

KASDI MERBAH OUARGLA UNIVERSITY

Faculty of New Information and Communication Technologies

Department of Electronics and Telecommunications



Thesis

Academic Master

Field: Science and Technology

Sector: Telecommunications

Specialty: Telecommunication System

Presented by:

MILOUDI Tarek

CHIKH BOUBAKER Fateh

-Theme-

**SECURE TELEMEDICINE
TRANSMISSION USING
WATERMARKING TECHNIQUES**

Submit Date :

On: 06/2022

BOARD OF EXAMINERS:

Dr. CHERGUI Abdelhakim	Chairman	MAB	UKMO
Dr. Sayeh Mouad	Supervisor	MCB	UKMO
Dr. Dahraoui Nadia	Examiner	MCB	UKMO

Academic Year: 2021 /2022

Dedication

In the name of Allah all the praise is due to him alone, the sustainer of the entire world.

First of all, I owe much tribute to Allah who gave me strength and courage to complete this work. To my parents and my uncles specially my grandmother, I say it is impossible to thank you adequately for all the sacrifices that you made for me to get here, for loving me unconditionally and always being by my side. To my friends El Tashma members Tarek, Tarek, kais, Mustafa. To my English teacher Ben Ayad Rihem and my teachers Benkhatou Belkacem and Benkhatou Fadila, may god bless you all.

Tarek.

I dedicate this work to my parents for their incessant support and their love, Throughout my school career all my beloved siblings my uncles, my aunts and my all family. I also dedicate this dissertation to my friends Azouz, Fares, Djamel, Yazid, the handicaps who have supported me throughout the process. And my class mates I will always appreciate all what they have done, thank you all.

Fateh.

Acknowledgements

We would like to send our heartfelt appreciation to our supervisor Dr. Med Sayeh Mouad provided us with generous suggestions and endless advice to polish the work.

Special thanks go to the jury members Dr. CHERGUI Abdelhakim and Dr. Nadia Dahraoui who provided more suggestions and constructive criticism to ameliorate our work.

We are so grateful for those people who have cooperated and supported us throughout conducting the research.

We would like to thank the participants who allowed much time to share their ideas with us.

ملخص:

في ظل الأعداد المتزايدة من الصور الرقمية الطبية والحاجة إلى مشاركتها بين المتخصصين والمستشفيات من أجل تشخيص أفضل وأكثر دقة، تتطلب حماية خصوصية المرضى. ومن هذا المنطلق، هناك حاجة إلى وضع علامات مائية على الصور الطبية. ومع ذلك، يجب القيام به بعناية خاصة لسببين. أولاً، لا يمكن لعملية أو إجراء العلامات المائية المساس بجودة الصورة. ثانياً، يجب أن تكون معلومات المريض السرية المضمنة في الصورة قابلة للاسترداد بالكامل دون خطر حدوث خطأ بعد فك ضغط الصورة. على الرغم من البحث المكثف الذي تم إجراؤه في هذا المجال، لا توجد حتى الآن طريقة متاحة للوفاء بجميع متطلبات وضع العلامات المائية على الصور الطبية. تهدف هذه الدراسة إلى تقديم مسح مفيد حول العلامات المائية وتقديم منظور واضح للباحثين المهتمين من خلال تحليل نقاط القوة والضعف في الأساليب المختلفة الموجودة مثل DWT مع SVD أو بدون SVD.

Abstract:

Under the growing numbers of medical digital images and the need to share them in between specialists and hospitals for better and more accurate diagnosis require that patient's privacy should be protected. As a matter of this, there is a need for medical image watermarking. However, it needs to be performed with special care for two reasons. Firstly, the watermarking process or procedure can't compromise the quality of the image. Secondly, confidential patient information embedded within the image should be fully retrievable without risk of error after image decompressing. Despite extensive research undertaken in this field, there is still no method available to fulfill all the requirements of medical image watermarking. This study aims to provide a useful survey on watermarking and offers clear perspective for interested researchers by analyzing the strengths and weaknesses of different existing methods such DWT with SVD or without the SVD.

Keywords :

SVD, DWT, Securer Telemedicine Watermarking

Résumé

Compte tenu du nombre croissant d'images numériques médicales et de la nécessité de les partager entre les spécialistes et les hôpitaux pour obtenir un diagnostic meilleur et plus précis, il faut protéger la vie privée des patients. Dans ce cas, il est nécessaire de faire un filigrane d'image médicale. Cependant, il doit être effectué avec un soin particulier pour deux raisons. Tout d'abord, le processus ou la procédure de filigrane ne peut pas compromettre la qualité de l'image. Deuxièmement, les informations confidentielles du patient intégrées dans l'image doivent être entièrement récupérables sans risque d'erreur après décompression de l'image.

Malgré des recherches approfondies menées dans ce domaine, il n'existe toujours pas de méthode permettant de satisfaire à toutes les exigences du filigrane d'image médicale. Cette étude vise à fournir une enquête utile sur le filigrane et à offrir une perspective claire aux chercheurs intéressés en analysant les forces et les faiblesses de différentes méthodes existantes

mots-clés :

SVD, DWT, Tatouage de télémédecine sécurisé

.telles que DWT avec SVD ou sans SVD

List of Contents

General Introduction

CHAPTER I : MEDECAL IMAGING

I.1 Introduction.....	1
I.2 Medical Imaging	2
I.3 Medical Imaging Types.....	2
I.3.1 X-Ray Projection Imaging	2
I.4 Digital image.....	5
I.5 Digital medical image	5
I.6 Medical image security requirements	5
I.7 Picture archiving and communication system (PACS).....	7
I.8 Digital Imaging and Communication in Medicine (DICOM).....	7
I.9 DICOM security profiles.....	9
I.10 Medical image security applications	11
I.10.1 Watermarking applications in the medical image.....	11
I.10.2 steganography security applications	12
I.10.3 Watermarking, Steganography and Cryptography.....	13
Conclusion.....	14

CHAPTER II : WATERMARKING TECHNIQUES

II.1 Introduction.....	15
II.2 Importance and Necessity of Watermarking	16
II.3 Classifications of Digital Watermarks	17
II.4 Potential Characteristics of Digital Watermarks	18
II.5 Framework for Watermarking	19
II.6 Application of digital image watermarking.....	21
II.7 Domains of image watermarking.....	22
Watermarking based on spread spectrum.....	22
II.7.1 Spatial domain	23
II.7.1.1 Least significant bit (LSB).....	23
II.7.1.2 Local binary pattern (LBP).....	24
II.7.2 Frequency domain.....	25
II.7.2.1 Discrete wavelet transform (DWT)	25
II.7.2.2 Discrete cosine transform (DCT).....	28
II.7.2.3 Singular value decomposition (SVD).....	30
II.8.1 Watermarking Attacks	33
II.8.2 Benchmark Tools for Image Watermarking	34
II.9 Essential Requirements for Medical Image Watermarking.....	36

II.10 Performance Measures.....	38
II.10.1 Mean Square Error (MSE).....	38
II.10.2 Peak Signal-to-Noise Ratio (PSNR).....	38
II.10.3 Weighted Peak Signal to Noise Ratio (WPSNR).....	38
II.10.4 Universal Image Quality Index.....	39
II.10.5 Structural Similarity Index Measure (SSIM).....	40
II.10.6 Normalized Correlation (NC).....	40
II.10.7 Bit Error Rate (BER).....	40
Conclusion.....	41

CHAPTER III : Watermarking Experimental Analysis and Results

III.1 Introduction	42
III.2 Medical image Watermarking using two levels of DWT and SVD.....	42
III.2.1 Watermark Embedding Algorithm.....	42
III.2.2 Watermark Extraction Algorithm.....	43
III.2.3 Simulation of Watermarking using two levels of DWT and SVD.....	44
III.3 Watermarking using three levels of DWT without SVD	45
III.3.1 Watermark Embedding Algorithm.....	45
III.3.2 Watermark Extraction Algorithm.....	46
III.3.3 Simulation of Watermarking using three levels of DWT without SVD	47
III.4 Experimental Results and Discussion after applying different Attacks	48
III.4.1 Applying attacks on first method (two levels of DWT with SVD).....	49
III.4.2 Applying attacks on second method (three levels of DWT without SVD).....	52
III.4.3 Experimental Results after using different wavelet families	55
III.4.4 Experimental Results Comparing proposed method with other reported method.....	56
Conclusion.....	57
Summary.....	58

List of figures

Figure I.1: Medical image components.....8

Figure I.2: RONI & ROI medical image..... 8

Figure I.3 Data security system field.....13

Figure II.1: The prisoner’s problem.....16

Figure II.2: Classification of watermarking techniques.....18

Figure II.3: The watermark process (a) embedding and (b) extraction.....21

Figure II.4: Watermarking domains.....24

Figure II.5: Local Binary Pattern of eight neighbors.....26

Figure II.6: 2-level- DWT decomposition27

Figure II.7: Image DCT frequency coefficients.....30

Figure II.8: Classification of possible attacks in digital watermarking.....34

Figure II.9: Main advantages of medical image watermarking.....37

Figure II.10: Major security requirements for EPR data.....37

Figure III.1 The cover image (a), and the watermarked image (b).....44

Figure III.2 The original watermark (c), and the extracted watermark44

Figure III.3 The cover image (e), and watermarked image (f)46

Figure III.4 The original watermark image (j) and the extracted watermark image (h).....47

Figure III.5 The attacked watermark brain-cancer images:48

Figure III.6 Test images.....49

Figure III.7 Extracted watermarks from Attacked watermarked images using (two levels of DWT with SVD)50

Figure III.8 The attacked watermarked images:.....51

Figure III.9 Extracted watermarks from Attacked watermarked images using (three levels of DWT without SVD).....52

Figure III.10 PSNR comparison results in different wavelets on test images method (two levels of DWT with SVD).....54

Figure III.11 PSNR comparison results in different wavelets on test images, method (three levels of DWT without SVD)55

List of Tables

Table II.1: LSB watermarking approach.....25

Table II.2: Difference between Spatial domain and Frequency domain32

Table III.1 PSNR, and NC performance at different factor alpha..... 44

Table III.2 PSNR, and Visual quality of the watermarked at deferent Scale factor.....47

Table III.3 PSNR and NCC result obtained from simulations using same watermark image.....51

Table III.4 PSNR and NCC result obtained from simulations using same watermark Image.....53

Table III.5 PSNR values with different wavelets applied on four test images on method (two levels of DWT with SVD).....54

Table III.6 PSNR values with different wavelets applied on four test images on method (three levels of DWT without SVD).....55

Table III.7 Comparison of PSNR and NC values with other reported method..... 56

List of Abbreviation

- BER:** Bit Error Rate
- DCT:** Discrete cosine transform
- DICOM:** Digital imaging and communication in medicine
- DFT:** Discrete Fourier transform
- DWT:** Discrete wavelet transform
- EPR:** Electronic patient record
- ICT:** Information and communication technology
- LBP:** Local binary pattern
- LSB:** Least significant bit
- MSE:** Mean square error
- NC:** Normalized Correlation
- PACS:** Picture archiving and communication system
- PSNR:** Peak signal-to-noise ratio
- QF:** Quality factor
- ROI:** Region of interest
- RONI:** Region of non-interest
- SSIM:** Structural Similarity Index Measure
- SVD:** Singular value decomposition
- TAF:** Tamper Assessment Factor
- WPSNR:** Weighted Peak Signal to Noise Ratio

General Introduction

The improvement of digital communication and information technology, the sharing of data becomes very easy and fast. Nowadays there is a generation of internet-based sharing and it takes only few seconds to share one's personal image to the world. Today, Digital image processing tools are very easily available and it is getting advanced day by day [A, B]. It's easy to claim false ownership and create illegal copy of shared images as these images are very easily available on internet. The manipulation or change of images is becoming a piece of cake with the advancement of image processing tools. There are different ways to protect the lawful ownership of images. The most popular way to do so, is the digital image watermarking, which is a quite powerful tool for ownership check along with tamper detection. Good watermarking methods for copyright protection applications need to achieve some watermarking important requirements, such as the robustness and imperceptibility. The robustness is very important it means that the proposed methods must resist against different kinds of attacks. The watermarked image needs to have a good transparency or imperceptibility. Finally, the watermark extraction process could be blind which means that it doesn't need the original cover image for watermark extraction. This document contains three chapters structured in following manners:

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

Chapter two dealt with different medical image watermarking techniques and their importance. Watermarking frame work, watermarking requirement, watermarking advantages and the benchmark tools are also presented. Watermarking performance measurement are explained.

Chapter three presents two proposed watermarking techniques. Simulation and experimental results are shown. Performance comparison of the two proposed methods are analyzed.

I.1 Introduction

Medical imaging refers to various technologies that are used to view the human body in the name of “diagnosis, monitor, or treat medical conditions”. All imaging modalities have in common that the medical condition becomes visible by some form of contrast, meaning that the feature of interest like “Neoplasm” can be recognized & identified in the image and inspected by a qualified radiologist. The image can be viewed as a model of the imaged tissue such as “muscles nerve epithelial and connective”.

Images in the background of this book are digital. This points to a precise resolution with the pixel as the smallest element. As well, all imaging modalities lead to some degradation of the image when compared to the original object. mostly, the degradation consists of blur “loss of detail” and noise (unwanted contrast). all imaging modalities have some basic principles in common, like the interpretation as a system and its mathematical treatment. The image itself can be regarded as a multidimensional signal. In many cases, the steps in image formation can be viewed as linear systems, which allow simplified mathematical treatment.

Each type of technology provides various data about the area of the anatomy being examined or treated, related to possible disease, injury, or the effectiveness of medical treatment”.

Lastly this chapter deals with Medical image, Medical image types, digital image as well as archiving systems and communication systems in medicine.

I.2 Medical Imaging

Medical imaging, also noted as radiology, is the field of medicine that medical experts recreate various image's parts of the body for diagnostic or treatment purposes. Medical imaging procedures include non-invasive tests that allow doctors to diagnose injuries and diseases without being intrusive, Medical imaging is the key part of the improved outcomes of modern medicine, there is different types of medical imaging procedures.

I.3 Medical Imaging Types

According to [1] medical images can be easily obtained without invasive data extraction due to technology improvements. There are multiple image modalities that could be regarded to categorize the various types of medical images

I.3.1 X-Ray Projection Imaging

X-ray imaging is the oldest medical imaging modality, having entered clinical use shortly after the invention of X-rays in 1895. X-ray imaging is a projection technique, with images traditionally formed on photosensitive film, though direct digital X-ray imaging is becoming more common. X-ray imaging is a qualitative modality in its most common form. X-rays are high-energy photons, and atomic interaction with inner shell electrons is essential for both X-ray generation and X-ray contrast generation. Soft-tissue contrast is relatively low, but bones and air contrast are excellent. Contrast agents can be used to improve contrast in some cases. Ionization of tissue along the beam path is an undesirable (but unavoidable) side effect of the photon-atom interaction, which can cause radiation damage. X-ray images can reveal very subtle features, and their popularity is boosted further by the low cost of equipment and the simple imaging procedure.

I.3.2 Computed Tomography (CT)

Computed tomography (CT), so called computed axial tomography (CAT), is a volumetric imaging modality based on X-ray absorption. Unlike projection X-ray imaging A two or three-dimensional absorber map can be reconstructed using CT. In terms of soft tissue contrast, CT hugely exceeds projection X-ray imaging, but the spatial resolution of a clinical whole-body CT scanner is significantly lower than that of plain X-ray imaging. Despite this, CT can detect small tumors, structural detail in trabecular bone, and alveolar tissue in the lungs. In the 1971 CT was introduced. It is the first imaging modality in which the computer is used to reconstruct images: a series of X-ray projections is transformed to produce the cross-sectional image. Since the first CT scanners were introduced, significant advances have been made in

contrast, image quality, spatial resolution, and acquisition time. Modern clinical CT scanners are extremely fast, producing a 2D cross-sectional image in under a second. In-plane spatial resolution can be as low as 100 μm , and specialized CT microscopes can provide voxels as small as 10 μm . Clinical CT scanners, however, they are prohibitively expensive, costing millions of dollars. This translates to a relatively high cost per CT scan, preventing its wider adoption.

I.3.3 Ultrasound Imaging

The properties of sound waves in tissue are used in ultrasound imaging. Pressure waves in the low megahertz range travel at the speed of sound through tissue, being refracted and partially reflected at interfaces. As a result, ultrasound contrast is related to echogenic inhomogeneities in tissue. The travel time of an echogenic object can be used to determine its depth. Two-dimensional scans are possible by emitting focused sound waves in different directions. Because of the complex relationship between inhomogeneous tissue and echoes, differences in sound speed in different tissues, and the high noise component caused by the weak signal and high amplification, ultrasound images are highly qualitative in nature. Despite the fact that soft tissue contrast is good in ultrasound images, it fails in the presence of bone and air. Although ultrasound images can be produced using only analog circuitry, modern ultrasound devices employ computerized image processing for image formation, enhancement, and visualization. Ultrasound imaging is extremely popular due to its inexpensive instrumentation and ease of use. An ultrasound exam, on the other hand, necessitates the presence of an experienced operator to adjust different parameters for optimum contrast, and ultrasound images typically necessitate the presence of an experienced radiologist to interpret the image.

I.3.4 Nuclear Imaging

Nuclear imaging, like X-ray and CT imaging, employs radiation. In contrast to X-ray imaging, the body is injected with radioactive compounds as radiation sources. Which are typically linked to pharmacologically active substances ("radiopharmaceuticals") that accumulate in specific locations throughout the body for instance, consider a tumor. The spatial distribution of the radiopharmaceutical can be determined using either projection techniques or volumetric computerized image reconstruction. Metabolic processes can thus be imaged and used to make a diagnosis. Three-dimensional reconstructions are obtained similarly to CT, resulting in a modality known as single-photon emission computed tomography (SPECT). Positron emission tomography (PET), a parallel technology, employs positron emitters to produce coincident pairs of gamma photons. It has a higher detection sensitivity and signal-to-

noise ratio than SPECT. SPECT and PET have lower resolution than CT, with voxel sizes not much smaller than 1 cm. To provide a spatial reference, SPECT or PET image are frequently superimposed on CT or MR images. The cost of nuclear imaging modalities is one barrier to their widespread use. Furthermore, the radioactive labels have very short half-lives, (few hours), and most radiopharmaceuticals must be manufactured on-site. This necessitates the presence of a reactor for isotope generation in nuclear imaging centers.

I.3.5 Magnetic Resonance Imaging

Magnetic resonance imaging (MRI) is a volumetric imaging modality that, to some extent, resembles computed tomography. Whereas, the underlying physical principles, are fundamentally different from CT. MRI is based on the orientation of protons inside a strong magnetic field, whereas CT uses high-energy photons and the interaction of photons with electrons of the atomic shell to generate contrast. With resonant radiofrequency waves, this orientation can be changed, and the return of the protons to their equilibrium state can be measured. The relaxation time constants are highly tissue-dependent, and MRI has far superior soft tissue contrast to CT. MRI, on the other hand, takes significantly longer to acquire images than CT, unless special high-speed protocols are used (which often suffer from poor image quality). Furthermore, modern MRI scanners necessitate the use of a superconductive magnet with liquid helium cooling infrastructure, extremely sensitive radiofrequency amplifiers, and a completely shielded room against electromagnetic interference. As a result, MRI equipment is extremely expensive. with scanner hardware costing several million dollars and correspondingly high recurring costs for maintenance. MRI scanners, on the other hand, produce images with a high diagnostic value, and MRI can be used to monitor some physiological processes (e.g., water diffusion, blood oxygenation), so it partially overlaps with nuclear imaging modalities. Because MRI is a radiation-free modality, it is frequently used in clinical studies involving volunteers.

I.4 Digital image

A digital image is a two-dimensional array of positive integer values $f(x,y)$, where $1 \leq x \leq M$ and $1 \leq y \leq N$. M and N are nonnegative integer values representing the number of row and column, respectively. The coordinate (x, y) represents the image pixel position. $f(x,y)$ represents the image pixel values. In the case of a three-dimensional image, $f(x,y,z)$ is used where, $1 \leq z \leq Y$ and Y is a nonnegative integer [2].

I.5 Digital medical image

The normal method to generate digital medical image is to capture the image on X- ray films or radiographs, computed radiography (CR), and digital radiography (DR) techniques, Medical imaging examinations include computed tomography (CT), X-ray computed tomography (XCT), nuclear medicine (NM), positron emission tomography (PET), single photon emission computed tomography (SPECT), ultrasonography (US), magnetic resonance imaging (MRI), digital fluorography (DF), and digital subtraction angiography (DSA) [2].

I.6 Medical image security requirements

The health insurance portability and accountability act (HIPAA) requires medial image security to ensure that patient information privacy is protected [3]. The DICOM standard suggests an optional guide for producing medical images. In telemedicine, however, the medical image is transmitted via network between the referring site and the expert site. The security term becomes crucial and critical issue. It is not only for storing data in the medical system, but also for transmitting data over the network in telemedicine.

That's to keep the patient's information in terms of privacy, authenticity, and integrity. The following are some examples of these characterizations: Confidentiality entails denying others access to patient information. While the integrity refers to the safety of medical images transmitted from any tampering, modifying, or changing. Furthermore, the authenticity is used to validate the source of the image which belongs to the correct patient. [4].

To achieve the highest level of security for patient information, medical information, and other patient-related information a lot of work is done in this field. The following section discusses the characteristics of the medical image.

I.6.1 Medical image confidentiality

The confidentiality means that the authorized users are able to access, modify, or perform any other permitted process on the patient information while preventing unauthorized users from accessing to them or editing the information. It is regarded as the first step in ensuring the security of patient information privacy. [5].

The patient information has to be kept confidentially following its law and ethics. The information must have the critical and important quality of trustworthiness. Furthermore, during the transition, the confidentiality of the information must be ensured. Moreover, the data Used must keep patient information secure within the responsible team, such as the physician and the lab worker, etc. [6].

It is legal to break confidentiality when the patient agrees to reveal his or her information or if it improves and serves the public health sector [7].

I.6.2 Medical image integrity

A code of ethics for health informatics professionals (HIPs) has provided us with guidance and health information protection principles [8]. The integrity is a critical and important point. The patient information integrity means that the data is free of any intentional or unintentional modification by an unauthorized person. So, the person in charge of the medical information in the telemedicine system must detect any attack lunched by an unauthorized person.

I.6.3 Medical image authentication

The goal of medical image authentication is to identify the image source, ownership, and keep its origin as it was sent from the source. This means that no falsification occurs during the transmission process. Medical image authentication is used to improve tamper detection and tamper recovery. Authentication and integrity are inextricably linked [5].

The medical image authentication goes through the following process: Inserting data from the source side into the cover host image, the images should then be sent to the receiver, who extracts the embedded data in the host image and determine whether it is authenticated or not. Medical image authentication schemes are classified as follows: Based on a digital signature (meta data) and watermarking based.

To verify the data's authenticity, the header data or physician digital signature that is stored alongside the medical image is used. [9] .[10] [11] Watermarking involves embedding invisible information in host data, authenticity then is extracted and verified. Watermarking is a popular method for achieving security. [12] [13].

I.7 Picture archiving and communication system (PACS)

PACS is regarded as the server of the medical images. It receives and stores images from devices like Hospital Information System (HIS) and Radiology Information System (RIS). PACS are considering the various radiological imaging modalities, it consists information about the patient and data related to his case. Two components are indispensable in PACS which are ...database server and archiving system.

The HIS and RIS send the image's examination to the PACS server. The latter elicits the descriptive data from the DICOM header. Afterwards, actualizes the database system then bounds and limits the target of the newly generated data, PACS compresses and stores data or update the database system when the amount of information is huge.

PACS can be combined to the Teleradiology system in the medical field. It can provide the clinic with the important data about the patient. While it is used as a server consisting of the database for the hospital medical images. PACS can import medical image from the outside imaging center, then distributes the reports to the HIS and other medical expert system of the hospital. Besides, the image center can send it to the expert system as in the Teleradiology model. [14].

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

The incorporation of various digital products, modalities, archiving, and information of medical system terms necessitated the creation of a standard format for medical images. Digital Imaging and Communications in Medicine (DICOM) is the standard format for storing, transmitting, saving, and using medical images, DICOM was created in 1983 by a collaboration between The American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) to create a standard for data transfer. The ACR-NEMA standard versions 1 were published in 1985 and improved the method of storing and transferring data in a non-proprietary form. The second version improved the standard definition, data structure, and encoding. DICOM version 3 was released in 1993, with the main difference which was based on network protocol via TCP/IP protocol. The data structure model was built around a distinct definition for services and objects like image objects, patient objects, and so on.

The DICOM header components are the patient information, physician details, and hospital information, which are referred to as information object definition IODs. Each of these objects in the header has a meaning. The data is divided into several groups, each one contains

connected data, like group 10 which contains patient data, unique identifiers (UID) in terms of image technology details like X-Ray exposure

The DICOM body contains significant data about the patient case, we can divide it into the region of interest (ROI), which is normally in the center, and the region of non-interest (RONI), which is the image's border. Figures I.1 and I.2 depict the medical image components [15].

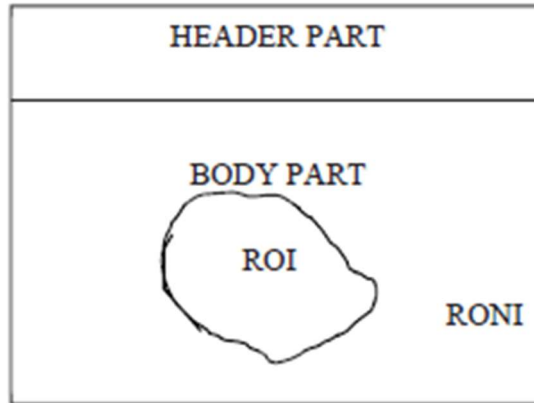


Figure I.1: Medical image components

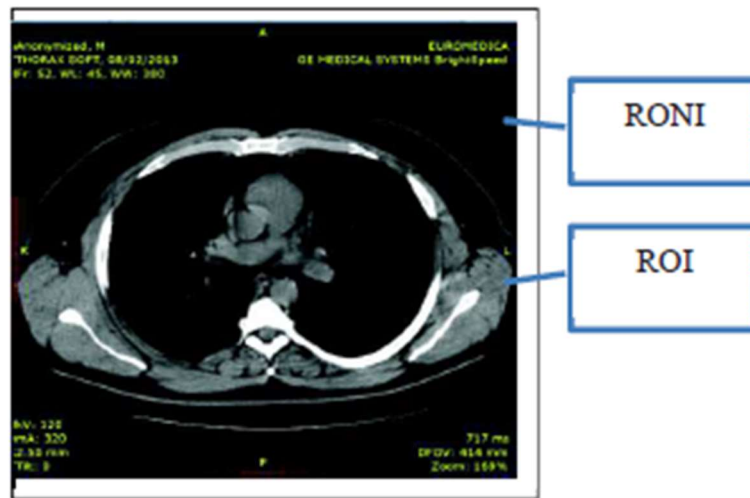


Figure I.2: RONI & ROI medical image

DICOM services are being developed and improved via the research. OFFIS (Oldenburger Forschungs und Entwicklungsinstitut Für Informatik The Oldenburger Institut) is the DICOM team's main European partner. It is a German institution that was found in 1991 in Oldenburg. The institute is interested in three domains of research: energy, health, and transportation [16].

I.9 DICOM security profiles

DICOM is a medical image standard. It has addressed the security issue [17]. Four security profiles have been added to DICOM: secure use profiles, secure transport connection profiles, digital signature profiles, and media storage secure profiles [17]. These security profiles deal with the attributes by utilizing associations security, object authentication, and file security. The following section goes over these security profiles.

I.9.1 Secure use profiles

Secure use profiles guide the use of attributes and other security profiles in a specific mode. The profiles cover the secure use of online electronic storage, bit maintaining, and electronic signatures.

I.9.2 Secure transport connection profiles

These profiles are specialized in the technique used in DICOM applications in order to establish a secure data exchange over a network and internet. Secure transport connection protects the information during the transmission. These profiles are similar to the secure socket layer (SSL), SSL is used in the security of the online web site. Secure transport connection profiles are an application of the asymmetric cryptography. So, the receiver is the only one who has an access to the message sent and no one else can decode it. In these profiles, there are two opportunities to implement secure transport connection over: transport layer security (TLS) and integrated secure communication layer (ISCL). The profiles provide DICOM with restricted features that are mandatory for implementation.

I.9.3 Digital signature profiles

Tools for digital signature integrity checks are supported by digital signature profiles. A digital signature allows for the validation of the identity structure that is generated, approved, or changed a DICOM data. The digital signature generator must first identify the DICOM data set before embedding the MAC and hash value. The MAC value should then be embedded in the digital signature. While the receiver can validate the received data's authenticity and integrity by recalculating the MAC value and comparing it to the embedded MAC value. Depending on the content that will be embedded in DICOM, the profiles provide three potential methods of digital signature implementation (base, creator, and authentication).

I.9.4 Media storage security profiles

To protect the DICOM data against unauthorized access of the information, the media security profiles support a secure tool. The profile compresses data with a cryptographic wrapper to define a structure of the DICOM protection. This method of security is regarded as an application of asymmetric cryptography techniques. These security profiles enable image encryption using DES, DSA, and other exciting encryption techniques. However, after decryption, the information is no longer secure. As a result, verifying its authenticity, and reliability is difficult [18]. Moreover, the DICOM security standard fails to protect the confidentiality and integrity of medical image data. The attacker, on the other hand, can easily remove its header and regenerate a fake one. As a result, to ensure image security during storage and transmission, we can consider watermarking as a solution. This way, it can provide a long-term guarantee of data confidentiality and integrity [19].

Furthermore, watermarking and cryptography techniques are used on medical data to improve image security.

The following is a general illustration of how encryption and embedding methods are applied at the sender side:

- Image preprocessing: segmenting and extracting the relevant patient information from the DICOM header.
- Data encryption: encrypting medical data and generating ciphered data form.
- Data embedding: the process of embedding secret information in medical data.

When the extraction and decryption processes are used on the receiver side, the following steps are taken:

- Extracting the secret information from the medical data received.
- Decrypting the medical data.
- Ensuring the integrity, authenticity, and confidentiality of the received data

I.10 Medical image security applications

There are numerous works proposed on medical image watermarking and cryptography techniques for security issues. This section discusses the most important and critical approaches to watermarking and cryptography applications in medicine. Despite the fact that there are many works in the spatial domain, few of them presented watermarking approaches in the frequency

domain. Previous research indicates that the frequency domain outperforms the spatial domain in terms of security robustness. However, the spatial domain is superior in terms of complexity. Because the work is with real-time applications (Telemedicine), the contribution focuses on the spatial domain for a lower complexity goal, as well as on improving the compromise between robustness, capacity, and imperceptibility requirements. In the medical sector, existing security applications are classified into two types. The first are pure watermarking techniques used in frequency and spatial domains. The second category includes medical image applications based on cryptography and watermarking techniques. Watermarking applications in the medical image.

I.10.1 Watermarking applications in the medical image

The authors of [20] presented multiple and fragile image watermarking of DICOM medical images based on a four-level Haar-DWT frequency domain. The approach addressed the issues of source authentication, medical information authentication, and patient analysis details transmission. The reference watermark, Tamper Assessment Factor (TAF), and physician's signature are also used. The authenticity was satisfied against some attacks when using the Haar wavelet technique, but for other attacks such as rotation and cropping, contrast, flip, blurring, sharpening, salt and pepper noise, and Gaussian noise, a significant loss of the embedded data is observed.

[21] presents another frequency domain watermarking approach. For medical images, a new and robust technique is proposed. The strategy aimed to protect the content's copyright while also ensuring the accuracy of the patient information. It entails dividing the image into three wavelet transforms and employing a graph theory approach to find the best places to embed the watermark key. The algorithm provides good invisibility and robustness, particularly against LSB attacks, and is reliable enough to trace the intruder. The authors of [22] presented a zero watermarking blind technique that uses both DWT and DCT to improve the robustness against common and geometric attacks as well as the invisibility of the watermark. Furthermore, the approach aimed to provide a confidential and integrity (privacy) security issues of medical information transmission between hospitals. The technique had aided in the selection of areas of interest (ROI). The embedding process entails applying Arnold transform to the binary watermarking image, then decomposing the image into one layer DWT, and finally computing DCT for the entire LL part to obtain the featured vector. The feature vector with the lowest frequency is chosen, and the sign sequence is obtained.

The experimental results show that JPEG compression and Median Filter attacks have a high level of robustness against different attacks but a low level of weakness. [23] proposed a medical image system for image integrity verification. The signature information is extracted from the ROI or the pixel blocks of the Region of Interest by the system (ROI). The extracted signature is then embedded in the image's non-significant Region of Non-Interest (RONI). The extracted signature is compared to the recomputed signature at three levels of protection: L1, L2, and L3. There is a distinct and independent signature for each integrity level. Level one is concerned with detection, while level two is concerned with localization, and level three is concerned with image degradation approximation. The system is limited to certain types of degradation and modification, such as compression, filtering, rotation, and brightness. However, it did not cover other types of attacks. It does not apply to all tampered images.

The authors of [24] presented a blind zero watermarking approach in the frequency domain. The method is used in medical images and is based on the Discrete Cosine Transform (DCT). The scheme combines a visual feature vector and an encryption technique. To begin, the DCT technique is applied to the medical image, and the 9th lowest frequency coefficients are selected. The sign sequence of low frequency coefficients was then obtained. Based on the HASH function cryptography, they compute the key sequence using the watermark information and the feature vector. The visual properties of the watermark embedding are fully considered by the algorithm, resulting in a low degradation in the watermarked image. The approach provides adequate capacity while remaining simple. It is also highly resistant to cropping and scaling attacks. However, after noise, compressions, rotation, rotation, and translation attacks, the quality of the extracted watermark image is very low.

I.10.2 steganography security applications

Steganography is used in a variety of useful applications, such as material copyright control, improving the robustness of image search engines, and smart IDs (identity cards) in which individuals' details are embedded in their photographs. Other applications include video–audio synchronization, secure data transmission in businesses, TV broadcasting, TCP/IP packets (for example, a unique ID can be embedded into an image to analyze the network traffic of specific users) [25], and checksum embedding [26]. Petitcolas [27] demonstrated some modern applications, one of which was in Medical Imaging Systems, where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions, such as physician, patient's name, address, and other particulars. However, a connection must be maintained between the two as a result, embedding the patient's information

in the image could be a useful safety measure that aids in the resolution of such issues. Steganography would provide the ultimate authentication guarantee that no other security tool could provide. Miaou et al. [28] present a bi-polar multiple-base data hiding LSB embedding technique for electronic patient records. The difference in pixel values between an original image and its JPEG version is used as the number conversion base. Patient data concealment in digital images is also discussed by Nirinjan and Anand [29] and Li et al. [30].

I.10.3 Watermarking, Steganography and Cryptography

The watermarking concept is related with two fields: cryptography and steganography, and the three-concept classified under data security system field Fig. I.3.

Cryptography is a method used to send an encrypted message that only the authorized person can decode it, and when the message is decrypted it is not protected anymore and this is the main difference between cryptography and watermarking.

Steganography used to hide message or an information within another object (image, video, audio) known as a data [31] In order to be undetectable, while the goal of watermarking is to embed a message that cannot be removed.

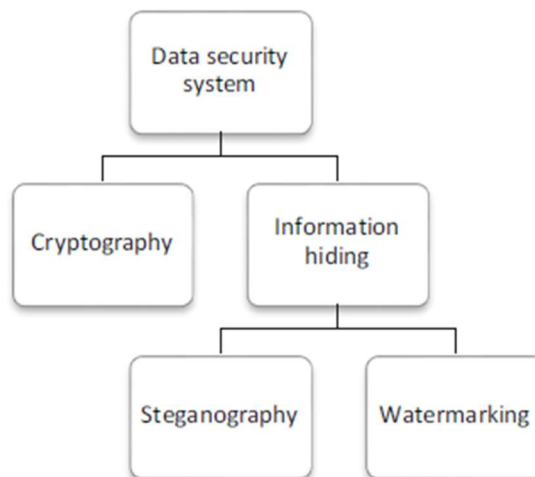


Fig I.3 Data security system field

Conclusion

Images is a chief aspect in health care. Technology evolution in medical image has helped doctors to get an insight into the human anatomy without the necessity to cut the body and to get the best possible diagnosis, treatment, or other surgical procedures by image analysis gained after high-quality resolution and noise removal.

The medical image is one of the most important part in the telemedicine and the health care sector. Therefore, the security of medical image is necessary to prevent the intentional or unintentional distortion. Meanwhile, the confidentiality, the authenticity and the integrity are working together. They can't be separated and each one depends on the other. In the literate review, there are two ways to obtain the security of medical images: "watermarking and meta data (digital signature).in addition Encryption technique are used to increase the security level too".

DICOM security profiles allows encrypting the image by using the DES, DSA and other exciting encryption techniques in the DICOM header. Since the data after decrypting will not be protected. So, it is not easy to verify its integrity, authenticity and reliability. Also, the DICOM security standard doesn't preserve the confidentiality and integrity of the medical image data. Where, its header can be easily removed and a fake header can be regenerated by an attacker. So, watermarking is a solution to ensure the image security through the storage and transmission. This way can provide a standard guarantee of confidentiality and integrity of the data. The watermarking current solutions don't provide efficient techniques to cover the confidentiality, integrity and authenticity of the digital medical data. Besides, the existing approaches don't offer a good compromise between the watermarking requirements "robustness, imperceptibility and capacity" as well as complexity, since we work with real time applications (telemedicine).

The main object of this work is to fill some gaps of the previous solutions and to ensure the security of the medical image while the transmission and storing by providing watermarking solutions with better compromise between the watermarking requirements and cryptography solutions ensuring symmetric key security with less complexity.

II.1 Introduction

In the previous last years, digital document distribution over an open channel using information and communication technology (ICT) has proven to be an indispensable and cost effective method for the dissemination and distribution of digital media files. However, due to malicious attacks/hacking of open channel information, the prevention of copyright violation, ownership identification, and identity theft remains a difficult issue. The primary goal of these attacks/hacking is to modify, or remove the document watermark in order to illegally claim ownership or prevent information transfer to intended recipients. As a result, addressing these critical challenges is an intriguing problem for field researchers. Simmons proposed the classic-model for invisible communication as the prisoner's problem [32] in 1984, as shown in Fig. II.1. The two prisoners in Fig. II.1 want to devise an escape plan, but all communications between them are arbitrated by the warden.

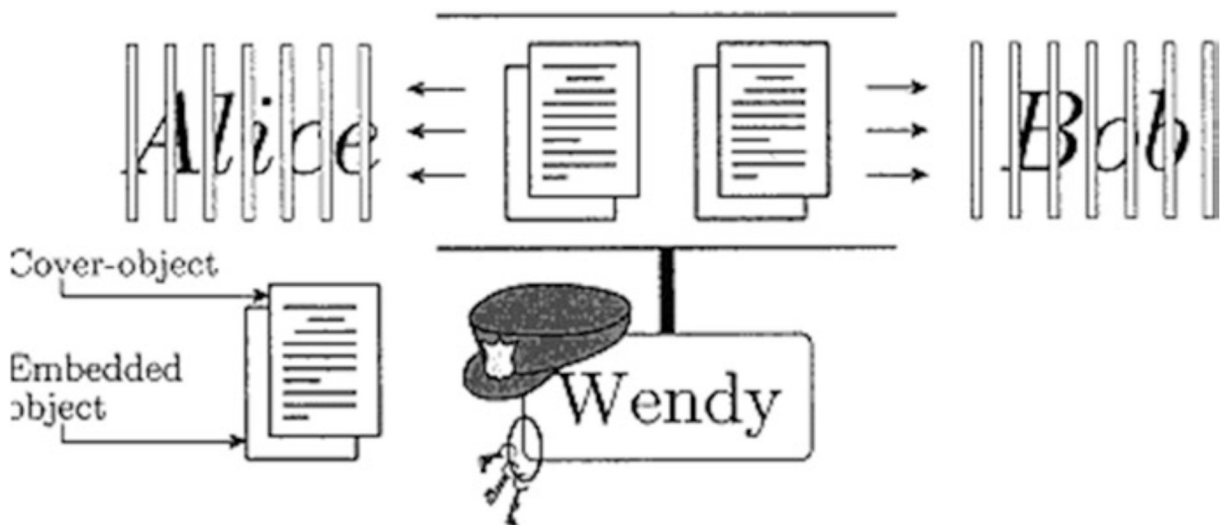


Figure II.1: The prisoner's problem [33]

They are not permitted to communicate using encryption, and if any suspicious communication is detected, the two prisoners will be placed in solitary confinement, preventing any information exchange. As a result, in order to avoid arousing warden suspicion, the prisoners decided to communicate invisibly, and they considered hiding meaningful information in some cover message. To put this into action, one of the inmates drew a picture of a blue cow lying on a green meadow and sent it to another prisoner. As a result, the Warden is unable to perceive the colors of objects in the image that is transmitting some information, which is an example of data concealment. As an evident from the above example, the *data hiding is a technique for*

hiding data within a cover message without causing perceptual distortion for identification, annotation, and copyright. However, the constraints that affect the data hiding process [34] are: the amount of data to be hidden, the need for these data to be invariant under conditions where a cover (host) media is subjected to distortions such as lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. Data hiding techniques are fundamentally divided into two categories: (1) digital watermarking and (2) steganography [35]. The 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 make an assertion about the authenticity and/or originality of the object is known as digital watermarking [36]. The basic concept of digital watermarking is closely related to the steganography (so called covered writing) which focuses on the hidden message bandwidth while hiding 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.

Watermarking has been used for centuries, but the field of digital watermarking and its numerous applications has grown exponentially in the last 30 years as a result of modern developments in multimedia data processing, improvements in digital signal processing, and the availability of high-speed computational platforms. Watermarking has the potential to be used for a variety of purposes, including ownership assertion, fingerprinting, copy prevention/control, secure telemedicine, e-commerce, e-governance, media forensics, digital libraries, web publishing, media file archiving, artificial intelligence [37–39], and digital cinema [40], where a watermark can be embedded in every frame. Because of these intriguing applications of watermarking, it has received special attention in the current work thus it is discussed in depth.

II.2 Importance and Necessity of Watermarking

Even though, cryptography is the most known method that is used to protect digital content however it is not able to facilitate monitoring and handling the content after decryption by the owner. This cryptographic limitation may result in illegal copying, distribution, or misuse of private information. Cryptographic techniques protect content in transit, but no further protection is provided after decryption. Watermarking, which protects the content even after decryption, addresses a major limitation of cryptography. Watermarking techniques embed imperceptible watermarking information into the main content, preventing the watermark from being removed or causing inconvenience to users. A watermark can be created to withstand various procedures such as decryption, re-encryption, compression, and geometrical

manipulations [41]. Telemedicine applications have recently begun to play an important role in the development and use of technology in the medical field.

DICOM (digital imaging and communications in medicine) is a fundamental criterion for communicating electronic patient record (EPR) data. A header containing important patient information is also attached to the medical image file in DICOM. Watermarking can effectively address the protection of this header during transmission and storage to achieve guaranteed security and authenticity [42].

II.3 Classifications of Digital Watermarks

The general classification of watermarking techniques is shown in Figure II.2 [36]. Watermarking methods are classified into four types based on the type of data to be watermarked: text watermarking, image watermarking, audio watermarking, and video watermarking. However, because images have a higher data embedding capacity, the current work focuses on watermarking with images as cover media. Watermarks are classified into three types based on their human perception: visible watermark, Invisible-Robust watermark, Invisible-Fragile watermark and Dual watermark. Visible watermark is a secondary translucent image that is overlaid on top of the primary image. A careful inspection reveals the watermark to a casual viewer. The invisible-strong watermark is embedded in such a way that changes to pixel values are perceptually undetectable, and the watermark can only be recovered using an appropriate decoding mechanism. Any manipulation or modification in the invisible-fragile watermark of the cover would alter or destroy the watermark.

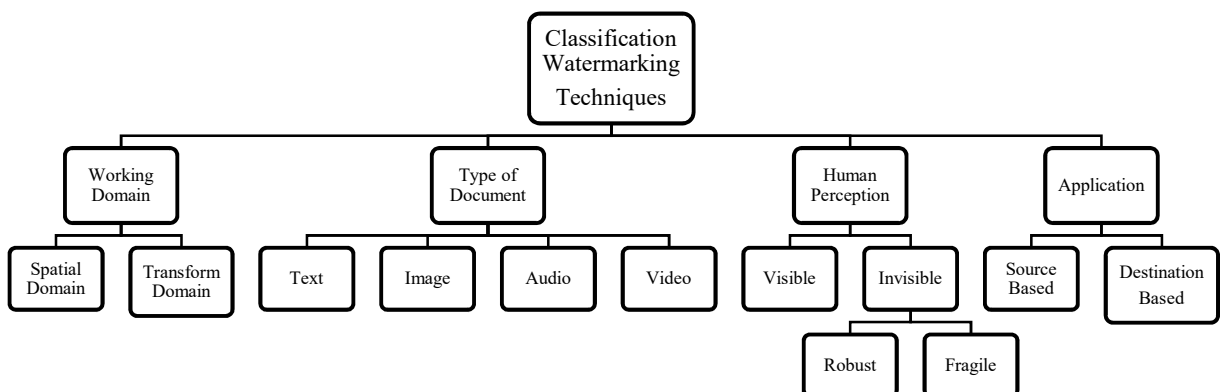


Figure II.2: Classification of watermarking techniques [36]

Dual watermark is a combination of a visible and an invisible watermark [36]. An invisible watermark is used as a backup for the visible watermark in this type of watermark. The watermark could be applied in spatial and transform domains depending on the working domain. The watermark could be source or destination based, depending on the application, with the former preferred for ownership identification or authentication and the latter used for uniquely identifying the buyer. In source-based watermarking, a unique watermark identifying the owner is embedded in all copies of the cover image being distributed, whereas in destination-based watermarking, each distributed copy receives a unique watermark identifying the specific buyer, which is used to trace the buyer in the event of illegal distribution/reselling. Watermarking techniques are further classified as reversible and irreversible. [43, 44].

Reversible watermarking avoids irreversible distortions in the host cover image by using techniques that provide extraction of the watermark from the watermarked cover document. Therefore, these techniques are preferred for medical image watermarking to reduce the probability of incorrect diagnosis.

Reversible watermarking prevents irreversible distortions in the host cover image by employing techniques that allow the watermark to be extracted from the watermarked cover document. As a result, these techniques are preferred for medical image watermarking in order to reduce the likelihood of incorrect diagnosis.

II.4 Potential Characteristics of Digital Watermarks

The key characteristics of digital watermarks [45, 46] are:

1. *Robustness*

If a digital watermark resists a designated class of transformations, it is called robust and thus can be used for copyright protection. The robustness criterion focuses on (1) The presence or absence of watermark after distortion in the data and, (2) Its detection by the watermark detector.

2. *Imperceptibility*

The imperceptibility can be considered as a measure of perceptual transparency of watermark and it refers to the similarity of original and watermarked images.

3. *Capacity*

It is the amount of information that can be embedded in a cover. This amount of information highly depends on the applications such as copyright protection,

fingerprinting, authentication and confidentiality of medical data, as the information to be embedded may be a logo image, a number etc.

4. *Security*

The security of watermark implies that the watermark should be difficult to remove or alter without damaging the cover image. The level of watermark security requirement can vary depending upon the application.

5. *Data-payload*

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

6. *Fragility*

The fragile watermark basically aims at the content authentication. This is reverse of the robustness criterion. The watermarks may be designed to withstand various degrees of acceptable modifications in the watermarks on account of distortions in the media content. Here, watermark differs from a digital signature which requires 100% match.

7. *Computational cost:*

The computational cost basically refers to the cost of embedding the watermark into a cover and extracting it from the digital cover. In some applications, it is important that the embedding process be as fast and simple as possible while the extraction can be more time consuming. In other applications, the speed of extraction is absolutely crucial.

8. *Tamper resistance:*

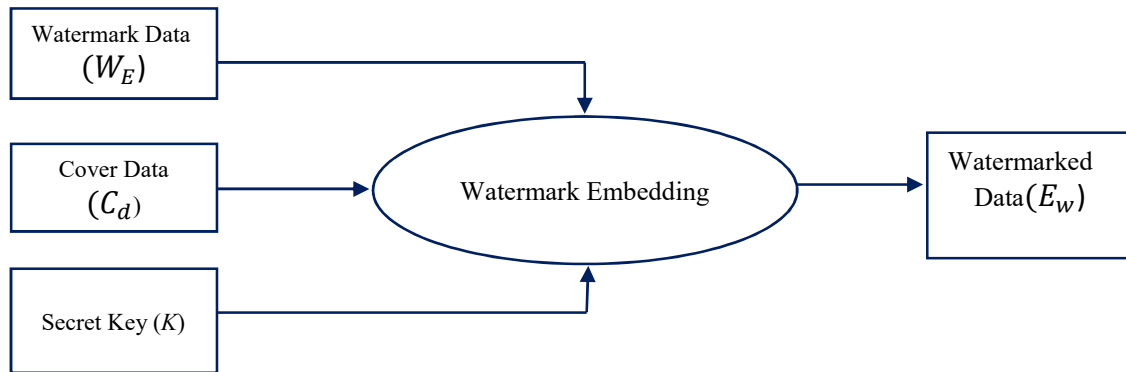
Tamper-detection of watermarks is used to check the authenticity of digital photographs. Watermarks of this type are sensitive to any change of the watermark data; thus, by checking the integrity of the watermark, the system can determine whether or not the watermark has ever been modified or replaced.

II.5 Framework for Watermarking

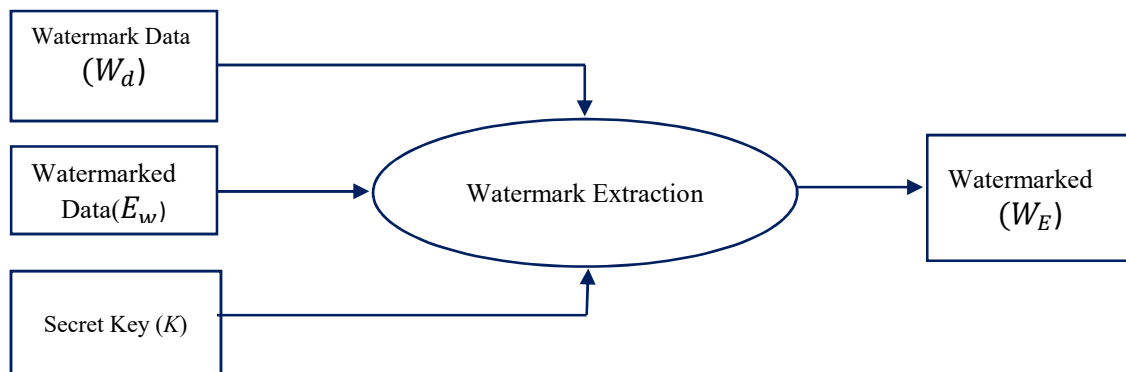
In general, the watermarking system consists of two processes - encoding and extraction process [35] as shown in Fig.II.3. Referring Fig.II.3a it is evident that there are three inputs: a watermark, the original cover media and the optional public or secret key to generate a watermarked image. Figure II.3a depicts the extraction process which takes the input as

watermarked image/original data (cover), secret or public key and test data from which cover image and its proprietorship can be determined [47, 48]. Therefore, from Fig. II.3a, a general watermarked cover image (W) is expressed as the function (F) of watermark data (Wd), a cover data (Cd) and a secret key (K) i.e.

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



(a)



(b)

Figure II.3: The watermark process (a) embedding and (b) extraction [35]

The watermark embedding process is defined as:

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

Further, the watermark extraction process is defined as:

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

II.6 Application of digital image watermarking

The watermarking is applied in many and different fields to achieve and/or to improve the security. The watermarking approach can reach many security goals (copyright protection, transaction and finger print ...). Each goal requires the appropriate properties among those mentioned in the previous section [49] [50]. We can classify the most important applications as follows:

II.6.1 Copyright protection

One of the watermarking goals is to provide *copyright* for media material. It is about embedding the copyright information into the host image. The watermarked image has to resist against different kinds of attacks (removing, modifying, or adding new watermark). The technique proves the copyright owner into the material to avoid non-owners from claiming to be the legal owners of the data. The owner of the material can extract his/her watermark from the watermarked image to prove the right on the watermarked material. The watermarking approach in this application should be robust and invisible. Moreover, this application will not prevent the user from the copy of the digital image [51] [52].

II.6.2 Transaction tracking or fingerprinting

Fingerprinting requires the embedding of a different watermark for each customer. The watermark is usually related to the customer information like the customer identity. It makes it possible to track the images and to find where illegal copies are happening. Moreover, it makes it possible to detect the customer who breaks the rules and conditions of the agreements. This kind of application needs robust and invisible watermarking technique [53] [54].

II.6.3 Authentication

The watermark is applied to the host image in order to verify its *authenticity*. In the extraction phase, the extractor can extract the watermark, then compare the extracted watermark with the original watermark to determine if the received data is authentic or not. These kind of applications deals with fragile and semi-fragile watermarking systems. Moreover, the original watermark it is required during the extraction phase [55] [56].

II.6.4 Integrity

The *integrity* aspects refer to the image safety. The watermark is embedded into the original host. During the transmission process the watermarked image could be attacked (intentional or unintentional). The extractor will extract the embedded watermark and compare with the

original watermark to verify its integrity. Any modification or small change in the watermarked image should be noticeable at the receiver side. This application requires fragile watermarking approach [57] [58].

II.6.5 Tamper detection

Tamper detection is very critical in some fields as telemedicine in order to fight against counterfeiting of images. The hacker tries to tamper the watermarked image in unnoticeable way, where the normal user thinks it is un-tampered. The embedded watermark should be extracted by the authorized user. The user has to know if the image is attacked or tampered and where the tampering happened. It is desirable of the approach to be a reverse approach, which means the technique can recover the original content after the watermark extraction. The watermarking system should be fragile [59] [60] [61].

II.7 Domains of image watermarking

Watermarking based on spread spectrum

The spread spectrum is a technique that is used in radio telecommunications in particular the military to disperse a signal over a wide band frequency so as to make it discreet and resistant to interference [62]. It is clear that this model is immediately applicable to multimedia watermark.

We describe the approach proposed by [63], which is based on a pseudo pre-formatting the data to be embedded by dividing it at the image size. It then generates a random key of the size of the pre-formatted data and then applies a simplistic term binary operator "XOR" of this key and the spread data. It adds the result to the host image for a sharp image.

This is especially interesting because it reveals several fundamental concepts of image watermarking algorithms, such as the spread spectrum, the use of a secret key, amplitude modulation, and so on...

The watermark information is embedded in the host image by the watermarking system. There are numerous methods and techniques for embedding or extracting the watermark. Based on the algorithm and method used to embed the watermark in the host image and extract the embedded watermark from the watermarked image, we can divide watermarking techniques into two categories: spatial domain and transform domain, as shown in Figure II.4 [50], the techniques in each domain will be discussed in the following section.

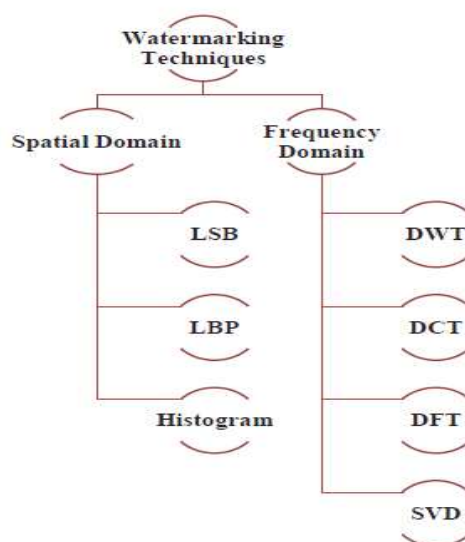


Figure II.4: Watermarking domains

II.7.1 Spatial domain

The spatial domain refers to the fact that the watermark information is embedded directly into the pixels of the host image. The watermark is typically embedded in the least significant bit of the host image. The spatial domain techniques are fast, simple, and have a high capacity. Furthermore, a small watermark can be embedded several times in the original host, so that after the attacks, the authorized user can recover the watermark from the other. When it comes to removing the watermark, the chances of removing all of them is very low [64] [65].

The spatial domain's weakness in geometric attacks, particularly noisy and compression attacks, is that the watermark can be easily changed by a third party [64]. In the spatial domain, there are numerous watermarking approaches. In the following section, we will go over some of the most common techniques.

II.7.1.1 Least significant bit (LSB)

The signal sample contains the Least Significant Bit (LSB). It is exchanged in the input signal by embedding a data bit in the pixels' least significant bit. The human eye cannot detect LSB. The basic idea behind LSB is to present the pixel value in binary form in 8 bits, then replace the LSB value with the watermark value: 0 turns into 1, and 1 turns into 0. The altered binary values are then converted into decimal pixel values. In reality, the change is to add or subtract one from the bit value. This change will have no effect on image quality and will be imperceptible. This technique is extremely sensitive to changes and vulnerable to attacks such as noise, rotation, compression, or even the act of removing all the least bits. [66] [67] [68]. The bit position is assigned from 1 to N, where N refers to the number of bits used to represent the data. LSB will be the bit number 1 while the N is the Most Significant Bit (MSB) as it is presented in the in the following figure (figure II.5).

Bit Position

Original value $(149)_{10}$

Watermarked value $(148)_{10}$

Table II.1: LSB watermarking approach

N(MSB)						2	1(LSB)
1	0	P	1	0	1	0	1
1	0	0	1	0	1	0	0

An invisible watermarking technique based on the LSB was presented by the authors of [69]. The height and width of the original image and the watermark image, and then scaling the original with scaling factor. After that, they generate a watermark object are calculated by the approach steps. After that, embedding the watermark LSB set into the original LSB set.

II.7.1.2 Local binary pattern (LBP)

This method is used for analyzing and classifying texture [70] The image is divided into non-overlapping square blocks in LBP watermarking, and the local pixel difference is calculated by calculating the spatial relative between the significant pixel and its adjacent pixel in each block. The local pixel difference is used for watermark embedding and extraction and is considered the threshold. The advantages of LBP over LSB are its resistance to luminance modification, difference alteration, and other attacks, as well as its vulnerability to other attacks such as filtering and blurring. LBP is useful in semi-fragile watermarking methods [71]. The general idea of local binary pattern of eight neighbors are highlighted in figure II.5. while the embedding and extraction place is D_8 , the LBP of D_8 is calculated from its neighbors.

D_1	D_8	D_7
D_2	D_8	D_6
D_3	D_4	D_5

Figure II.5: Local Binary Pattern of eight neighbors

In [72], a framework based on the Local Binary Pattern (LBP) in order to embed multi-level watermarking is proposed. The approach divided the image into non-overlapping 3 by 3 regions. Each local region is divided into three items: a vector containing the central pixel values, a vector containing the magnitude obtained from the differences between the central pixel and its neighbors and a vector of the sign value of the differences. The obtained vector's values are based on the Local Binary Pattern (LBP). The watermark is embedded by changing of the sign vector value in a local region. The approach was robust against some kinds of attacks like noise, contrast adjustment, luminance modification.

II.7.2 Frequency domain

The frequency watermarking techniques are considered more robust than spatial watermarking techniques. Frequency domain or transform domain is more complex in computational complexity than spatial domain. The embedding and extraction process of all watermarking approaches in the frequency domain can be described as follows:

- The embedding process deals with the image decomposition, watermark embedding and reversible image decomposing.
- The extraction process deals with the image decomposition, watermark extraction and reversible image decomposition.

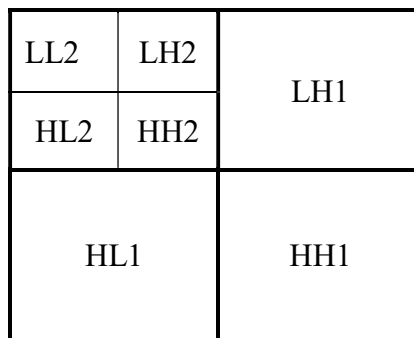
The most known watermarking techniques in the frequency domain are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT). They will be discussed in details in the following section.

II.7.2.1 Discrete wavelet transform (DWT)

Wavelets are mathematical functions. Discrete wavelet transform is a mathematical implementation for a hierarchical decomposition of an image. The transform is based on the waves called wavelets. The wavelet provides the frequency and the spatial explanation of the image. DWT does a multiresolution decomposition description of the image. The decomposition procedure splits the image into low and high frequencies. The low frequencies contain the most important part of image information, while the high frequencies comprise the other information details. The watermark can be embedded in low or high frequency. Low frequency provides a good robustness, but with a degradation of the host image after embedding. Moreover, it is desirable to embed in the high frequency because it will not be noticeable by the human eye, but the robustness is low. Meanwhile, the wavelet transforms deals with the compression, it provides a good robustness against JPEG attacks and filtering because the watermark is distributed through the image and is not located in specific pixels.

For one level DWT, the image is decomposed into four sub-bands: Low-Low (LL), Low-High (LH), High-Low (HL) and High –High (HH). In the case of two levels DWT decomposition, it produces another four sub-sub-band from the sub-band. We can reverse the approach by applying the inverse wavelet

Figure II.6 presents the second level wavelet



decomposition (IDWT).
general diagram of the decomposition.

Figure II.6: 2-level- DWT decomposition

The general algorithm used for embedding the watermark in the original image is represented by the following formula:

$$iw_n = i_n + s * w_n \tag{II.4}$$

where n is the watermark strength factor, s is the watermark embedding position, iw_n is the

watermarked image, i_n is the original image and w_n is the watermark image.

The DWT schemes advantages comparing with the other techniques in the frequency domain are: good space frequency localization, multi-resolution properties, multi-scale analysis, flexible and simply adaptability to image, low complexity and a fast computation.

In [73], Ahmad et al. proposed non-blind watermarking techniques in the frequency domain in three levels DWT. The watermark is embedded in the low frequency sub-band using blending technique. In the embedding phase, three level DWT is applied to the original and the watermark image. Then, they embed the watermark in the original image by using the linear interpolation (II.5)

$$i_{wl3} = k * i_{l3} + q * w_{l3} \quad (II.5)$$

Where i_{wi} is the third level DWT watermarked image, k and q are factors $k, q \in]0,1[$, w_{i3} is the third level DWT watermark, i_{i3} is the third level DWT original image.

The inverse DWT (IDWT) is applied to obtain the watermarked image. In the extraction phase, three level DWT is applied to the watermarked image and the original image. Then, by using the linear interpolation (II.6) can retrieve the embedded watermark or by (II.7) to retrieve the original image.

$$R_{wi} = i_{wl3} - k * i_{l3} \quad (II.6)$$

$$R_{il} = i_{wl3} - q * w_{l3} \quad (II.7)$$

where R_{wi3} and R_{il3} are the low frequency retrieved watermark, low frequency retrieved original image, respectively.

The approach provides acceptable imperceptibility if q is close to zero and k is close to one. If the extractor wants to retrieve the watermark image, the original image is required. If he/she wants to retrieve the original image, the original watermark is required. The approach is robust against frequent attacks, but it has low robustness against noise attacks.

In the work of [74], it is proposed a blind watermarking technique. The watermark is embedded as a secrete medical information into host color image using DWT. The watermark is embedded in the low level (LL) sub bands of the blue channel of the original image. The embedding process is: decomposition of the host image into three color channels, embedding of the watermark into the LL sub band of the blue color channel of the host image based on discrete wavelet transforms (DWT) three levels. Then, they compressed the data with Zigzag techniques to convert two dimensions to one-dimension image. Finally, inverse DWT is applied to obtain

the perceptual watermarked image. In the extraction process, the watermarked image is decomposed based on DWT, the LL sub-band is divided into three color channels. The blue channel is chosen. Then inverse Zigzag technique is applied to obtain two-dimension blue channel image. Finally, inverse DWT is applied to achieve the watermark image. The experimental result shows that the method is imperceptible and gives a high quality without attacks. But it also shows that the method has a low robustness against cropping, filtering and noising attacks. [75] proposed a digital image watermarking technique in the frequency domain based on DWT. The original image and the watermark image are decomposed into two levels DWT. Then, they calculated the image feature matrix and applied hash function for each sub-band (LL, LH, HL, HH).

Then, based on XOR function, they embedded the watermark into the original image. Finally, the inverse DWT is applied. The image features are analyzed into its factored form using DWT. The produced coefficient data are quantized to obtain the image hash. The proposed approach achieved high PSNR (good quality) with low computational complexity and execution time.

II.7.2.2 Discrete cosine transform (DCT)

DCT is used to convert a signal from the spatial domain to the frequency domain [76]. It has a high level of robustness when compared to the JPEG standard for image compression [77]. It divides the image into non-overlapping $m \times m$ blocks, with the left top coefficient representing the DC coefficient value and the others representing the AC coefficients [78]. The block size is normally 8 by 8 items. Low frequencies are more sensitive to the human eye than high frequencies. DCT divides the image into three frequency bands: low, medium, and high frequency.

The low frequency contains the majority of the image's information, while the high frequency contains the image's details. When the watermark is inserted at a low frequency, it is robust but visible. Meanwhile, if it is inserted at a high frequency, the watermark will be visible but weaker. To avoid image degradation and to switch between imperceptibility and robustness, embed the watermark in the middle frequency band [79]. Signal's DCT coefficient transformation is represented by equation (II.8), while the inverse discrete cosine transform is represented by equation (2.9). [78].

$$F(u, v) = \frac{2}{N} c(u)c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x, y) \cos \left[\frac{\pi}{N} u \left(x + \frac{1}{2} \right) \right] \cos \left[\frac{\pi}{N} v \left(y + \frac{1}{2} \right) \right] \quad (\text{II.8})$$

$$F(x, y) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} c(u)c(v)F(u, v) \cos \left[\frac{\pi}{N} u \left(x + \frac{1}{2} \right) \right] \cos \left[\frac{\pi}{N} v \left(y + \frac{1}{2} \right) \right] \quad (\text{II.9})$$

Where $c(u), c(v) = (2)^{-\frac{1}{2}}$ for $u, v = 0$. And $c(u), c(v) = 1$ for $u, v = 1, 2, \dots, n-1$. $p(x, y)$ is the pixel value at position (x, y) .

Figure II.7 illustrates the general idea of the obtained image matrix after applying the DCT transform.

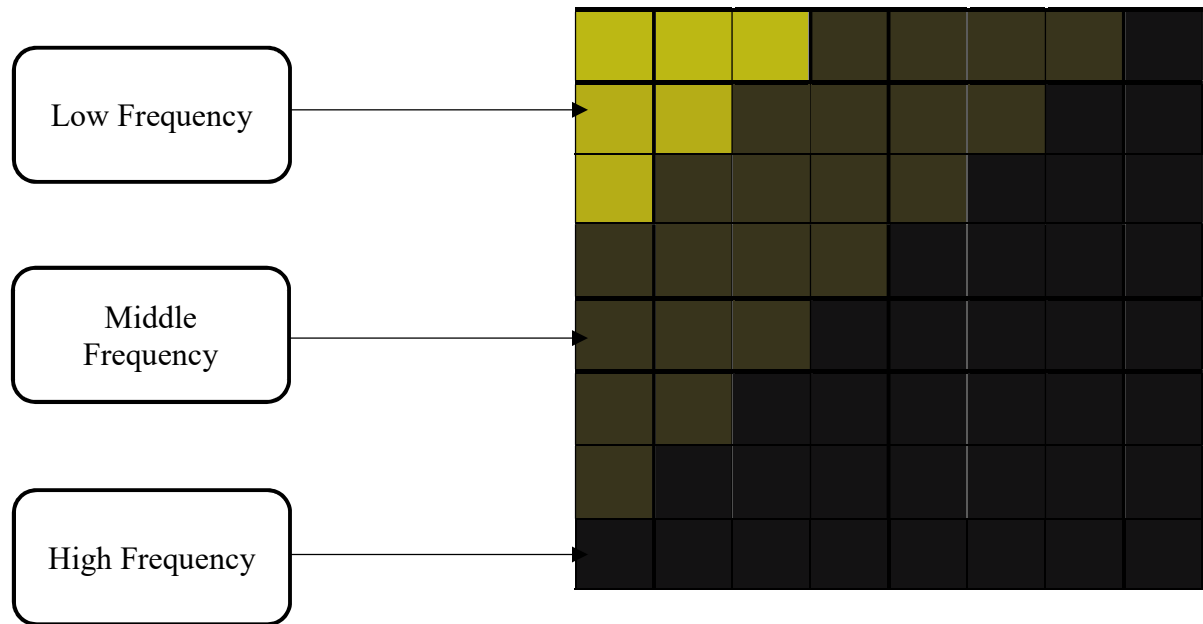


Figure II.7: Image DCT frequency coefficients.

The DWT transform is more suitable to human visual system than DCT transform. Also, DWT provides a multi-resolution decomposition, which can be shown at different levels of resolution and sequential procedures from low to high resolution. The DCT is based on a block which is not the case for DWT. Whereas, a higher compression ratio will affect in the blocks, and the visual artifacts are less evident in DWT than DCT. Meanwhile, DCT is a fully transforms frame which means any modification will be noticeable through the whole image while in DWT it is noticeable only locally [80]. The work in [81] proposed a blind zero watermarking approach on the medical image features based on DCT. In the process the original image is transformed to DCT coefficients, then the 9 lowest frequencies are chosen: $F(1,1), \dots, F(1,9)$. The value of low frequency coefficient is changed after attacks, but the vector of the signs of the coefficients remained unchanged even with strong geometric attacks. The feature vector is then generated. After that, watermarking and feature vector are used to generate the key sequence. The binary

key sequence is computed by a HASH function. The key should be stored for using in the extraction process. One is used to represent positive or zero coefficient value while zero is used to represent a negative value for coefficients. In the extraction phase, the feature vector is generated. It consists of the signs sequence of the DCT coefficients. Then, the watermark is extracted by using the embedding key is extracted. The experimental results prove that the algorithm was robust and could detect the watermark without attacks, and with some common attacks (non-geometric attacks). But in the case of noise attacks, the image quality is not acceptable where the PSNR is around 10. In case of the filter attacks, the PSNR is around 20. Also, for JPEG attacks the PSNR is around 20. In geometric attacks, such as rotation and translation attacks PSNR are respectively around 12 and 13 dB. Moreover, the method provides a satisfying capacity; the computational complexity and the memory use are low. The authors in [82] proposed a novel blind watermarking technique based on the DC components in the spatial domain. They merged the frequency and spatial domains in order to get better robustness and security for color host image. The proposed algorithm keeps the distribution features of the frequency coefficients and it has avoided the error resulting from the frequency transformation. The embedding steps were converting the image from RGB color into YCrCb color. Then, after obtaining the luminance Y of the YCrCb, dividing it into overlapped 8×8 -pixel blocks. The method computes the DC coefficient $C_{i,j}(0,0)$ of each block. Based on the watermark information it decides the modifying magnitudes T1, T2. The possibility quantization can be computed by modifying magnitude T1, T2 and calculating the value for watermark embedding in DC coefficients for each block. Finally, the watermarked image is converted from YCbCr color into RGB color. In the extraction phase, the watermarked image is converted into YCrCb. Then, the luminance Y is obtained, and divided into 8×8 blocks. Next, the DC coefficient is obtained and the watermark value is computed. Finally, the inverse Arnold transform is applied to obtain the extracted watermark image. SSIM is used to measure the imperceptibility between the host image and the watermarked image (HVS). The proposed algorithm had high watermark invisibility and robustness against non-geometric attacks like JPEG compression and filter and geometric attacks like cropping, scaling, and rotation.

II.7.2.3 Singular value decomposition (SVD)

Singular Value Decomposition SVD is another frequency transformation method. It is a linear arithmetical implementation to decompose a matrix into its eigenvectors and eigenvalues. It has been widely used in the compression field cause its capability to provide the low rank calculation by alteration of an image into a new representation [83]. The SVD can

decompose a set of connected variables into unconnected variables. Moreover, singular values of an image are satisfying constancy, that is, when a small degradation is added to an image, its SV's do not modify significantly; and SV's represent mainly algebraic image features [84]. Let us denote the image as I . I is a square image, N and M are the image dimensions. The SVD of I is defined as:

$$I_{N \times M} = U_{N \times M} * S_{N \times M} * V_{M \times N}^T \quad (\text{II.10})$$

U and V are orthogonal matrices, and S is a diagonal matrix. The left eigenvalues (left SVs) are represented by matrix U , the right eigenvalues (right SVs) are represented by matrix V , and the eigenvalues are represented by matrix S . (SVs). These singular values are arranged on the diagonal in descending order, with the highest value at the top left of the matrix and the lowest value at the bottom. In watermarking schemes, the inverse SVD is applied after SVD decomposition and embedding the watermark in a chosen matrix to produce a meaningful image. The authors of [85] proposed a blind reversible watermarking scheme to ensure the copyright protection of medical images. The method employs the Recursive Dither Modulation (RDM) and Differential Evolution (DE) optimization techniques. They added a second watermark to the original image. Steps for embedding a watermark divide the original image into blocks. The scrambling algorithm is then applied to both the signature and logo data, along with an encryption algorithm, to generate encrypted watermark text. Each block was subjected to a two-level wavelet transform, which selected the low frequency coefficients. For each block, SVD was applied to the low frequency wavelet coefficient. The watermark was embedded through quantization using the RDM method. Following the embedding, the watermarked image was obtained using inverse SVD and inverse DWT. The watermarked image was divided into blocks during the extraction phase. Then, a two-level DWT was used. To generate the singular values, the SVD algorithm was used in the low frequency blocks. The singular values are then normalized, and the message is shuffled again, reshuffling the extract shuffled message. This last one was used to generate the watermark. The authors struck an appropriate balance between robustness, imperceptibility, and capacity. The algorithm is computationally complex. Benhocine [86] proposed a new implementation of the SVD technique in an image watermarking approach's embedding and extraction process. The authors intended for it to be highly resistant to geometric and non-geometric attacks. They included the watermark in three SVD cases. The first case involved embedding the watermark in each of the three SVD matrices (U , S , V). The watermark was then embedded in U and V matrices in the second case. The third

scenario involved embedding the watermark in a S matrix. The linear interpolation (II.11) is used for the embedding.

$$SVD_{iw} = (1 - t)SVD_w + t * SVD_i \quad (II.11)$$

where SVD represents the S, V and U matrices of the watermarked image, SVD_w represents S, V and U matrices of the watermark image SVD_i represents S, V and U matrices of the original image.

$$t \in]0,1[.$$

For the extraction process, it was done using the following linear interpolation (II.12)

$$SVD_{wa} = \frac{1}{t}SVD_{wi} - \frac{1-t}{t} * SVD_{iwa} \quad (II.12)$$

Where SVD_{wa} represents the S, V and U matrices of the extracted watermark image. SVD_{wi} represents S, V and U matrices of the original watermark image. SVD_{iwa} represents S, V and U matrices of the watermarked image. The experimental results showed the robustness of the approach. Moreover, the watermark was imperceptible when t factor was close to one. The best quality to embed the watermark was in the S matrix.

Some of the research works hybrid the techniques in the same domain or in different domains. For example, [87] and [88] hybrid DWT and DCT in the transform domain. The work of [89] combines DWT, DCT and SVD, while the works in [90], [91] combined the spatial and frequency domain into image watermarking approaches.

Types of Processing	Advantages	Disadvantages
Spatial Domain	Comparatively simple and faster operation	Vulnerable to compression, geometric distortion, and Filtering
Frequency Domain	Compression compatible and robust against many geometric distortions (e.g., rotation, scaling, translation, cropping) and Filtering	Comparatively higher computational time and complexity

Table II.2: Difference between Spatial domain and Frequency domain

II.8 Digital Watermarking Attacks and Benchmark Tools

In recent years, digital image watermarking has become one of the most widely used techniques for preventing copyright infringement, ownership identification, and identity theft. However, due to malicious attacks/hacking of open channel information, the robustness/security of the watermark in a medical application have been challenging issues. [95]. The aim behind attacks can be modifying, or even deleting the document watermark from its cover data to claim ownership or preventing the information transfer to intended recipients illegally.

II.8.1 Watermarking Attacks

There are several types of malicious attacks that result in the partial or complete destruction of the embed identification key and necessitate the use of a more advanced watermarking scheme. [92, 95–98]. Figure II.8 depicts the potential attacks on watermarking systems. The following are the major attacks:

1. Active/Removal Attacks: In this type of attack, the hacker tries deliberately to remove the watermark or simply make it undetectable. They are aimed at distorting a hidden watermark beyond recognition. The active attacks include Analytical de-noising, lossy compression, quantization, re-modulation, collusion and averaging attacks. This is a big issue in copyright protection, fingerprinting or copy control for example.

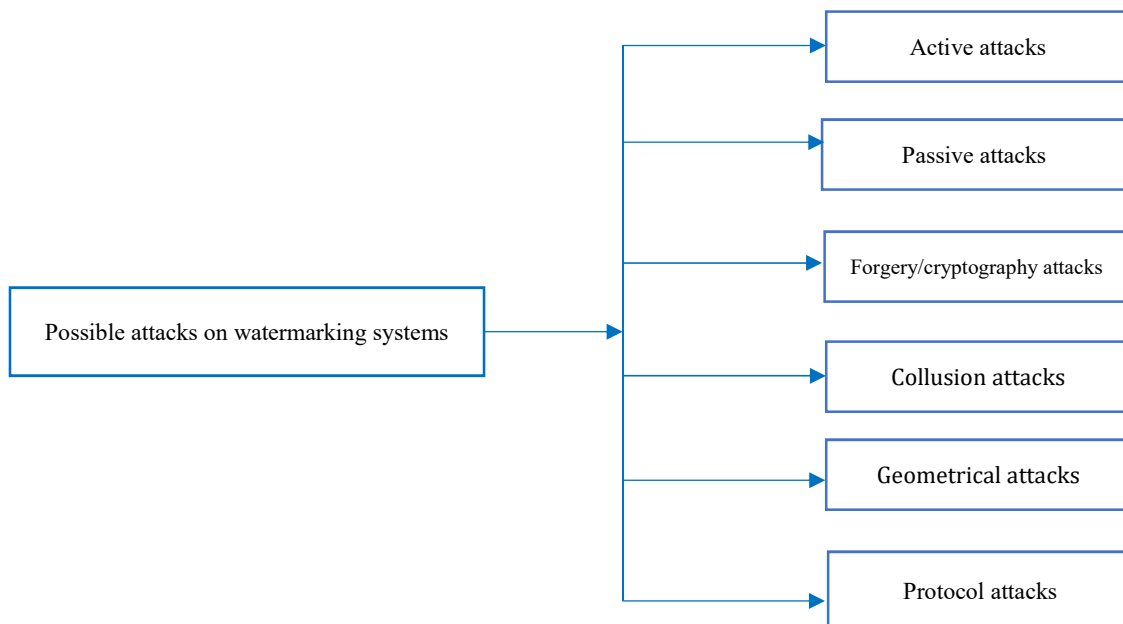


Figure II.8: Classification of possible attacks in digital watermarking

2. Passive Attacks: Hacker tries to determine whether there is a watermark and identify it. However, no damage or removal is done. As the reader should understand, protection against

passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one wants to grant.

3. *Forgery/Cryptography Attacks:* This is another type of active attacks. In such attacks, the hacker embeds a new, valid watermark rather than removing one. This will help him to manipulate the protected data as he wants and then, re-implant a new given key to replace the destructed one, thus making the corrupted image seems genuine. One of the similar techniques in this category brute force attacks used in cryptography which aim to finds hidden information through an exhaustive search. For these types of attacks, it is very important to use a key of secure length as reported in [95]. The Oracle attack is the same category of the cryptographic attacks in which a non-watermarked image is created when a watermark detector device is available.

4. *Collusion Attacks:* In such attacks, the intention of the hacker is the same as for the active attacks but the approach is slightly different. The attacker uses many instances of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in finger printing applications but is not widely spread because the attacker should be able to access several copies of the same data and that the number needed can be very important. Collusion Attacks should be considered because if the attacker has access to more than one copy of watermarked image, the user can predict/remove the watermarked data by colluding them given key to replace the destructed one, thus making the corrupted image seem genuine.

5. *Geometrical Attacks:* The goal of geometrical attacks is to change/distort the hidden watermark by modifying the stego data spatially or temporally. The watermark detector loses synchronization with the hidden watermark as a result of this type of active attack. The popular integrated software for geometrical attacks is Unzign and Stirmark.

6. *Protocol Attacks:* The goal of these types of passive attacks is to attack the concept of the watermarking application rather than destroy or disable detection of the hidden watermark through local or global data manipulation. The concept of initial protocol attacks was abandoned. The other type of protocol attack is a copy attack, which involves copying a watermark from one image to another without knowing the key used for watermark embedding in order to create ambiguity about the true ownership of data.

II.8.2 Benchmark Tools for Image Watermarking

Digital watermarking algorithms Benchmarking is the process of comparing and evaluating their performance under a fair and normally (semi-)automated environment [99]. The most useful benchmarking tools for watermarking are StirMark [100– b], Checkmark [c,

d], Optimark [e, f] and Certimark [g]. As reported in [99] Stir-Mark benchmark is the most popular and excellent software tool that is used to identify the robustness performance of the different watermarking systems. This tool simulates various common attacks on image watermarking algorithms. Algorithms that do not withstand Stir-Mark attacks should be considered insecure. Unfortunately, it does not accurately model the watermarking process and thus has a limited ability to impair sophisticated image watermarking techniques. Furthermore, the Stir-Mark benchmark tool is heavily weighted toward geometric transformations, which do not take prior knowledge about the watermark into account. [w]. Therefore, Pereira et al. [d] developed another benchmark tool ‘Checkmark’. This tool is essentially an improved version of Stirmark with the following significant changes. [99]:

1. The Checkmark tool includes Wiener filtering, soft shrinkage, hard thresholding, Copy, Template removal and JPEG 2000 as new attacks,

2. Weighted PSNR and Watson’s metric are included instead of just PSNT to determine the visual quality of the image.

3. The checkmark tool is implemented in MATLAB; however, the Stirmark is implemented in C++. Another important benchmark tool is Optimark [e, f] which is a benchmarking software package for image watermarking algorithms providing a graphical user interface (GUI) implemented in C/C++. To use optimark determine the performance of watermarking algorithm, users may select a set of test images, define different watermark embedding keys and messages for multiple trials of the watermarking detector and decoder, and select a set of attacks among different types of attacks and its combinations. Further, it allows the assessment of several statistical characteristics of an image watermarking algorithm. The Certimark benchmark tool was developed by EU-funded research project in 2000–2002 [99]. Objective of this tool is to design a benchmarking collection module which allows users to assess the suitability and to set application scenarios for their needs, and to set up a standard certification process for watermarking technologies [g]. Unfortunately, source codes are not publicly available for this tool. In addition to that some researcher proposed benchmark tool based on web system [h–m], mesh benchmark [n] and OR-benchmark tool [99] for evaluating the performance of watermarking algorithms. The brief comparison of the above benchmarking tool has been discussed detail in [99].

II.9 Essential Requirements for Medical Image Watermarking

In recent times, medical images have played an important role in instant diagnosis, understanding of critical diseases, and avoiding misdiagnosis in tele-medicine, tele-ophthalmology, tele-diagnosis, and tele-consultancy services. Furthermore, medical identity theft is a major security concern in telemedicine. [o, p]. Robert Siciliano, CEO of IDTheftSecurity.com, an identity theft expert, says, that would be a big fat yes. In terms of medical identity theft, it's almost like the ideal crime. The long-distance nature of this type of treatment contributes to the overall anonymity. [q]. Medical images contain sensitive information, and when they are transmitted over an unsecured network, they are vulnerable to corruption from noisy transmission channels and attacks by hackers or malicious individuals. These attacks may include obtaining sensitive patient information, changing patient information in the image header, and tampering with image pixel content. Furthermore, medical identity theft is a growing and dangerous crime, and an identity theft resource center conducted a survey that revealed that medical-related identity theft accounted for nearly half of all identity thefts reported in the United States in 2013, according to USA Today. [r]. These demand development of secure medical data/image watermarking schemes. Figure II.9 shows some potential advantages of medical image watermarking. The main advantages of the medical image watermarking [s–v] are:

1. Because the patient record is embedded within the image, storing the medical image and the patient record together requires less storage space.
2. Reduced bandwidth requirement during transmission because the additional bandwidth requirement for metadata transmission can be avoided if the data is hidden in the image itself.

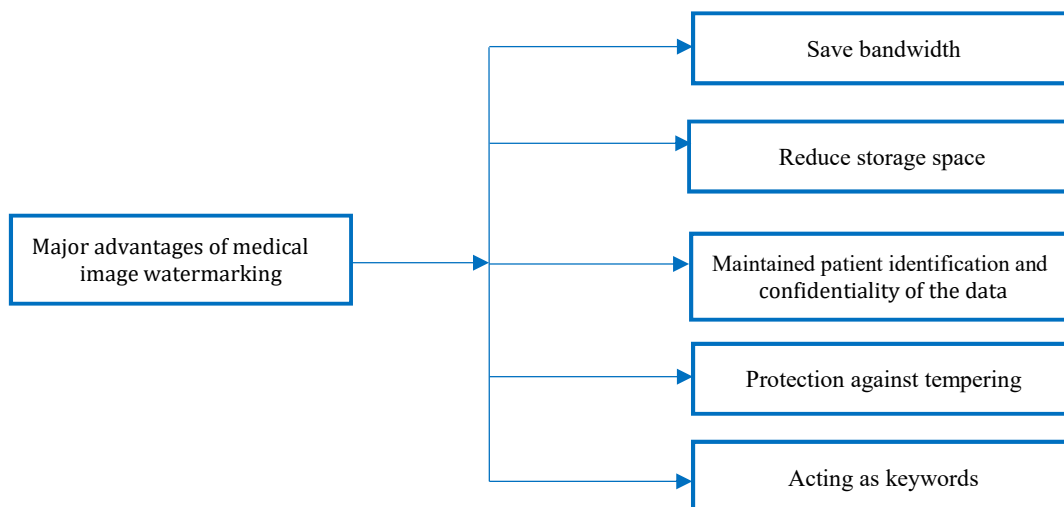


Figure II.9: Main advantages of medical image watermarking

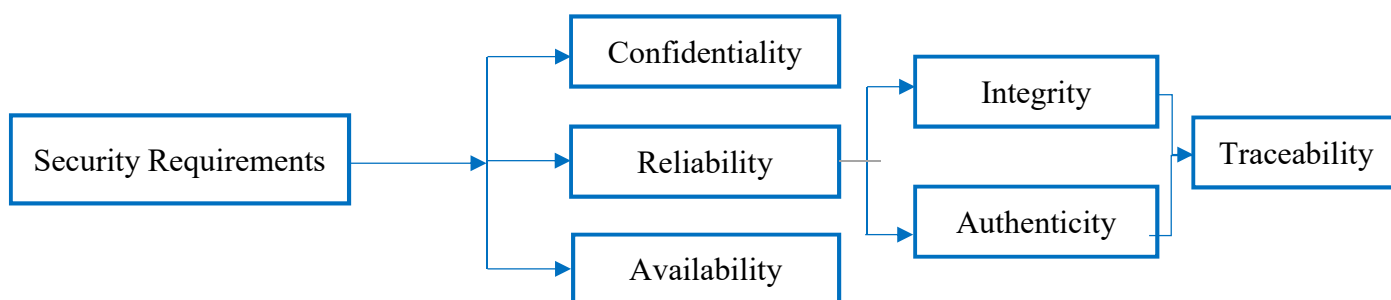


Figure II.10: Major security requirements for EPR data [x]

3. Because the patient data is hidden in the cover image, ownership identification and confidentiality are preserved

4. Protection against tampering because the consequences of tampered medical data can cost a life due to incorrect diagnosis.

5. Hidden watermarks can act as keywords, allowing for efficient archiving and data retrieval from querying mechanisms. Furthermore, it offers a valuable solution to potential problems such as medical data management and distribution. [w].

However, when embedding additional data within medical images, extreme caution is required because the additional information must not degrade image quality. The exchange of electronic patient record (EPR) data over unsecured channels demanded a high level of security. As shown in Fig. II.10, it consists of three mandatory security requirements [x]:

1. Confidentiality i.e. only the authorized users have to access the information

2. Reliability has two important outcomes: (a) integrity—the information has not been tampered with by unauthorized individuals; and (b) authentication—proof that the information does indeed belong to the correct source. Further, the traceability is an important component of the reliability and use to trace the information along its distribution.

3. The availability of an information system refers to its ability to be used by authorized users under normal scheduled conditions of access and exercise. The most important issues concerning EPR data exchange via unsecured channels are authentication, integration, and confidentiality. [s, x]. If a suitable watermark is used, all these requirements will be fulfilled

II.10 Performance Measures

The performance of a medical image watermarking algorithms is mainly evaluated on the basis of its *imperceptibility* and *robustness*.

II.10.1 Mean Square Error (MSE)

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

$$MSE = \frac{1}{X*Y} \sum_{i=1}^X \sum_{j=1}^Y (I_{ij} - W_{ij})^2 \quad (II.13)$$

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

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

Peak Signal to Noise Ratio is a parameter that measures imperceptibility (PSNR). A higher PSNR indicates that the watermarked image is more similar to the original image, implying that the watermark is less noticeable. In general, the watermarked image with PSNR value more than 28 dB is acceptable [z]. The PSNR is defined as:

$$PSNR = 10 \log \frac{(255)^2}{MSE} \quad (II.14)$$

II.10.3 Weighted Peak Signal to Noise Ratio (WPSNR)

The WPSNR is modified version of the PSNR [z]. The WPSNR defined as:

$$WPSNR = 10 \log_{10} \frac{(255)^2}{NVF * MSE} \quad (II.15)$$

where the *noise visibility function (NVF)* depends on a texture masking function. Its values range from zero (for extremely textured areas) to one (for smooth areas of an image).

II.10.4 Universal Image Quality Index

Wang and Bovik [z.]. They define a universal image quality index as a significant performance parameter for determining image distortion as a function of correlation loss, luminance distortion, and contrast distortion. The image distortion is significantly better determined by the Universal image quality index parameter than by other image distortion metrics such as MSE. Suppose X is the original image and Y is possibly distorted image whereas,

$X = \{x_i, i = 1, 2, 3, \dots, N\}$ and $Y = \{y_i, i = 1, 2, 3, \dots, N\}$. The universal image quality index is defined as:

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma_x^2 + \sigma_y^2)(\bar{x}^2 + \bar{y}^2)} \quad (II.16)$$

$$\text{Where } \bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \text{ and } \bar{y} = \frac{1}{N} \sum_{i=1}^N y_i, \sigma_x^2 = \frac{1}{N-1} \sum_{i=1}^N (x_i - \bar{x})^2$$

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

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

$$Q = \left\{ \begin{array}{l} \text{loss of correlation } \left\{ \frac{\sigma_{xy}}{\sigma_x \sigma_y} \right\} \cdot \text{luminance distortion } \left\{ \frac{2\bar{x}\bar{y}}{(\bar{x})^2 + (\bar{y})^2} \right\} \\ \cdot \text{contrast distortion } \left\{ \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \right\} \end{array} \right\}$$

These components define as:

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

II.10.5 Structural Similarity Index Measure (SSIM)

The SSIM [aa] can be defined as:

$$SSIM(x, y) = f(I(x, y), c(x, y), s(x, y)) \quad (II.17)$$

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

II.10.6 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 [ab].

$$NC = \sum_{X=1}^{i=1} \sum_{Y=1}^{j=1} (W_{Original_{ij}} * W_{recovered_{ij}}) / \sum_{X=1}^{i=1} \sum_{Y=1}^{j=1} W_{original_{ij}}^2 \quad (II.18)$$

Where $W_{Original_{ij}}$ is a pixel of the original/hidden watermark of size $X \times Y$ and $W_{recovered_{ij}}$ is a pixel of the recovered watermark of size $X \times Y$.

II.10.7 Bit Error Rate (BER)

The BER is defined as the ratio of the number of incorrectly decoded bits and total number of bits [ab]. This parameter is suitable for random binary sequence watermark. Ideally BER value should be equal to 0.

$$BER = (\text{Number of incorrectly decoded bits}) / (\text{Total number of bits}) \quad (II.19)$$

Conclusion

This chapter deals with some basic spatial and transform domain techniques. Then the important performance parameters for medical and digital image watermarking. It contains peak signal to noise ratio (PNSR), weighted peak signal to noise ratio (WPSNR), Universal image quality index, Structural similarity index measure (SSIM), normalized correlation (NC), and bit error rate (BER). Furthermore, a small description of various types of attacks and important benchmarking instruments along with their performance comparison for digital image watermarking was presented. It is observed that the types of attacks have a crucial impact on the performance of efficient and robust watermarking algorithm (s). Furthermore, the improvements of the efficient benchmarking instruments are necessary to require with rich features in near future. But, the available benchmarking tools are insufficient.

III.1 Introduction

According to image domain, the watermark could be applied in spatial and transform domain. In the transform domain techniques, the data is embedded by modulating the coefficients of a transform discrete wavelet transform (DWT), discrete cosine transform (DCT), singular value decomposition (SVD) and discrete Fourier transform (DFT). However, the transform domain watermarking techniques are computationally complex but they provide better robustness of watermarked data. In this section we proposed two approaches of medical image watermarking. The first method is using two levels DWT transform domain sub-band on which an SVD decomposition is made, In the second approach only three levels DWT transform domain sub-band is used without SVD decomposition. Simulation and experimental results are discussed below.

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

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 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

Cover Image: Q: ultrasound.jpg (UT)

Watermark Image: I_W: logo1.jpg

I: Read the cover image

I1_W: Read the watermark image

alpha: Scale factor

DWT and SVD: Transform domain techniques

Haar: Wavelet filters

[LL1,HL1,LH1,HH1]: First level DWT coefficients for cover image

[LL2,HL2,LH2,HH2]: Second level DWT coefficients for cover image

STEP 2: Reading images

Reading and Resizing cover image: $Q = \text{imresize}(\text{imread}(\text{'ultrasound.jpg'}), [512,512]);$

Applying gray level on cover image: $I = \text{rgb2gray}(Q);$

STEP 3: Applying DWT

Applying First level DWT coefficients for cover image:

$[LL1,HL1,LH1,HH1] = \text{dwt2}(I, \text{'haar'});$

Applying Second level DWT coefficients for cover image:

$[LL2, HL2, LH2, HH2] = \text{dwt2}(LL1, \text{'haar'});$

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

Applying SVD on LL2: $[Uy, Sy, Vy] = \text{svd}(LL2); q = \text{size}(Sy);$

STEP 5: Reading watermark image:

Reading watermark image: $I_w = \text{imresize}(\text{imread}(\text{'logo1'}), [512,512]);$

Resizing watermark image: $I_w = I_w(:, :, 1); I1_w = \text{imresize}(I_w, p);$

Applying SVD on watermark image: $[Uw, Sw, Vw] = \text{svd}(\text{double}(I1_w));$

STEP 6: Image Watermark Embedding

Embedding watermark: $\text{smark} = Sy + \alpha * Sw;$

Rebuild the sub-bands using SVD: $LL2_1 = Uy * \text{smark} * Vy';$

Applying the invers DWT to get watermarked image:

$LL1_1 = \text{idwt2}(LL2_1, HL2, LH2, HH2, \text{'haar'});$

$I_1 = \text{idwt2}(LL1_1, HL1, LH1, HH1, \text{'haar'});$

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)

$[LL1_wmv, HL1_wmv, LH1_wmv, HH1_wmv] = \text{dwt2}(I_1, \text{'haar'});$

$[LL2_wmv, HL2_wmv, LH2_wmv, HH2_wmv] = \text{dwt2}(LL1_wmv, \text{'haar'});$

STEP 2: Applying SVD on the selected sub-bands

$Swrec = (Sy_wmv - Sy) / \alpha;$

$Wmy = Uw * Swrec * Vw';$

III.2.3 Simulation of Watermarking using two levels of DWT and SVD

The performance of the proposed watermarking technique is based on DWT and SVD. In the proposed method the cover medical image is of size 264×191 . The watermark image is of size 222×227 . The robustness of the image watermark is evaluated by determining NC. The quality of impressibility of the watermarked image is evaluated by PSNR. 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.1 shows the cover and watermarked image respectively. Figure III.2 shows original and extracted watermarks respectively. Table III.1 shows the PSNR, and NC performance of the proposed method at different scale factor. It is found that higher scale factor results in stronger robustness of the extracted watermark while smaller scale factor provides better PSNR values between original and watermarked medical images.

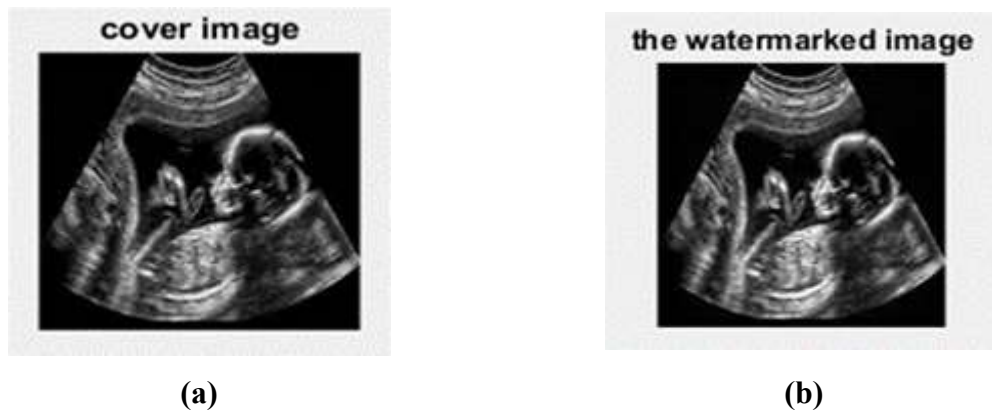


Fig III.1 the cover image (a), and the watermarked image (b)



Fig III.2 The original watermark (a) and the extracted watermark(b)

Table III.1 PSNR, NC performance at different scale factor values

Scale factor	0.03	0.01	0.1	0.5
PSNR	70.3489	74.6003	65.0620	58.2338
NC	0.87	0.83	0.91	0.93

Discussion:

It is observed in this method that the maximum PSNR value is 74.60 dB at scale factor = 0.01. Here, the NC value is 0.83. However, the maximum NC value is 0.93 at scale factor = 0.5. Here, the PSNR value is 58.23 dB. It is found that the higher scale factor results stronger robustness of extracting watermark whereas the lower scale factor provides better visual quality of the watermarked image.

III.3 Watermarking using three levels of DWT without SVD**III.3.1 Watermark Embedding Algorithm**

In this algorithm, the considered cover medical image is transformed by three levels of DWT where the low frequency sub-band is used to embed the watermark. The watermark image is also transformed by three levels of DWT and the low frequency sub-band is used as watermark. Embedding algorithm details for medical image watermark is formulated as follows:

STEP 1: Variable Declaration

Cover image: 'handxray.jpg'

Watermark image: 'watermark2.jpg'

I: Read the cover image ('handxray.jpg') (x-ray)

ax: Read the watermark image ('watermark2.jpg')

a: scale factor Hint: Try with different scaling factor values (ex: 0.5,0.1,0.03,0.05), Lower the value to make watermark less visible. a=0.03

DWT: Transform domain technique

Haar: Wavelet filters

[ca1,ch1,cv1,cd1]: First level of DWT transform on cover image

[ca2,ch2,cv2,cd2]: Second level of DWT transform on cover image

[ca3,ch3,cv3,cd3]: Third level of DWT transform on cover image

STEP 2: Read the Images

Reading cover image: I=imread('handxray.jpg');

Resizing cover image: I=imresize(I,[512 512]);

Convert to gray level: I=rgb2gray(I); I=im2double(I);

Reading watermark image: ax=imread('watermark2.jpg'); ax=rgb2gray(ax);

Resizing watermark image: ax=imresize(ax,[512 512]); ax=im2double(ax);

STEP 3: Applying 3 levels of DWT on cover image

[ca1,ch1,cv1,cd1]=dwt2(I,'haar');

[ca2,ch2,cv2,cd2]=dwt2(ca1,'haar');

[ca3,ch3,cv3,cd3]=dwt2(ca2,'haar');

STEP 4: Applying 3 levels of DWT on watermark image

[lca1,lch1,lc1v1,lcd1]=dwt2(ax,'haar');

[lca2,lch2,lc2v1,lcd2]=dwt2(lca1,'haar');

[lca3,lch3,lc3v1,lcd3]=dwt2(lca2,'haar');

STEP 5: Image Watermark Embedding

Input scale factor

Embedding watermark: newca3=[ca3+(a).*lca3];

Construction of Watermark Image

Applying the invers DWT to get watermarked image:

newca2= idwt2(newca3,ch3,cv3,cd3,'haar');

newca1= idwt2(newca2,ch2,cv2,cd2,'haar');

watermarked_image= idwt2(newca1,ch1,cv1,cd1,'haar');

III.2.2 Watermark Extraction Algorithm

STEP 1 Applying three levels of DWT on the watermarked image

[nlca1,nlch1,nlcv1,nlcd1]=dwt2(watermarked_image,'haar');

[nlca2,nlch2,nlcv2,nlcd2]=dwt2(nlca1,'haar');

[nlca3,nlch3,nlcv3,nlcd3]=dwt2(nlca2,'haar');

wca3= [(newca3-ca3)./a];

STEP 2: Applying the invers of DWT

```
wca2= idwt2(wca3,[ ],[ ],[ ],'haar');
```

```
wca1= idwt2(wca2,[ ],[ ],[ ],'haar');
```

```
extracted_watermarkimage= idwt2(wca1,[ ],[ ],[ ],'haar');
```

III.3.3 Simulation of Watermarking using three levels of DWT without SVD

The performance of the proposed watermarking technique is based on using three levels of DWT without SVD. In this method we used cover medical image size of 239 x 211 and a watermark image size of 222×227. The imperceptibility between the watermarked image and cover image is evaluated by determining PSNR.

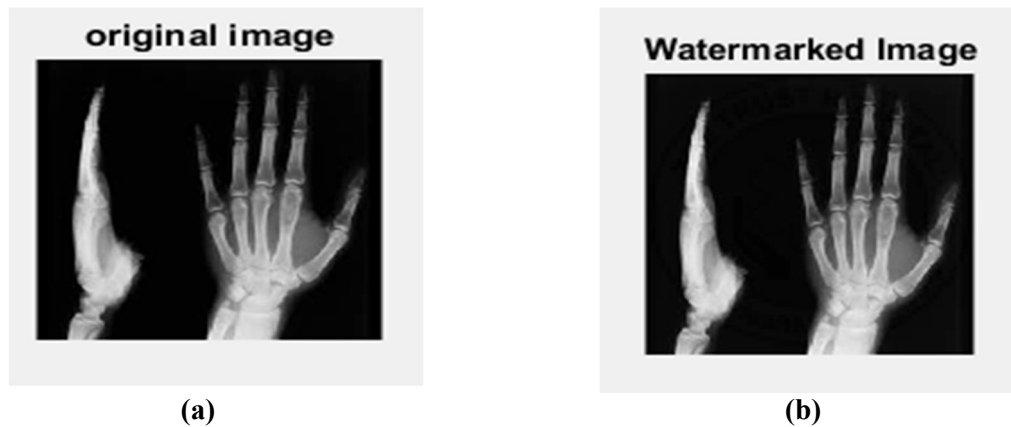


Fig III.3 shows the cover image (a), and watermarked image (b)



Fig III.4 the original watermark image (a), and the extracted watermark image (b)

Table III.2 PSNR, and Visual quality of the watermarked at deferent Scale factor

Scale factor	PSNR (dB)	Quality of watermarked image
0.01	75.5401	Very good imperceptibility
0.03	70.4101	Good imperceptibility
0.5	52.4531	Bad imperceptibility
1	49.4850	Very bad imperceptibility

Discussion:

The quality of the watermarked image depends on the imperceptibility of image by determining PSNR at different scale factor value. Higher PSNR value gives a good quality. Table III.2 shows PSNR at different scale factor. The clearest quality of image is with the higher PSNR value. Low PSNR accords to bad quality of image. At scale factor: 0.01 and PSNR: 75.54 dB allows to show the image with a very good quality, while at scale factor: 0.5 and PSNR: 52.45 dB shows us a bad quality comparing to the first value.

III.4 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 methods, we have applied eight different types of attacks on the watermarked images obtained from the two methods that was discussed above (two levels of DWT with SVD, and three levels of DWT without SVD). The attacks are: Average filter attack (AVFA), Rotation attack (RTA), Cropping attack (CRA), Histogram Equalization attack, Median filter attack (MFA), Median filter attack (MFA), Salt & pepper noise attack, shear attack.

III.4.1 Applying attacks on first method (two levels of DWT with SVD)

The attacked watermarked brain-cancer images using different attacks are shown in Fig.3.5.

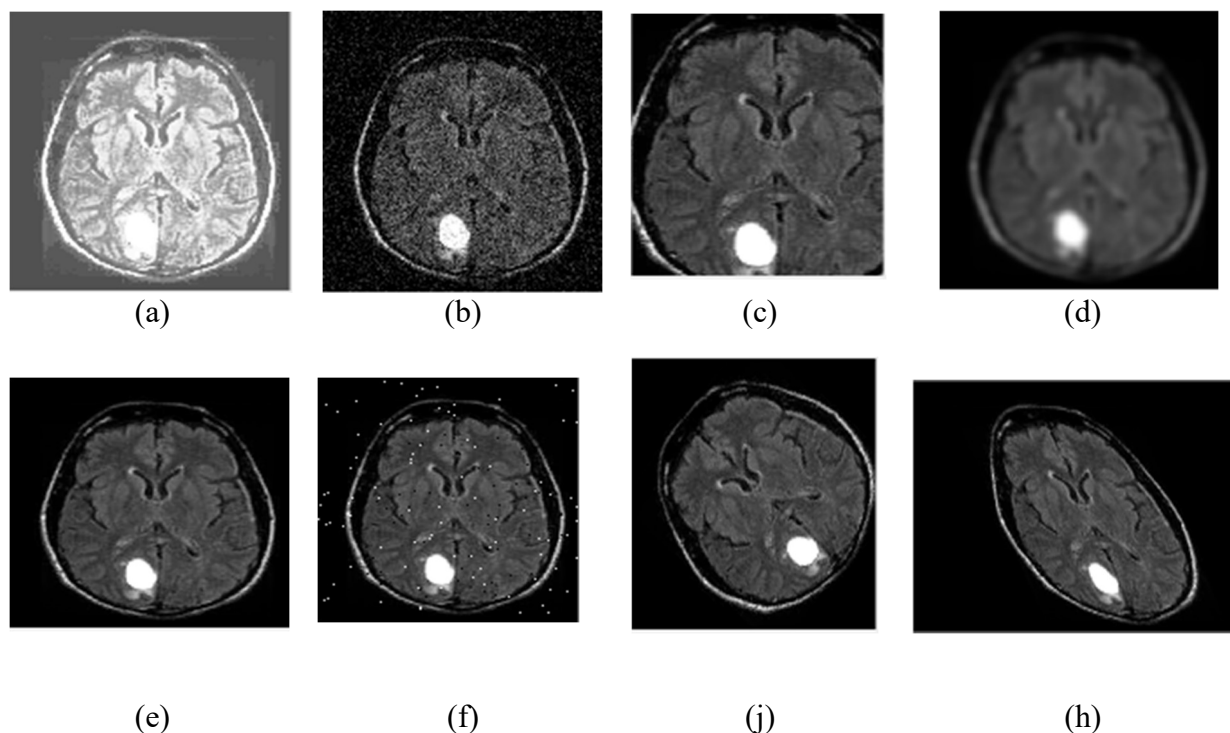
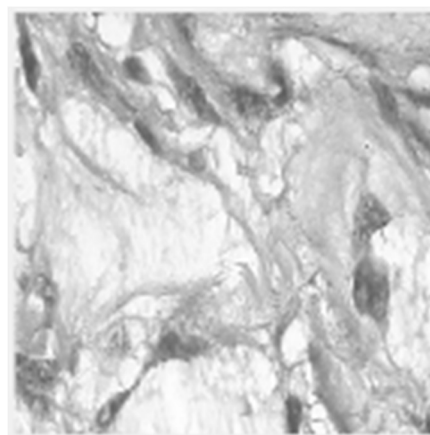


Fig III.5 The attacked watermarked brain-cancer images: histogram equalization attack (a), gaussian noise attack (b), cropping attack (c), mean attack (d), median filter attack (e), salt & pepper attack (f), rotation attack (j), shear attack (h)

The resisting of the embedded watermark to applied attacks is checked by extracting the watermark from the attacked images using the proposed extracting procedures. In Fig.III.7, extracted watermarks from the attacked watermarked images are shown. From the figures, we can notice that the proposed method gives good quality extracted watermark image against all the attacks except the rotation attack. The quality of the extracted watermark can be measured using many metrics.



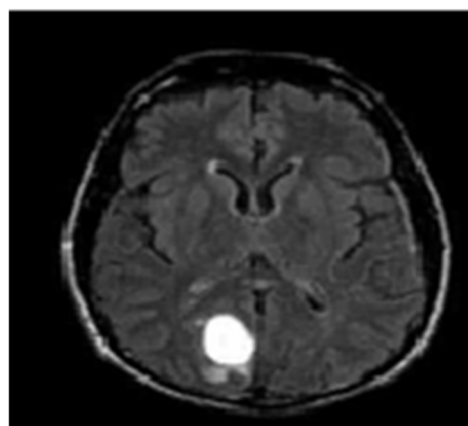
(a)



(b)



(c)



(d)

Fig III.6 shows test images Hand x-ray (a) MRI (b) CT brain-cancer (c) Ultrasound (d)

The PSNR and NC performance of the proposed technique (two levels of DWT with SVD) at different scale factors of the image watermark are evaluated. In this method we used four types of medical images. After applying eight different attacks on every image, the PSNR and NC performance of all attacks are shown in table III.3.





































Attacks	Extracted watermark from cover image			
	Hand x-ray	CT brain-cancer	MRI	Ultrasound
	Logo1			
Attack free				
shear attack				
Rotation attack (RTA)				
Cropping attack (CRA)				
Median filter attack (MFA)				
Histogram Equalization attack				
Salt & pepper noise attack				
Gaussian Noise attack (GNA)				
Mean Filter attack				

Fig III.7 Extracted watermarks from Attacked watermarked images using (two levels of DWT with SVD)

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

Performed Attacks	Hand-X-ray		CT-brain		MRI Breast cancer		Ultrasound	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Attack free	78.0349	1	72.7305	1	73.0941	1	75.0620	1
Gaussian Noise	63.5360	0.95592	65.7123	0.95591	62.662	0.95644	61.2275	0.95585
Salt & pepper	71.1830	0.97306	71.2339	0.96619	71.1970	0.97754	71.0697	0.97284
Histogram	52.7940	0.7541	51.3753	0.7541	51.3450	0.7541	52.4202	0.7541
Median filter	75.2080	0.91573	70.0674	0.91573	72.688	0.91573	72.8077	0.91573
Cropping attack	53.6500	0.06896	61.2093	0.06896	61.38	0.06896	54.5293	0.06896
Rotation attack	53.8750	-0.0812	60.9949	-0.0812	55.122	-0.0812	54.8579	-0.0812
shear attack	54.7940	-0.1152	51.3753	-0.1152	51.375	-0.1152	52.4202	-0.1152
Mean Filter	63.6330	0.53851	66.5013	0.53851	64.6000	0.53851	60.3699	0.53851

III.4.2 Applying attacks on second method (three levels of DWT without SVD)

The attacked watermarked ultrasound images using different attacks are shown in Fig.III.7.

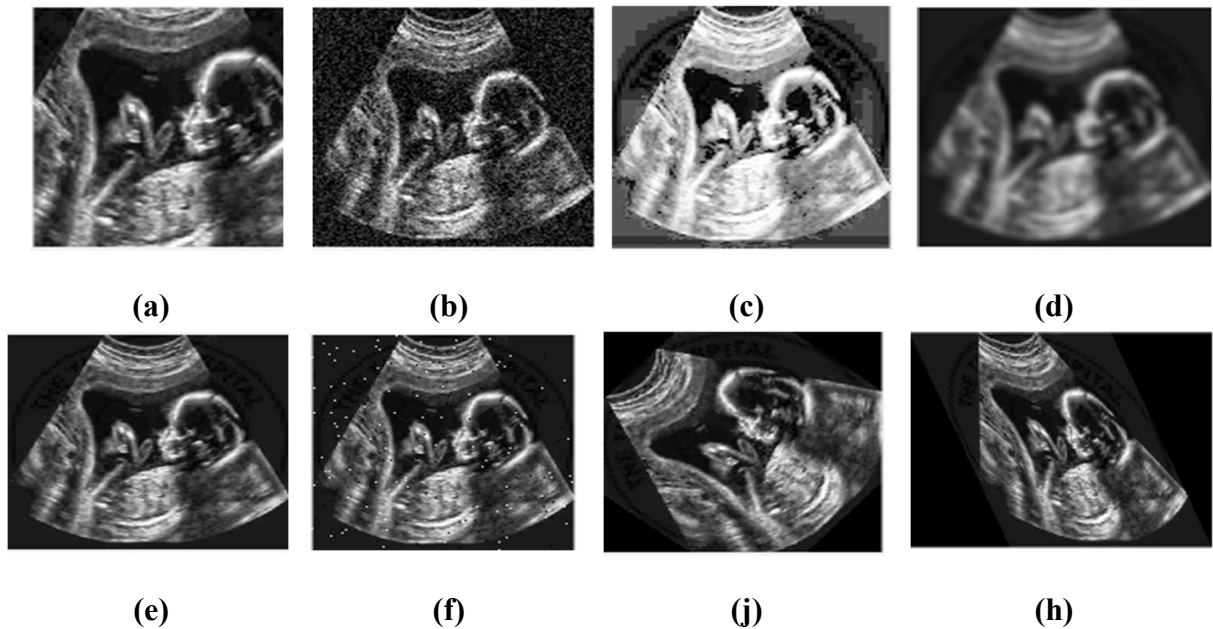


Fig III.8 shows the attacked watermarked images: (a) cropping attack, (b) gaussian noise attack, (c) histogram equalization attack, (d) mean attack, (e) median filter attack, (f) salt & pepper attack, (j) rotation attack, (h) shear attack.

Attacks	Extracted watermark from cover image			
	Hand x-ray	CT braincancer	MRI	Ultrasound
	Logo1			
Attack free				
shear attack				
Rotation attack (RTA)				
Cropping attack (CRA)				
Median filter attack (MFA)				
Histogram Equalization attack				
Salt & pepper noise attack				
Gaussian Noise attack (GNA)				
Mean Filter attack				

Fig III.9 Extracted watermarks from Attacked watermarked images using (three levels of DWT without SVD)

We applied the same attacks on this proposed method (three levels of DWT without SVD). Fig III.8 shows the extracted watermark results after applying eight different attacks. Table III.4 shows PSNR and NCC performance for every attack. We used the same scale factor $a=0.1$.

Table III.4 PSNR and NCC result obtained from simulations using same watermark image

Performed Attacks	Hand-X-ray		CT-brain		MRI Breast cancer		Ultrasound	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Attack free	70.2396	0.84970	78.6705	0.8497	75.4105	0.84950	72.0403	0.8497
Gaussian Noise	63.1820	0.96179	66.0190	0.96195	65.1250	0.96181	60.4900	0.9617
Salt & pepper	72.1140	0.97930	71.1630	0.97848	72.1730	0.97953	71.2440	0.9788
Histogram	53.5410	0.89232	51.3930	0.89238	51.1700	0.89232	52.6790	0.8923
Median filter	68.4450	0.99929	76.0674	0.99929	73.688	0.99929	70.8077	0.99573
Cropping	53.5110	0.17198	60.8520	0.17198	66.0830	0.17193	54.0810	0.17200
Rotation attack	53.6940	-0.0249	60.4640	-0.0249	55.5490	-0.0249	54.2790	-0.0249
shear attack	54.4830	-0.1818	61.3160	-0.1818	52.7820	-0.1818	55.6730	-0.1818
Mean Filter	63.2280	0.80527	65.0190	0.8057	69.4950	0.8057	60.1050	0.8057

Discussion:

The obtained result on table III.3 (two levels of DWT with SVD), and table III.4 (three levels of DWT without SVD), shows PSNR and NCC performance after the watermarked image is attacked. We note that PSNR and NCC values on the two different methods have approximately the same result. In the first method (three levels of DWT without SVD) we can observe that the watermark is more robust to the attacks than the watermark in the second method (two levels of DWT with SVD). Also, it can be observed that the watermarked images have been affected by three attacks which are the rotation attack, shear attack and cropping attack. Their result obtained under 0.5 and that means the robustness against those attacks is very low.

III.4.3 Experimental Results after using different wavelet families

In this section we applied four different wavelet families on four test medical images using two methods (two levels of DWT with SVD) and (three levels of DWT without SVD). The wavelets are: Haar, Daubechies, Coiflets and Biorthogonal. Table 3.5 shows PSNR values at the four wavelets using the first method. PSNR comparison are shown in fig 3.9. Table 3.6 shows PSNR values at four wavelets using the second method. Fig 3.10 shows PSNR comparison on this proposed method.

Table III.5 shows PSNR values with different wavelets applied on four test images on method (two levels of DWT with SVD)

Wavelets type	Hand X-ray	CT-brain cancer	Ultrasound	MRI Breast cancer
haar	71.5244	76.5528	68.733	78.5687
Daubechies	72.5244	76.5528	68.733	78.5687
Coiflets	71.4883	76.3833	68.6055	78.7944
Biorthogonal	62.0394	64.5732	58.8558	68.6782

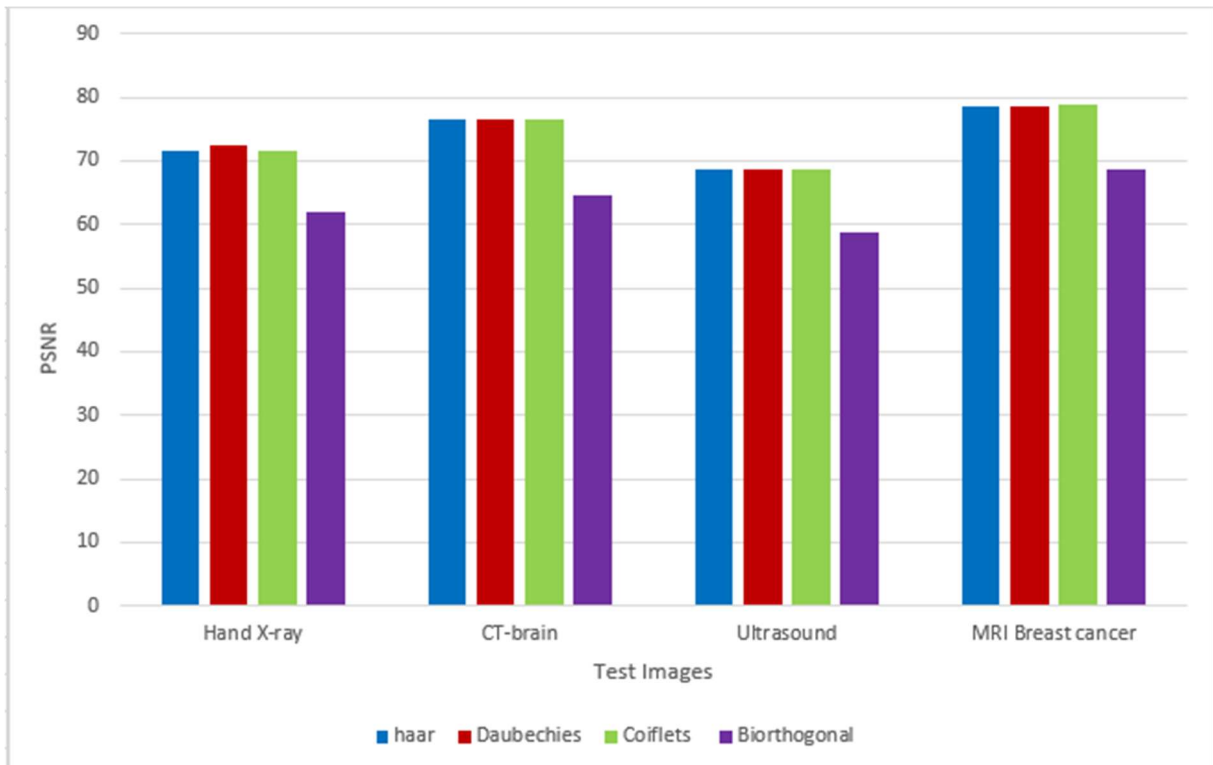


Fig III.10 PSNR comparison results in different wavelets on test images method (two levels of DWT with SVD)

Table III.6 shows PSNR values with different wavelets applied on four test images on method (three levels of DWT without SVD)

wavelets type	Hand X-ray	CT brain	Ultrasound	MRI Breast cancer
haar	67.7374	74.3993	69.2541	65.5338
Daubechies	67.7374	74.3993	69.2541	65.5338
Coiflets	70.4045	72.2816	67.6253	68.3229
Biorthogonal	65.2396	69.6704	64.4105	62.0403

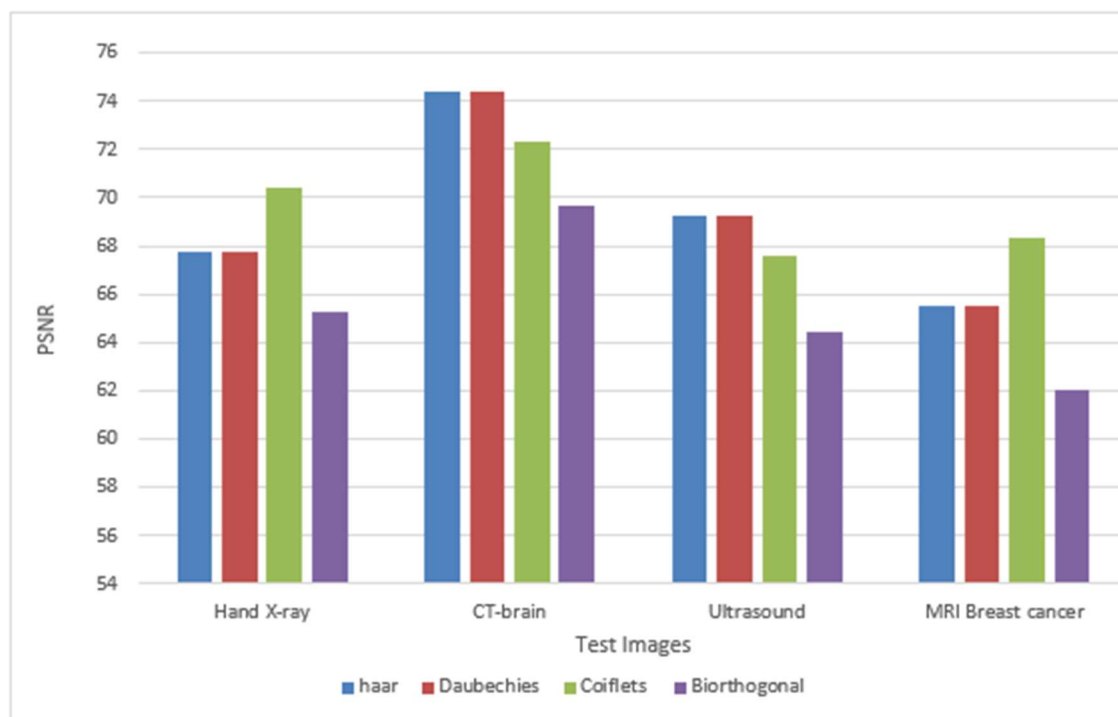


Fig III.11 PSNR comparison results in different wavelets on test images, method (three levels of DWT without SVD)

III.4.4 Experimental Results Comparing proposed method with other reported method

Table III.7 Comparison of PSNR and NC values with other reported method

Gain factor	Singh et al. [ac]		Borko Furht [ad]		Proposed method	
	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC
0.01	28.17	0.5247	54.26	0.87	75.5401	0.785
0.05	28.02	0.9288	48.42	0.93	68.1866	0.8136
0.09	217	0.9668	42.68	0.98	65.7057	0.835
0.1	26.85	0.9697	39.58	0.984	65.2396	0.8497

Discussion:

As we can see, this proposed method offers higher imperceptibility and little bit low robustness at all considered gain factor as compared with the other reported methods.

Referring to table III.7, the maximum NC value with proposed method has been obtained as 0.8497 against 0.9697 and 0.984 obtained by Singh et al. in [ac], and [Borko Furth] [ad] methods at gain factor = 0.1. However, the minimum NC value with proposed method has been obtained as 0.785 against 0.5247 and 0.87 obtained by Singh et al. in [ac], [Borko Furth] [ad] methods at gain factor = 0.01.

We also see that the maximum PSNR value has been obtained with Singh et al. in [ac], is 28.17 dB 54.26 dB, [Borko Furth] [ad] methods. while, the maximum PSNR value has been obtained by the proposed method is 75.5401 dB at gain factor = 0.01.

On the other hand, the minimum PSNR value has been obtained with Singh et al. in [ac], is 26.85 dB and 39.58 dB [Borko Furth] [ad] methods. while, the minimum PSNR value has been obtained by the proposed method is 65.2396 dB at gain factor = 0.1.

Over all, the performance of the proposed method is better than the other reported technique by Singh et al. in [ac], [Borko Furth] [ad] methods in terms of imperceptibility. Finally, the overall PSNR and NC performance of the proposed method highly depends on the size of the watermarks, gain factor and the noise variation.

Conclusion

This chapter dealt with image watermarking techniques based on DWT and SVD on frequency domain. We used two methods to obtain the results. The first method is two levels of DWT with SVD and second one is three levels of DWT without SVD. We also applied four different wavelet families. The methods 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 and SVD applied together offer better performance in terms of imperceptibility and robustness as compared to DWT applied individually.

Summary

This document proposed secure transmission using watermarking techniques considering medical image watermarks. Experimental results were obtained by changing watermark size and scale factor. Performance of the developed scheme was tested against various attacks like rotation, compression, filtering, and histogram equalization.

The imperceptibility and robustness of the proposed method is tested with major experiments. The experimental results point that the proposed method offers good imperceptibility for the watermarked images, which is evaluated by PSNR. The performance of the proposed method against different attacks of the watermarked image is evaluated by correlation coefficients of extracted watermark logos and some subjective image tests. The experimental results show that the proposed method can be effectively resist against geometric and non-geometric attacks.

The embedding of many techniques was combined to improve the robustness of the watermarks and the quality of the watermarked image which is the prime objective of the research. However, it may have increased the application complexity to some measures which needs to be examined separately. We also need to study approaches that will improve the performance such as robustness, imperceptibility, security and capacity at the same time. We would like to do more researches on lossless data hiding techniques specially for medical applications, which can be reported in future communication.

References

- [A]. Nayak NR, Mishra BK, Rath AK, Swain S (2015) Improving the efficiency of color image segmentation using an enhanced clustering methodology. *International Journal of Applied Evolutionary Computation (IJAEC)* 6(2):50–62
- [B]. Haouzia A, Noumeir R (2008) Methods for image authentication: a survey. *Multimed Tools Appl* 39(1):1–46
- [1] M. A. Haidekker, *Medical Imaging Technology*, SpringerBriefs in Physics, DOI: 10.1007/978-1-4614-7073-1_1, © The Author(s) 2013
- [2] Huang, H. K. (2011). *PACS and imaging informatics: basic principles and applications*. John Wiley & Sons. pp. 33-6
- [3] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public Law, 104*,191.
- [4] Bouslimi, D., Coatrieux, G., Cozic, M., & Roux, C. A joint encryption/watermarking system for verifying the reliability of medical images. *Information Technology in Biomedicine, IEEE Transactions on*, 16(5), 891-899. (2012).
- [5] Al-Haj, A. Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. *Journal of digital imaging*, 1-9. (2014).
- [6] Abbing, H. R. Medical Confidentiality and Patient Safety: Reporting Procedures. *European journal of health law*, 21(3), 245-259. (2014).
- [7] Klutas, Edna May, RN,M.P.H., C.O.H.N. “Confidentiality of medical information”. *Occupational Health Nursing*, 25(4), 14-17. (1977).
- [8] http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf
- [9] Schneider, M., & Chang, S. F. A robust content based digital signature for image authentication. In *Image Processing, 1996. Proceedings., International Conference on* (Vol. 3, pp. 227-230). IEEE. (1996).
- [10] Umamageswari, A., & R Suresh, G. “A New Cryptographic Digital Signature for Secure Medical Image Communication in Telemedicine”. *International Journal of Computer Applications*, 86(11), 4-9. (2014).
- [11] Lo, C. C., & Hu, Y. C. “A novel reversible image authentication scheme for digital images”. *Signal Processing*, 98, 174-185. (2014).
- [12] Vellaisamy, S., & Ramesh, V. (2014). Inversion attack resilient zero-watermarking scheme for medical image authentication. *IET Image Processing*, 8(12), 718-727.
- [13] Memon, N. A., Keerio, Z. A., & Abbasi, F. “Dual Watermarking of CT Scan Medical Images for Content Authentication and Copyright Protection”. In *Communication Technologies, Information Security and Sustainable Development* (pp. 173-183). Springer International Publishing. (2014).
- [14] Huang, H. K. (2011) Picture Archiving and Communication System Components and Workflow. *PACS and Imaging Informatics: Basic Principles and Applications, Second Edition*, 217-235.
- [15] Bairagi, V. K., & Sapkal, A. M. “ROI based DICOM Image Compression for Telemedicine”. *Digital Image Processing*, 3(11), 662-666. (2011).
- [16] <http://www.offis.de/en/start.html>

References

- [17] McAuliffe, M. J., Lalonde, F. M., McGarry, D., Gandler, W., Csaky, K., & Trus, B. L. (2001). Medical image processing, analysis and visualization in clinical research. In *Computer Based Medical Systems, 2001. CBMS 2001. Proceedings. 14th IEEE Symposium on* (pp. 381-386). IEEE.
- [18] Bouslimi, D., Coatrieux, G., & Roux, C. "A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images". *Computer methods and programs in biomedicine*, 106(1), 47-54. (2012).
- [19] Huang, H. K. (2011). PACS and imaging informatics: basic principles and applications chapter 17 Image/Data Security. John Wiley & Sons. pp 519- 558
- [20] Kannammal, A., & Rani, S. S. (2011). Authentication of DICOM medical images using multiple fragile watermarking techniques in wavelet transform domain. *IJCSI*.
- [21] Fakhari, P., Vahedi, E., & Lucas, C. (2011). Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. *Digital Signal Processing*, 21(3), 433-446.
- [22] Dong, C., Li, J., & Chen, Y. W. (2012, May). A DWT-DCT Based Robust Multiple Watermarks for Medical Image. In *Photonics and Optoelectronics (SOPO), 2012 Symposium on* (pp. 1-4). IEEE.
- [23] Coatrieux, G., Huang, H., Shu, H., Luo, L., & Roux, C. (2013). A watermarkingbased medical image integrity control system and an image moment signature for tampering characterization. *Biomedical and Health Informatics, IEEE Journal of*, 17(6), 1057-1067.
- [24] Li, J., Dong, C., Huang, M., Zhang, H., & Chen, Y. W. (2012). A Novel Robust Watermarking for Medical Image. *Advances in Information Sciences & Service Sciences*, 4(11).
- [25] N.F.Johnson,S.Jajodia,Exploringsteganography:seeingtheunseen, IEEE Computer31(2)(1998)26–34.
- [26] W.Bender,W.Butera,D.Gruhl,R.Hwang,F.J.Paiz,S.Pogreb, Applicationsfordatahiding,IBMSystemsJournal39(3&4)(2000) 547–568.
- [27] F.A.P.Petitcolas, Introduction to information hiding,in: S.Katzenbeisser,F.A.P.Petitcolas(Eds.),Information Hiding Techniquesfor Steganography and DigitalWatermarking,ArtechHouse,Inc., Norwood,2000
- [28] S.Miaou,C.Hsu,Y.Tsai,H.Chao, Asecuredata hiding technique with heterogeneous data-combining capability or electronic patient records, in:Proceedings of the IEEE22nd AnnualE MBS International Conference,Chicago,USA,July23–28,2000, pp. 280–283
- [29] Y.Li,C.Li,C.Wei, Protection of mammograms using blind steganography and watermarking, in: Proceedings of the IEEE International Symposium on Information Assurance and Security, 2007,pp.496–499.
- [30] American Telemedicine Association. What is telemedicine. Retrieved form <http://www.americantelemed.org/learn>. (2013).
- [31] Cavaro-Ménard, C., Lu, Z. G., & Le Callet, P. " QoE for telemedicine: challenges and trends". In *SPIE Optical Engineering+ Applications* (pp. 88561A-88561A). International Society for Optics and Photonics.. (2013)
- [32]. G.J. Simmons, The prisoner's problem and the subliminal channel, in *Advances in Cryptology*, Proceedings of CRYPTO 83, (Plenum Press, New York, 1984), pp. 51–67
- [33]. S. Craver, On public-key steganography, The presence of an active warden technical report RC 20931, IBM, 1997

References

- [34]. W. Bender, D. Gruhl, N. Morimoto, A. Lou, Techniques for data hiding. *IBM Syst. J.* **35**(3&4), 313–336 (1996)
- [35]. S. Katzenbeisser, F.A.P. Petitcolas, *Information hiding techniques for steganography and digital watermarking* (Artech House, London, 2000)
- [36]. S.P. Mohanty, Watermarking of digital images, M.S. Thesis, Indian Institute of Science, India, 1999
- [37]. N. Morimoto, Digital watermarking technology with practical applications. *Inf. Sci. Special Issue on Multimedia Inf. Technol., Part 1* **2**(4), 107–111 (1999)
- [38]. F. Hartung, F. Ramme, Digital rights management and watermarking of multimedia content for m-commerce applications. *IEEE Commun. Mag.* **38**(11), 78–84 (2000)
- [39]. B.L. Gunjal, S.N. Mali, Applications of digital image watermarking in industries, pp. 5–7, CSI Communications, 2012
- [40]. R. Chandramouli, N. Memon, M. Rabbani, Digital watermarking, encyclopedia of imaging. *Sci. Technol.*, 1–21 (2002)
- [41]. 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
- [42]. S.A.K. Mostafa, N. El-sheimy, A.S. Tolba, F.M. Abdelkader, H.M. Elhindy, Wavelet packets based blind watermarking for medical image management. *Open Biomed. Eng. J.* **4**, 93–98 (2010)
- [43]. 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)
- [44]. S. Lee, C.D. Chang, T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform. *IEEE Trans. Inf. Foren. Security* **2**(3), 330–321 (2007)
- [45]. H.C. Huang, W.C. Fang, Techniques and application of intelligent multimedia data hiding. *Telecommun. Syst.* **44**(3-4), 241–251 (2010)
- [46]. 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
- [47]. F. Cayre, C. Fontaine and T. Furon, Watermarking security: theory and practice, *IEEE Trans. Signal Process.*, **53** (10), 3976–3987 (2005)
- [48]. 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
- [49] Jabade, V. S., & Gengaje, D. S. R. (2011). Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications (0975–8887) Volume*, 28-35.
- [50] Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R. (2014). Watermarking Techniques used in Medical Images: a Survey. *Journal of digital imaging*, **27**(6), 714-729.
- [51] Kutter, M., & Petitcolas, F. A. (1999, April). Fair benchmark for image watermarking systems. In *Electronic Imaging'99* (pp. 226-239). International Society for Optics and Photonics.
- [52] Wang, S. H., & Lin, Y. P. (2004). Wavelet tree quantization for copyright protection watermarking. *Image Processing, IEEE Transactions on*, **13**(2), 154-165.
- [53] Pankanti, S., & Yeung, M. M. (1999, April). Verification watermarks on fingerprint recognition and retrieval. In *Electronic Imaging'99* (pp. 66-78). International Society for Optics and Photonics.
- [54] Günsel, B., Uludag, U., & Tekalp, A. M. (2002). Robust watermarking of fingerprint images. *Pattern Recognition*, **35**(12), 2739-2747.
- [55] Kundur, D., & Hatzinakos, D. (1999). Digital watermarking for telltale tamper proofing and authentication. *Proceedings of the IEEE*, **87**(7), 1167-1180.

References

- [56] Lu, C. S., & Liao, H. Y. M. (2001). Multipurpose watermarking for image authentication and protection. *Image Processing, IEEE Transactions on*, 10(10), 1579-1592.
- [57] Coatrieux, G., Huang, H., Shu, H., Luo, L., & Roux, C. (2013). A watermarking based medical image integrity control system and an image moment signature for tampering characterization. *Biomedical and Health Informatics, IEEE Journal of*, 17(6), 1057-1067.
- [58] Wong, P. W. (1998). A watermark for image integrity and ownership verification. In *IS AND TS PICS CONFERENCE* (pp. 374-379). SOCIETY FOR IMAGING SCIENCE & TECHNOLOGY.
- [59] Tan, C. K., Ng, J. C., Xu, X., Poh, C. L., Guan, Y. L., & Sheah, K. (2011). Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. *Journal of Digital Imaging*, 24(3), 528-540.
- [60] Fridrich, J. (1998, October). Image watermarking for tamper detection. In *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on* (Vol. 2, pp. 404-408). IEEE.
- [61] Lin, P. L., Hsieh, C. K., & Huang, P. W. (2005). A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern recognition*, 38(12), 2519-2529.
- [62] Wong, K., Tanaka, K., Takagi, K., & Nakajima, Y. (2009). Complete video quality preserving data hiding. *Circuits and Systems for Video Technology, IEEE Transactions on*, 19(10), 1499-1512.
- [63] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM systems journal*, 35(3.4), 313-336.
- [64] Su, Q., Niu, Y., Wang, Q., & Sheng, G. (2013). A blind color image watermarking based on DC component in the spatial domain. *Optik-International. Journal for Light and Electron Optics*, 124(23), 6255-6260.
- [65] Thanh, T. M., Hiep, P. T., & Tam, T. M. (2014). A New Spatial q-log Domain for Image Watermarking. *International Journal of Intelligent Information Processing*, 5(1).
- [66] Agung, B. W. R., & Permana, F. P. (2012, July). Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression. In *Communication, Networks and Satellite (ComNetSat), 2012 IEEE International Conference on* (pp. 167-171). IEEE
- [67] Chopra, D., Gupta, P., Gaur Sanjay, B. C., & Gupta, A. (2012). Lsb Based Digital Image Watermarking For Gray Scale Image. *IOSR Journal of Computer Engineering (IOSRJCE) ISSN*, 2278-0661.
- [68] Bajaj, S., & Shukla, M. (2014). Performance Evaluation of an approach for Secret data transfer using interpolation and LSB substitution with Watermarking. *International Journal of Computer Science & Information Technologies*, 5(5).
- [69] Jain, J., & Johari, P. (2014). Digital Image Watermarking Based on LSB for Gray Scale Image. *IJCSNS*, 14(6), 108.
- [70] Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(7), 971-987.
- [71] Sachnev, V., Kim, H. J., Nam, J., Suresh, S., & Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. *Circuits and Systems for Video Technology, IEEE Transactions on*, 19(7), 989-999.
- [72] Wenyin, Z., & Shih, F. Y. (2011). Semi-fragile spatial watermarking based on local binary pattern operators. *Optics Communications*, 284(16), 3904-3912.
- [73] Ahmad, A., Sinha, G. R., & Kashyap, N. (2014). 3-Level DWT Image Watermarking against Frequency and Geometrical Attacks. *International Journal of Computer Network and Information Security (IJCNIS)*, 6(12), 58.
- [74] Basheera, S., Prakash, D. B., & Naganjaneyulu, P. V. (2011). Blind Medical Image Watermarking Technique for Secure Recovery of Hidden Data. In *Advances in Digital Image Processing and Information Technology* (pp. 185-192). Springer Berlin Heidelberg.

References

- [75] Maneesha, P., Yogendra K., (2015). Digital Watermarking Algorithm for Embedding Color Image using Two Level DWT. *International Journal of Computer Applications(IJCA)*. (pp. 19-24), 116(13).
- [76] Paunwala, M., & Patnaik, S. (2012). Dct watermarking approach for security enhancement of multimodal system. *International Scholarly Research Notices,2012*.
- [77] Tataru, R. L., El Assad, S., & Déforges, O. (2012, December). Improved blind DCT watermarking by using chaotic sequences. In *Internet Technology And Secured Transactions, 2012 International Conference for* (pp. 46-50). IEEE.
- [78] Laouamer, l., (2012). Sûreté et Sécurité desÉchanges de DonnéesÉlectroniques: Algorithmes de Tatouaged'Images.PhD. Dissertation. Université de Bretagne Occidentale.
- [79] Laouamer, L., & Tayan, O. (2015). A Semi-Blind Robust DCT Watermarking Approach for Sensitive Text Images. *Arabian Journal for Science and Engineering*, 40(4), 1097- 1109.
- [80] Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on* (pp. 709-716). IEEE.
- [81] Li, J., Dong, C., Huang, M., Zhang, H., & Chen, Y. W. (2012). A Novel Robust Watermarking for Medical Image. *Advances in Information Sciences & Service Sciences*, 4(11).
- [82] Lin, W. H., Wang, Y. R., Horng, S. J., Kao, T. W., & Pan, Y. (2009). A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications*, 36(9), 11509-11516.
- [83] Ranade, A., Mahabalarao, S. S., & Kale, S. (2007). A variation on SVD based image compression. *Image and Vision Computing*, 25(6), 771-777.
- [84] Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *Multimedia, IEEE Transactions on*, 4(1), 121-128.
- [85] Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T., & Lei, H. (2014). Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, 41(7), 3178-3188.
- [86] Benhocine, A., Laouamer, L., Nana, L., & Pascu, A. C. (2013). New images watermarking scheme based on singular value decomposition. *Journal of Information Hiding and Multimedia Signal Processing*, 4(1), 9-18.
- [87] Nema, A., & Mohan, R. (2014). Digital Image Watermarking using Adaptive DCTDWT. *IJEIR*, 3(2), 156-159.
- [88] ElGamal, A. F., Mosa, N. A., & ElSaid, W. K. (2013). Block-based Watermarking for Color Images using DCT and DWT. *International Journal of Computer Applications (0975–8887) Volume*.
- [89] Jose, S., Roy, R. C., & Shashidharan, S. (2012). Robust image watermarking based on DCT-DWT-SVD method. *International Journal of Computer Applications*, 58(21), 12-16.
- [90] Lenarczyk, P., & Piotrowski, Z. (2013). Parallel blind digital image watermarking in spatial and frequency domains. *Telecommunication Systems*,54(3), 287-303.
- [91] Oueslati, S., Cherif, A., & Solaiman, B. (2013). Multiple Binary Images Watermarking in Spatial and Frequency Domains. *International Journal of Computer Theory & Engineering*, 5(4).
- [92]. 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
- [93]. Z. Wang, A.C. Bovik, A universal image quality index. *IEEE Signal Process. Lett.* **9**(3), 81–84 (2002)
- [94]. A.K. Singh, Improved hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools Appl.* **76**(6), 8881–8900 (2017)

References

- [95] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun, Attack modelling: towards a second generation watermarking benchmark. *Signal Process.* **81**(6), 1177–1214 (2001)*Process.* **94**, 118–127 (2014)
- [96]. 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)
- [97]. C. Song, S. Sudirman, M. Merabti, D. Llewellyn-Jones, Analysis of digital image watermark attacks, in 7th IEEE Consumer Communications and Networking Conference, Las Vegas, Nevada, USA, pp. 941–945, January 09–12, 2010
- [98]. H. Nyeem, W. Boles, C. Boyd, Digital image watermarking: its formal model, fundamental properties and possible attacks. *EURASIP J. Adv. Signal Process.* **135**, 1–22 (2014)
- [99] H. Wang, A.T.S. Ho, S. Li, OR-benchmark: an open and reconfigurable digital watermarking benchmarking framework, June 02, 2015
- [100]. F.A.P. Petitcolas, M. Steinebach, F. Raynal, J. Dittman, C. Fontaine, N. Fates, in *A Public Automated Web-Based Evaluation Service for Watermarking Schemes: Stir Mark Benchmark*, ed. by P.W. Wong, E.J. Delp. Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 4314, 2001
- [a]. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Attacks on copyright marking systems, in *Information Hiding, Second International Workshop*, ed. by D. Aucsmith (Ed), (Springer-Verlag, Portland, OR, 1998), pp. 219–239*
- [b]. F.A.P. Petitcolas, Watermarking schemes evaluation. *IEEE Signal Process. Mag.* **17**(5), 58–64 (2000)
- [c]. <http://watermarking.unige.ch/Checkmark/>
- [d] S. Pereira, S. Voloshynovskiy, M. Madučeno, S. Marchand-Maillet, T. Pun, Second generation benchmarking and application oriented evaluation, in *Information Hiding Workshop*, Pittsburgh, PA, 2001
- [e]. 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
- f-47. <http://poseidon.csd.auth.gr/optimark/> distribution of vertex norms. *IEEE Trans. Signal Process.* **55**(1), 142–155 (2007)
- [g]. 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
- [h]. Y.H. Lin, J.L. Wu, A digital blind watermarking for depth-image based rendering 3D images. *IEEE Trans. Broadcasting* **57**(2), 602–611 (2011)
- [i]. H.D. Kim, J.W. Lee, T.W. Oh, H.K. Lee, Robust DT-CWT Watermarking for DIBR 3D Images. *IEEE Trans. Broadcasting* **58**(4), 533–543 (2012)
- [j]. A. Kejariwal, S. Gupta, A. Nicolau, N.D. Dutt, R. Gupta, Energy efficient watermarking on mobile devices using proxy-based partitioning. *IEEE Trans. VLSI Syst. G-k-14*(6), 625–636 (2006) 52. S.G. Shini, T. Tony, K. Chithraranja, Cloud based medical image exchange-security challenges. *Process. Eng.* **38**, 3454–3461 (2012) 1-52. S.G. Shini, T. Tony, K. Chithraranja, Cloud based medical image exchange-security challenges. *Process. Eng.* **38**, 3454–3461 (2012)
- [m]. X. Cao, F. Zhangjie, X. Sun, A privacy-preserving outsourcing data storage scheme with fragile digital watermarking-based data auditing. *J. Elect. Computer Eng.* **2016**, 1–7 (2016)
- [n]. C.-T. Yang, C.-H. Lin, G.-L. Chang, Implementation of image watermarking processes on cloud computing environments, security-enriched urban computing and smart grid. *Ser. Commun. Computer Inf. Sci.* **223**, 131–140 (2011) o-20. M. Terry, Medical identity theft and telemedicine security. *Telemed. e-Health* **15**(10), 928–932 (2009)
- [p]-21. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Multiple watermarking on medical images using selective DWT coefficients. *J. Med. Imaging Health Inf.* **5**(3), 607–614 (2015)

References

- [q]-22. D. Bowman., <http://www.fiercehealthit.com/story/researchers-use-digitalwatermarks-protectmedical-images> (2012).
- [r]-23. M. Ollove., www.usatoday.com/story/stateline-identity-thefts-medical/5279351 (2014).
- [s]-24. 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)
- [t]-25. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible dual watermarking for telemedicine applications. *Wirel. Pers. Commun.* **80**(4), 1415–1433 (2014)
- [u]- 26. A. Sharma, A.K. Singh, S.P. Ghrera, Robust and secure multiple watermarking technique for medical images. *Wirel. Pers. Commun.* **92**(4), 1611–1624 (2017)
- [v]-27. 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)
- [w]-28. A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Senior member, ieemultiple image watermarking applied to health information management. *IEEE Trans. Inf. Technol. Biomed.* **10**(4), 722–732 (2006)
- [x]-29. 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
- [y]- 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)
- [z]- 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
- [aa]- Z. Wang, A.C. Bovik, A universal image quality index. *IEEE Signal Process. Lett.* **9**(3), 81–84 (2002)
- [ab]-A.K. Singh, Improved hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools Appl.* **76**(6), 8881–8900 (2017)
- [ac]. 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), 606–614 (2015)
- [ad]. Amit Kumar, Singh, Basant Kumar, Ghanshyam Singh, Anand Mohan, *Multimedia Systems and Applications*, ISBN 978-3-319-57698-5 ISBN 978-3-319-57699-2 (eBook) DOI 10.1007/978-3-319-57699-2