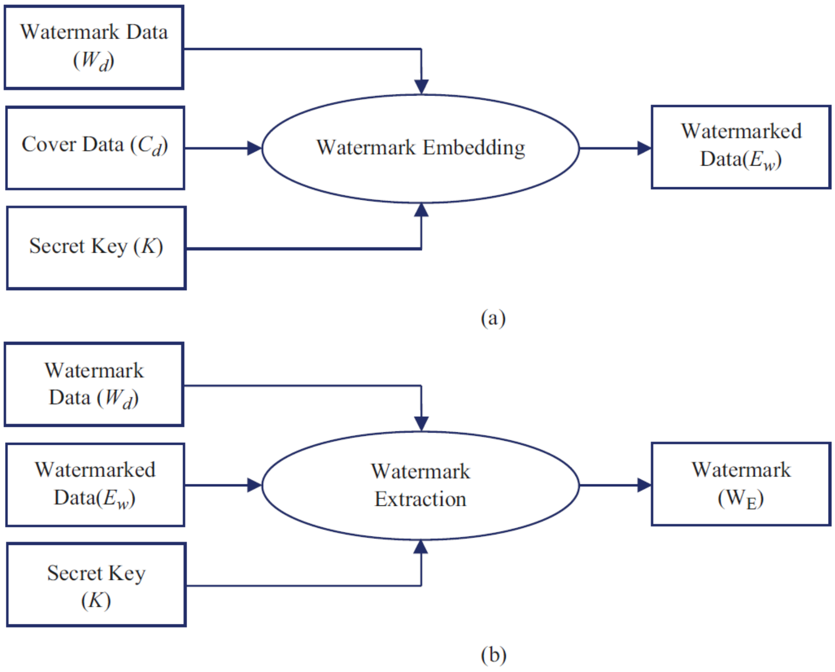


Figure II.3 The watermark process (**a**) embedding and (**b**) extraction [26].

II.6 Recent Applications of Digital Watermark

Digital watermarking has found various recent applications, as illustrated in Figure II.4. Some important and emerging applications include [29, 30, 36, 38]:

1. Fingerprinting: This application involves embedding identification information in watermarked content to trace the source of illegal distribution.

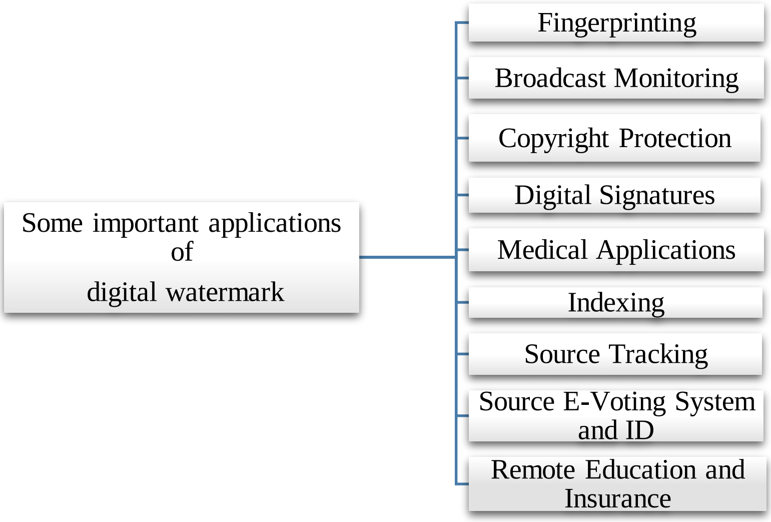


Figure II.4 Potential applications of watermarking

2. Broadcast monitoring: Content owners can utilize watermarking to automatically verify the broadcasting details of their content, such as location, time, and duration, on terrestrial, cable, or satellite television. Watermarking also plays a crucial role in protecting intellectual property in e-governance, e-commerce, copy control, media identification, and tracking.

3. Copyright protection: Digital watermarking is used to provide copyright protection to digital data by hiding secret information. Many content owners embed watermarks in images to communicate and safeguard image copyrights, ensuring compliance with guidelines and facilitating effective enforcement.

4. Digital signatures: 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 [39].

9. Remote education and insurance companies: Remote education and insurance companies are two additional areas where digital watermarking finds applications. In developing countries, distance education is becoming increasingly popular due to teacher shortages and other challenges in rural areas. However, the dissemination of valuable content and effective teacher-student interaction pose significant challenges in remote education. Secured data transmission is crucial in distance learning, and digital watermarking offers a potential solution to address these challenges. Furthermore, insurance companies, including health and vehicle insurers, are utilizing image processing applications. Health insurance companies store scanned copies of their client's medical data, which may require processing and transmission to central administrative offices. Similarly, car companies rely on image databases for insurance-related decision-making in cases of vehicle damage during accidents.

II.7 Essential Requirements for Medical Image

In recent times, medical images have become crucial in telemedicine, teleophthalmology, telediagnosis, and tele-consultancy services. They play a significant role in instant diagnosis, understanding critical diseases, and preventing misdiagnosis. However, the security of medical images is a major concern, particularly in the context of medical identity theft in telemedicine. The long-distance nature of such treatments amplifies the potential for anonymity and security breaches.

When medical images are transmitted over unsecured networks, they are vulnerable to various threats, including data corruption during transmission and attacks by hackers seeking to obtain sensitive patient information. These attacks can involve manipulating patient information in the image header, tampering with the image pixel content, and accessing confidential patient data. Medical identity theft, in particular, is a growing and dangerous crime that can have severe consequences. Secure medical data/image watermarking schemes are necessary to address these challenges effectively.

Medical image watermarking offers several advantages, as depicted in Figure II.5, including:

1. Reduced storage space requirements: By embedding the patient record within the image itself, the need for separate storage space for the image and patient record is eliminated.

2. Decreased bandwidth requirements: Additional metadata transmission bandwidth can be avoided by hiding the data within the image itself during transmission.

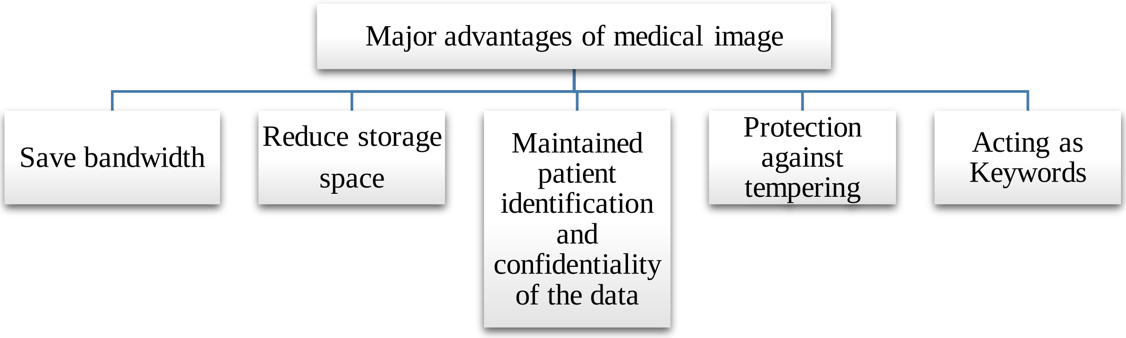

Major advantages of medical image
Save bandwidth
Reduce storage space
Maintained patient identification and confidentiality of the data
Protection against tempering
Acting as Keywords

Figure II.5 Main advantages of medical image watermarking

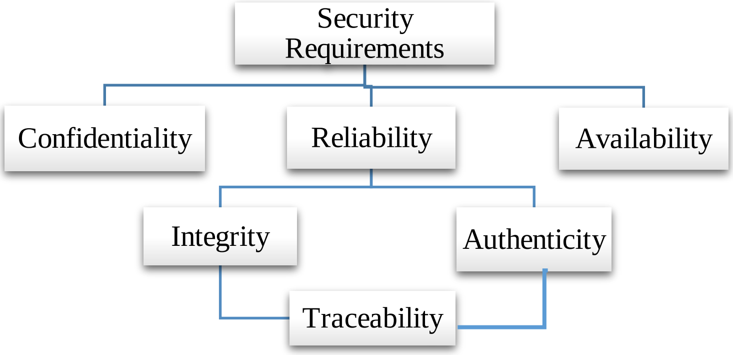


Figure II.6 Major security requirements for EPR data [41]

3. Ownership identification and confidentiality: Patient data is hidden within the cover image, ensuring ownership identification and maintaining the confidentiality of patient information.

4. Protection against tampering: Tampering with medical data can have life-threatening consequences due to incorrect diagnosis. Watermarking protects against tampering, ensuring data integrity.

5. Efficient archiving and data retrieval: Hidden watermarks can serve as keywords for efficient archiving and data retrieval mechanisms, facilitating medical data management and distribution.

However, embedding additional data within medical images requires careful consideration to avoid compromising image quality. The exchange of electronic patient record (EPR) data through unsecured channels necessitates a high level of security. Figure II.6 illustrates three essential security requirements for EPR data exchange [41]:

1. Confidentiality: Only authorized users should have access to the information, to ensure its confidentiality.

2. Reliability: This encompasses information integrity (preventing unauthorized modifications) and authentication (verifying the source). Traceability is also important in ensuring reliability and tracking information distribution.

3. Availability: The information system should be accessible and usable by entitled users under normal scheduled conditions.

Authentication, integrity, and confidentiality are critical concerns in EPR data exchange through unsecured channels [40, 41], and suitable watermarks can fulfill these requirements effectively.

II.8 Domains of image watermarking

Watermarking using the spread spectrum:

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:

1. 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.

2. 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 [42].

II.8.1 Spatial Domain Techniques

Spatial domain techniques [44] involve directly modifying the pixel values of the cover media to embed the data. The simplest approach in spatial domain techniques is to add a pseudo-random noise pattern to the luminance values of an image [45]. These techniques do not involve transferring the protected images to the transform domain, resulting in reduced computation time for watermark embedding and extraction processes. However, spatial domain techniques are less resilient against signal processing attacks. The following important spatial domain techniques are described below.

II.8.1.1 Least Substitution Bit (LSB)

Least significant bit modification is the most commonly used algorithm for spatial domain watermarking. Here, the least significant bit (LSB) of randomly chosen pixels can be altered to hide the most significant bit (MSB) of another. It generates a random signal by using a specific key. The watermark is inserted into the least significant bits of the host image and can be extracted in the same way. Several techniques may process the host image. This type of algorithm is easy to implement and is simple. The least significant bits carry less relevant information and, thus, the quality of the host image is not affected. It provides high perceptual transparency with a negligible impact on the host image. However, this algorithm can be affected by undesirable noise, cropping, lossy compression, and so on, and may be attacked by a hacker by setting all the LSB bits to “1,” modifying the embedded watermark easily without any difficulty. The LSB technique can easily be understood by the example depicted in Figure II.**7**. Suppose two pixel values in the host image are 130 (10,000,010) and 150 (10,010,110). Then, using the LSB technique, if the embedded watermark is 10, then the watermarked pixel values will be 131 (10,000,011) and 150 (10,010,110), respectively .

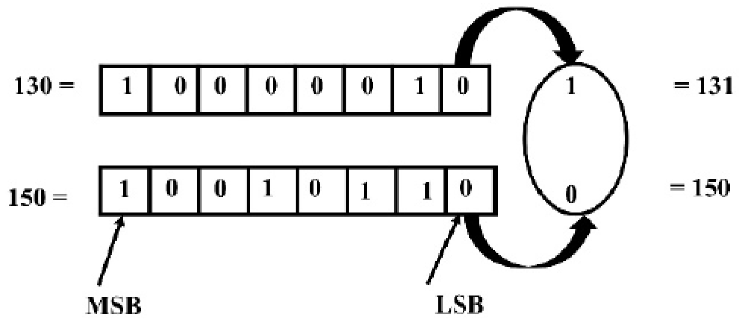


Figure II.7 Basic least significant bit (LSB) technique example .

Several researchers have studied modifications of the LSB technique, which are commonly related to the spatial domain. LSB techniques have been developed based on a bit-plane of digital discrete signals (e.g., audio or images). A bit-plane that represents the signal is a set of bits having the same bit position in each of the binary numbers. Most techniques use only one bit-plane for embedding. This technique works on the least significant bit (i.e., the eighth bit-planes), but others have used three bit-planes (i.e., the sixth–eighth bit-planes) or even four bit-planes (i.e., the fifth–eighth bit-planes) for embedding with acceptable image quality. The four least significant bits (i.e., the fifth–eighth bits of the cover image) can be replaced with the chosen bit of the secret image by simply using an OR operation in a specific manner [43]. This method first converts the host image into a stream of binary bits, outputs zero in the embedded bit, and then shifts the secret image to the right by 4 bits. Then, an OR operation is performed on these two (i.e., the host and secret images) to obtain the combined image. This operation is illustrated in Figure II.8 .

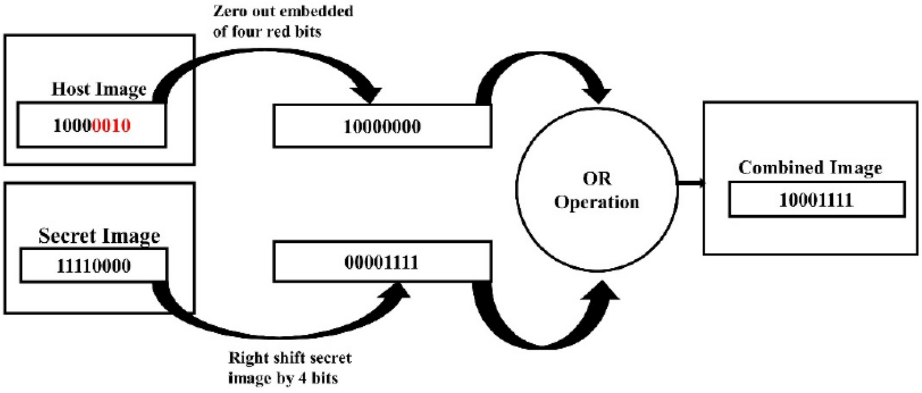


Figure II.8 Block diagram of the LSB method (four bit-planes).

II.8.1.2 Patchwork Technique

Initially, the patchwork technique was proposed by Bender et al. [46] in 1995. This technique is a statistical process based on a pseudorandom in which patchwork imperceptibly embeds in a cover image a specific statistic, one that has a Gaussian distribution [47]. In the embedding process of the patchwork technique, the owner chooses *n*-pixel pairs pseudo-randomly according to a secret key and modifies the luminance values of the *n*-pairs of pixels. If the luminance values are x_i and y_i, the modified luminance values are determined by adding '1' to all values of x_i and subtract'*1'* to all values of y_i i. e. $\overline{x_\iota} = x_i + 1$ and $\overline{y_\iota} = y_i - 1$. The same secret key will be used in the extraction process of the technique (which is based on statistical assumption) and determine the sum $(S) = \sum_n^{i=1} \overline{x_\iota} - \overline{y_\iota}$. If the sum (S) = 2n ; the cover image contained the watermark, otherwise it should be near/approximately zero. In [47, 48], the robustness performance of the patchwork technique is improved in that the cover image hides a watermark longer than one bit.

II.8.2 Transform Domain Techniques

The spatial domain techniques are easy ways to embed secret information, but these techniques are highly vulnerable to even small cover modifications [49]. Anyone can simply apply signal processing techniques to destroy entire secret information.

In many cases, even small changes resulting from loss compression systems lead to total information loss. However, the embedding of information in the transform domain provides greater robustness to watermarked data. The transform domain techniques hide secret information in significant areas of the cover image which makes them highly robust to signal processing attacks than the spatial domain techniques. The important transform domain techniques are presented in the next sub-sections.

II.8.2.1 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 ($\|\psi\| = 1$) [49]. A family of wavelets can be obtained by scaling ψ by s and translating it by u.

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

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:

$$f(u,s) = \int_{\infty}^{-\infty}(t)\, s^{-1/2}\psi'\left(\frac{t-u}{s}\right) \qquad \text{(II.3)}$$

where $\psi'(.)$ is the complex conjugate of $\psi(.)$. Equation (II.3) 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 DWT provides sufficient information both for analysis and synthesis of the original signal with a significant reduction in the computation time. In addition, DWT is considerably easier to implement in comparison to the continuous wavelet transform (CWT). DWT is one of the well-known techniques for sub-band image coding which has considerable attention in various signal processing applications, including image watermarking. 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 [50]. It has the advantages such as the similarity of the data structure concerning the resolution and available decomposition at any level [51].

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

$$S_{x,y} = \int_{\infty}^{-\infty} \psi'_{x,y}(t)\, S(t)\, dt \qquad \text{(II.4)}$$

The inverse of the DWT is defined as:

$$S(t) = C_{\psi} \sum_{x} \sum_{y} S_{x,y}\, \psi_{x,y}(t) \qquad \text{(II.5)}$$

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

DWT separates an image into a set of four non-overlapping multi-resolution sub-bands denoted as lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH), and diagonal (HH) detail components [52]. The process can then be repeated to compute multiple-scale wavelet decomposition. Since the human eyes are much more sensitive to the low-frequency part (LL sub-band), the watermark can be embedded into the other three sub-bands (HL, LH, and HH sub-band) to maintain better image quality. shows the pyramid structure of three levels DWT sub-band. The energy of an image is concentrated in the high decomposition levels corresponding to the perceptually significant low-frequency coefficients. 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 [53]. Figure II.9 shows the Decomposition of CT test image using DWT . The main advantages of wavelet transform domain for watermarking applications are [54–55]:

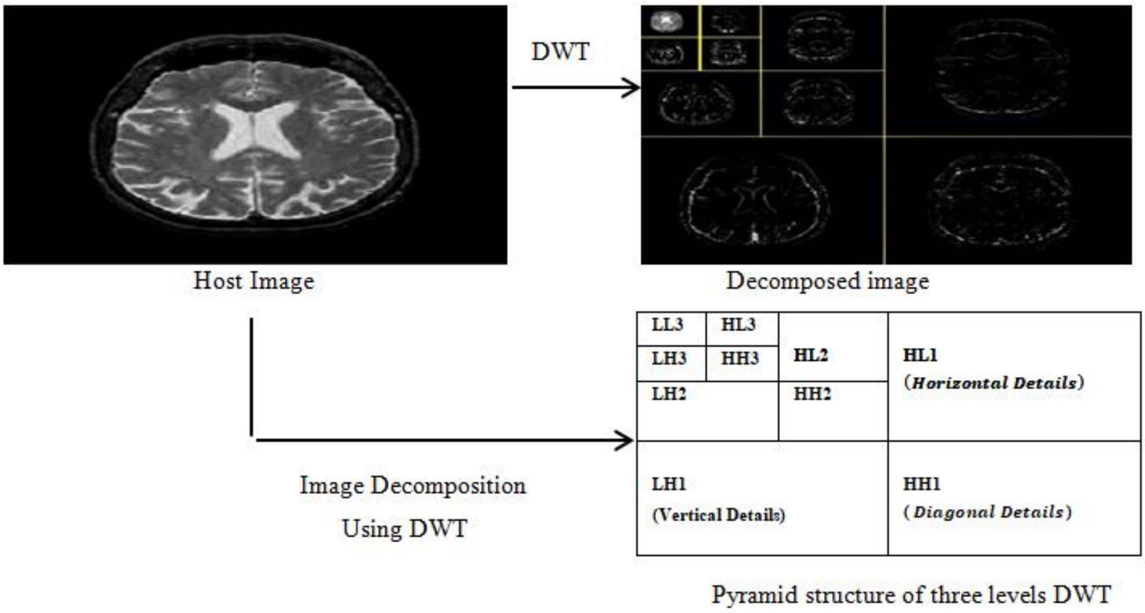


Figure II.9 Decomposition of CT test image using DWT .

1. Space frequency localization: Used for the analysis of edges and textured areas as it provides good space-frequency localization.

2. Multi-resolution representation: The multi-resolution property of the wavelet transform can be used to exploit the fact that the response of the human eye is different to high and low-frequency components of an image.

3. Multi-scale analysis: Wavelets have non-uniform frequency spectra which facilitate multi-scale analysis.

4. Adaptability: Flexible and easily adaptable to a given set of images or applications.

5. Linear complexity: Linear computational complexity of O(n) is present for the wavelet transform .

6. DWT can be applied to the entire image without imposing block structure as used by DCT, thereby reducing blocking artefact.

There are a wide variety of popular wavelet algorithms, including Daubechies wavelets, Mexican Hat wavelets, and Morlet wavelets [56]. These wavelet algorithms have the advantage of better resolution for smoothly changing time series. However, they have the disadvantage of being more computationally complex than the Haar wavelets. In addition, the Haar wavelet transform is fast, memory efficient and exactly reversible without the edge effects that are present in other wavelet transforms.

As discussed above, the DWT offers various important properties for medical image watermarking. However, it suffers from poor directional information. Do and Vetterli [57] proposed a directional transform called contour let transform, which has the properties of multi-resolution, localization, critical sampling, rich directionality using a directional filter bank, and anisotropy. The contour let transform can be seen as a discrete form of a particular curve let transform, which is also a popular multi-scale directional transform [58]. However, the curve lets transform has better directional geometry/features than contour let.

II.8.2.2 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 [59]. 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 an orthogonal square matrix V. Let A be a square matrix of order n. then according to SVD it can be represented mathematically as:

$$A = U\,S\,V^T \qquad \text{(II.6)}$$

With : $U \times U^T = I$ and $V \times V^T = I.$

Where, I represents 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.8.3 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.9. Performance Measures:

The performance of a medical image watermarking algorithm is mainly evaluated based on its imperceptibility and robustness.

II.9.1 Mean Square Error (MSE)

The MSE contains the cumulative squared error between the original and watermarked image [60]. 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 in the equation (II.7):

$$MSE = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{i=1}^{Y} \left(I_{ij} - W_{ij}\right)^2 \qquad \text{(II.7)}$$

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.9.2 Peak Signal-to-Noise Ratio (PSNR)

The imperceptibility is measured by the parameter Peak Signal to Noise Ratio (PSNR). A larger PSNR indicates that the watermarked image more closely resembles the original image which conveys the meaning that the watermark is more imperceptible. In general, the watermarked image with a PSNR value greater than 28 dB is acceptable [61]. The PSNR is defined as in the equation (II.8):

$$PSNR = 10log\frac{(MAX)^2}{MSE} \qquad \text{(II.8)}$$

MAX : the maximum value between the maximum value of the original image and the maximum value of the watermarked image arrays. In other words, it is the larger of the two maximum values.

II.9.3 Universal Image Quality Index

Wang and Bovik [62] 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, $X = \{x_i, i = 1,2,3, \ldots \ldots, N\}$ and $Y = \{y_i, i = 1,2,3, \ldots \ldots, N\}$. The universal image quality Index is defined in the equation (II.9): $Q = \frac{4\sigma_{xy}\overline{xy}}{(\sigma_x^2+\sigma_y^2)(\bar{x}^2+\bar{y}^2)}$ (II.9)

Where: $\bar{x} = \frac{1}{N}\sum_N^{i=1} x_i$, $\bar{y} = \frac{1}{N}\sum_N^{i=1} y_i$, $\sigma_x^2 = \frac{1}{N-1}\sum_N^{i=1}(x_i - \bar{x})^2$, $\sigma_y^2 = \frac{1}{N-1}\sum_N^{i=1}(y_i - \bar{y})^2$, $and\ \sigma_{xy} = \frac{1}{N-1}\sum_N^{i=1}(x_i - \bar{x})(y_i - \bar{y})$.

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

$$\boldsymbol{Q} = \left\{\begin{matrix} loss\ of\ correlation\left(\frac{\sigma_{xy}}{\sigma_x\sigma_y}\right).luminance\ distortion\left(\frac{2\overline{xy}}{(\bar{x})^2+(\bar{y})^2}\right). \\ contrast\ distortion\left(\frac{2\sigma_x\sigma_y}{\sigma_x^2+\sigma_y^2}\right) \end{matrix}\right\} \qquad \text{(II.10)}$$

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.9.4 Structural Similarity Index Measure (SSIM)

The SSIM [61], as shown by the equation (II.11) :

$$SSIM(x,y) = f\big(l(x,y), c(x,y), s(x,y)\big) \qquad \text{(II.11)}$$

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.9.5 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. However, ideally it should be 1 but the value 0.7 is acceptable [63].and the equation Normalized Correlation (NC) (II.12):

$$NC = \frac{\sum_X^{i=1}\sum_Y^{j=1}\left(W_{original_{ij}} \times W_{recovered_{ij}}\right)}{\sum_X^{i=1}\sum_Y^{j=1} W^2{}_{original_{ij}}} \qquad \text{(II.12)}$$

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.9.6 Bit Error Rate (BER)

The BER is defined as the ratio of the number of incorrectly decoded bits and the total number of bits [63]. Ideally, the BER value should be equal to 0. and the equation Bit Error Rate (BER) (II.13):

$$BER = (Number\ of\ incorrectly\ decoded\ bits)/(Total\ number\ of\ bits) \qquad \text{(II.13)}$$

II.10. Digital Watermarking Attacks and Benchmark Tools

In recent years, digital image watermarking has become the most widely used technique for copyright protection, ownership identification, and prevention of identity theft. However, ensuring the robustness and security of watermarks in medical applications has been a challenging issue due to potential malicious attacks and hacking attempts targeting open-channel information [64]. These attacks aim to alter, modify, or even remove the document watermark from its cover data, either to illegally claim ownership or to prevent information transfer to intended recipients.

II.10.1 Watermarking Attacks

Various types of malicious attacks can result in the partial or total destruction of the embedded identification key, requiring more advanced watermarking schemes [61, 64]. Figure II.10 illustrates possible attacks on watermarking systems. The important attacks are discussed below:

1. Active/Removal Attacks: In this type of attack, the hacker intentionally tries to remove or make the watermark undetectable. These attacks aim to distort the hidden watermark to a point where it becomes unrecognizable. Active attacks include de-noising, loss compression, quantization, re-modulation, collusion, and averaging attacks. Copyright protection, fingerprinting, and copy control are often affected by these attacks.

2. Passive Attacks: In passive attacks, the hacker attempts to determine the presence of a watermark and identify its characteristics without causing damage or removal. Protection against passive attacks is crucial in covert communications where revealing the presence of a watermark can compromise the intended secrecy.

3. Forgery/Cryptography Attacks: This type of attack involves the hacker embedding a new, valid watermark instead of removing an existing one. This allows the hacker to manipulate the protected data as desired and replace the destroyed watermark with a new key, making the manipulated image appear genuine. Brute force attacks used in cryptography, aiming to discover hidden information through exhaustive searches, are similar techniques in this category. To protect against these attacks, it is essential to use a secure and sufficiently long key [64]. The Oracle attack falls under the same category as cryptographic attacks, where a non-watermarked image is created when a watermark detector device is available.

4. Collusion Attacks: In collusion attacks, the hacker's intention is similar to active attacks, but the approach is slightly different. The attacker utilizes multiple instances of the same data, each containing a different watermark, to construct a new copy without any watermark. This poses a problem in fingerprinting applications but is less common due to the challenge of accessing multiple copies of the same data. Collusion attacks are concerning because if the attacker has access to more than one copy of the watermarked image, they can predict or remove the watermarked data by colluding with the given key, making the manipulated image appear genuine.

5. Geometrical Attacks: Geometrical attacks aim to alter or distort the hidden watermark through spatial or temporal alterations of the stego data. Such active attacks cause the watermark detector to lose synchronization with the hidden watermark. Unzign and StirMark are popular integrated software tools used for geometrical attacks.

6. Protocol Attacks: These types of passive attacks target the concept of the watermarking application rather than destroying or disabling the detection of the hidden watermark through local or global data manipulation. The concept of first protocol attacks was introduced. Copy attacks are another group of protocol attacks, where a watermark is copied from one image to another without knowledge of the key used for watermark embedding, creating ambiguity regarding the true ownership of the data.

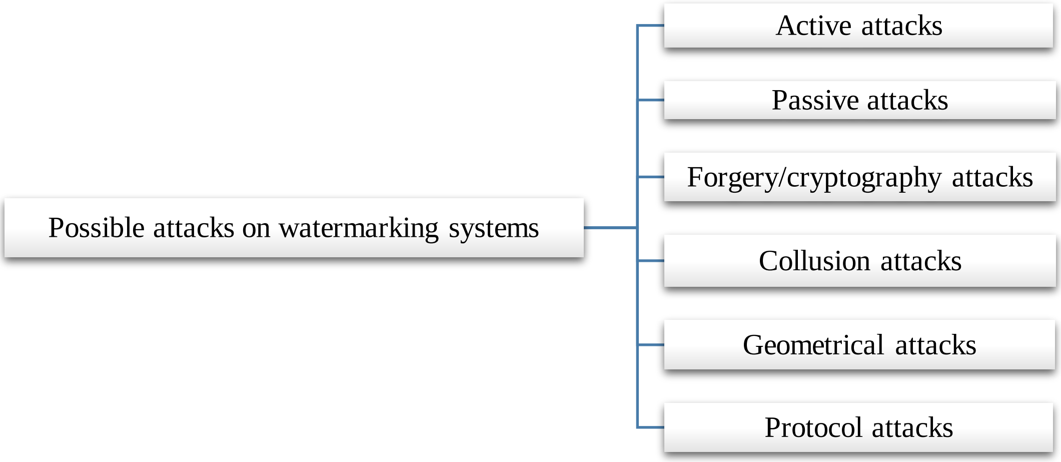


Figure II.10 Classification of possible attacks in digital watermarking

II.10.2 Benchmark Tools for Image

The benchmarking of digital watermarking algorithms involves evaluating and comparing their performance in a fair and typically automated environment [66]. Several important benchmarking tools are available for watermarking, including StirMark, CheckMark, Optimark, and Certimark. StirMark is a widely used and excellent software tool for assessing the robustness of different watermarking systems. It simulates various common attacks on image watermarking algorithms, exposing vulnerabilities and insecurity [66]. However, it has limitations as it does not accurately model the watermarking process and focuses heavily on geometric transformations without considering prior knowledge about the watermark [65]. To address these limitations, the CheckMark tool was developed as an improved version of StirMark by Pereira et al. [67]. CheckMark introduces new attacks such as Wiener filtering, soft shrinkage, hard thresholding, Copy, Template removal, and JPEG 2000. It also includes weighted PSNR and Watson's metric for assessing visual image quality. Unlike StirMark, CheckMark is implemented in MATLAB [66].

Another significant benchmarking tool is Optimark, which provides a graphical user interface (GUI) implemented in C/C++. It allows users to select test images, define different watermark embedding keys and messages, and evaluate the watermarking algorithm's performance through multiple trials with various attacks and statistical characteristics assessment [68].

The Certimark benchmark tool, developed by an EU-funded research project, aims to establish a benchmarking collection module for users to assess suitability and define application scenarios. It also establishes a standard certification process for watermarking technologies [69]. However, the source codes for this tool are not publicly available [66].

In addition to these tools, some researchers have proposed benchmark tools based on web systems, mesh benchmarking[70], and OR-benchmark tools for evaluating watermarking algorithm performance [66]. A detailed comparison of these benchmarking tools can be found in [66].

II.11. CONCLUSION

This chapter covers some basic spatial domain and transformation techniques. Then the key performance parameters for watermarked digital and medical imaging. It includes peak signal-to-noise ratio (PNSR), Universal Image Quality Index, Structure Similarity Index (SSIM) measurement, Normalized Correlation (NC), and Bit Error Rate (BER). In addition, a brief overview of different attack types and key benchmarking tools and their performance comparison for the digital image watermark was also provided. It is noted that the attack types have a crucial impact on the performance of efficient and robust watermarking algorithms. In addition, improvements to efficient benchmarking tools are needed to enable full functionality shortly. However, the available benchmarking tools are not enough.

III.1 Introduction

Watermarks can be applied to images in both the spatial and transform domains, depending on the characteristics of the image. Transform domain techniques involve embedding data by manipulating the coefficients of various transforms, such as the discrete wavelet transform (DWT), discrete cosine transform (DCT), singular value decomposition (SVD), and discrete Fourier transform (DFT). Although transform domain watermarking techniques can be computationally complex, they provide improved resilience for the watermarked data. In this section, we propose an approach for watermarking medical images. The method utilizes a two-level DWT transform domain sub-band, on which SVD decomposition is performed using spread spectrum techniques with a text watermark image. We present simulation and experimental results to assess the effectiveness of our proposed method.

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

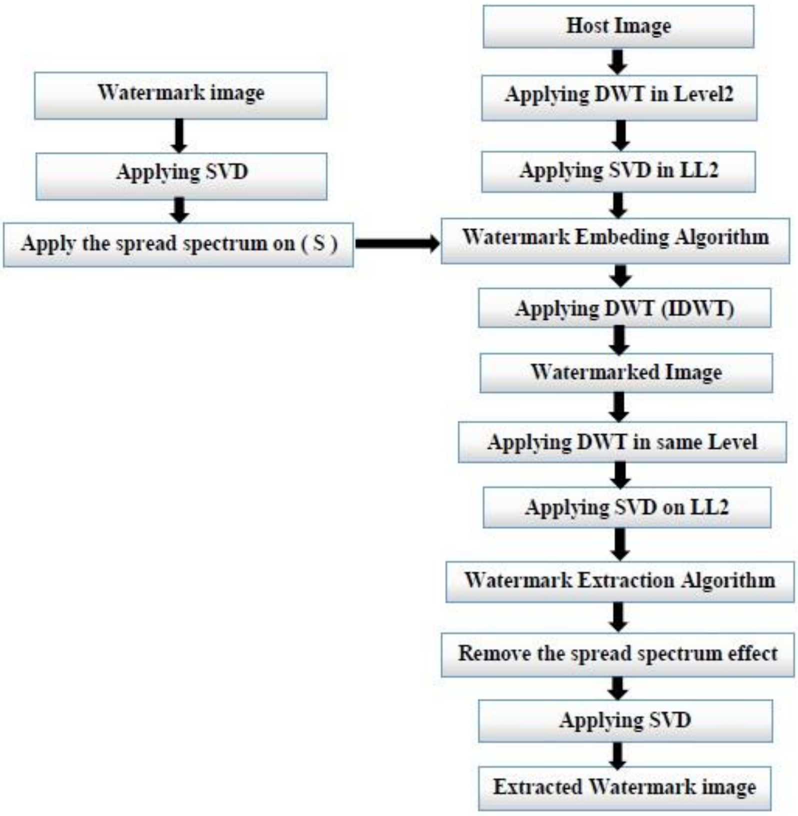

Watermark image
Applying SVD
Apply the spread spectrum on (S)
Host Image
Applying DWT in Level2
Applying SVD in LL2
Watermark Embeding Algorithm
Applying DWT (IDWT)
Watermarked Image
Applying DWT in same Level
Applying SVD on LL2
Watermark Extraction Algorithm
Remove the spread spectrum effect
Applying SVD
Extracted Watermark image

Figure III.1 Watermark Embedding and Extraction Algorithm.

III.2.1 Watermark Embedding Algorithm

In this algorithm, the considered cover image is transformed by two levels DWT where the low frequency sub-band is decomposed by SVD. The watermark image is also transformed by DWT and SVD. The singular value of watermark information is spreaded with spread facture and embedded in the singular value of the cover image by scale factor alpha. The embedding algorithm details for medical image watermark is formulated as follows:

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('MR-03.jpg');**

host_image= imresize(host_image,[1024 1024]);

STEP 3: Applying DWT

Applying First level DWT coefficients for cover image:

[LL1,HL1,LH1,HH1]= dwt2(host_image,'haar');

Applying Second level DWT coefficients for cover image:

[LL2, HL2, LH2, HH2] = dwt2(LL1,'haar');

STEP 4: Choice of sub-bands in Cover and apply SVD on the selected sub-bands

Applying SVD on LL2: **[Uy,Sy,Vy] = svd(LL2); q=size(Sy);**

STEP5: Define text watermark image:

Define a text watermark and convert it to an image using the `insertText` function:

```
text1 = 'AZZOUZI KAIROUANI';

text2 = 'CDM EL MANAR';

text3 = 'DD/MM/YYYY';

textWatermark = sprintf('%s\n', text1, text2,text3);

textImage = insertText(uint8(zeros(size(host_image))), [1 1], textWatermark, 'FontSize', 72, 'BoxColor', 'black', 'BoxOpacity', 0.25, 'TextColor', 'white');
```

Resizing watermark image: **textImage = textImage(:, :, 1);**

```
watermark_image= imresize(textImage, p);
```

Applying SVD on watermark image:

```
[Uw,Sw,Vw]= svd(double(watermark_image));
```

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: **LL2_1= Uy*smark*Vy';**

Applying the invers DWT to get watermarked image:

```
LL1_1 = idwt2(LL2_1, HL2, LH2, HH2, 'haar');

watermarked_image = idwt2(LL1_1, HL1, LH1, HH1, 'haar');
```

III.2.2 Watermark Extraction Algorithm

The extraction algorithm of the image watermark is just reverse process of the embedding algorithm. The details of the extraction algorithm for the image watermark is presented as follows:

STEP 1: Perform two levels of DWT on Watermarked image (possibly distorted)

```
[LL1_wmv,HL1_wmv,LH1_wmv,HH1_wmv] = dwt2(watermarked_image,'haar');
```

```
[LL2_wmv,HL2_wmv,LH2_wmv,HH2_wmv] = dwt2(LL1_wmv, 'haar');
```

STEP 2: Applying SVD on the selected sub-bands

```
[Uy_wmv, Sy_wmv, Vy_wmv] = svd(LL2_wmv);
```

Extract the spreaded watermark: **extractedspreadedSw = (Sy_wmv - Sy) / alpha;**

Remove the spread spectrum effect:

```
extractedSw = extractedspreadedSw - spreadFactor * pns ;
```

```
Extracted_watermark = Uw * extractedSw * Vw';
```

III.2.3 Simulation of Watermarking Algorithms

The performance of the proposed watermarking technique is based on DWT, SVD and spread spectrum. In the proposed method the cover medical image (MRI image) is of size 256 × 256. Figure III.2 shows the different type of medical images used as cover image.

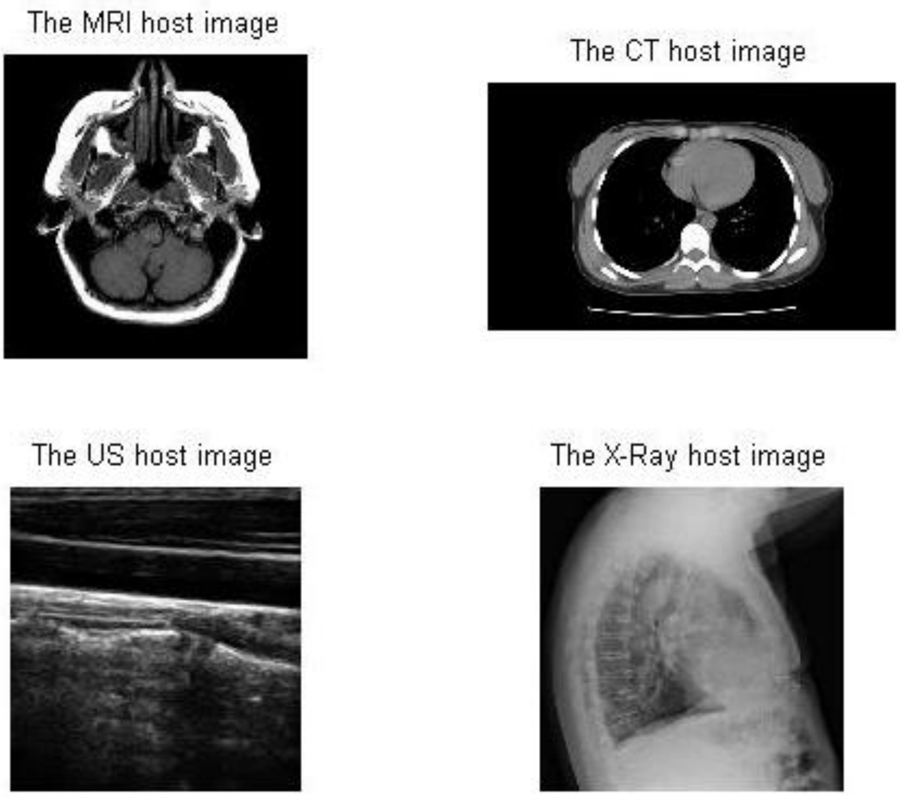


Figure III.2 the different type of medical images used as cover image.

The robustness of the image watermark is evaluated by determining NC. The quality of impressibility of the watermarked image is evaluated by PSNR and SSIM. It is quite apparent that size of the watermark affects quality of the watermarked image. However, degradation in quality of the watermarked image will not be observable if the size of watermark is small. Figure III.3 shows the cover and original watermark image respectively. Figure III.4 shows the watermarked and extracted watermark image respectively. Table III.1 shows the PSNR, SSIM and NC performance of the proposed method at different scale factor. It is found that smaller scale factor provides better PSNR values between original and watermarked medical images.

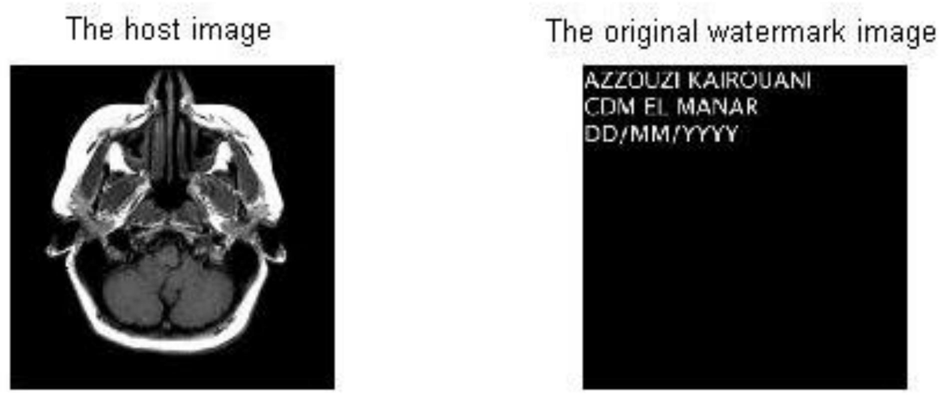


Figure III.3 the cover and original watermark image.

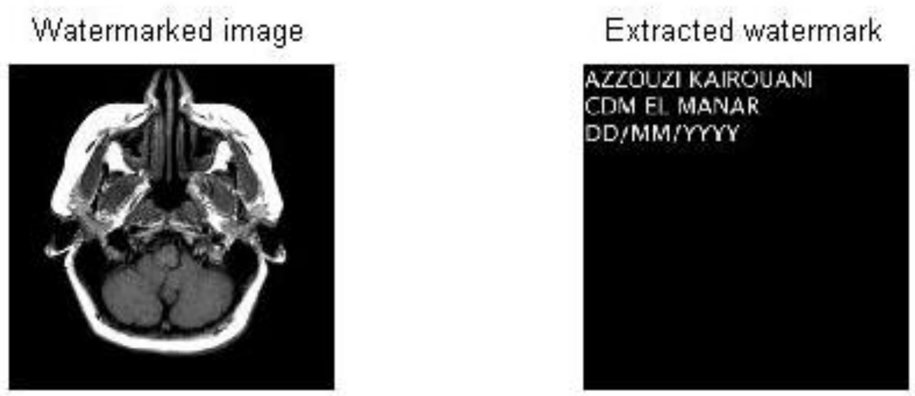


Figure III.4 the watermarked and extracted watermark image.

Table III.1 the PSNR, SSIM and NC performance at different scale factor.

Type of cover image	Scale Factor	PSNR	SSIM	NC
X-ray	0.01	95.682	1	1
	0.03	61.6898	0.99984	0.99954
	0.05	50.8494	0.9994	1
	0.1	47.0976	0.99806	1
	1	27.5548	0.94885	0.99988
CT	0.01	91.3471	1	0.99947
	0.03	58.8539	0.99991	0.99942
	0.05	55.2239	0.99993	0.99954
	0.1	50.2453	0.99973	0.99947
	1	30.9057	0.9879	0.99957
Ultrasound	0.01	81.5699	1	1
	0.03	58.8823	0.99996	1
	0.05	54.4878	0.99987	1
	0.1	48.6156	0.99931	1
	1	29.4	0.97164	0.99991
MRI	0.01	95.8343	1	0.99973
	0.03	59.63	0.99984	0.99954
	0.05	56.7112	0.99977	0.99968
	0.1	50.924	0.99916	0.99966
	1	32.8245	0.98042	0.99962

Table III.2 PSNR, and Visual quality of the watermarked image at different scale factor.

Scale Factor	PSNR	Quality of watermarked image
0.01	95.8343	Very good imperceptibility
0.03	59.63	Good imperceptibility
0.05	56.7112	Bad imperceptibility
0.1	50.924	Very bad imperceptibility
1	32.8245	Worst imperceptibility

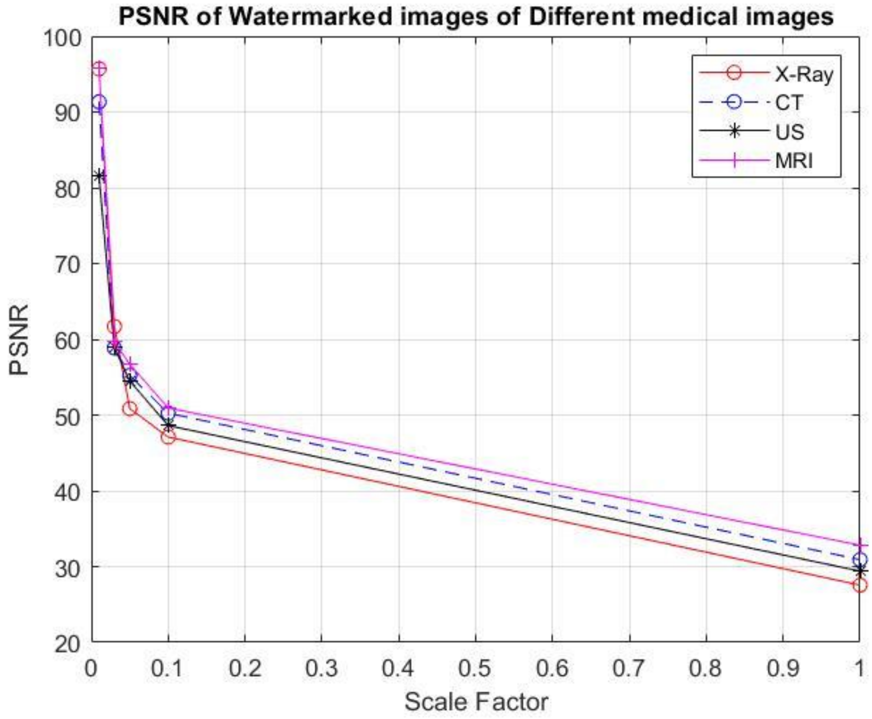


Figure III.5 the PSNR performance at different scale factor.

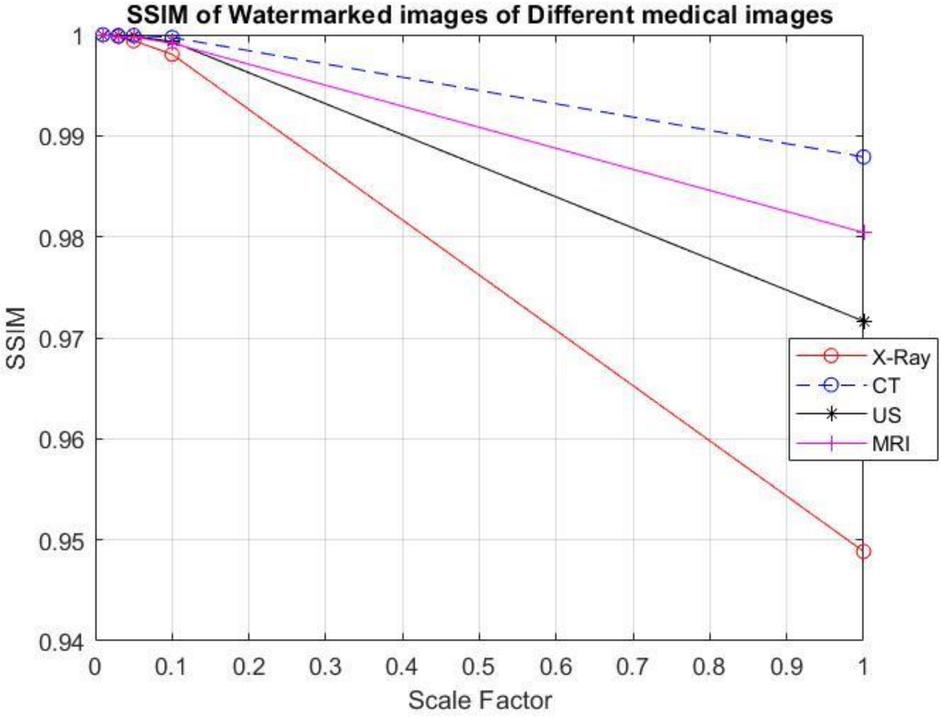


Figure III.6 the SSIM performance at different scale factor.

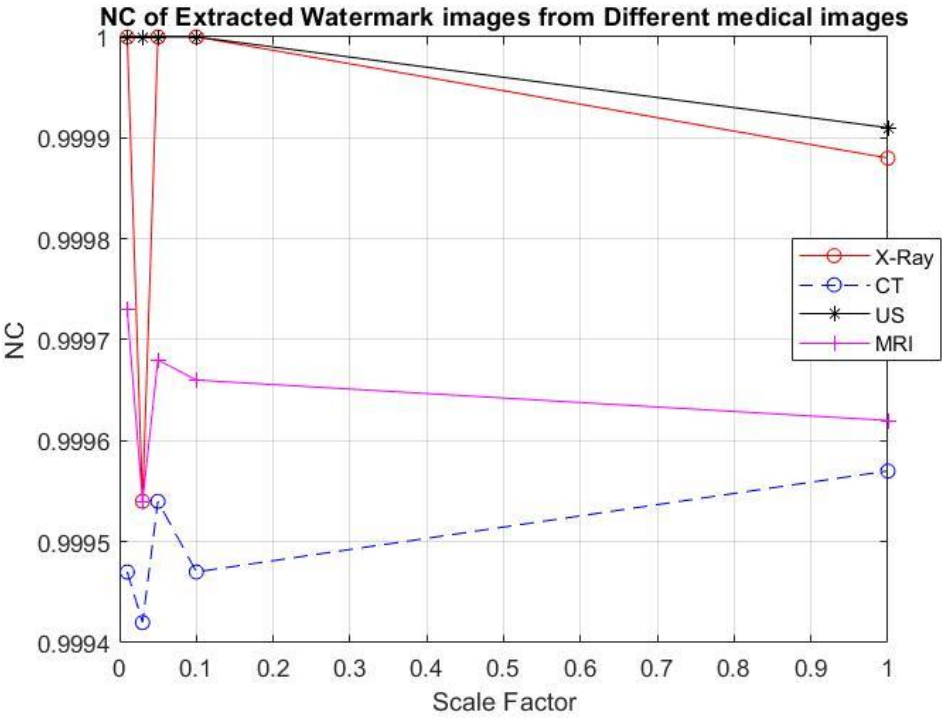


Figure III.7 the NC performance at different scale factor.

Discussion:

The performance of watermarked image quality is measured by evaluating some performance metrics and benchmark tools, such as PSNR, and SSIM. The performance of extracted watermark image quality is measured by Normalized Correlation (NC). These benchmark tools are commonly used to assess the performance of watermarking systems. The quality of the watermarked image is determined by its imperceptibility, which can be assessed using the Peak Signal-to-Noise Ratio (PSNR), and SSIM at different scale factor values. A higher PSNR value indicates better quality. Table III.1, and Table III.2 presents the PSNR, and SSIM values at different scale factors and the visual quality of the watermarked image. The image exhibits the most apparent quality when the PSNR value is higher.

A low PSNR corresponds to poor watermarked image quality. For example, a scale factor of 0.01 and a PSNR of 95.8343 dB result in excellent image quality, while a scale factor of 0.1 and a PSNR of 50.924 dB indicate inferior quality compared to the first value.

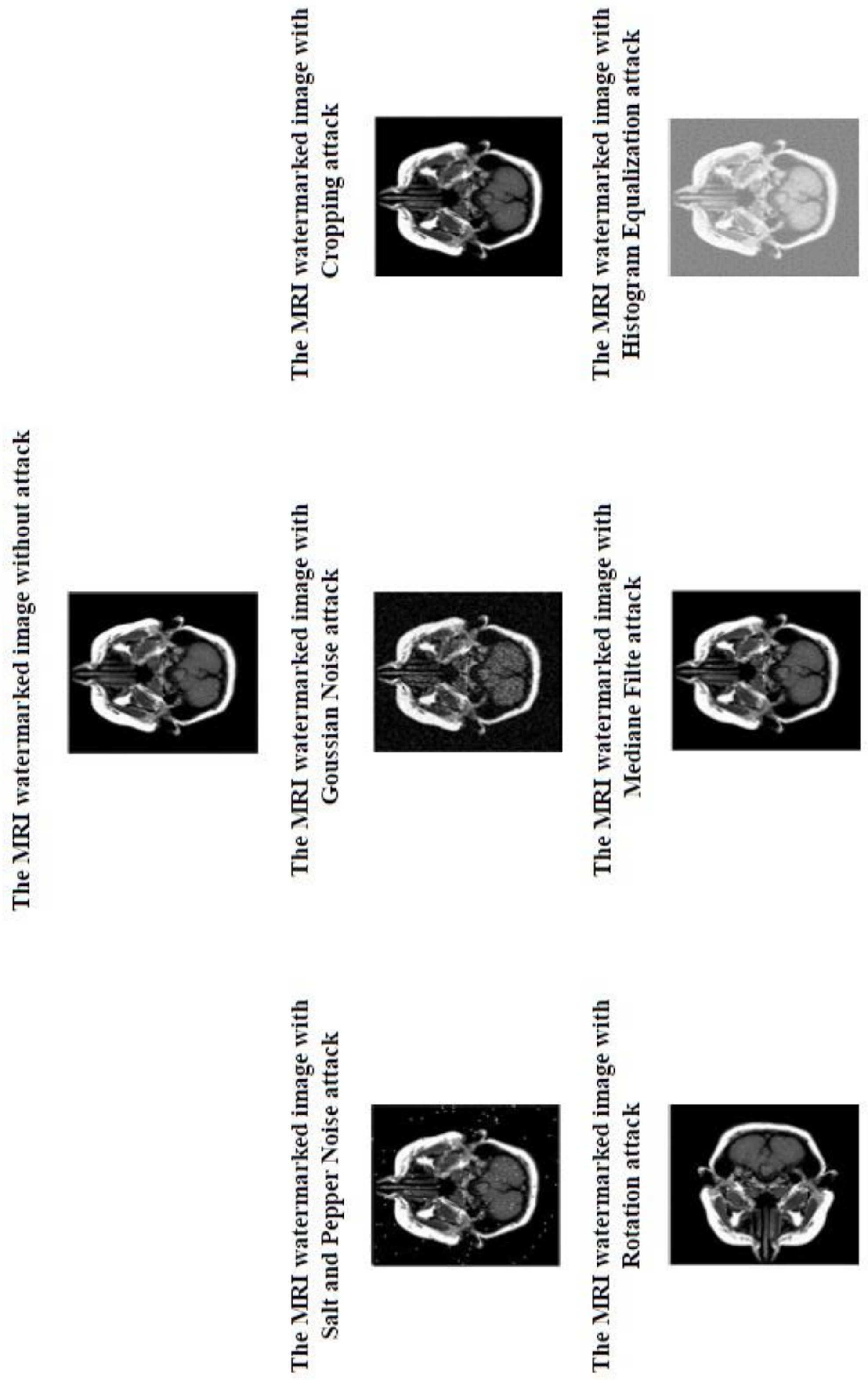
A low NC corresponds to poor extracted watermark image quality, it's by host image type. For example in (MRI case), a scale factor of 0.01 and a NC of 0.99973 result in excellent extracted watermark image quality, while a scale factor of 0.1 and a NC of 0.99966 indicate inferior quality compared to the first value.

III.3 Experimental Results and Discussion after applying different Attacks

The term robustness refers to the ability of the embedded watermark to resist different attacks. Any image processing technique which can degrade or destroy the embedded watermark are considered as an attack. In this section, to evaluate the robustness level of the proposed method, we have applied six different types of attacks on the watermarked images obtained from the method that was discussed above (two levels of DWT with SVD, and spread spectrum). The attacks are: Rotation attack (RTA), Cropping attack (CRA), Histogram Equalization attack, Median filter attack (MFA), Gaussian noise attack, and Salt & Pepper noise attack.

III.3.1 Applying attacks

Figure III.8 illustrates the watermarked MRI 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 Figure III.9, Figure III.10, Figure III.11, and Figure III.12. Upon examination of these figures, it is evident that our proposed method successfully produces high-quality extracted watermark images in most cases, with the exception of the Histogram equalization attack and rotation attack. Numerous metrics can be employed to gauge the quality of the extracted watermark. We evaluate the performance of the proposed technique, specifically the PSNR and NC, on the image watermark using a uniform scale factor of a=0.01. Our method utilizes four different types of medical images and subjects each image to six distinct attacks. The PSNR and NC performance of all attacks are detailed in table III.3.



The MRI watermarked image without attack

The MRI watermarked image with Salt and Pepper Noise attack

The MRI watermarked image with Goussian Noise attack

The MRI watermarked image with Cropping attack

The MRI watermarked image with Rotation attack

The MRI watermarked image with Mediane Filte attack

The MRI watermarked image with Histogram Equalization attack

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

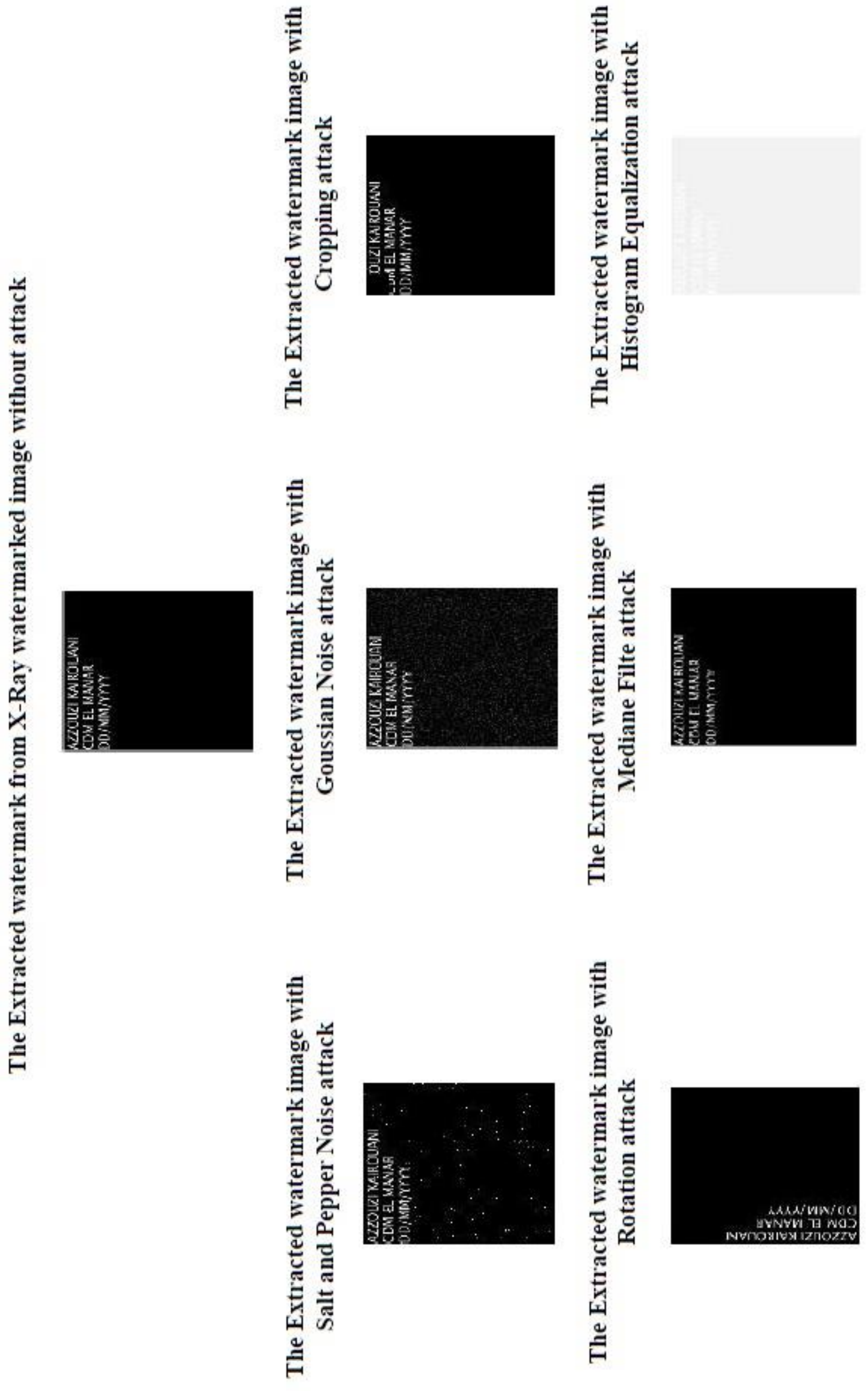
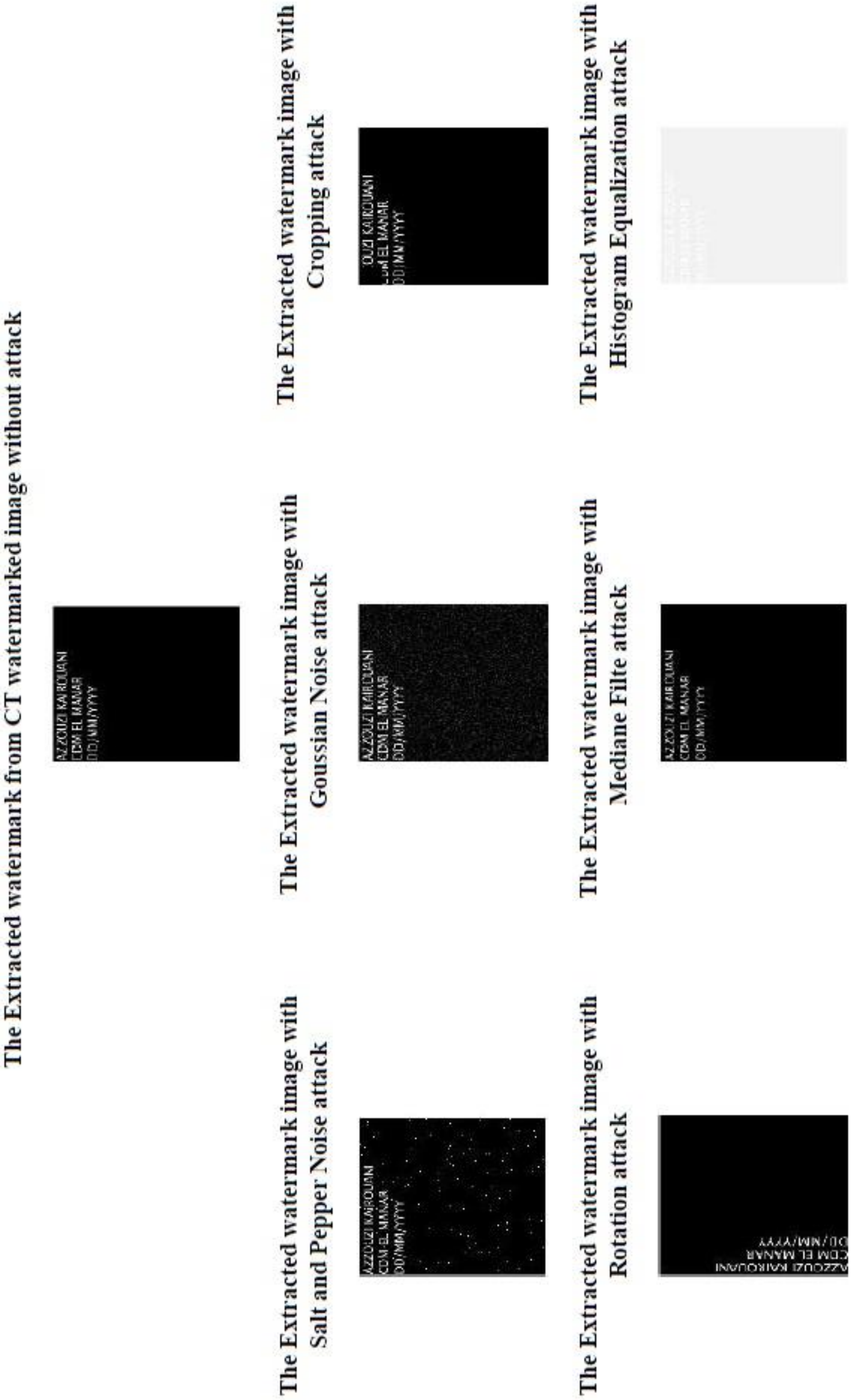

The Extracted watermark from X-Ray watermarked image without attack
AZZOUZI KAIROUANI
CDM EL MANAR
DD/MM/YYYY
The Extracted watermark image with Salt and Pepper Noise attack
The Extracted watermark image with Goussian Noise attack
The Extracted watermark image with Cropping attack
The Extracted watermark image with Rotation attack
The Extracted watermark image with Mediane Filte attack
The Extracted watermark image with Histogram Equalization attack

Figure III.9 Extracted watermarks from Attacked watermarked images (X-Ray).



The Extracted watermark from CT watermarked image without attack

The Extracted watermark image with Salt and Pepper Noise attack

The Extracted watermark image with Goussian Noise attack

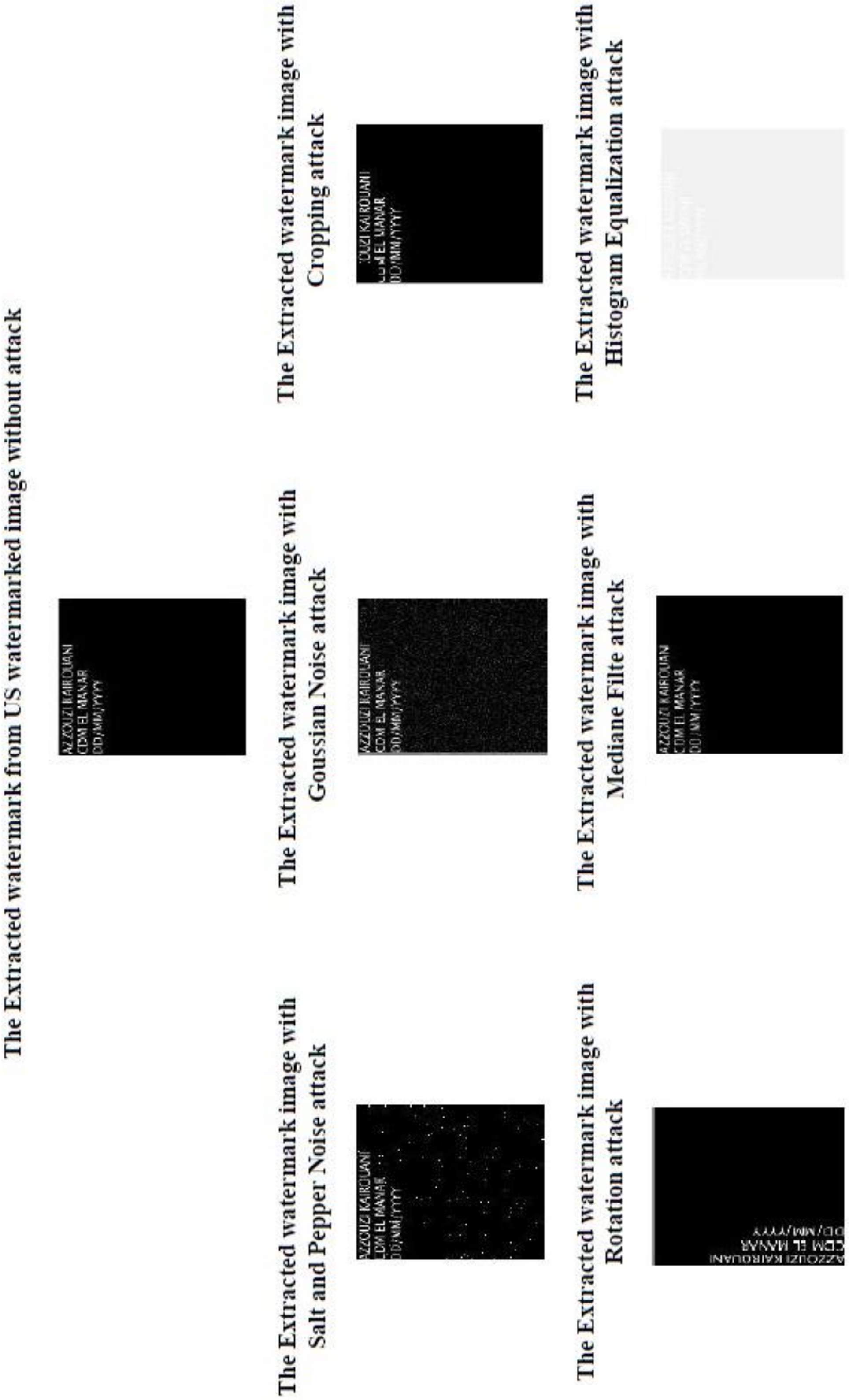
The Extracted watermark image with Cropping attack

The Extracted watermark image with Rotation attack

The Extracted watermark image with Mediane Filte attack

The Extracted watermark image with Histogram Equalization attack

Figure III.10 Extracted watermarks from Attacked watermarked images (CT).



The Extracted watermark from US watermarked image without attack

The Extracted watermark image with Salt and Pepper Noise attack

The Extracted watermark image with Goussian Noise attack

The Extracted watermark image with Cropping attack

The Extracted watermark image with Rotation attack

The Extracted watermark image with Mediane Filte attack

The Extracted watermark image with Histogram Equalization attack

Figure III.11 Extracted watermarks from Attacked watermarked images (US).

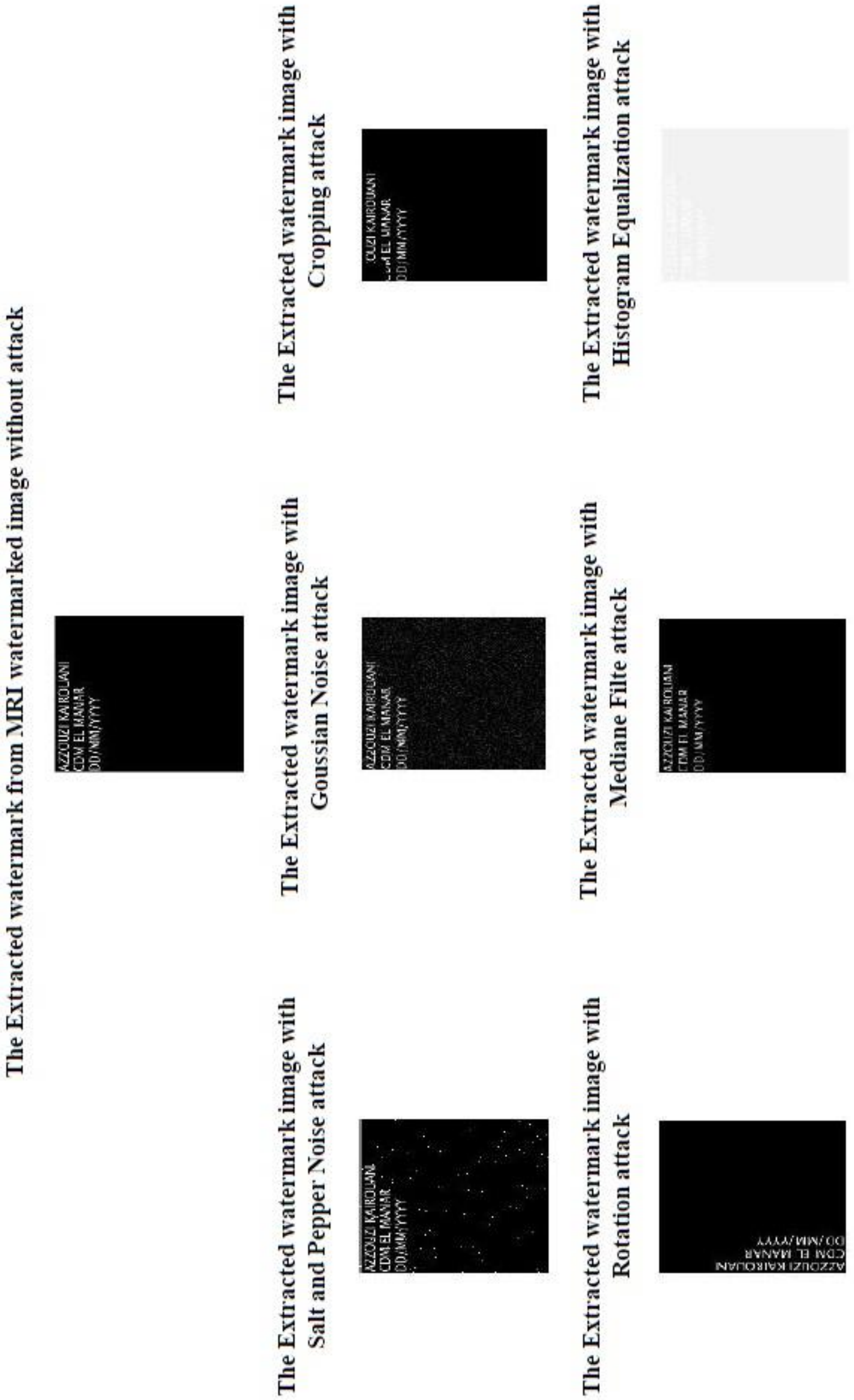

The Extracted watermark from MRI watermarked image without attack
AZZOUZI KAIROUANI
CDM EL MANAR
DD/MM/YYYY
The Extracted watermark image with Salt and Pepper Noise attack
The Extracted watermark image with Goussian Noise attack
The Extracted watermark image with Cropping attack
The Extracted watermark image with Rotation attack
The Extracted watermark image with Mediane Filte attack
The Extracted watermark image with Histogram Equalization attack

Figure III.12 Extracted watermarks from Attacked watermarked images (MRI).

Table III.3 PSNR and NC result obtained from simulations using same watermark image

Type of cover image	Performed Attacks	PSNR	NC
X-ray	Attack free	95.682	1
	Salt & Pepper	24.9772	0.99496
	Gaussian	20.4434	0.48573
	Cropping	70.8792	0.99414
	Rotation	6.5887	0.89746
	Median Filtre	46.6658	0.96861
	Histogram equalization	18.669	0.006073
CT	Attack free	91.3471	0.99947
	Salt & Pepper	23.5467	0.99385
	Gaussian	22.1484	0.48486
	Cropping	80.9278	0.99352
	Rotation	11.4388	0.89684
	Median Filtre	52.0744	0.96861
	Histogram equalization	3.4662	0.006073
Ultrasound	Attack free	81.5699	1
	Salt & Pepper	24.0942	0.99541
	Gaussian	21.2191	0.48357
	Cropping	45.857	0.99414
	Rotation	12.2123	0.89746
	Median Filtre	52.9656	0.96861
	Histogram equalization	8.5336	0.006073
MRI	Attack free	95.8343	0.99973
	Salt & Pepper	23.4175	0.99484
	Gaussian	21.8892	0.4856
	Cropping	80.9484	0.99387
	Rotation	8.8941	0.89719
	Median Filtre	31.4562	0.96861
	Histogram equalization	6.1058	0.006073

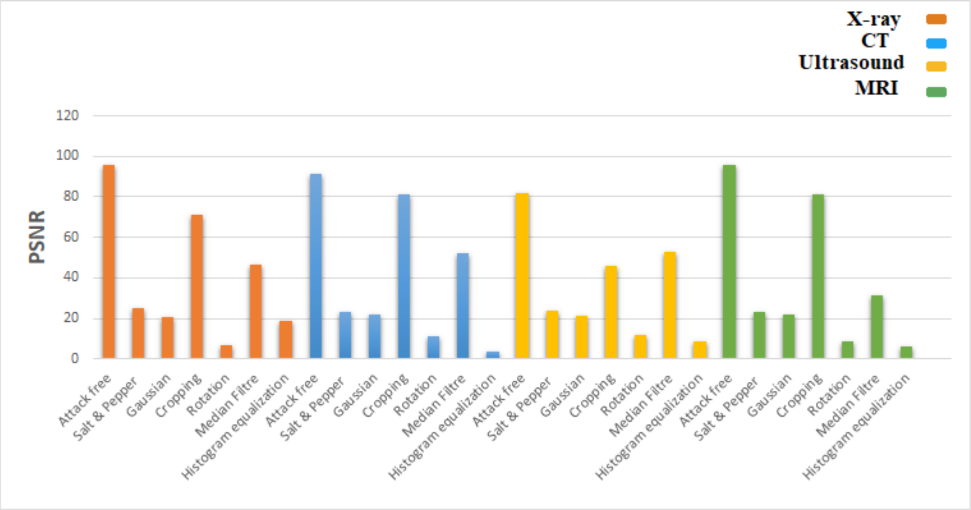


Figure III.13 PSNR result obtained from simulations using same watermark image.

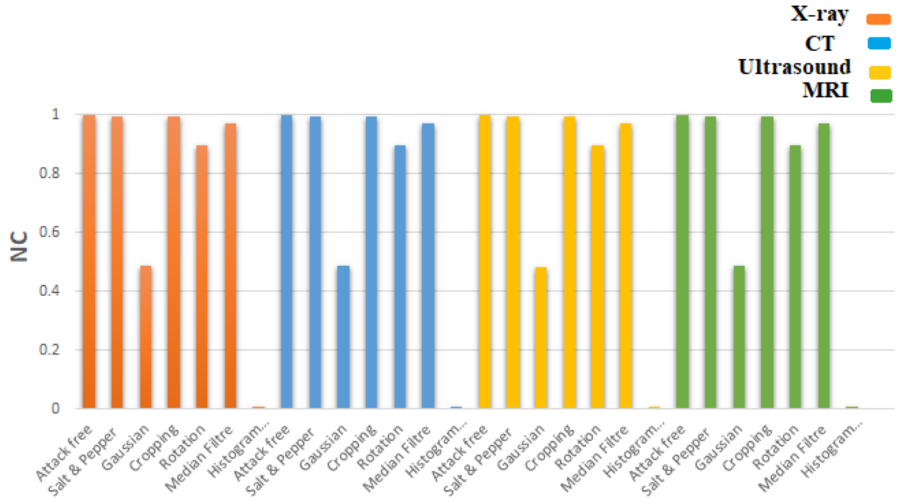


Figure III.14 NC result obtained from simulations using same watermark image.

Discussion:

From the above Figures, and Figure III.13, Figure III.14, we note it is evident that our proposed method successfully produces high-quality extracted watermark images in most cases, with the exception of the Histogram equalization attack and rotation attack.

Where we found that the Histogram equalization attack and rotation attack greatly affected the values of PSNR. And as for NC values we found that the Histogram equalization attack it's the only one who greatly influenced.

III.4 CONCLUSION

This chapter dealt, method an approach for watermarking medical images. Of The method utilize a two-level DWT transform domain sub-band, on which SVD decomposition is performed using spread spectrum techniques with a text watermark image.

The method have been found potentially useful in achieving enhanced robustness of the watermark which can be gainfully extracted in medical as well as other applications. In addition, the proposed method offers optimal trade-off between robustness, perceptual quality (imperceptibility) of the cover image.

DWT, SVD and spread spectrum applied together offer better performance in terms of imperceptibility.

Summary:

This document proposes a secure transmission method using watermarking techniques for medical image watermarks. The performance of the method is evaluated through experimental results, which include changing watermark size and scale factor and testing against various attacks such as rotation, filtering, and histogram equalization. The experiments demonstrate that the proposed method offers good imperceptibility for watermarked images, as measured by PSNR, and it effectively resists geometric and non-geometric attacks, as indicated by correlation coefficients of extracted watermark images. The study combines multiple techniques to enhance the robustness of the watermarks and the quality of the watermarked image. However, the increased application complexity resulting from the combined techniques requires separate examination. Future research should focus on lossless data hiding techniques specifically tailored for medical applications, with a focus on improving performance in terms of robustness, imperceptibility, security, and capacity. These research findings can be reported in future communications.

References

[1]. Thanki R, Borra S, Dey N, Ashour A (2018) Medical imaging and its objective quality assessment: an introduction. In: Classification in BioApps. Springer, Cham, pp 3–32

[2]. Rao K, Rao V (2006) Medical image processing. In: Proceedings of workshop on medical image processing and applications

[3]. Gonzalez, R. C., & Woods, R. E. (2018). Digital image processing. Pearson Education India.

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

[5]. American Hospital Association (2015) The promise of telehealth for hospitals, health systems,and their communities, Trend Watch. American Hospital Association, Chicago, IL

[6]. ISO (2016). ISO 27799:2016, Health informatics – information security management in healthusing ISO/IEC 27002 (Online). Available: https://www.iso.org/standard/62777.html

[7]. DICOM (2009). DICOM, part 15: security and system management profiles, PS 3.15 – 2009(Online). Available: ftp://medical.nema.org/medical/dicom/2009/

[8]. Ruotsalainen P (2010) Privacy and security in teleradiology. Eur J Radiol 73:31–35

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

[10]. 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

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

[12]. Sahni, O., &Talanow, R. (2020). Picture Archiving and Communication Systems (PACS). In StatPearls [Internet]. StatPearls Publishing. Available from: https://www.ncbi.nlm.nih.gov/books/NBK470281/

[13].Pianykh, O. S. (2018). Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide. Springer. https://www.springer.com/gp/book/9783319650483

[14].DICOM Standard: http://dicom.nema.org/medical/dicom/current/output/html/part15.html (2023)

[15]. Dey N, Ashour A, Chakraborty S, Banerjee S, Gospodinova E, Gospodinov M, Hassanien AE (2017) Watermarking in biomedical signal processing. In: Intelligent techniques in signal processing for multimedia security. Springer International Publishing, Cham, pp 345–369

[16]. Nyeem H, Boles W, Boyd C (2013) A review of medical image watermarking requirements for teleradiology. J Digit Imaging 26(2):326–343

[17]. Thanki R, Borra S, Borisagar KR (2018) A hybrid watermarking technique for copyright protection of medical signals in teleradiology, Handbook of research on information security in biomedical signal. IGI Global, pp 320–349

[18]. Liew S, Zain J (2010) Experiment of tamper detection and recovery watermarking in PACS. Second international conference on computer research and development, pp. 387–390

[19]. Borra S, Lakshmi HR, Dey N, Ashour AS, Shid F (2017) Digital image watermarking tools: state-of-the-art. In: Information technology and intelligent transportation systems: proceedings

[20]. Das S, Kundu M (2012) Effective management of medical information through a novel blind watermarking technique. J Med Syst 36(5):3339–3351

[21]. Al-Qershi, O. M., & Abdulla, W. H. (2021). An Overview of Watermarking Techniques for Medical Images: Issues and Challenges. Journal of MedicalSystems, 45(7), 78. https://doi.org/10.1007/s10916-021-01751-2

[22]. Jain, A., & Kapoor, P. (2019). Steganography: A review of techniques and applications. International Journal of Computer Applications, 182(39), 7-11.

[23]. Desai, H.V., Beri, P., Raj, D.J.: Steganography, Cryptography, Watermarking: A Comparative Study. p. 3, (2010).

[24]. Craver S (1997) On public-key steganography in the presence of an active warden. IBM technical report RC 20931.

[25]. W. Bender, D. Gruhl, N. Morimoto, A. Lou, Techniques for data hiding. IBM Syst. J. 35(3&4), 313–336 (1996)

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

[27]. S.P. Mohanty, Watermarking of digital images, M.S. Thesis, Indian Institute of Science, India, 1999

[28]. N. Morimoto, Digital watermarking technology with practical applications. Inf. Sci. Special Issue on Multimedia Inf. Technol., Part 1 **2**(4), 107–111 (1999)

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

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

[31]. R. Chandramouli, N. Memon, M. Rabbani, Digital watermarking, encyclopedia of imaging. Sci. Technol., 1–21 (2002)

[32]. 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

[33]. 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)

[34]. J.B. Feng, I.C. Lin, C.S. Tsai, Y.P. Chu, Reversible watermarking: current and key issues. Int. J. Network Security **2**(3), 161–170 (2006)

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

[36]. 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

[37]. 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

[38]. 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)

[39]. http://www.digitalwatermarkingalliance.org/faqs.asp (2023)

[40]. 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)

[41]. 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

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

[43]. Habes, A. Information Hiding in BMP Image Implementation, Analysis and Evaluation. Inf. Transm. Comput.Netw. **2006**, 6, 1–10.

[44]. 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

[45]. 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)

[46]. 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

[47]. 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

[48]. 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

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

[50]. 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

[51]. C.-C. Lai, C.-C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans. Instrum. Meas. 59(11), 3060–3063 (2010)

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

[53]. 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)

[54]. P. Meerwald, A. Uhl, Survey of wavelet-domain watermarking algorithms, in Proceedings of the SPIE Security and Watermarking of Multimedia Contents III, San Jose, pp. 505–516, 2001

[55]. A.H. Paquet, R.K. Ward, Wavelet-based digital watermarking for authentication, in Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, Winnipeg, pp. 879–884, 2002

[56]. X.-y. Chen, Y.-y. Zhan, Multi-scale anomaly detection algorithm based on infrequent pattern of time series. J. Comput. Appl. Math. 214(1), 227–237 (2008)

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

[58]. G. Jianwei Ma, Plonka, The curvelet transform. IEEE Signal Process. Mag. 27(2), 118–133 (2010)

[59]. 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 .

[60]. 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)

[61]. 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

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

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

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

[65]. 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)

[66]. H. Wang, A.T.S. Ho, S. Li, OR-benchmark: an open and reconfigurable digital watermarking benchmarking framework, June 02, 2015

[67]. S. Pereira, S. Voloshynovskiy, M. Maduẽno, S. Marchand-Maillet, T. Pun, Second generation benchmarking and application oriented evaluation, in Information Hiding Workshop, Pittsburgh, PA, 2001

[68]. V. Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, P. Pitas, A benchmarking protocol for watermarking methods, in Proceedings of the IEEE International Conference on Image Processing, vol. 3, Thessaloniki, Greece, pp. 1023–1026, 2001

[69]. J.C. Vorbruggen, F. Cayre, The Certimark benchmark: architecture and future perspectives, in Proceedings of 2002 IEEE International Conference on Multimedia and Expo (ICME 2002), vol. 2, pp. 485–488, 2002

[70]. K. Wang, G. Lavoue, F. Denis, A. Baskurt, X. He, A benchmark for 3D mesh watermarking, in Proceedings of 2010 IEEE International Conference on Shape Modeling and Applications (SMI 2010), pp. 231–235, 2010