REPUBLIQUE ALGERIENNE DEMOCRATIC ET POPULAIRE
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
Université Ferhat Abbas Sétif-1
Faculté des Sciences
Département d'Informatique

THÈSE

Présenté par

Abdallah SOUALMI

Pour L'obtention du diplôme de

Doctorat 3^{éme} cycle LMD en Informatique

Option : Système Intelligent et Apprentissage Automatique

Thème

Protection des contenus des images médicales dans le Cloud par camouflage d'informations secrètes pour aide à la télémédecine

Soutenue Le: 04 /05 /2021 **Devant La Commission D'examen**

Pr. Abdelhamid BENHOCINE	Prof. Université Ferhat Abbas Setif-1	Président
Dr. Adel ALTI	MCA. Université Ferhat Abbas Setif-1	Rapporteur
Dr. Lamri LAOUAMER	MCA. Université Qassim – Arabie Saudite	Co-Rapporteur
Dr. Lyazid TOUMI	MCA. Université Ferhat Abbas Setif-1	Examinateur
Dr. Samir AKHROUF	MCA. Université Mohamed Boudiaf M'sila	Examinateur

ALGERIAN REPUBLICAIN DEMOCRATIC AND POPULAIRE
Ministry of High Education and Scientific Research
University of Ferhat Abbas Sétif-1
Faculty of Sciences
Computer Science Department

THESIS

Presented By

Abdallah SOUALMI

As a Requirement to aim for the degree of

Doctorate 3rd cycle LMD in Computer Science

Option: Smart System and Machine Learning

Title

Protection of Medical images Content on the Cloud by Secret Information Hiding for Supporting Telemedicine

Defended On: 04 /05 /2021 **Board of Examiners :**

Pr. Abdelhamid BENHOCINE	Prof. University of Ferhat Abbas Setif-1	President
Dr. Adel ALTI	MCA. University of Ferhat Abbas Setif-1	Reporter
Dr. Lamri LAOUAMER	MCA. University of Qassim – Saudi Arabia	Co-Reporter
Dr. Lyazid TOUMI	MCA. University of Ferhat Abbas Setif-1	Examiner
Dr. Samir AKHROUF	MCA. University of Mohamed Boudiaf M’sila	Examiner

بسم الله الرحمن الرحيم

Acknowledgement

First, I would like to express my sincere gratitude and thanks to my thesis advisors: Adel Alti and Lamri Laouamer for their valuable guidance's and precious advices during all the thesis period to accomplish this work.

I also express my thanks to Professor Morad Benyoucef who gives me an opportunity for an internship in the electronics lab at Telfer School of Management in the University of Ottawa.

Secondly, I would like to thank the jury members for giving me the honor of evaluating this work.

Finally, my thanks and gratitude are dedicated to my precious parents my life sunshine, my brothers, my grandfather and my friends: Yassin, Rabie, Madjed, Kheirou, Ilyes and Hamza for their support during all my life.

Thanks All.

Abstract

The protection of the transmitted and stored electronic patient information's; need the ensuring of many criteria such: confidentiality, integrity, and robustness against all intentional or unintentional attempts that used to access or destroy these data. For these purposes, we have brought many contributions in crypto watermarking. The main one is the proposition of two robust methods: a blind medical image watermarking technique based on DCT transform, Weber descriptor, and Arnold chaotic map, and a semi blind technique using DCT and Schur Decompositions. The second contribution is the proposal of two new semi-fragile techniques for medical image authentication with low computational complexity. The first technique combines DWT and Schur transforms, while the second technique combines Schur transform and Chaotic sequence. The last contribution is two fragile watermarking methods, which achieves high imperceptibility and better integrity checking of medical data. The first method combines the SURF and weber descriptors and Arnold chaotic map while the second based on Schur transform.

Key words: Watermarking, Medical Data Security, Integrity, Robustness, Imperceptibility, Computational complexity, Attacks, DICOM.

List of Content

List of Content……………………………………………………………………………...I

List Of Figures III

List Of Tables.. VIIII

List Of Abbreviations..VIII

General Introduction 1

Part 1: Theoretical Background.. 4

Chapter 1 Data Protection In Unsecured Environment 5

1.1 Introduction.. 6

1.2 Data Security 6

1.2.1 DEFINITION 6

1.2.2 NOTIONS OF DATA SECURITY 6

1.2.3 DATA SECURITY SYSTEMS 7

1.3 Cryptography 7

1.4 Digital Watermarking Concepts 8

1.4.1 HUMAN VISUAL SYSTEM (HVS) 9

1.4.1.1 Contrast *9*

1.4.1.2 Just Noticeable Difference (JND)... *9*

1.4.1.3 Blue Component.. *9*

1.4.2 DIGITAL WATERMARKING CLASSIFICATION... 9

1.4.2.1 Classification Based On The Embedding Domain *10*

1.4.2.2 Classification Based On The Extraction Mode *15*

1.4.2.3 Classification Based On Robustness *17*

1.4.3 DIGITAL WATERMARKING PROPERTIES 17

1.4.3.1 Imperceptibility *17*

1.4.3.2 Embedding Capacity (Payload)... *17*

1.4.3.3 Computational Complexity *17*

1.4.3.4 Security... *18*

1.4.3.5 Robustness.. *18*

1.4.4 MALICIOUS ATTACKS AND QUALITY MEASURES... 18

1.4.4.1 Malicious Attacks *18*
1.4.4.2 Quality Measures *23*
1.4.5 APPLICATION OF DIGITAL WATERMARKING 25
1.4.5.1 Copyright Protection *25*
1.4.5.2 Fingerprinting *25*
1.4.5.3 Authentication *25*
1.4.5.4 Tamper Detection *25*
1.4.5.5 Content Description *26*
1.4.5.6 Content Archiving *26*
1.4.5.7 Broadcast Monitoring *26*
1.5 Conclusion 26
Chapter 2: Literature Reviews 27
2.1 Introduction 28
2.2 Robust Watermarking Approaches 28
2.3 Semi-Fragile Watermarking Approaches 34
2.4 Fragile Watermarking Approaches 40
2.5 Comparison And Evaluation 44
2.6 Conclusion 45
Part 2: Contributions 46
Chapter 3: Robust Medical Image Watermarking Techniques 47
3.1 Introduction 48
3.2 Robust Medical Images Watermarking Methods 48
3.2.1 A NEW BLIND MEDICAL IMAGE WATERMARKING BASED ON WEBER DESCRIPTORS 48
3.2.1.1 Weber Law Descriptors (Wds) 49
3.2.1.2 Arnold Chaotic Map 49
3.2.1.3 Proposed Watermarking Method 50
3.2.1.4 Experimental Results And Discussions 54
3.2.2 SCHUR AND DCT DECOMPOSITION BASED MEDICAL IMAGES WATERMARKING 60
3.2.2.1 Digital Imaging And Communication In Medicine (DICOM) 61
3.2.2.2 Proposed Watermarking Method 63
3.2.2.3 Experimental Results 66
3.3 Synthesis And Discussion 70
3.4 Conclusion 71
Chapter 4 Semi-Fragile Medical Image Watermarking Techniques 72
4.1 Introduction 73

4.2 Semi-Fragile Watermarking Approach's ... 73

4.2.1 A DWT AND SCHUR DECOMPOSITION BASED BLIN IMAGE WATERMARKING METHOD ... 73

4.2.1.1 Proposed Watermarking Method ... *73*

4.2.1.2 Experimental Results And Evaluation ... *77*

4.2.2 A NOVEL BLIND MEDICAL IMAGE WATERMARKING SCHEME ... 80

4.2.2.1 Chaotic Sequence ... *80*

4.2.2.2 Proposed Watermark Embedding And Extracting Processes ... *80*

4.2.2.3 Experimental Results And Discussion ... *85*

4.3 Synthesis And Discussions ... 93

4.4 Conclusion ... 94

Chapter 5 Fragile Medical Image Watermarking Techniques ... 95

5.1 Introduction ... 96

5.2 Proposed Fragile Medical Image Watermarking Methods ... 96

5.2.1 A NOVEL BLIND FRAGILE WATERMARKING ... 96

5.2.1.1 Speed Up Robust Features (SURF) Descriptor And Detector ... 96

5.2.1.2 Watermark Embedding And Extracting Processes ... 97

5.2.1.3 Experimental And Performance Results ... 102

5.2.2 A BLIND FRAGILE BASED MEDICAL IMAGE AUTHENTICATION 105

5.2.2.1 Watermark Embedding Phase ... 106

5.2.2.2 Watermark Extraction Phase ... 107

5.2.2.3 Experimental Results ... 108

5.3 Synthesis And Discussions ... 111

5.4 Conclusion ... 111

General Conclusion ... 112

References ... 116

List of Figures

Figure 1.1: Data Security System [4]..……………………………………………… 7

Figure 1.2: The generic model of the watermarking process ………………………. 8

Figure 1.3: DCT bands Coefficients………………………………………………… 11

Figure 1.4: DCT transform illustration……………………………………………… 12

Figure 1.5: DWT sub-bands (Level 1)………………………………………………. 12

Figure 1.6: Example of DWT transform…………………………………………….. 13

Figure 1.7: NTT transform illustration……………………………………………… 14

Figure 1.8: Blind watermarking illustration………………………………………… 16

Figure 1.9: Semi-blind watermarking illustration………………………………….. 16

Figure 1.10: Non-blind watermarking illustration………………………………….. 16

Figure 1.11: Digital watermarking system propriety requirement…………………. 18

Figure 1.12: JPEG compression attack with different compression factor………… 19

Figure 1.13: noise attacks illustration………………………………………………. 19

Figure 1.14: median filtering attacks illustration…………………………………... 20

Figure 1.15: dithering attack demonstration……………………………………….. 20

Figure 1.16: histogram equalization attack demonstration ……………………….. 21

Figure 1.17: gamma correction attack demonstration……………………………… 21

Figure 1.18: rotation attack demonstration………………………………………… 23

Figure 1.19: cropping attack demonstration……………………………………….. 23

Figure 1.20: scaling attack demonstration…………………………………………. 23

Figure 1.21: translation attack demonstration……………………………………… 23

Figure 2.1: Singh et al [64] embedding block diagram…………………………….. 29

Figure 2.2: Dong et al [95] embedding operation. ………………………………… 30

Figure 2.3: Liu et al [72] block diagram of watermark embedding………………… 30

Figure 2.4: Wang et al [71] embedding operation………………………………….. 31

Figure 2.5: Roy et al [21] embedding block diagram………………………………. 32

Figure 2.6: Vaidya et al [44] embedding process…………………………………… 32

Figure 2.7: Huo et al [101] watermark embedding process………………………… 34

Figure 2.8: Prasad et al [99] watermark embedding process……………………….. 35

Figure 2.9: Falgun et al.[81] block diagram of watermark embedding…………….. 36

Figure 2.10: Moussavi et al [82] block diagram of watermark embedding………… 37

Figure 2.11: Hou et al [97] main steps of watermark embedding process………….. 38

Figure 2.12: Khalil et al [91] embedding process block diagram………………… 41
Figure 2.13: watermark embedding process of work presented in [88]………….. 42
Figure 2.14: main steps of watermark embedding of work presented in [89]……. 43
Figure 3.1: Watermark embedding process…………………………………….. 51
Figure 3.2: Watermark Bit embedding phase…………………………………… 52
Figure 3.3: Watermark extracting process………………………………………. 53
Figure 3.4: Watermark Bits extracting phase…………………………………… 55
Figure 3.5: Cover medical images and Watermark…………………………….. 55
Figure 3.6: DICOM File Basic Structure……………………………………….. 62
Figure 3.7: DICOM Header Element….……………………………………... 63
Figure 3.8: DICOM meta information Example..………………………………. 63
Figure 3.9: DICOM meta information representation ……………………………. 64
Figure 3.10: DICOM image principal component…...…………………………….. 64
Figure 3.11: General generic model of the proposed method……………………… 65
Figure 3.12: Watermark embedding process…………………………………….. 66
Figure 3.13: Example of new blocks pixel intensity after embedding ……………… 66
Figure 3.14: Watermark extracting process of the proposed method……………... 67
Figure 3.15: Watermark image used in experiment…………………………….. 68
Figure 3.16: Sample of medical images used in experimentation…………………. 68
Figure 3.17: Watermarked images with different values of α…………………….. 69
Figure 3.18: PSNR (dB) comparison results with recent works described ………. 70
Figure 4.1 Watermark embedding process main steps……………………………. 76
Figure 4.2 Watermarking extraction process main steps……………………………… 77
Figure 4.3 Sample of medical images used and watermark used in experimentation… 78
Figure 4.4: Watermark embedding process……………………………………….. 84
Figure 4.5: Example of new blocks pixel intensity values after embedding ……… 83
Figure 4.6: Watermark extracting process…………………………………………… 85
Figure 4.7: binary Watermark image used in experimentation……………………... 85
Figure 4.8: Sample of host images used in experimentation………………………... 86
Figure 4.9: Imperceptibility comparison between the proposed method ………….. 86
Figure 5.1: Watermark embedding process……………………………………….. 97
Figure 5.2: Watermark Bits embedding phase…………………………………… 98
Figure 5.3: 3x3 Block illustration………………………………………………… 99
Figure 5.4: Watermark extraction process……………………………………….. 100
Figure 5.5: Watermark Bits extracting phase…………………………………….. 101
Figure 5.6: Medical cover image and Watermark image. …………………………. 102

Figure 5.7: Generic model for the proposed method……………………………… 105
Figure 5.8: Watermark embedding main steps…………………………………….. 106
Figure 5.9: Example of new blocks pixel intensities after embedding of bits……. 107
Figure 5.10: Watermark extracting main steps…………………………………….. 108
Figure 5.11: Watermark image used in the experimentation……………………… 108
Figure 5.12: Sample of image used in the experimentation………………………. 109
Figure 5.13: Imperceptibility comparison..………………………………………… 109

List of Tables

Table 2.1: Comparison of robust watermarking works……………………………. 33

Table 2.2: Comparison of semi-fragile watermarking works……………………… 38

Table 2.3: Comparison of different fragile watermarking works………………….. 43

Table 3.1: Example of the realized application executed on image (a) and (b)…… 56

Table 3.2: PSNR values between the original and the watermarked images……… 57

Table 3.3: The obtained Robustness measurement (using Stirmark Benchmark)…. 57

Table 3.4: The obtained robustness measurement (Using MATLAB)…………….. 59

Table 3.5: Time required for embedding and extracting the watermark…………. 60

Table 3.6: The obtained PSNR values of our method compared with other works… 61

Table 3.7: The obtained computational complexity compared with other works…. 61

Table 3.8: Performance analysis under NC values………………………………… 61

Table 3.9: Imperceptibility evaluation of the proposed watermarking method…… 69

Table 3.10: NC values of the extracted watermark………………………………… 70

Table 3.11: Robustness comparisons between the proposed method and [65, 44].. 71

Table 4.1 PSNR (dB) values of the proposed method……………………………. 79

Table 4.2 List of attacks used in experimentation……………………………….... 79

Table 4.3 Robustness measurement under NC values…………………………….. 79

Table 4.4 Comparisons of imperceptibility results using medical images……..... ……. 80

Table 4.5 Robustness comparison with works presented in [65, 81, 82]…………… 80

Table 4.6 PSNR values (dB) using different watermark size………………………. 86

Table 4.7 PSNR values (dB) using different watermark size………………………. 86

Table 4.8: The Applied attacks names abbreviation………………………………… 87

Table 4.9: the attacked watermarked images and the extracted one ……………… 88

Table 4.10: The NC and BER values of the extracted watermark from different images. 90

Table 4.11: NC values comparison after salt & pepper noise attack (Sp)………… 91

Table 4.12: NC values comparison after DICOM JPEG Compression lossy attack 91

Table 4.13: Features comparison between some recent works and the proposed … 91

Table 5.1: PSNR values between the original and the watermarked images………….. 102

Table 5.2: Time required for embedding and extracting the watermark……………… 103

Table 5.3: Tamper detection precision of our technique……………………………… 103

Table 5.4: Comparison of the PSNR between our method and [43, 86-90]………….. 104

Table 5.5: Imperceptibility evaluation of the proposed watermarking method………. 109

Table 5.6: execution time measurement……………………………………………… 110

List of Abbreviations

BER	Bit Error Rate
BND	Binocular Notification Difference
BT	Binomial Transform
BTC	Block Truncation Coding
CRC	Correlation Coefficient
CT	Contourlet Transform
dB	Decibel
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DICOM	Digital Imaging and Communicating in Medicine
DWT	Discrete Wavelet Transform
DTVWT	Dual-Tree Complex Wavelet Transform
EPR	Electronic Patient Record
FSDWT	Faber Schauder Discrete Wavelet Transform
GA	Genetic Algorithm
HH	High High Sub-band
HL	High Low Sub-band
HVS	Human Visual System
HWT	Haar Wavelet Transform
IIDWT	Integer to Integer Discrete Wavelet Transform
JPEG	Joint Photographic Experts Group
JND	Just Noticeable Difference
LBP	Local Binary Pattern
LH	Low High sub-band
LL	Low Low sub-band
LSB	Least significant Bit
LUD	Lower Upper Decomposition
LVQ	Lattice Vector Quantization
LWT	Lifting Wavelet Transform
MDE	Modified Difference Expansion
MSE	Mean Square Error
NC	Normalized Correlation
NTT	Number Theoretic Transform
OHT	Ordered Hadamard Transform
PSNR	Peak Signal Noise Ratio
QIM	Quantization Index Modulation
RESC	Rescale
RGB	Red Green Blue
RML	Remove Line Attack
RNDDIST	Random Distortion
ROI	Region Of Interest
RONI	Region Of Non-Interest

SVD	Singular Value Decomposition
SSIM	Structural Similarity
ST	Slant Transform
SURF	Speed Up Robust Features
WDs	Weber Descriptors

General Introduction

In the last years, Networks technology has witnessed a great development and enhancement in different fields. The main field that influence people advancement is Internet. Internet becomes a backbone in our daily life. It is an easy and fast solution to access, deliver, use services, and exchange multimedia data (texts, images, audios and videos) among different sites. However, the moving of services and data through Internet has revealed many security challenges espeically on user's data integrity and authenticity. Information security is the process of keeping data protected from unauthorized access, and illegal using of data. In this context, the focus of data security is to make sure that it's safe and away from any destructive forces or malicious behavior. Therefore, unauthorized access to sensitive data or information can cause many problems such as corruption and violation of privacy. In order to guarantee the security, the implementation of advanced security techniques is extremely required.

The E-health applications basically uses telecommunication technologies; to supply healthcare where the patient and medical personnel are geographically distant.

The medical image is considered as main core in telemedicine, it's used for diagnosis in hospitals, as a result, if the image undergoes any modification and even the slightest, the interpretation of the physician could differ, and consequently this could provoke wrong diagnosis. For that reason, medical images request strong security. Where the interchanging of medical images between clinics and hospitals, is happened through unsecured networks; this could provoke losing, corruption or stealing of data.

Among the previous solutions for the security threats that can be considered as one of the powerful protection systems is cryptography. It consists of making the data unreadable for unauthorized side. However, it protects the information's only during its transmission; this means that once data are decrypted, we couldn't prevent their modification or illegal reproduction. The watermarking is proposed as the cryptography complement. It consists of embedding data in an image to ensure integrity and authenticity; where the physician will be able to detect the alteration of the medical image and will not use the image for diagnosis if it is not authorized. However, the main condition that must be respected is that the physician must be able to extract the embedded watermark perfectly without loses.

In e-Health the watermarking is used to embed information related to the medical image; e.g. patient information's which composite from physician name, hospital name…etc. (case of DICOM format), these information's are very useful in telemedicine; and the the received data mustn't affected, modified or sent by intended sender.

The transmission of medical data requires the presence of three major's elements; namely, confidentiality, authenticity, and reliability (integrity and availability). The confidentiality is ensured when an unauthorized user can't access or modify the medical image information. Authenticity means that the received medical image is obtained from the authorized sender. Integrity means that the received medical image should not be altered during transmission. The availability means that the medical image is available when it is requested from the physician.

Despit that, several watermarking algorithms have been proposed, a number of new techniques or improved ones have been developed–and each method contains a number of associated advantages as well as specific limits, many recent methods are illustrated in details in chapter 2.

The main objective in our research is to ensure and prove the authenticity and integrity of medical data. Where the main purpose of these researches; is to support the health care system in order to implement a secure, imperceptible and fast system based on watermarking methods.

Thesis Organization

The thesis contains five chapters; the first two chapters are more theoretical; describing the main principles and some relevant previous studies in watermarking. The chapters three to five present our contributions in image watermarking.

The chapter one, presents the basics requirement and the main principles of watermarking techniques.

The chapter two, presents a literature review of digital image watermarking. In this chapter we present three watermarking categories: robust, semi-fragile and fragile recent watermarking methods.

Chapter three carried the proposed robust watermarking methods in detail. It comprises three sections; the first one is an introduction, in the second we present a new blind robust watermarking method based on Weber descriptors and Discrete Cosine Transform (DCT) and the third section discusses a new robust semi-blind watermarking approach based on DCT and Schur decomposition.

Chapter four presents our semi-fragile watermarking contribution in detail. It contains two methods; the first as a new blind method using Discrete Wavelet Transform (DWT) and Schur Decomposition, while the second is a fast-blind method based on Schur decomposition and chaotic sequence.

chapter five present our contribution in fragile watermarking methods. It contains a new blind fast and imperceptible watermarking method based on Weber descriptors and surf points, and the second method is based on Schur and Arnold scrambling.

Finally, Conclusion and perspectives are presented to conclude this thesis.

Part 1: Theoretical Background

Chapter 1

Data Protection in Unsecured Environment

Content

1.1 Introduction……………………………………………………………………6

1.2 Data Security…………………………………………………………….…..6

1.2.1 DEFINITION……………………………………………………….……….6

1.2.2 NOTIONS OF DATA SECURITY……………………………….....……….6

1.2.3 DATA SECURITY SYSTEMS...7

1.3 Cryptography……………………………………………………………….7

1.4 Digital Watermarking Concepts……………..…….…………………...…8

1.4.1 HUMAN VISUAL SYSTEM (HVS) …………………………………......…9

1.4.2 DIGITAL WATERMARKING CLASSIFICATION……………………………....9

1.4.3 DIGITAL WATERMARKING PROPERTIES………………………………..…17

1.4.4 MALICIOUS ATTACKS AND QUALITY MEASURES…….……………….……18

1.4.5 APPLICATION OF DIGITAL WATERMARKING. …….…………….……..25

1.5 Conclusion..26

1.1 Introduction

Nowadays, the emergence of high-throughput applications in multimedia networks has often a great interest to research community. This applications are characterized by an important and voluminous amount of data compared to traditional applications. Consequently, It becomes an integral part of multiple real-life domains (*military, health, education ...etc.*) [1, 6, 25, 38]. Protecting such information's is the main institutional concerns. Data security and privacy continuous to be a fundamental requirement which need developing new strategies that considers the specific characteristics properties of these kinds of applications [23, 28, 51]. It is necessary that encryption and watermarking techniques must be performed at the source data which makes sense to really protect data upon starting. We can tackle the full data security issues through important three steps, monitoring data, gaining visibility in the unsecured environment and managing access.

This chapter is organized as follows: section 2 focusses on different security aspects. Section 3 defines the encryption concepts. Section 4 describes digital watermarking techniques, watermarking systems classification, watermarking systems property, malicious attacks, and quality measures. We particularly focus on image watermarking and their application techniques. Section 5 concludes the chapter.

1.2 Data Security

1.2.1 Definition

Data security is the protection of confidential information from unauthorized party [4]; where only authorized users could access and/or modify any information.

1.2.2 Notions of data security

The information security follows three principals' concepts [4]; refers to confidentiality, reliability, and availability. The confidentiality means that only the authorized persons could accede information. The reliability could be defined in terms of two principal's concepts: integrity and authentication. Integrity refers to the ability to allow only authorized person to change information. Authentication provides the identification of the sender of data. Finally, the availability designs the capacity of a system to be exploited by authorized users in normal conditions.

1.2.3 Data security systems

The data security systems are composed of two essential components called: cryptography and watermarking (Figure 1.1).

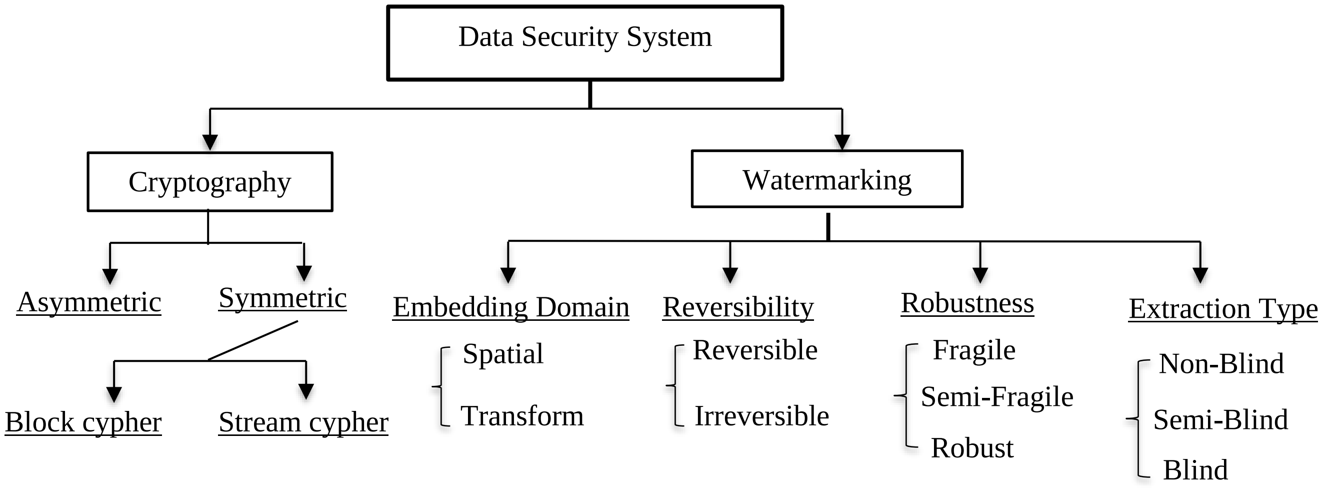


Figure 1.1 Data Security System [4].

1.3 Cryptography

The cryptography is the ability to make the content of the document unreadable and unintelligible, which cannot be understood by unauthorized users. The cryptography methods are divided into "Symmetric key cryptography", "Asymmetric key cryptography" or hash function encryption methods [4].

The symmetric key encryption algorithm is a class of algorithms that use the same secret key by both sender and receiver for encrypting/decrypting data's. Prior to transmission of a plain data, the key distribution center provides both the sender and the recipient with a shared key. The most popular symmetric algorithms are: AES, DES…etc. Stream and block ciphers are usually used with symmetric keys. A stream cipher is a method of representing plain data as a stream of data (bit or byte), and it encrypts/decrypts one stream at the same time. While in the block cipher, the plain data are divided into blocks. where each block contains a set of bites or bytes, and it encrypts/decrypts its input one block at the same time.

The asymmetric key encryption is a class of algorithms which require two separate keys, one is private and the other is public. The sender encrypts the plain data using the public key whereas the receiver decrypts cipher data using the private key.

The hash function encryption is a one-way function [4], which mean that it's difficult to obtain the plain data from the hashed one. It generates static output data size called the hash code from a variable plain data, and any slight change or modification in the input text will provide us with a different text as output, which is farthest than any previous one [52].

The cryptography protects the document only during its transmission, which means that once the document is decoded, we cannot protect it against any unauthorized or undesirable changes or deletion of data [40].

1.4 Digital watermarking concepts

The digital watermarking technique has emerged as an alternative that can complement the cryptography. It consists of embedding the data information into a host image [16, 36, 110-112] to enhance data integrity, protect the benefits of the document and prohibit the illegal reproduction [9, 18, 23, 35]. Figure 1.2 shows the generic model of a watermarking framework.

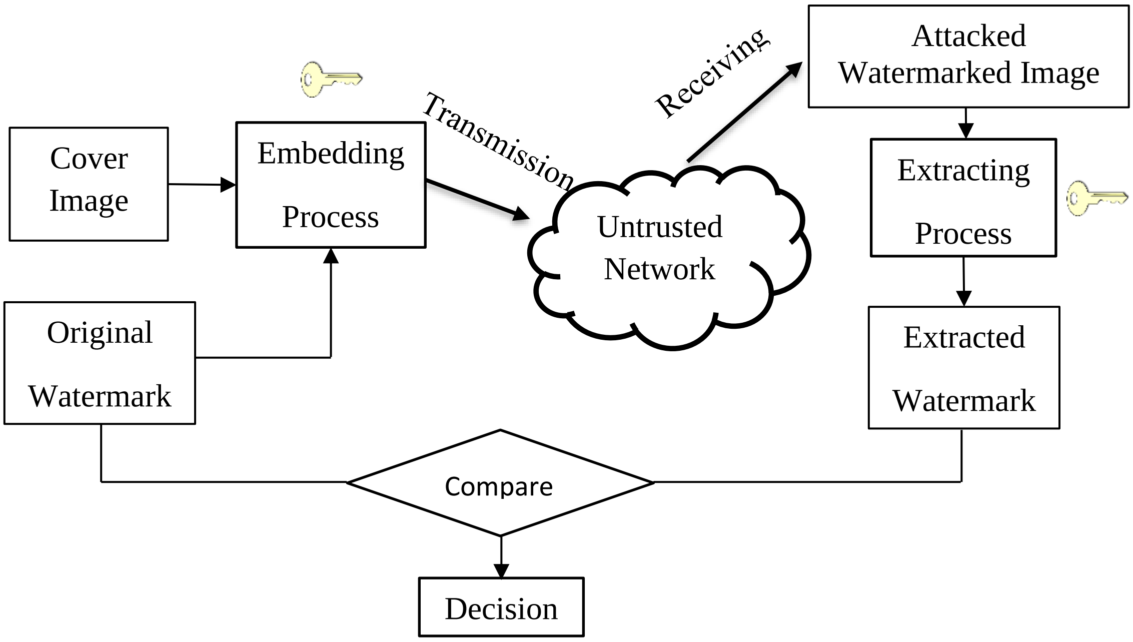


Figure 1.2 The generic model of the watermarking process.

In the following, we will discuss the most important properties of digital watermarking methods and techniques.

1.4.1 Human Visual System (HVS)

HVS is a complex system which is composed of three principles tasks: encoding, representation and interpretation [102, 103]. In the sequel, the HVS has dependability on the eye anatomy, where is based on physiological models that are described in microscopic level [102]. Among the principal elements that affect directly the HVS interpretation we mention: contrast, blue color component and Just Noticeable Difference (JND).

1.4.1.1 Contrast

Contrast is the ratio value between the brightness of a pixel or image part and brightness of his background [103].

The contrast value depends on relative variations of luminance for such periodic pattern [102] and calculated using the following equation:

$$C=(Lmax-Lmin)/(Lmax+Lmin) \qquad (1.1)$$

Where Lmax and Lmin are the maximum and minimum luminance values of a periodic pattern of a sinusoidal grating.

1.4.1.2 Just Noticeable Difference (JND)

The JND defines the smallest visibility threshold of the HVS [107]. The properties of HVS directly are exercised by the JND profiles. JND profiles are categorized in two folds: pixel-based and sub-band based (e.g. DCT, DWT, ..etc.), the pixel-based profiles are derived in the pixel domain and consider luminance adaptation, this refers to the masking effect of the luminance for background effect and contrast masking effects which leads to the reduction of visibility of one visual signal at the presence of another one.

1.4.1.3 Blue Component

The human eye is less sensitive to the blue color than red or green colors [104]. To this end, increasing blue color intensity in order to embed the watermark doesn’t affect so much the image quality.

1.4.2 Digital watermarking classification

As shown in Figure 1.1, the watermarking methods could be classified using many criteria. In the following we will describe some available classification on literature.

1.4.2.1 Classification based on the embedding domain

The watermarking techniques can be categorized as *spatial* or *frequency* techniques [10, 12].

- *Spatial domain methods*

The spatial watermarking techniques are directly operated on image pixels [21] which make the embedding/extracting operations require less computationally. However, these techniques lack robustness. As follow we present the most popular watermarking methods in spatial domain.

a. Least Significant Bit (LSB)

The principle of LSB is to present the pixel intensity value into binary representation in 8 bits, and then replaced by the least significant bit (the first in right) by the watermark bit value. The binary representation converted into decimal value to obtain the watermarked pixel intensity value. The interest of LSB and modified bit *(add or subtract 1*) is imperceptible and does not affect the image quality. However, the major drawback of LSB is their low robustness especially against nosing, rotation, compression and LSB removing [55, 56].

b. Local Binary Pattern (LBP)

LBP consist to decompose the image pixels into non-overlapping blocks of size NxN, and then the spatial relative between the significant pixel and its adjacent pixel in each block is calculated to obtain the local pixel differently. The local pixel difference is used for embedding and extraction of watermark. The LBP watermarking offers good robustness with against some attacks such: luminance modification and difference alteration, however it offers low robustness to other attacks such filtering and blurring [4].

c. Histogram Modification

The principle of this technique is to build a histogram based on pixel values, and then embed the watermark intensities by modifying the values between the maximum and minimum points of the histogram. The histogram modification technique provides a fast watermarking method. However, it suffers from the limited embedding capacity, because it’s limited by the number of points that is having the maximum value [57, 58].

- *Transform domain methods*

The frequency techniques are based on data computed from transform coefficients [17] such as: Discrete Cosine Transform (DCT) [21], Discrete Wavelet Transform (DWT) [33, 49, 53], Singular Value Decomposition (SVD) [31, 32]. The embedding/extracting operations require an important computational complexity but these techniques are often more robustness [3, 70]. As follow we present the most popular transform used frequency domain methods.

a. Discrete Cosine Transform (DCT)

The DCT basically separates the image (or block) into three parts of different frequency levels namely: *low*, *middle* and *high-frequency* coefficients (Figure 1.3), Embedding the watermark into middle-frequency coefficients give additional resistance to compression techniques without affecting the host image quality. The DCT coefficients contain two types of information's. The first one consists of the average intensity of the image, called DC coefficients, the second type called AC coefficients, as we move from DC coefficients to AC, the significant information about the image decreases. For an image I of size N × M, it transformed into DCT coefficients (DCT_I) illustrated in Eq. (1.2), while the DCT inverse is obtained using Eq. (1.3) [21, 42].

$$T_{I}= \frac{2}{\sqrt{n*m}} C(i).C(j) \sum_{x=0}^{n-1} \sum_{y=0}^{m-1} B(x,y) * \cos\left[\left(\frac{2x+1}{2n}\right)*i\pi\right] * \cos\left[\left(\frac{2y+1}{2m}\right)*j\pi\right] \qquad (1.2)$$

$$T_{I}= \frac{2}{\sqrt{n*m}} \sum_{x=0}^{n-1} \sum_{y=0}^{m-1} C(i).C(j)*T_{I}(x,y)*\cos\left[\left(\frac{2x+1}{2n}\right)*i\pi\right]*\cos\left[\left(\frac{2y+1}{2m}\right)*j\pi\right] \qquad (1.3)$$

Where $$C(i), C(j) = \begin{cases} \frac{1}{\sqrt{2}} \text{ if } i, j = 0. \\ 1 \text{ otherwise.} \end{cases} \qquad (1.4)$$

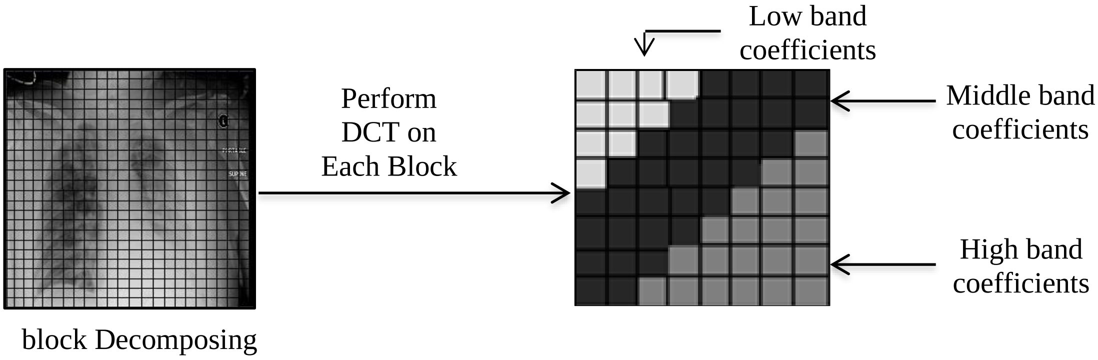
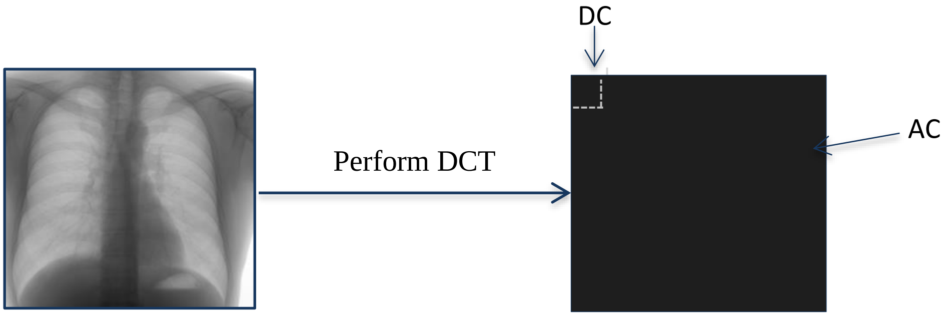


Figure 1.3 DCT bands Coefficients.

Figure 1.4 illustrate a medical image and it's transform.



Original image

Original image after DCT

Figure 1.4 DCT transform illustration.

DCT coefficients are widely used in JPEG File representation, where each chunks of the JPEG Bitstream contain encoded data which combines all encoded DCs and ACs coefficients from each block of the original image [105].

b. Discrete Wavelet Transform (DWT)

DWT [33, 49, 53, 73] decomposes an image into four sub-bands: a lower resolution approximation component (LL), horizontal components (HL), vertical component (LH) and diagonal component (HH) (Figure 1.5). The number of the sub-bands depends on the number of the decomposition level.

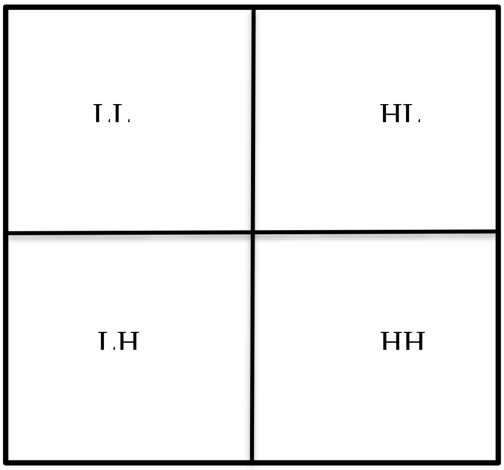


Figure 1.5 DWT sub-bands (Level 1).

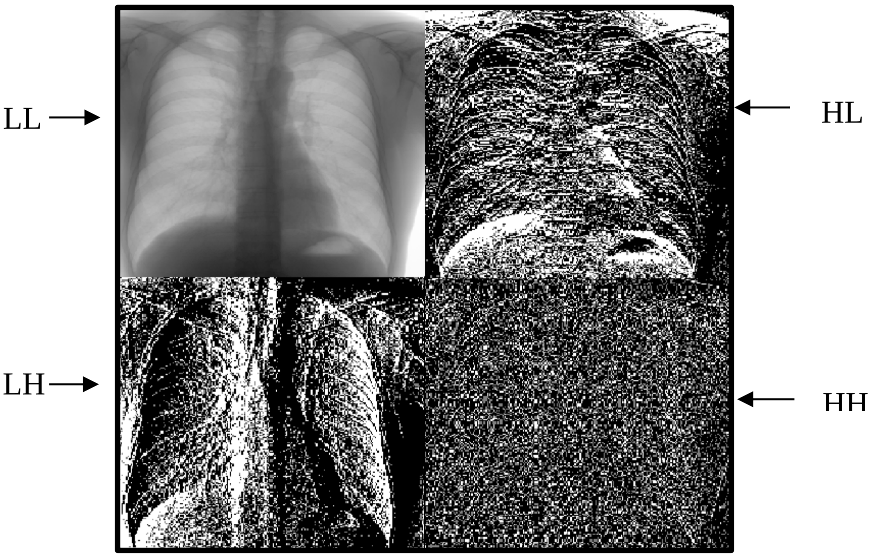


Figure 1.6 example of DWT Transform.

The energy of the high-frequency components (HL, LH, HH) is less, which represent the information's of the image, the low-frequency part concentrates most of the energy of the image and it can be decomposed continuously. The energy of the image is diffused better, with the more levels the image is decomposed by wavelet transform [39, 54]. The energy is calculated as follow:

$$E=\frac{1}{NnxMn}\Sigma i\Sigma j|In(i,j)| \qquad (1.5)$$

where n is the decomposition level, (In) is the coefficients of the corresponding sub-band, and Nn and Mn are sub-band dimensions.

Figure 1.6 illustrates an example after carrying DWT on image.

c. Number Theatrical Transform (NTT)

NTT [11], is a popular transform decomposition based on DFT. The NTT of a sequence $\mathbf{x} = \{\boldsymbol{x_n}\}_{\mathbf{n=0}}^{\boldsymbol{N-1}}$ composed of N elements defined in the Galois Field GF(*q*) of order q is a sequence= $\{\boldsymbol{X_k}\}_{\mathbf{k=0}}^{\boldsymbol{N-1}}$:

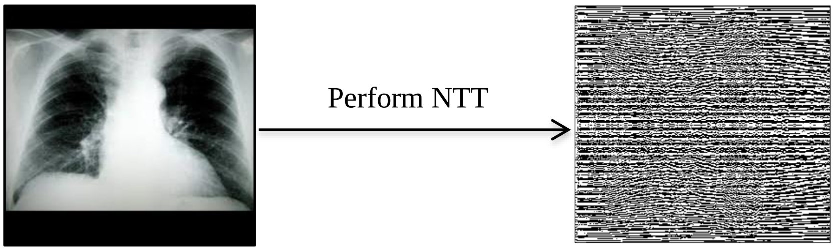
$$X_K = \left\langle \sum_{n=0}^{N} x_n \mathcal{S}^{nk} \right\rangle_q \qquad (1.6)$$

Where $k = 0, 1 \dots N-1$ and $\boldsymbol{\delta}$ represents the term generator of the order N, equal to the sequence length of the transform, of the field GF (q). The order N of the element $\boldsymbol{\delta}$, with $\mathbf{0} < \boldsymbol{N} < \boldsymbol{q} - \mathbf{1}$ is the value of the smallest positive integer p for which$\langle \boldsymbol{\delta}^{\mathbf{p}} = \mathbf{1} \rangle_{\boldsymbol{q}}$.

In case of images, the period N is the most important characteristic of NTT. Therefore we have to search for modulus q for which at least one N^{-1} δ exists. In this case, the determination of N^{-1} is possible by equation (2):

$$N^{-1} = q - ent(\frac{q}{N}) \qquad (1.7)$$

A root δ is guaranteed if $\boldsymbol{pgcd}(\boldsymbol{q}, \boldsymbol{\delta}) = \mathbf{1}$, i.e., it is not necessary that q is a prime number (case of $q=77=7 \cdot 11$ or $q=143=11 \cdot 13$). But it is necessary that $= \boldsymbol{pgcd}(\boldsymbol{q}, \boldsymbol{\delta}) = \mathbf{1}$. (Fig 1.7 show an example of using NTT on a medical image).



Original image Original image after applying NTT

Figure 1.7 NTT transform illustration.

d. Singular Value Decomposition (SVD)

SVD [31, 32, 109] is a mathematical model used to decompose a matrix (I) of size MxN to three matrix : U, V and S.

$$SVD(I)= [U, V, S] \qquad (1.8)$$

$$\text{And} \qquad I= U*S*V^T. \qquad (1.9)$$

Where U is an orthogonal matrix of size MxM, V is an orthogonal matrix of size NxN , and S is a pseudo diagonal of size MxN:

$$S=\begin{bmatrix} S1 & 0 & 0 \\ 0 & S2 & 0 \\ \dots \dots \dots & \dots \dots \dots & \dots \dots \\ 0 \dots \dots . & \dots \dots . & \dots . Sn \end{bmatrix}$$

S1..Sn are the singular values of I (real values non-negative which verify: S1>S2>..>Sn).

In general, SVD have much interests in image processing, and especially in watermarking domain:

1. Present the energy of the image, this mean that the maximum of energy in minimum singular value's.
2. The singular values of an image have a good stability: the image quality can be kept even the singular values are slightly tampered.
3. The SVD is unique, which mean that we couldn't get similar SVD for different images.

e. Schur Decomposition

Schur Decomposition [68, 69] is a mathematical model used to decompose a square matrix A into two matrices U and V:

$$Schur(A) = [U, V] \qquad (1.10)$$

Where U is a unitary orthogonal Matrix, while V reveals the intrinsic information of A in that many attributes and structure of matrices are invariant under similarity transform.

Schur^{-1} is simply the product operation of:

$$Schur^{-1} = U * V * U^{-1} \qquad (1.11)$$

The Schur decomposition is employed to embed a watermark, since the perturbation which could happen due to data embedding process in the host image could be reduced when data is embedded on matrix V. This could improve significantly the imperceptibility [69].

- *Informed domain methods*

The informed watermarking methods basically based on adapting the watermark signal to the cover one where the principal purpose is to eliminate the cover signal interferences on the watermark signal [59, 60, 61]. These kinds of methods are characterized by a large embedding capacity and imperceptibility [61]. This makes it more attractive by researchers in this last previous year [59, 62].

1.4.2.2 Classification based on the extraction mode

In terms of watermark extraction process, the watermarking schemes are regrouped into three categories: blind, semi-blind and non-blind schemes [32, 47]. For the first category, the

Watermark extraction process doesn’t require any of the original image and watermark (Figure 1.8) [42]. For the second, the watermark is required (Figure 1.9) [14] and for the last one, the extraction operation necessitate the presence of the original image (Figure 1.10) [26, 34].

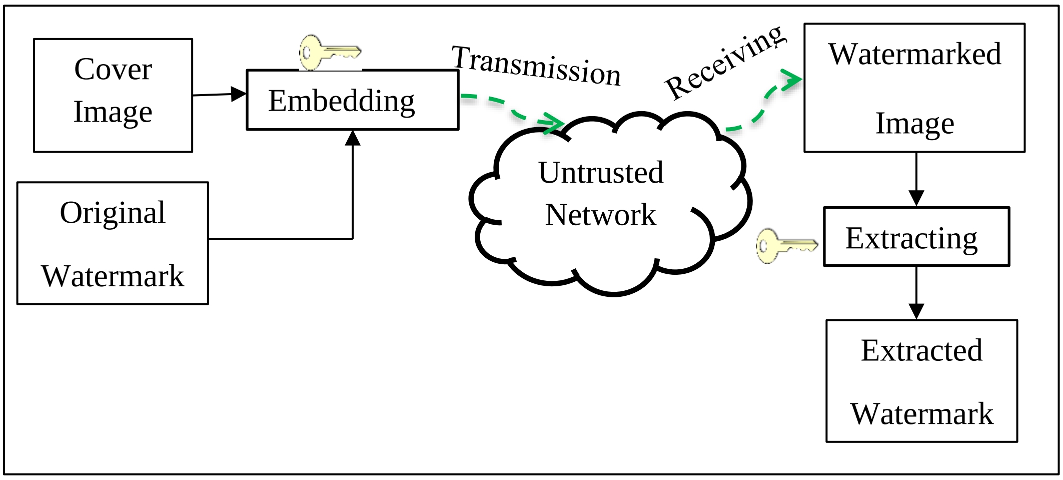


Figure 1.8 Blind Watermarking illustration.

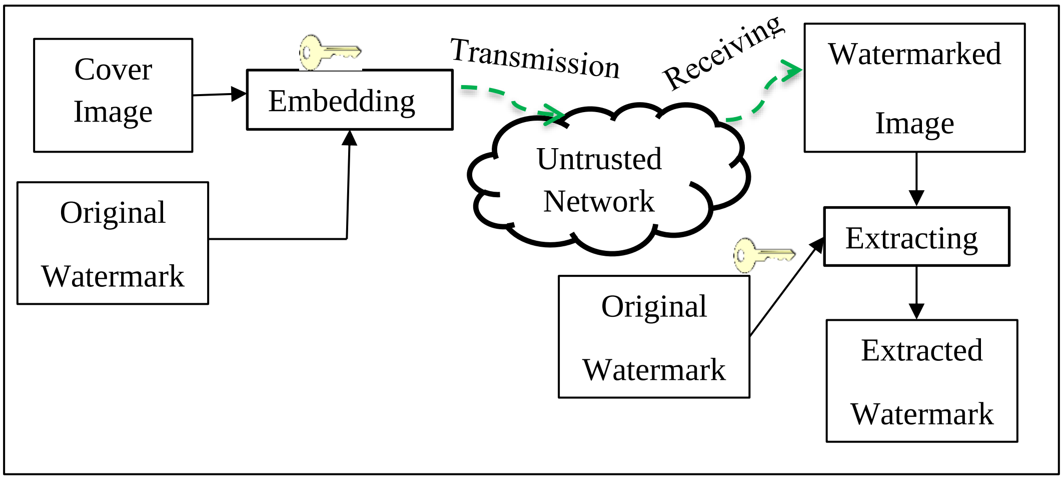


Figure 1.9 Semi-Blind Watermarking illustration.

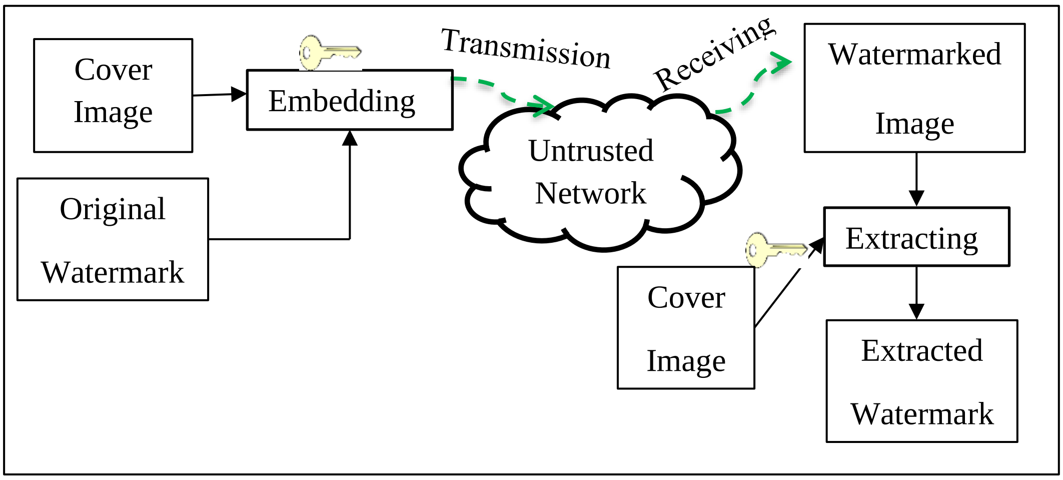


Figure 1.10 Non-Blind Watermarking illustration.

1.4.2.3 Classification based on robustness

Another classification of watermarking methods, called: robust, fragile, and semi-fragile [17, 35, 48]. In robust watermarking, the watermark is designed to resist after any operation used to alter the image [24, 43], while, in semi-fragile, the watermark needs to survive minor manipulation [15]. In fragile watermarking, the watermark collapse or degraded if the watermarked image undergoes any kind of alteration [13, 29]. These types of watermarking approaches have different applications, and they are employed according to the purpose of the watermarking system. For example, robust schemes could be used in order to prove the ownership and copyright protection, while fragile and semi-fragile are used for image authentication and data integrity checking [29]. It should be noted that, the majority of the watermarking techniques existing are semi-fragile or fragile.

1.4.3 Digital watermarking properties

The digital watermarking system has five important properties [11, 37] which must be achieved in any watermarking method: **imperceptibility**, **embedding capacity**, **complexity**, **security,** and **robustness** (Figure 1.11). Regardless of the kind of images, their sensitivity or the purpose of the watermark scheme, the approach must contain a trade-off between the five proprieties cited bellow.

- **Imperceptibility**

The imperceptibility is the similarity degree between the original image and the watermarked one [2].

- **Embedding capacity (Payload)**

The embedding capacity is the maximum amount of data could be hidden in the host image without degrading the image quality [29].

- **Computational complexity**

The computational complexity is the amount of time needed for the embedding and extracting operations [37].

- **Security**

Security refers to the security of the data embedded and extracted; it means that no one could remove or extract the watermark data without knowing the key used in embedding [7].

- **Robustness**

The robustness designs the degrees of resistance against any kind of manipulation [2].

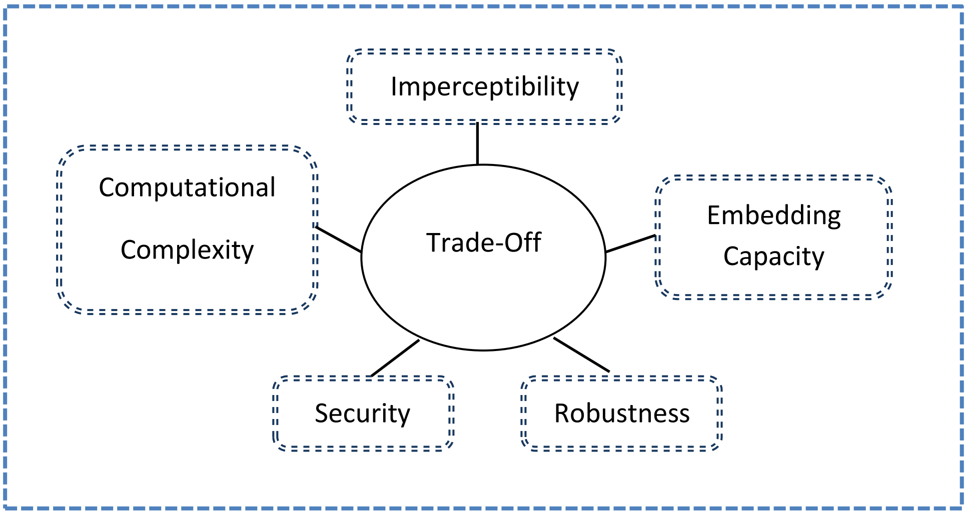


Figure 1.11 digital watermarking system propriety requirement.

1.4.4 Malicious attacks and quality Measures

The imperceptibility and robustness degrees are measured on term of the quality of watermarked image and the watermark extracted after attacks. In this section, we present the most known malicious attacks and quality measures used to analyze the imperceptibility and robustness.

1.4.4.1 Malicious attacks

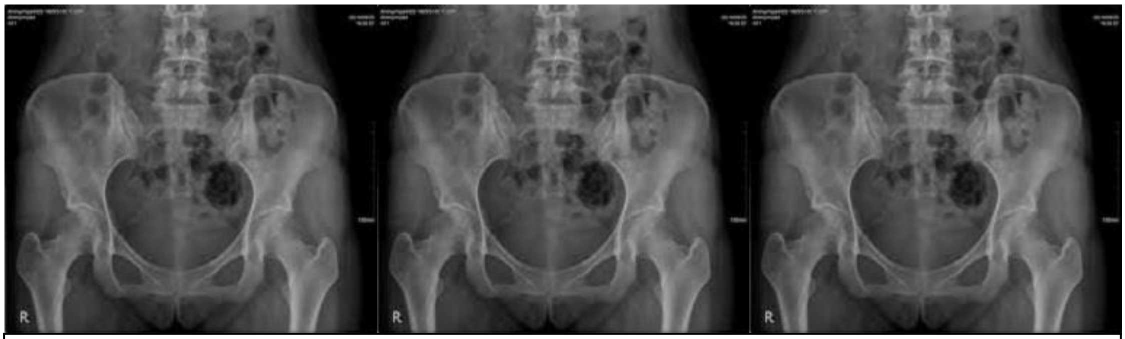
Several intentional attacks are cited in the literature, their common objective is to attempts to remove the watermark or confuse the authentication [30, 38, 41]. These attacks are regrouped into two principal groups namely: signal processing attacks and geometric attacks.

- *Signal processing attacks*

Called also image processing attacks, these types infect directly the signal of the image in order to remove the watermark [11]. Among the attacks of this category we cite:

a. JPEG compression

This attack decreases the image size by deleting the redundant information’s, and consequently affect the watermark data’s [19] (Figure 1.12 illustrate an example of JPEG Compression attack with Different Compression factors (QF)).

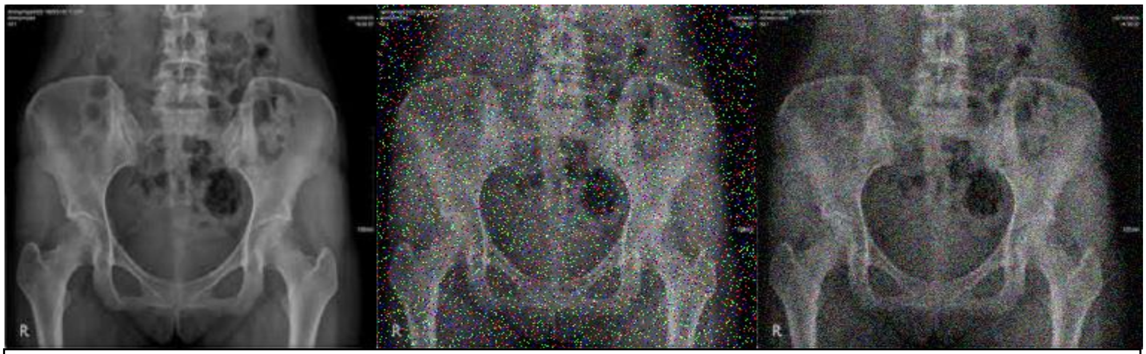


Watermarked image
JPEG Compression attack (QF=50)
JPEG Compression attack (QF=75)

Figure 1.12 JPEG compression attack with different compression factor.

b. Noising

The goal of this attack is to add noise (white, salt & pepper,..etc.) to the watermarked image in order to degrade the watermark quality and increase the difficulty of the extraction [49, 45]. The value of noise degree is in [0, 1]. (Figure 1.13 show an example of noising attack).

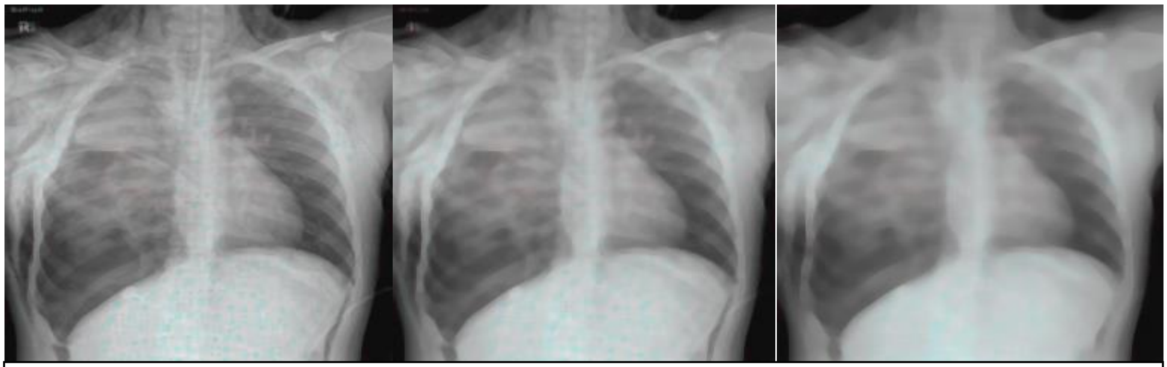


Watermarked image
Attacked watermarked image with salt & pepper noise
Attacked watermarked image with white noise

Figure 1.13 noise attacks illustration.

c. Filtering

Filtering attack is a signal processing operation which is used to reduce noise and enhance smoothness [44, 49]. Several filtering-based attacks are mentioned in literature, but the most known are Average filtering, Median filtering, and Weiner filtering. Average filtering replace each sample of the watermarked image with the average value of neighboring pixels [21]. Median filtering modifies the center pixel value with the middle value of the sorted pixel [20]. While Weiner filtering estimates the watermark data in order to generate the watermark embedded. This attack requires the basic knowledge of the embedding operation [20, 21]. (Figure 1.14 illustrate the Median filtering attack with different variation).

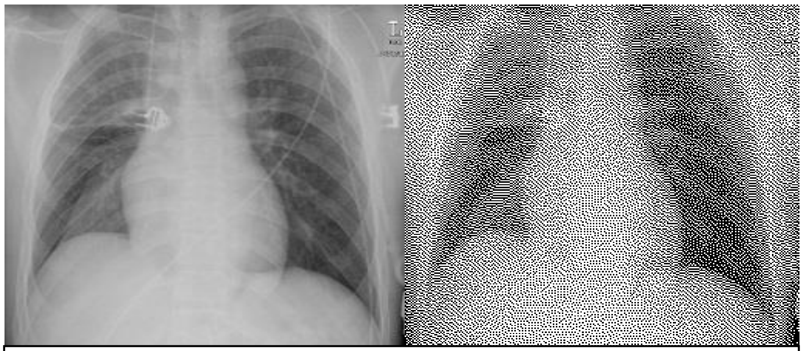


Watermarked image	Median_3	Median_7

Figure 1.14 Median Filtering attacks illustration.

d. Dithering

This attack is based on using a set of black and white points to represent the same number of image pixels and keep their integrated intensity. This makes the watermark distortion degree very important [27]. (Figure 1.15 illustrate an example of dithering attack).

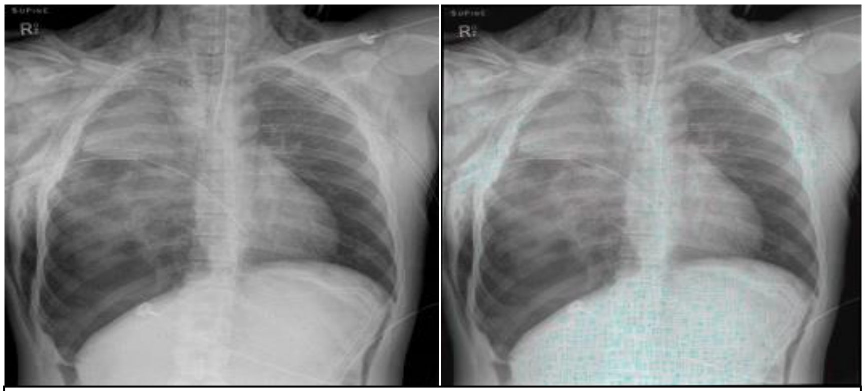


Watermarked image	Attacked watermarked image with dithering attack

Figure 1.15 dithering attack demonstration.

e. Histogram equalization

The role of this attack is to update some intensity of the histogram, this attack could even eliminate completely the watermark information [20]. (Figure 1.16 present an illustration of histogram equalization attack).



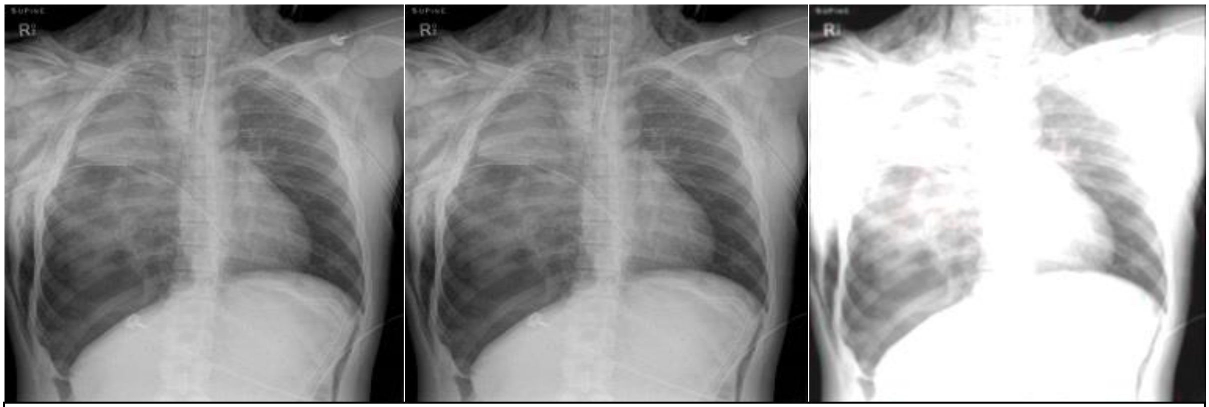
Watermarked image

Attacked watermarked image with histogram equalization

Figure 1.16 histogram equalization attack demonstration.

f. Gamma correction

Gamma correction attack aims to adjust the image quality with power low transformation in order to cause high distortion to the watermark [21]. (Figure 1.17 present an illustration of gamma correction attack with different variety of gamma).



Watermarked image

Gamma Correction 0.95°

Gamma Correction 0.50°

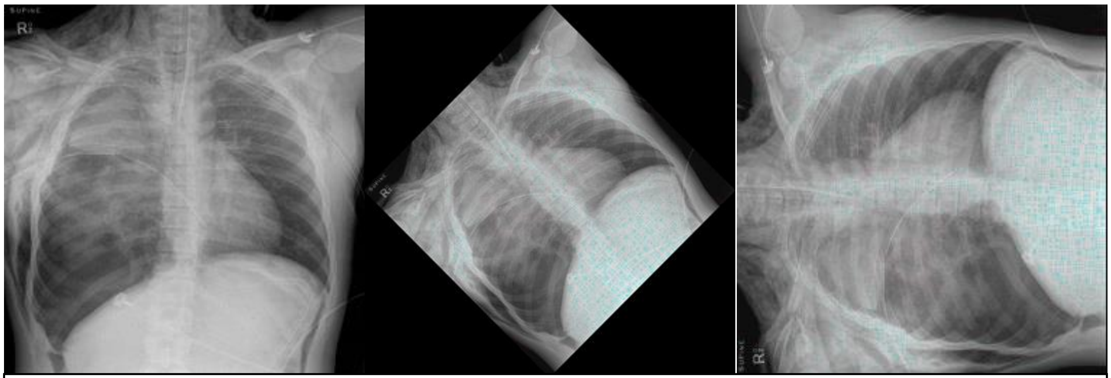
Figure 1.17 gamma correction attack demonstration.

- *Geometric attacks*

The mean purpose of this kind of attacks is to destroy the synchronization of detection in order to make the extraction process difficult and even impossible [22]. The most geometric attacks used are rotation, cropping, scaling and translation. (Fig 1.19 illustrate the gamma correction attack).

a. Rotation

The principle of this attack is to rotate the watermarked image from 0° to 360° in order to affect the watermark data [20, 44]. (Figure 1.18 present an illustration of rotation attack).



Watermarked image

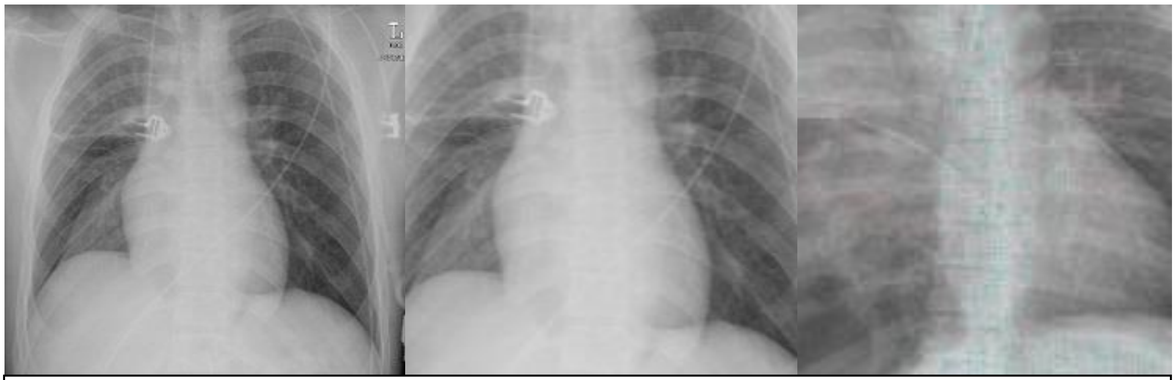
Rotation 45°

Rotation 90°

Figure 1.18 rotation attack demonstration.

b. Cropping

The essential task of this attack is the removing of the borders of uniform color in order to destabilize the extraction operation [45]. (Figure 1.19 present cropping attack with different variation).



Watermarked image

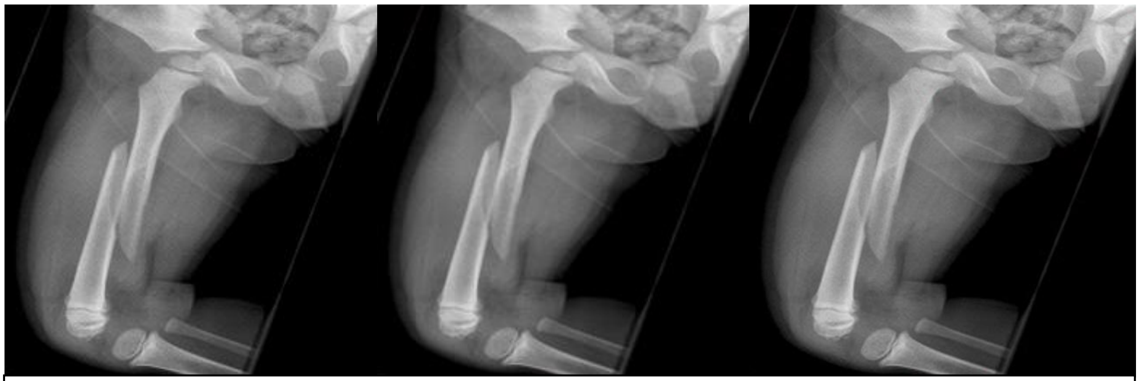
Cropping 75%

Cropping 50%

Figure 1.19 Cropping attack demonstration.

c. Scaling

Is the resizing of the watermarked image in order to increase the complexity of the extracting operation [21]. (Figure 1.20 show an illustration of scaling attack).

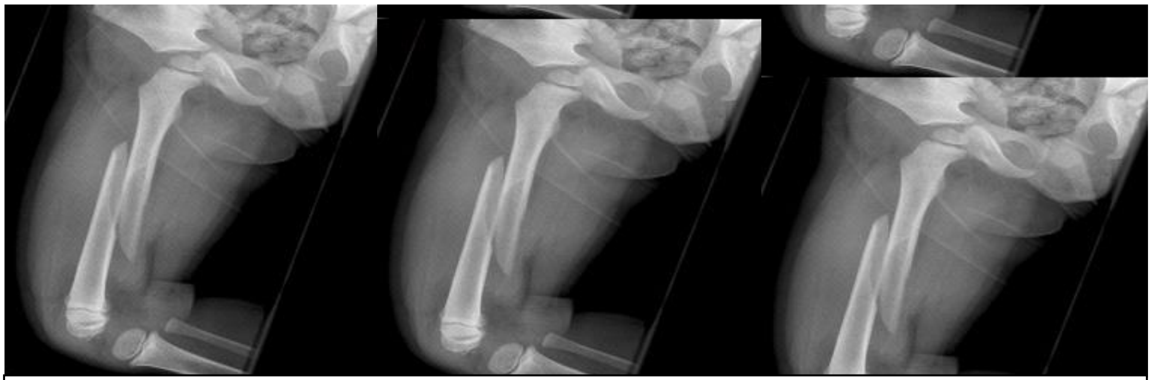


Watermarked image | Scaling 15% | scaling 30%

Figure 1.20 Scaling attack demonstration.

d. Translation

The Principe of this attack is to move the image pixels to a different location within the image size [44]. (Figure 1.21 present an illustration of translation attack).



Watermarked image | Translation 20 | Translation 50

Figure 1.21 Translation attack demonstration.

1.4.4.2 Quality measures

Imperceptibility and robustness of any watermarking method must be proved. To this end, the quality of the watermarked image and the extracted watermark is analyzed using several statistical measures.

- *Mean Square Error (MSE)*

The MSE is the average squared error between two images (I1,I2) of size NxM, calculated as follow [50]:

$$\text{MSE}=\frac{1}{NxM}\sum_{j=0}^{N-1}\sum_{k=0}^{M-1}(\text{I1}(\text{j},\text{k})-\text{I2}(\text{j},\text{k})) \qquad (1.12)$$

- *Peak Signal Noise Ratio (PSNR)*

This metric is used to evaluate the imperceptibility performance. A higher PSNR value indicates higher imperceptibility [50]. The PSNR is based on the MSE and calculated as follow:

$$\mathrm{PSNR(dB)}=10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \qquad (1.13)$$

- *Normalized Correlation (NC)*

This metric is used to compare the original watermark with the extracted one [5], A higher NC value mean the good robustness of the watermarking method.

$$\mathrm{NC}=\sum_{j=0}^{WN-1}\sum_{k=0}^{WM-1}(\mathrm{W1(j,k)}-\mathrm{W2(j,k)}) \qquad (1.14)$$

Where WNxWM are the watermark size and W1, W2 are the original watermark and the extracted one respectively.

- *Correlation coefficient (CRC)*

The CRC is used to quantify the linear relation between two images (I1, I2) of size NxM [46]. These images could be the host image and the watermarked one; in this case the purpose is to measure the imperceptibility degree. Or it could be the inserted watermark and the extracted one, The CRC is used to measure the robustness degree.

$$\mathrm{CRC}=\frac{\sum_{j=0}^{N-1}\sum_{k=0}^{M-1}I1(j,k)I2(j,k)}{\sqrt{\sum_{j=0}^{N-1}\sum_{k=0}^{M-1}\mathrm{I1(j,k)}^2*\sum_{j=0}^{N-1}\sum_{k=0}^{M-1}\mathrm{I2(j,k)}^2}} \qquad (1.15)$$

- *Bit Error Rate (BER)*

The BER shows the probability of watermark binary data that are received incorrectly [28]. The lower BER value indicates the better performance of the watermarking system.

$$\mathrm{BER}=100*\frac{\mathrm{CB}}{\mathrm{AB}} \qquad (1.16)$$

Where CB is the corrupted bits number of the watermark and AB is the number watermark bits.

- *Structural Similarity (SSIM)*

SSIM is used to measure the quality of the watermarked image or the watermark; it conducts a visual quality assessment similar to the Human Visual System (HVS) [39]. The SSIM is expressed as:

$$\text{SSIM}=\frac{(2\mu 1\mu 2+c1)(2\sigma j+c2)}{(\mu 1^2+\mu 2^2+c1)(\sigma 1^2+\sigma 2^2+c2)} \qquad (1.17)$$

Where $\mu 1$, $\mu 2$, $\sigma 1$, $\sigma 2$, σj are the average of the host image, the average of the watermarked image, the variance of the host image, variance of the watermarked image and the covariance of the watermarked images. c1 and c2 are two constant used to avoid the zero dominators.

1.4.5 Application of digital watermarking

The watermarking is applied in many applications and for many purposes [1, 6, 8, 25]. In the following we cite the important application of digital watermarking systems:

1.4.5.1 Copyright protection

The copyright protection is necessary for protecting the benefits of the ownership of documents; this could be effectuated by the embedding of ownership information’s as watermark into the cover documents [7, 29].

1.4.5.2 Fingerprinting

When a person obtains a document legally it could redistribute it illegally; this can be prevented by the embedding of owner information’s in the documents as an event of the ownership [7, 29].

1.4.5.3 Authentication

The authentication means to detect any modification in the cover document. This can be achieved by using fragile or semi-fragile watermark which has low robustness for alteration. For some works, content is very important and original copy is not available; to this end watermarks can be embedded and checked later on to verify if it has been changed or not [7, 29].

1.4.5.4 Tamper Detection

The watermarking system could be used for tamper detection by embedding fragile watermarks. If the watermark is degraded or erased, it indicates the presence of alteration and consequently, the digital content cannot be trusted. Tamper detection is very important for applications involving highly sensitive data like satellite imagery, medical imagery or as a forensic tool [7, 29].

1.4.5.5 Content Description

The embedded watermark could be the detailed information of the cover document (e.g. medical report, image description such caption and label…etc.). In this case of application, the main purpose of watermarking is not only secure the watermark but also gain the storage space [7, 29].

1.4.5.6 Content Archiving

The documents are identified by their names. However, the documents names can be easily changed. Hence embedding an object identifier or serial number within the document itself reduces the possibility of tampering; this also could facilitate documents archiving, classification and organization [7, 29].

1.4.5.7 Broadcast Monitoring

The embedded watermark could be used to identify when and where documents are delivered; it can be used to monitor unauthorized broadcast station or documents broadcasted by pirate station, this application has major applications in commercial advertisement broadcasting to monitor whether their advertisement was actually broadcasted at the right time and for right duration [7, 29].

1.5 Conclusion

Image watermarking is a challenging field that involves principles and techniques from different disciplines like image processing and encryption. Many researchers are focusing on the development of robust watermarking methods, where new research directions arise in image watermarking methods and the area is still in its stages of development. In this chapter, we have been discussing different concepts of data security and encryption. We also presented a global view of digital watermarking, its properties and classification and we took a closer look on image watermarking and its attacks.

In the next chapter, we will present a survey of watermarking methods available in literature, where the main purpose of this overview is to assist budding researchers in the field of digital image watermarking to understand existing methods and to enhance their research further.

Chapter 2

Literature Reviews

Content

2.1 Introduction……………………………..……………………………………....28

2.2 Robust Watermarking Approaches……………………………….…………..…....28

2.3 Semi-Fragile Watermarking Approaches………………………………………..….34

2.4 Fragile Watermarking Approaches…………………………………….………...40

2.5 Comparison And Evaluation………………………………………………….………..44

2.6 CONCLUSION……………………...………..….…………………….…….…....45

2.1 Introduction

We present through this chapter several image watermarking approaches that are currently available in literature aiming to provide images ownership proofing, copyright protection, authentication and integrity. To this end, the watermarking approaches are summarized and classified through there robustness into three major classes: robust, semi-fragile and fragile methods, where each of these classes have different applications, and they are employed according to the purpose of the watermarking system (see chapter 1), at the end of each section, several aspects are considered to synthesize the specification of each approach. These aspects including embedding capacity, security, imperceptibility, computational complexity, and robustness for the robust and semi-fragile methods.

The chapter is organized as follows: Section 2 presents robust watermarking approaches that aim to provide medical images ownership proofing. While section 3 presents semi-fragile watermarking approaches. Section 4 presents the fragile methods. Finally, Section 5 present a synthesis section, while section 6 present the conclusion.

2.2 Robust watermarking approaches

Many robust watermarking approaches have been proposed to address the issues of ownership proofing and copyright protection. In the following, some of robust watermarking approaches are presented. At the end of this section, the techniques are compared.

Hernandez et al. [84] present a new semi-blind based medical image watermarking method, the idea is to embed the watermark into the magnitude of the middle frequencies after DFT (Discrete Fourier Transform) on the original medical image. In the extraction process, the watermark bits are recovered using the bit correct rate between the original and the extracted watermark bits. This method gives good results in terms of imperceptibility and robustness against attacks used in experimentations. However, it offers low embedding capacity; also, it was not tested against several important attacks such as: noising, cropping and shearing.

Singh et al. [64] introduced a multiple watermarking method for medical image based on DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform) and SVD (Singular Value Decomposition). In the embedding process, the cover image is decomposed up with DWT. After that, DCT and SVD are performed on the watermark and the LL band of the host image. The singular values of the watermark are embedded in the singular values of the host image. In addition, the second watermark is embedded at HH band. The watermark is encrypted before embedding to enhance the security. Experimentation results show the good performance of the scheme in terms of robustness, embedding capacity and security. However, the imperceptibility is not much improved with this kind of image (PSNR value=33dB for ct-scanning image), also the scheme requires an important computational complexity. Figure 2.1 summarizes the watermark embedding steps.

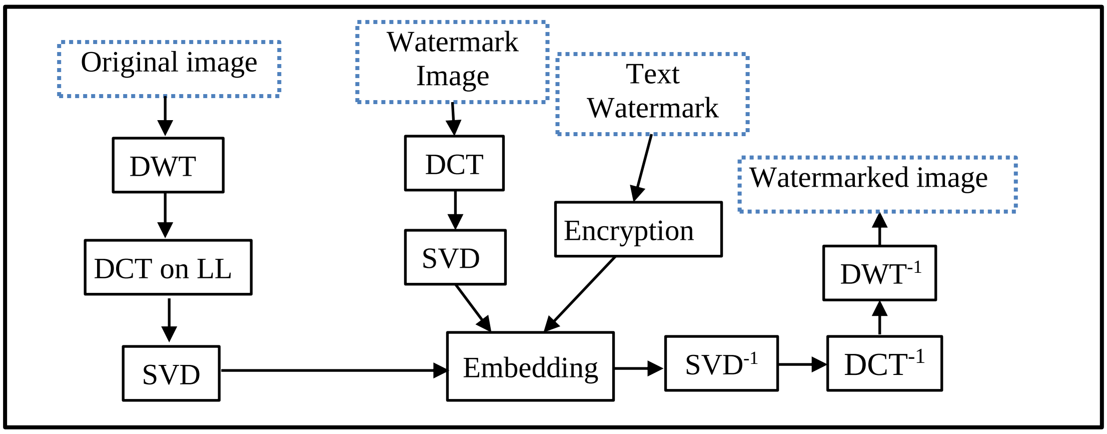


Figure 2.1 Singh et al [64] embedding block diagram.

Mansoori et al. [65] presented a novel method based on Ordered Hadamard Transform (OHT). The basic idea is to decompose the host image and the watermark into blocks and perform OHT on each block. After that, high frequency coefficients of the host image are substituted with the watermark coefficients without using any scaling factor, this guarantees the extraction of watermark with primary quality. This method offers several advantages of imperceptibility, computational complexity and embedding capacity. However, beside the low security degree, the scheme is vulnerable with some attacks like: JPEG compression (PSNR=16.73dB and NC=0.79) and salt & pepper noise (PSNR=11.17dB NC=0.75).

Dong et al.[8] Presented a robust technique for medical image based on DWT and DCT. Firstly, the host image is encrypted using DWT, DCT and logistic sequence to encrypt the host image. Then, the watermark is scrambled and embedded in the feature vector of the host image extracted from the DWT and DCT coefficients. Figure 2.2 summarize the embedding operation. This approach offers good performance in terms of security and robustness. However, it presents some vulnerability with rotation attack (2° and 4°) (NC value < 0.76), scaling attack (NC value < 0.71) and cropping attack (20°) (NC value < 0.66). Also, it require an enormous time for the embedding/extracting operations.

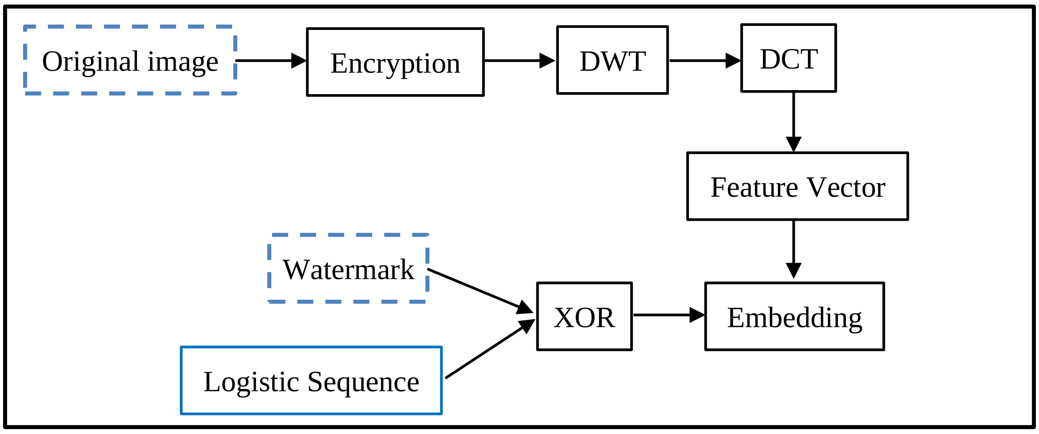


Figure 2.2 Dong et al.[8] embedding operation.

In Liu et al. [72] presents a blind watermarking method for color images. The idea is to embed two watermarks: robust and fragile; the first for copyright protection and the other for image authentication. The first is embedded by using DWT in YCbCr color space, while, fragile watermarking is based on LSB (Least Significant Bits) replacement approach in RGB components for image authentication. The experimental results indicated that the proposed watermarking method could resist various signal processing attacks and perfectly locate the altered emplacement of an attacked image. However, the method requires an enormous computational complexity, and it tested only against attacks with low degree (JPEG QF>=60, salt & pepper noise v<0.09, cropping < 30%). Figure 2.3 show the watermark embedding process.

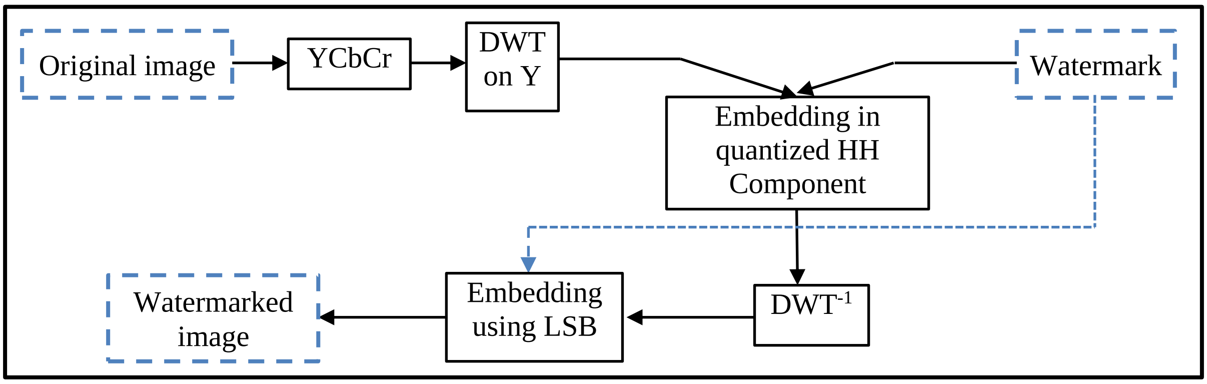


Figure 2.3 Liu et al.[72] block diagram of watermark embedding.

Wang et al. [71] proposed a robust watermarking approach in Contourlet Domain based on Schur decomposition and QIM (Quantization Index Modulation) technique. The idea is to perform the Countourlet transform on the host image. Then, perform DCT succeed by Schur decomposition on the low frequency coefficients blocks. The binary watermark is embedded using the quantization step of QIM. The embedding locations is chooses from each couples (DC, DC’) where the distance between DC and DC’ is greater than a predetermined threshold. (See Figure 2.4). This approach combines the advantages of the three famous methods, this give it good robustness and imperceptibility. But it requires an enormous computational complexity and the security degree is very low.

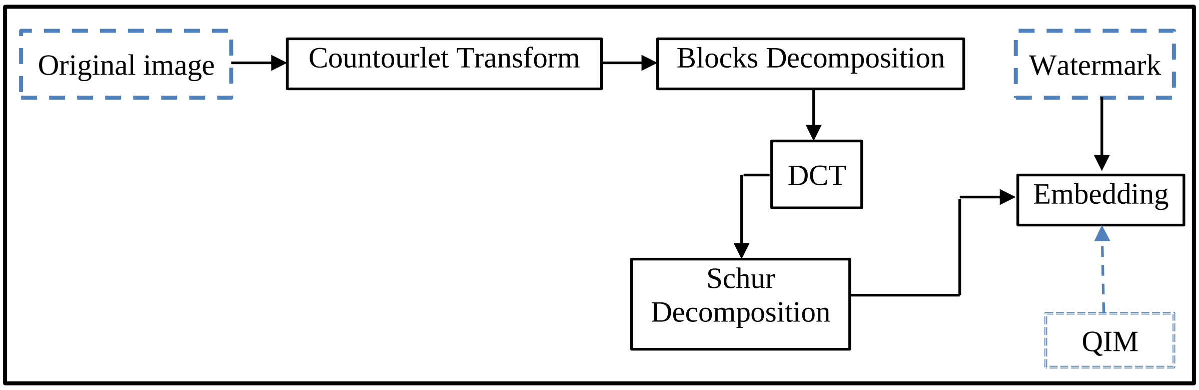


Figure 2.4 Wang et al.[71] embedding operation.

Ghadi et al. [67] presented a new robust and imperceptible watermarking technique in the spatial domain based on Jacobian matrix. The basic idea is to use the average intensity of the 8x8 blocks as an entry (key) of the Jacobian matrix to construct a meaningful watermark. The receiver uses the key for the Jacobian matrix to reconstruct the meaningful watermark. This work offers high robustness and imperceptibility. However, even that this technique works in spatial domain and without encrypting the watermark, it requires an important computational complexity.

Roy et al. [21] introduced a blind technique for colored image based on DCT, Repetition Code (RC) and Arnold chaotic map. The green and blue components of the original image are decomposed on blocks. Then, the DCT is performed on each of them. Several middle band coefficients according to the zigzag order are selected as an embedding location. Finally, the two watermarks are scrambled with Arnold chaotic map, and the corresponding bit of RC is embedded in the locations selected bellow. The scheme gets good trade-off between imperceptibility, robustness, and security. But, it require an important execution time and offers low embedding capacity, also the first watermark is corrupted with some attacks, like Gaussian noise: (PSNR < 21 and BER > 10%), salt & pepper noise(v=0.03): (PSNR~25 and BER=12%), cropping(256×256): (PSNR<12 and BER>12.8%). Figure 2.5 shows the principals steps for watermark embedding.

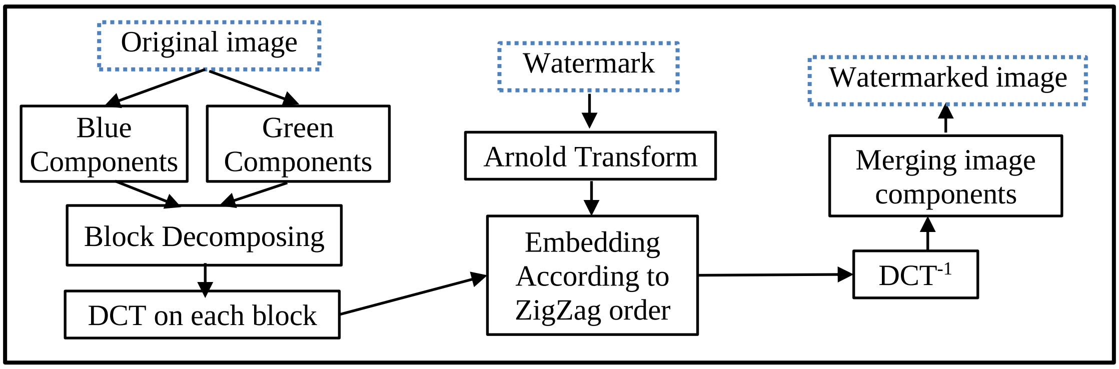


Figure 2.5 Roy et al [21] embedding block diagram.

P.S et al. [44] present a method combined DWT, Contourlet transforms (CT), Schur Decomposition, SVD and Arnold transform to enhance the imperceptibility, security, and robustness (See Figure 2.6). Experimentation results show that the scheme is not much robust with salt & pepper noise (v=0.2) (PSNR in [23 ,25] dB), Gaussian noise (v=0.1) (PSNR in [21,24] dB). Also, a high computational complexity is required for embedding and extracting operations.

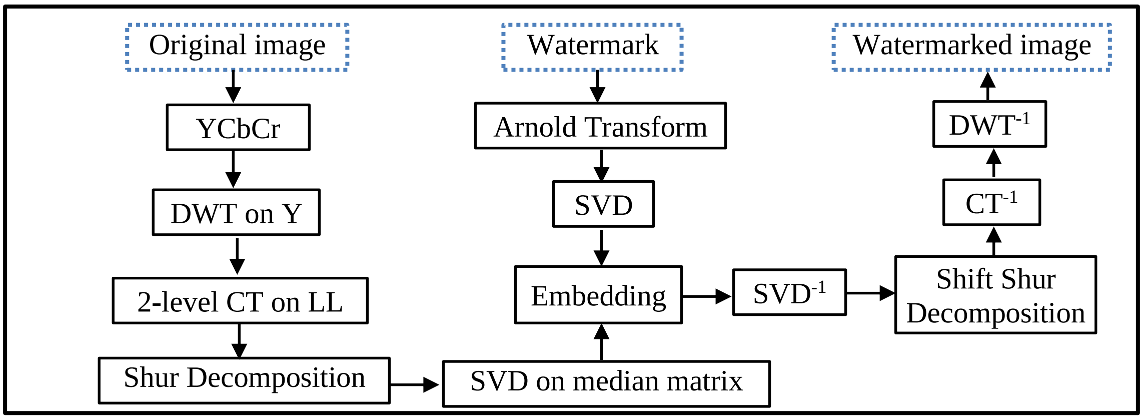


Figure 2.6 Vaidya et al [44] embedding process.

Singh et al. [46] developed a non-blind based watermarking method using non-linear chaotic map. The mean idea is to use chaotic map to generate keys to be used in the embedding process. A method for generating keys is proposed first followed by the embedding process. Finally, a robust extraction process is proposed to verify the presence of watermark. Simulation results prove the robustness and security of the proposed framework. Except that, the scheme was tested only with few attacks, the imperceptibility degree was not much improved (PSNR value between 31dB and 33 dB for gray scale image).

Table 2.1 show the comparison of the robust watermarking techniques cited bellows. The works are compared in terms of embedding domain (E.D), Strength points and drawbacks remarked.

Table 2.1 Comparison of robust watermarking works.

Works	E.D	Strength Points	Limits
Hernandez et al. [84]	Transform	Good robustness with many geometrical attacks, good imperceptibility, median computational complexity.	Low embedding capacity, the robustness with many famous attacks such: noising, cropping, shearing was mentioned.
Singh et al. [64]	Transform	Good robustness, embedding capacity and security	Low imperceptibility. High computational complexity.
Mansoori et al. [65]	Transform	Good imperceptibility, computational complexity and embedding capacity.	EG compression and salt & pepper noise, Low security.
Dogan et al. [8]	Transform	Good robustness and security.	Vulnerability with rotation attack (2° and 4°), scaling attack and cropping attack (20°). And require high computational complexity.
Liu et al. [72]	Transform	Good robustness and alter detection precision.	Require high computational complexity and the method tested only against attacks with low degree (JPEG QF>=60, salt & pepper noise v<0.09, cropping < 30%).
Wang [71]	Transform	Good robustness and imperceptibility.	Low security degree and require high computational complexity.
Ghadi [67]	Spatial	High robustness and imperceptibility.	Require an enormous computational complexity, offers low embedding

			capacity.
Roy et al. [21]	Transform	Good tradeoff between robustness, imperceptibility, and security.	Require an important execution time and offers low embedding capacity, also the watermark is corrupted with some attacks, such Gaussian noise, salt & pepper noise(v=0.03), cropping(256×256).
P.S et al. [44]	Transform	Good robustness and imperceptibility, High security.	High computational complexity, vulnerability with salt & pepper noise (v=0.2), Gaussian noise (v=0.1).
Pal et al. [46]	Spatial	Good robustness and security.	The method was tested only with few attacks, the imperceptibility degree was not much improved.

2.3 Semi-fragile Watermarking approaches

In Huo et al. [101], the authors proposed a DCT based watermarking method for tamper detection. Firstly, a watermark is generated from the cover image DCT coefficients, then an embedding location is generated using a key, finally, the watermark generated bellow is embedded in the location obtained. This method offers good effectiveness in terms of tamper detection and locating, medium imperceptibility, good robustness with JPEG compression attack. However, it requires an important computational complexity. Figure 2.7 show the watermark embedding main steps.

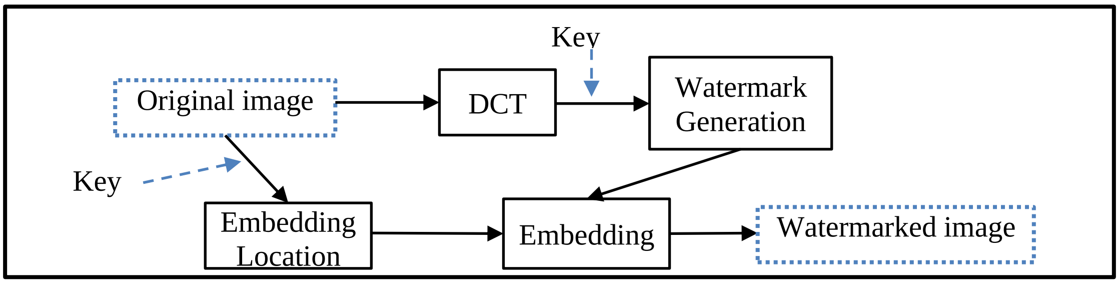


Figure 2.7 Huo et[101] watermark embedding process.

In Zhao et al. [98] presented a blind based image watermarking using Block Truncation Coding (BTC), the idea is to decompose the cover image into non-overlapping blocks, then perform BTC on each block, after that, each two watermark bits are embedded in each block by modifying the pixel values in the block to be equal to the parity of BTC quantized high mean and the parity of BTC quantized low mean. As a result, the proposed method gives good performances in terms of imperceptibility, embedding capacity and robustness with some attacks. However, this method does not provide any technique to protect the watermark bits, where the watermarks bits could be extracted easily.

Lakshmi et al. [99] proposed a hybrid method based on SVD and Binocular Notification Difference (BND). The main idea is to generate a watermark from the cover image using Mersenne Twister Algorithm, then encrypt it using chaotic map, after that, embed it in the cover image Singular Value’s using the BND scheme. The combination of SVD, BND and chaotic map bring a trade-off between imperceptibility, security, tamper detection and robustness with some attacks kinds, this is proved through the experimentation results. However, it requires an important computational complexity. Figure 8 illustrate the method embedding process.

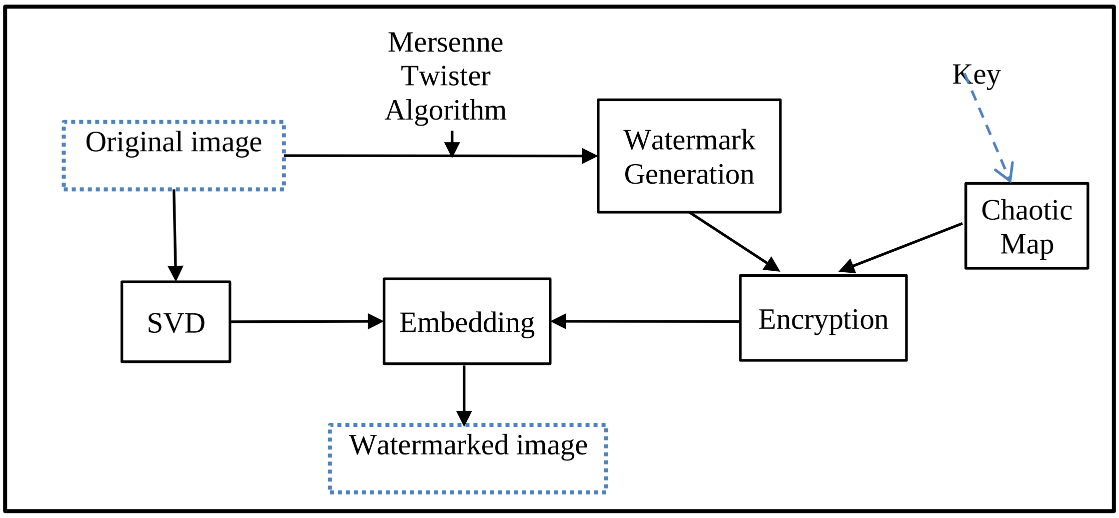


Figure 2.8 Prasad et al [99] watermark embedding process.

In Zhuvikin et al. [100], discusses a Haar Wavelet Transform (HWT) based image watermarking method for image authentication. The method works on using the HWT coefficients of the image central finite differences to embed the watermark data using quantization. This method provides good robustness with JPEG compression attack (QF≤30%) and medium embedding capacity and computational complexity. However, it offers low imperceptibility.

Ustubioglu et al. [80] proposed a non-blind watermarking technique for medical images using Modified Difference Expansion (MDE) and LSB techniques. The cover image is segmented into two areas: a center area and a border area. The first one is used to embed the watermark bits using MDE and LSB method, while the second is used to embed the location map and its hash value of pixel used as a location for embedding the watermark bits. The proposed method gives good performance in terms of imperceptibility and embedding capacity, except that, it requires an important computational complexity, also the data is embedded in ROI (Region of interest) and RONI (Region Of Non Interest); as a result, an attacker could add his own RONI to make the data extraction difficult or even impossible.

Falgun et al. [81] proposed a blind watermarking technique based on DWT and SVD, DWT is applied on ROI. Then the SVD is performed on LL sub-band. A pair of elements with similar values is identified from the left singular value matrix of the blocks selected. The values of these pairs are modified using certain threshold to embed a bit of watermark. The proposed method offers good robustness against some attacks such: salt & pepper noise (v<=0.005), histogram equalization attack, Gaussian noise (v<0.002) and JPEG compression attack. However, it requires an important computational complexity. Figure 2.9 illustrates the main steps of watermark embedding process.

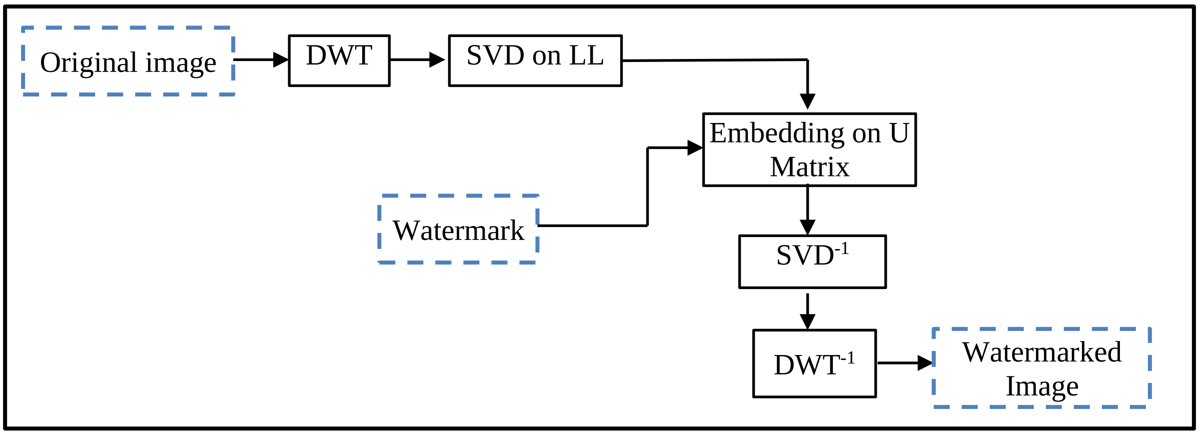


Figure 2.9 Falgun et al.[81] block diagram of watermark embedding.

Mousavi et al. [82] presented a blind technique for medical image in the spatial domain. The idea of the proposed technique is to encode the watermark bits referring to ROI pixel, which will be embedded on RONI of cover image using LSB method. This method offers good performances in terms of robustness with salt & pepper noise attack with different variety of noise density, security, and imperceptibility. However, the method was tested only against few attacks. Figure 2.10 show the watermark block diagram of embedding process.

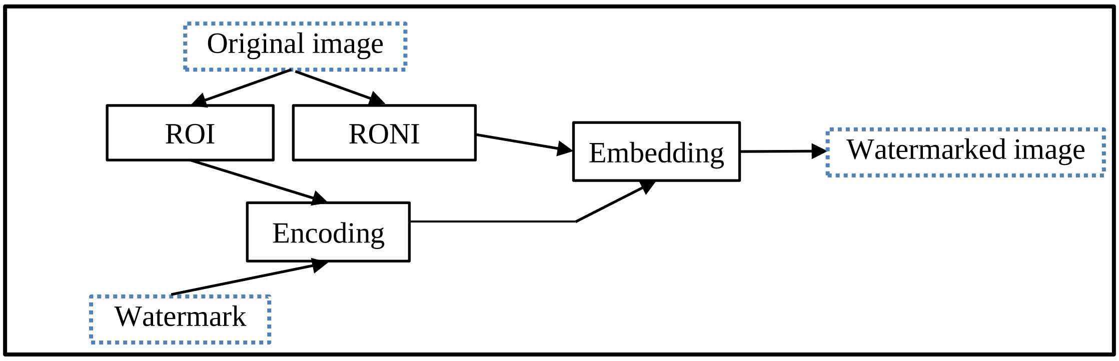


Figure 2.10 Moussavi et al.[82] block diagram of watermark embedding.

In Ali et al. [96], the authors proposed an informed watermarking method using DWT. the main idea consist of generating a digital signature (watermark) which is constituted from the feature distribution of the cover image, this signature is extracted from the DWT coefficients of the cover image, the signature is embedded in the cover image itself. The proposed method gives good results in terms of alter detection and localization whether the watermarked image is altered intentionally or unintentionally. However, it requires an important computational complexity, and the digital signature inserted wasn't secured.

In Hou et al. [97] proposed an informed watermarking method for alter detection and recovery, the proposed method working on generating a watermark using binary random matrix then embed it in Contourlet transform using the maximum absolute value quantization, finally, a watermark recovery which constituted from the average grey level, is embedded in the LSB of the cover image (see Figure 2.11). The proposed method offers the possibility of locating the alteration and recovery the tampered regions. While, it present a major drawback which is the low security of watermarks embedded and the important computational complexity, also, the imperceptibility degree wasn't mentioned.

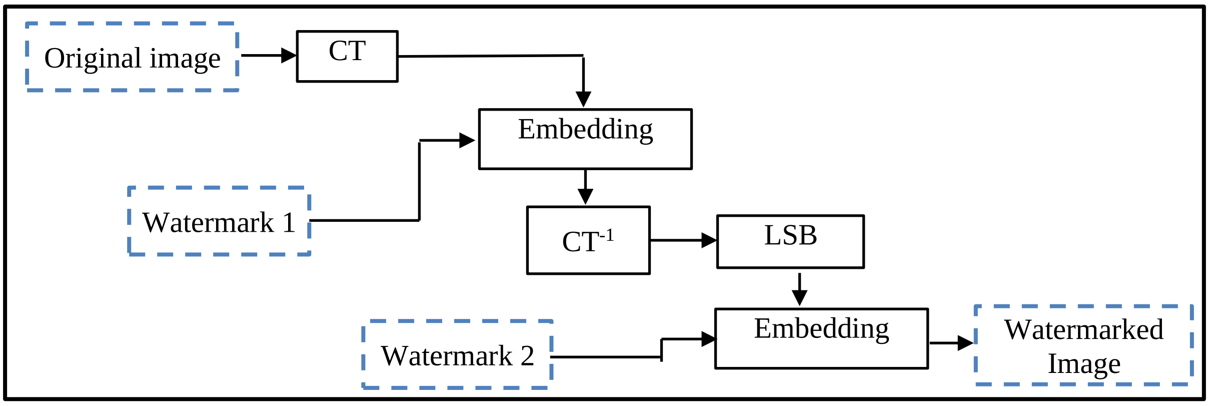


Figure 2.11 Hou et al.[97] main steps of watermark embedding process.

In Liu et al. [94] proposes a blind zero watermarking technique for encrypted medical images based on Dual-Tree Complex Wavelet Transform and Discrete Cosine Transform (DTCWT-DCT) and chaotic map. The main idea is to encrypt the watermark image using a logistic map and then embed it into the medical image after encrypting it using DTCWT-DCT and logistic map. In this method, the advantages of DTCWT-DCT are considered to enhance the performance of image watermarking in terms of good robustness. However, the computational complexity and imperceptibility are high.

Table 2.2 shows the comparison of the semi-fragile watermarking techniques cited bellows. The works are compared in terms of embedding domain (E.D), Strength points and drawbacks remarked.

Table 2.2 Comparison of semi-fragile watermarking works.

Works	E.D	Strength Points	Limits
Huo et al. [101]	Transform	Good effectiveness in terms of tamper detection and locating, security and robustness with JPEG compression attack.	High computational complexity. Median imperceptibility.
Zhao et al. [98]	Spatial	Good performances in terms of imperceptibility, embedding capacity and robustness with some attacks.	This method doesn’t provide any technique to protect the watermark bits, where the watermarks bits could be extracted easily.
Lakshmi et al. [99]	Transform	Good trade-off between imperceptibility, security, tamper detection and robustness with some attack’s kinds	Require high computational complexity.
Zhuvikin et al. [100]	Transform	Good robustness with JPEG compression attack (QF≤30%) and medium embedding capacity and computational complexity	Low imperceptibility.
		Good performance in terms of imperceptibility and embedding capacity.	Requires an important computational complexity, and the data is embedded in

Ustubioglu et al. [80]	Spatial		ROI and RONI, as a result an attacker could add his own RONI to make the data extraction difficult or even impossible.
Falgun et al. [81]	Transform	Good robustness against some attacks such: salt & pepper noise (v<=0.005), histogram equalization attack, Gaussian noise (v<0.002) and JPEG compression attack. Good imperceptibility and security.	Require high computational complexity.
Moussavi et al. [82]	Spatial	Good trade-off between robustness, security and computational complexity.	Low security, and the method use RONI to embed data, as a result an attacker could add his own RONI to make the data extraction difficult or even impossible.
Ali et al. [96]	Transform	Alter detection and localization whether the watermarked image is altered intentionally or unintentionally.	Require an important computational complexity, and the digital signature inserted wasn’t secured.
Hou et al. [97]	Spatial	Robustness with salt & pepper noise and JPEG compression, locate the alteration and recovery the tampered regions.	Imperceptibility degree wasn’t mentioned, low security of watermarks embedded and the important computational complexity.
Liu et al. [94]	Transform	Robustness against geometric attacks.	Imperceptibility mediocre and require high computational complexity.

2.4 Fragile Watermarking approaches

In Bouslimi et al. [83] presented a fragile based joint encryption/watermarking algorithm for medical image protection, the main idea is to embed the watermark twice; in the first, the watermark is embedded using QIM in the encrypted domain after carrying RC, while in the second is embedding in the spatial domain using LSB, this gives the possibility to control the integrity and authenticity. The proposed method gives good performances in terms of security, embedding capacity, while keeping a good imperceptibility. However, it requires an important computational complexity.

The authors Khalil et al. [91] present a blind watermarking method for holy Quran images authentication. The main idea is to use two layers of embedding to enhance the sensitivity of fragile watermarking: on wavelet and on spatial domains, the DWT is performed on the cover image to embed the watermark on DWT coefficients, these coefficients are inverted to spatial domain then the LSB is used to embed another watermark (see Figure 2.12). The proposed method gives good results in terms of data embedding capacity, imperceptibility and capacity of tamper detection, this proved by the experimental results. However, it require an important computational complexity for embedding, extracting and tamper detection processes.

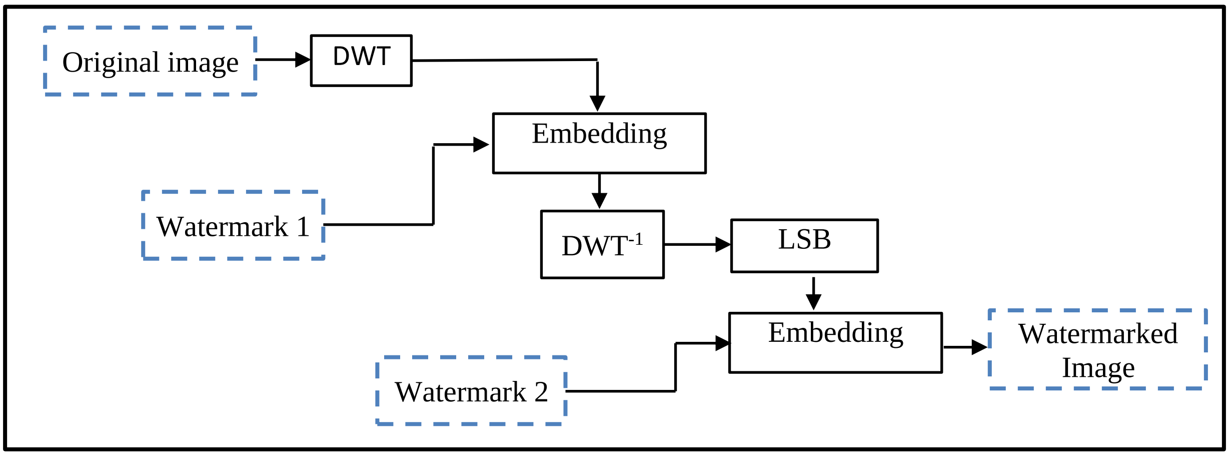


Figure 2.12 Khalil et al. [91] embedding process block diagram.

In Lin et al. [93] presented a reversible watermarking method for image authentication. The main idea is to generate watermark and authentication code from the cover image, and then embed it into the two rebuilt components of each color pixel by using an authentication table. The proposed method provides tamper detection performance while keeping good imperceptibility. However, it require an important time for embedding, extracting and tamper detection processing (generate authentication code, generate/read the authentication table…etc.), and the embedding capacity is mediocre.

The authors in Munir et al. [88] proposed a semi-blind watermarking technique for image authentication using chaotic map. The algorithm encrypts the watermark using chaotic map then embed it in the LSB of the host image. The proposed approach gives good watermark imperceptibility, with low processing time, while the watermark data are highly secured. However, the embedding capacity is mediocre. Figure 2.13 show the block diagram of watermark embedding phase.

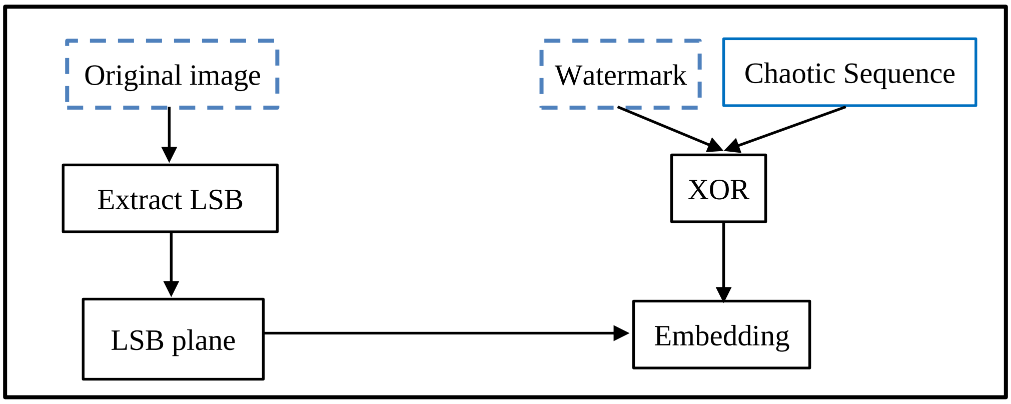


Figure 2.13 watermark embedding process of work presented in [88].

In Pinjari et al. [87], the authors present a new watermarking method for images authentication using Local Binary Pattern (LBP). The watermarking process is achieved in the spatial domain by embedding the watermark using two LSB. Then the pixel information’s are used by the LBP to generate a data key, this is used to secure the watermark. The proposed approach presents median imperceptibility and low computational complexity.

In Zhang et al. [92] the authors propose a hybrid watermarking method for image authentication and tamper detection based on SVD and LSB. Firstly, a watermark is generated from the cover image texture information, where the texture information’s are extracted from the singular value’s matrix. Then the generated watermark is embedded in the LSB of the cover image. The proposed method has high capacity for detecting and locating the altered area while keeping good imperceptibility. However, the embedding capacity is mediocre. Also, an attacker could easily modify the watermarked image, extract the texture information from the modified watermarked image, generate new watermark and embed it in LSB without paying attention from the receiver.

In Sikder et al. [89] the authors propose a new watermarking method based on both Slant Transform (ST) and Lower Upper Decomposition (LUD). Firstly, the watermark image is scrambled, and then the host image is separated into red, green, and blue components. The red channel is divided into 8×8 non-overlapping blocks. Secondly, the ST method is applied to convert each block in ST coefficients. Finally, LUD is applied to obtain the lower and upper triangular matrix from obtained ST coefficients. The watermark data's are embedded into the upper triangular matrix of ST coefficients. Figure 2.14 show the main steps of the proposed method watermark embedding. The proposed technique offers good imperceptibility but it require high computational complexity.

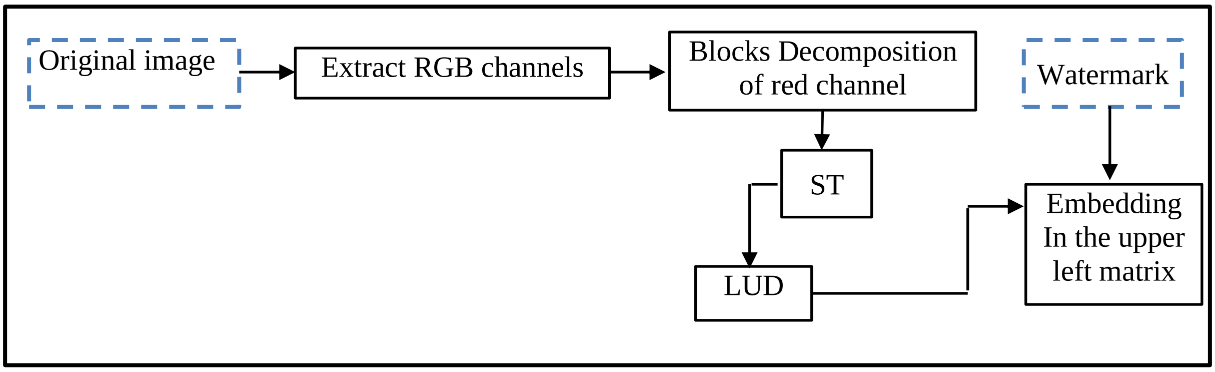

Original image
Extract RGB channels
Blocks Decomposition of red channel
Watermark
ST
LUD
Embedding In the upper left matrix

Figure 2.14 main steps of watermark embedding of work presented in [89].

In Haghighi et al. [43] proposed a fragile blind watermarking scheme based on LWT (Lifting Wavelet Transform), Chebyshev System and GA (Genetic Algorithm). The idea is to generates four compact digests using LWT by image blocks differencing, and then creates four chances for recovering each 2x2 destroyed block. While, the Chebyshev System is used to determine the mapping block for embedding, encrypting, and shuffling the information. Finally, the GA is used to optimize the embedding parameter in order to maximize the imperceptibility. This method offers good performances in terms of security, tamper detection and recovery accuracy and imperceptibility, however, it requires an important computational complexity.

In Garcia et al. [86], the authors present a fragile watermarking scheme using 2-LSB (Least Significant Bits), the idea is to decompose up the host image into non-overlapping blocks, then generate the watermarks from each blocks, which are embedded into different block using the 2-LSB, where a bit-adjustment phase is subsequently applied to increase the quality of the watermarked image. Finally, three recovery watermarks are embedded in different positions. This approach gives results when it comes to tamper detection and recovery, security, and computational complexity, but the imperceptibility degree is mediocre (less than 34dB).

Other works, such in Akhtarkavan et al. [90], authors proposes a fragile method based on LVQ (Lattice Vector Quantization). The main idea is to apply the IIDWT (Integer-to-Integer Discrete Wavelet Transform) on the host image. Then lattice vector quantization are used as an embedding area. This approach gives good trade-off between embedding capacity and imperceptibility; however, it requires high computational complexity.

Table 2.3 shows the comparison of the fragile watermarking techniques cited bellows. The works are compared in terms of embedding domain (E.D), Strength points and drawbacks remarked.

Table 2.3 Comparison of different fragile watermarking works.

Works	E.D	Strength Points	Limits
Bouslimi et al. [83]	Spatial + Transform	Good performances in terms of security, embedding capacity, while keeping a good imperceptibility.	Require an important computational complexity.
Khalil et al. [91]	Spatial + Transform	Good results in terms of data embedding capacity, imperceptibility and capacity of tamper detection.	Require an important computational complexity for embedding, extracting and tamper detection processes.
Lin et al. [93]	Spatial	Provides tamper detection performance while keeping good imperceptibility.	Require an important time for embedding, extracting and tamper detection processing, and the embedding capacity is mediocre.
Munir et al. [88]	Spatial	Good trade-off between imperceptibility, computational complexity and security.	Low embedding capacity.
Pinjari et al. [87]	Spatial	Low computational complexity.	Imperceptibility median to mediocre.

Zhang et al. [92]	Transform	High capacity for detecting and locating the altered area while keeping good imperceptibility.	The embedding capacity is mediocre. Also, an attacker could easily modify the watermarked image, extract the texture information from the modified watermarked image, generate new watermark and embed it in LSB without paying attention from the receiver.
Sikder et al. [89]	Transform	Good imperceptibility.	Require an important computational complexity.
Haghighi et al. [43]	Transform	Security, tamper detection and recovery accuracy and imperceptibility	Requires an important computational complexity.
Garcia et al. [86]	Spatial	Tamper detection and recovery, security, and computational complexity	Low imperceptibility.
Akhtarkavan et al. [90]	Transform	Good performances in terms of Embedding capacity and imperceptibility.	Require high processing time.

2.5 Comparison and evaluation

The performances of the approaches cited bellow are compared and evaluated in this section. These performances are analyzed through computational complexity, security, imperceptibility and embedding capacity, while for the robust and semi fragile- methods we add comparison on vulnerability with attacks.

We have observed that almost most of the robust transform-based approaches require an enormous computational complexity and gives median imperceptibility. While, spatial methods are fragile in almost, but it requires low computational complexity and improves good imperceptibility. Also, Non-blind extracting methods are less computationally complex and more robust against signal processing attacks, but they are impracticable. Semi-blind methods reduce the size of auxiliary data and consequently they help in increasing the embedding capacity, also they improve good imperceptibility especially in the case of zero-watermarking, but it’s less practicable. Blind methods are more computationally complex and require more space for embedding the auxiliary data, however this kind of schemes is more imperceptible, practicable and effective.

As a result, we suggest that robustness and embedding capacity could be assured with the hybridization in transform domain, extra security can be assured with the encryption of the watermark and the good imperceptibility could be assured using spatial domain as an embedding area. This make the proposing of a watermarking techniques that contain a trade-off between the watermarking requirements very difficult and necessitate a deep study of tools and methodology used.

2.6 Conclusion

With the appearance of new technologies, preserving security and authenticity of images becomes a fundamental and necessary requirement. Over previous years, various watermarking algorithms have been proposed by several different researchers, but each method has a number of associated advantages as well as drawbacks. In this chapter, we have presented many watermarking methods with explanations and comparisons between them. The methods are categorized into three major categories: robust, semi-fragile and fragile approaches. The performances of these approaches are analyzed through many factors: robustness, computational complexity, embedding capacity, security, and imperceptibility. From the analyses and study of these methods we conclude that the challenging problem of image watermarking is still on-going to develop a method that can provide watermark protection while keeping full imperceptibility. In this context, in the future works we try to propose a method that can provide better performances.

The next chapters will focus on our contributions in robust, semi-fragile and fragile methods.

Part 2: Contributions

Chapter 3

Robust Medical Image Watermarking Techniques

Content

3.1 Introduction……………………………………………………..…………..…..48

3.2 Robust Medical Images Watermarking Methods…………………..……...……48

3.2.1 A NEW BLIND WATERMARKING METHOD BASED ON WEBER DESCRIPTORS.....…48

3.2.1.1 Weber Law Descriptors (Wds)…………………………….…………...…….49

3.2.1.2 Arnold Chaotic Map……………………………………..……………...49

3.2.1.3 Proposed Watermarking Method…………………………………..…....50

3.2.1.4 Experimental Results And Discussions………………………………..…..54

3.2.2 SCHUR AND DCT DECOMPOSITION BASED MEDICAL IMAGES WATERMARKING...60

3.2.2.1 Digital Imaging And Communication In Medicine (DICOM)…..…….………..61

3.2.2.2 Proposed Watermarking Method……………………………….……….63

3.2.2.3 Experimental Results……………………………………………………....66

3.3 Synthesis And Discussion……………………………………………...…...70

3.4 Conclusion……….……………………………………...………………......71

3.1 Introduction

Image watermarking is considered as a backbone to support advanced multimedia security in various domains, particularly medical domain. It consists in embedding secret information into a cover image to prove the ownership, authenticating data and/or protecting copyright. However, the watermarked images could face threats, when transmitted through Internet which leads to fair quality of watermark and even erasing. A new challenge in image watermarking is to come up with a new robust method for ownership proofing which guarantees resistance of the watermark by preserving the watermarked image quality in terms of imperceptibility. Although existing watermarking techniques offer reliable methods for ownership proofing, they suffer from the poor image quality [44, 71, 72].

In order to achieve these goals, we present in this chapter the novelties and contributions in regards of the area of robust medical watermarking techniques in order to guarantee good robustness and high imperceptibility. The rest of the chapter is organized as follows. Section 2 focuses on our contribution, i.e., the robust watermarking approach based on DCT and Weber Descriptors to improve robustness of medical image watermarking scheme, and the semi-blind watermarking approach based on Schur decomposition and DCT for medical images ownership proofing. Section 3 synthesizes the proposed approaches and section 4 concludes the chapter with some lessons learned.

3.2 Robust medical images watermarking methods

In the studied works, some issues appear to be common between the watermarking techniques. These issues are of course related firstly to the robustness of the watermarking techniques and secondly to the imperceptibility aspects. In the following, we detail our contributions for securing medical image when dealing with robustness. One of the main aspects that we must consider is guarantying a watermark resistance strategy by preserving the watermarked image quality that can be achieved in transform domain.

3.2.1 A New Blind Medical Image Watermarking Based on Weber Descriptors and Arnold Chaotic Map

We present in this section, a new watermarking technique for medical image. The proposed technique combines Discrete Cosine Transform (DCT), Weber descriptors (WDs) and Arnold chaotic map. This combination brings three significant steps. First, the watermark image is scrambled using Arnold chaotic map. Second, the DCT is performed on each medical image block, and the watermark data are embedded in the DCT middle- band coefficients of each block. Finally, a new embedding and extracting technique is proposed, based on WDs without any loss by selecting the right coefficients. Through this approach, we improve the robustness of the proposed algorithm against several scenarios of attacks such as noising, filtering and JPEG compression.

3.2.1.1 Weber Law Descriptors (WDs)

The Weber Law Descriptors (WDs) represents the relation between the quantity and intensity [28]. It consists of two descriptors namely: *Differential Excitation* χ and *orientation* λ. The differential excitation χ of the pixel S is the relative differences of its neighbor's intensity. It's computed as follows:

$$\chi(i,j) = \arctan\left(\sum_{n=0}^{m-1} \frac{S(n)-S}{S}\right) \qquad (3.1)$$

Where m is the number of neighbors of S, i and j are the coordinate of the pixel S.

The orientation λ is the gradient orientation of the current pixel S. It can be computed in different angles using different neighbors. The orientation λ is computed using the following equation:

$$\lambda(i,j) = \arctan\left(\frac{S(i+4)-S(i)}{S(i+6)-S(i+2)}\right) \qquad (3.2)$$

Where $i=\{0\ldots\frac{n}{2}-1\}$ (n is the number of neighbors of the pixel S).

The embedding and extracting process of the proposed method is achieved in the frequency domain by using the WDs (λ) with the DC coefficients.

3.2.1.2 Arnold Chaotic Map

Arnold scrambling is a method in image encryption domain. It is the most commonly used map in chaos-based image encryption processes. The main idea, is to shift each pixel couples in order to generate a new image with the same size of the original image. The Arnold scrambling transformations is defined as follows:

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \bmod N, \text{ where } i', j', i, j = \{0..N-1\} \qquad (3.3)$$

Where i, j represent the pixel coordinate of the original image, i', j' represent the pixel coordinate of the scrambled image and N is the watermark size. The corresponding inverse of Arnold scrambling is obtained based on the following equation:

$$\begin{bmatrix} i \\ j \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} i' \\ j' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \right) \bmod N \tag{3.4}$$

In the proposed method, Arnold Chaotic map is used mainly to encrypt the watermark image in order to ensure its security.

3.2.1.3 Proposed Watermarking Method

The proposed method consists of two processes: the watermark embedding process and the watermark extraction process. Figure 3.1 to Figure 3.3 illustrates the watermark embedding and extraction processes respectively.

- Watermark embedding process

The watermark embedding process is illustrated in Figure 3.1. The used medical images are in grayscale of size 256 × 256. The embedding process consists of embedding the scrambled binary watermark. This process is achieved in two phases, namely: *preprocessing phase* and *embedding phase*.

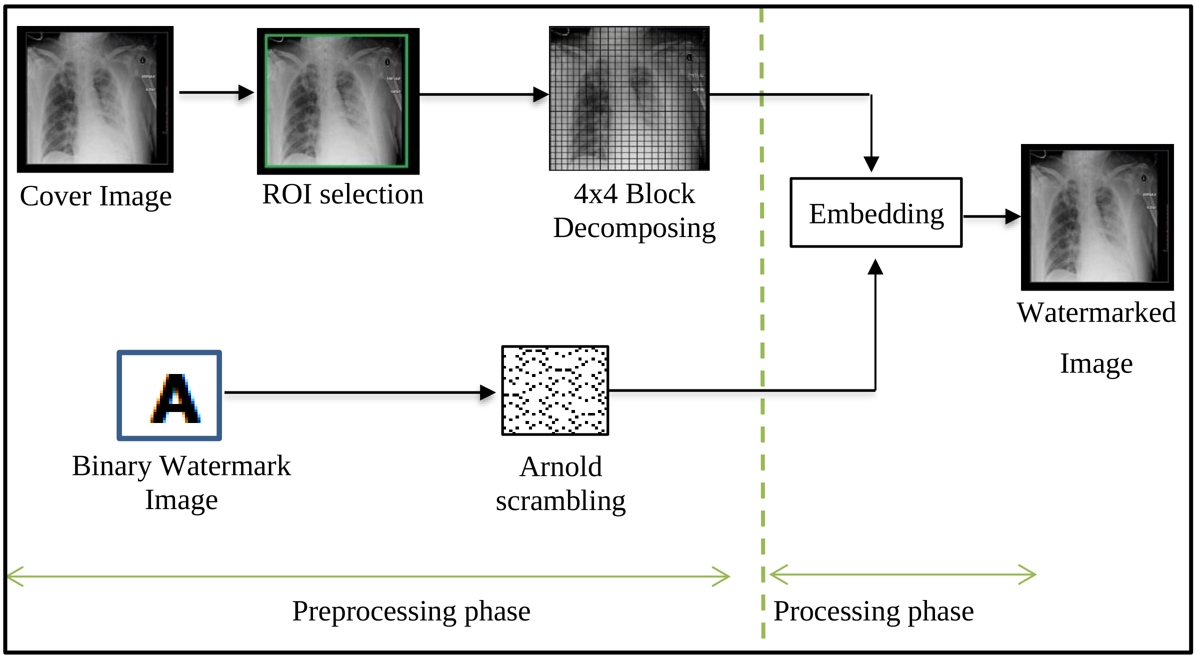


Figure 3.1 Watermark Embedding Process.

a. Preprocessing phase

The first step of the watermark embedding process is performed as follow:

Step 1: select the ROI from the whole medical image.

Step 2: decompose the ROI selected bellow into non-overlapping blocks of size 4x4 pixels, in order to conserve the image quality; one watermark intensity (Bit) is embedded on each block.
Step 3: scrambling the binary watermark image using Arnold Chaotic Map [108] in order to secure the watermark.

b. Watermark embedding phase (Processing phase)

This phase describes the main steps of embedding the binary watermark bits. Figure 3.2 shows the watermark bits embedding process steps which are described as follows:

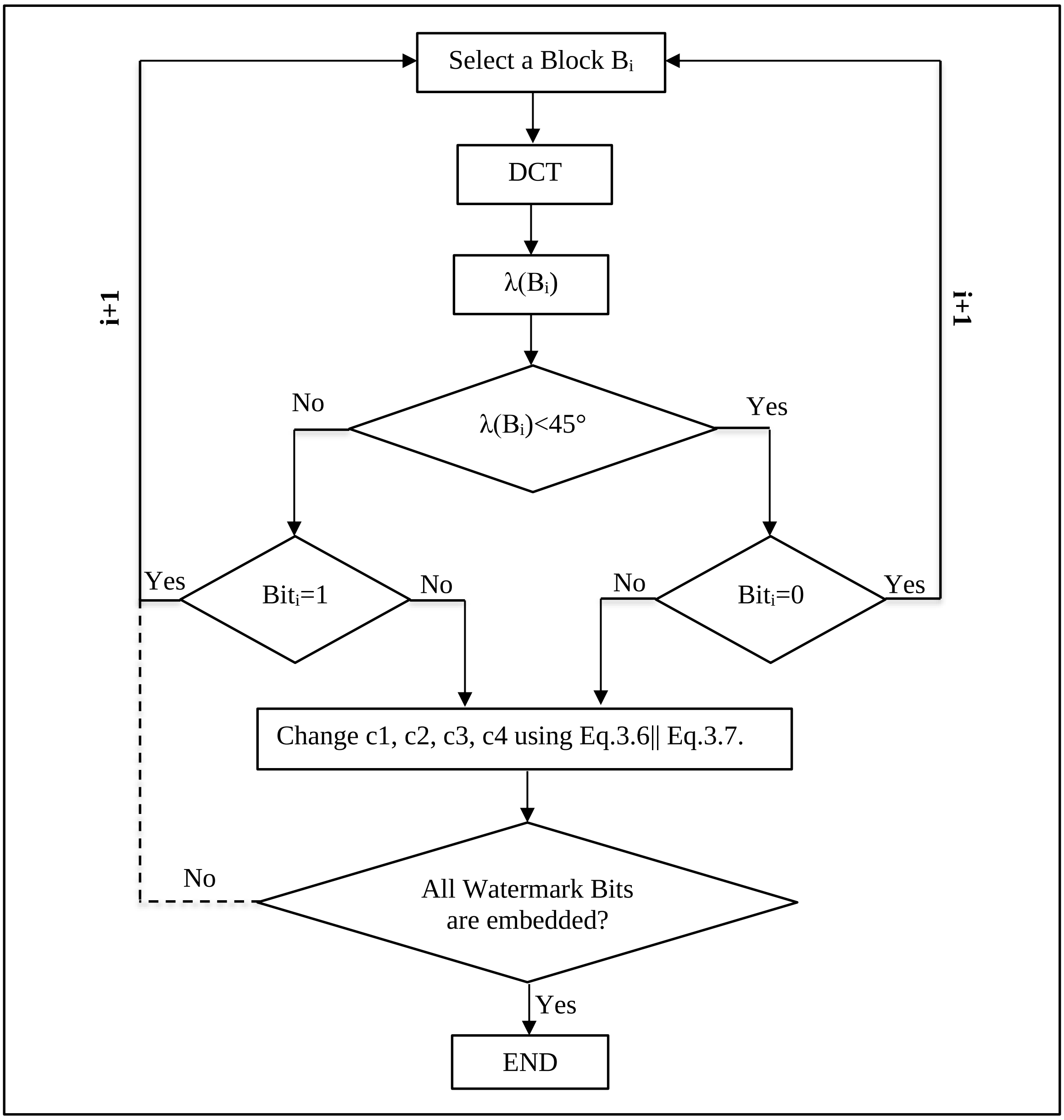


Figure 3.2 Watermark Bit embedding phase.

Step 4: select a block (B_i) and perform DCT on it. Then select 4 coefficients (c1, c2, c3, c4) from the middle band coefficients (the locations of the coefficients selected are the same for all blocks). These four coefficients are used to embed watermark intensity (one bit).

Step 5: calculate the orientation (λ) of B_i as follow:

$$\lambda(B_i) = \left| \mathrm{Arctan}\left(\frac{c1-c2}{c3-c4}\right) \right| \qquad (3.5)$$

Step 6: Select an intensity (Bit_i) from the scrambled binary watermark, and embed it according the following cases:

Case 1: $Bit_i = 1$ and $\lambda(B_i) < 45°$, in this case the values of c1, c2, c3, c4 are modified as follow:

$$\begin{cases} \text{Permute } (c1, c3). \\ \text{Permute } (c2, c4). \\ \quad c1 = c1 + K. \end{cases} \qquad (3.6)$$

Where K is an embedding strength used to reinforce the watermark presence.

Case 2: $Bit_i = 0$ and $\lambda(B_i) >= 45°$, in this case the values of c1, c2, c3, c4 are modified as follows:

$$\begin{cases} \text{Permute } (c1, c3). \\ \text{Permute } (c2, c4). \\ \quad c3 = c3 + K. \end{cases} \qquad (3.7)$$

Another case: past to step 7.

Step 7: perform the DCT inverse on B_i. If not all the watermark bit are embedded back to step 4 with i=i+1.

- Watermark extracting process

The watermark extracting process is shown in Figure 3.3. As mentioned below, the proposed method is blind, which mean only the embedding secret key is required to extract the watermark image. Similarly to embedding process, the extracting process executes also two phases: *preprocessing* phase and *watermark extracting* phase.

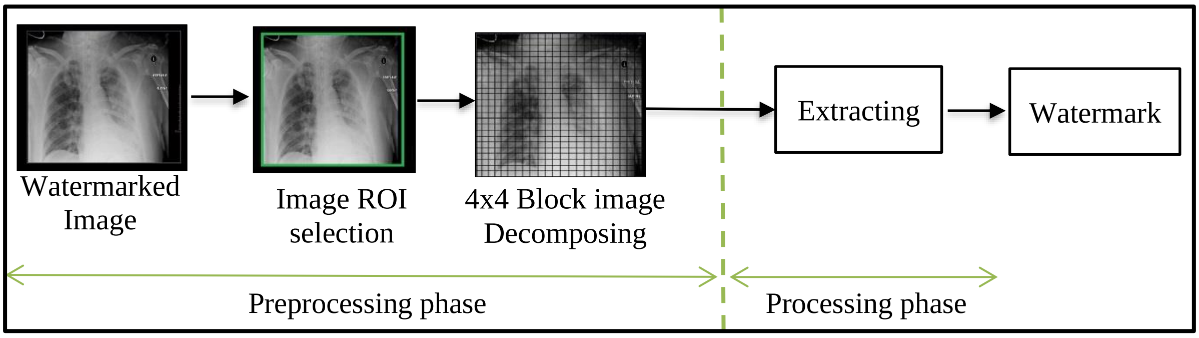


Figure 3.3 Watermark extracting process.

a. Preprocessing phase

Step 1: select the ROI from the whole medical image.

Step 2: decompose the ROI selected bellow into non-overlapping blocks of size 4x4.

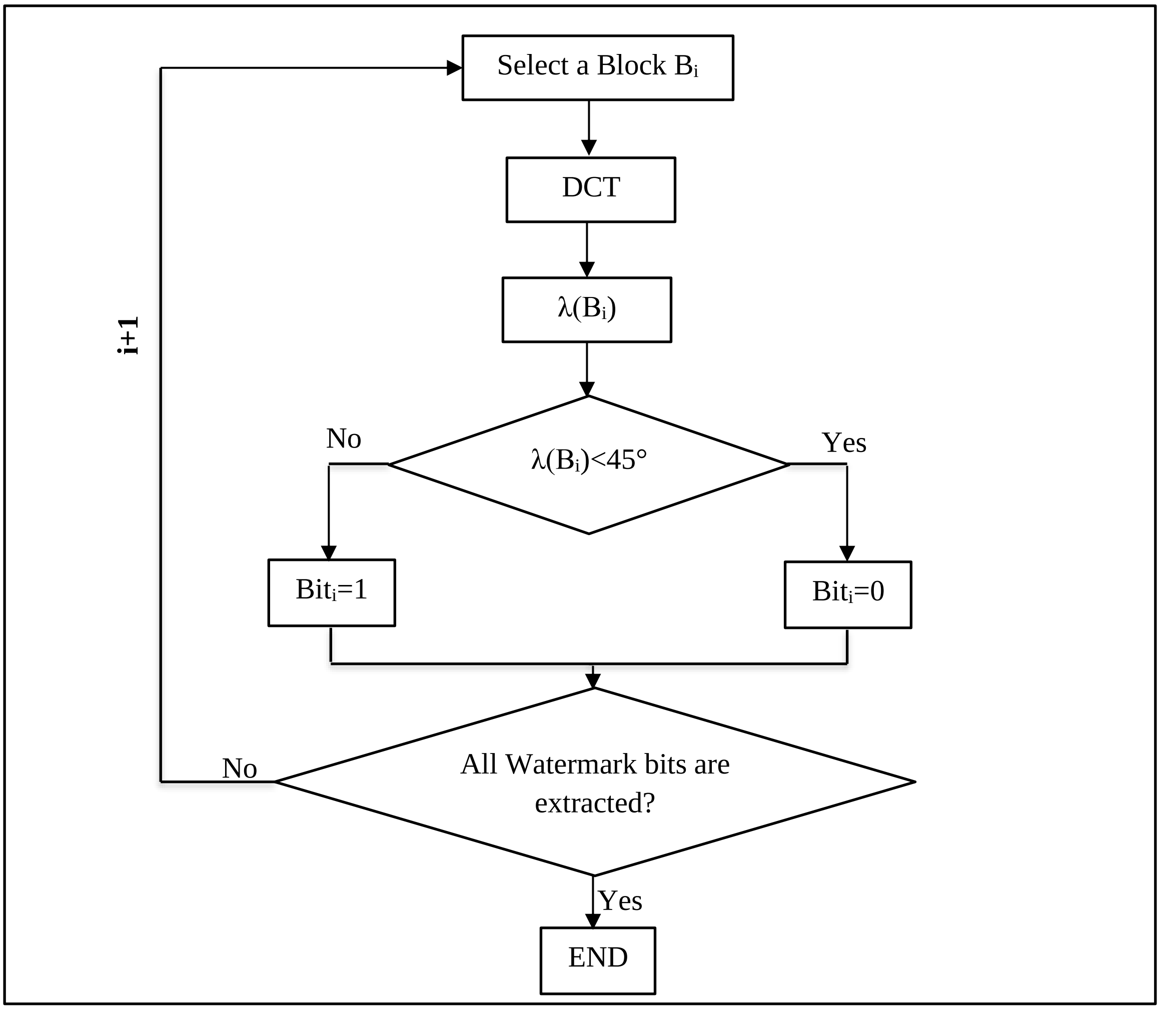


Figure 3.4 Watermark Bits extracting phase.

a. Watermark extracting phase (Processing phase)

The processing phase steps are shown in Figure 3.4.

Step 3: select a block (B_i) and perform DCT on it. Then select 4 coefficients from the middle band coefficients (the same coefficients locations used in embedding process).

Step 4: calculate $\lambda(B_i)$ using Eq.(3.5).

Step 5: the bit (Bit_i) of the scrambled binary watermark is extracted according the following cases:

Case 1: $\lambda(B_i)<45°$, in this case $Bit_i=0$.

Case 2: $\lambda(B_i)>=45°$, in this case $Bit_i=1$.

Step 6: perform the DCT inverse on B_i. If all the watermark bits are extracted go to step 7, else go back to step 3 with i=i+1.

Step 7: apply the invers Arnold scrambling on the extracted watermark image to get the original watermark image.

3.2.1.4 Experimental results and discussions

We performed our tests on grayscale medical image database that contains thirty images of size 256x256. The presented watermarking method use a binary watermark image of size 32x32 where each pixel could take two values *0* or *255* expressed as one byte (*0 for black and 1 for white*). In simulation, we defined the embedding strength K=30. We evaluated our proposed watermarking technique against several kind of attacks such as: noising, filtering and JPEG compression and other kind of geometric distortions.

The experimental results are evaluated using well-known metrics such: PSNR, NC and SSIM. Figure 3.5 show a sample of cover images and watermark used in experimentation. The used images are from [66]. Table 3.1 illustrates an example of the realized application of proposed method.

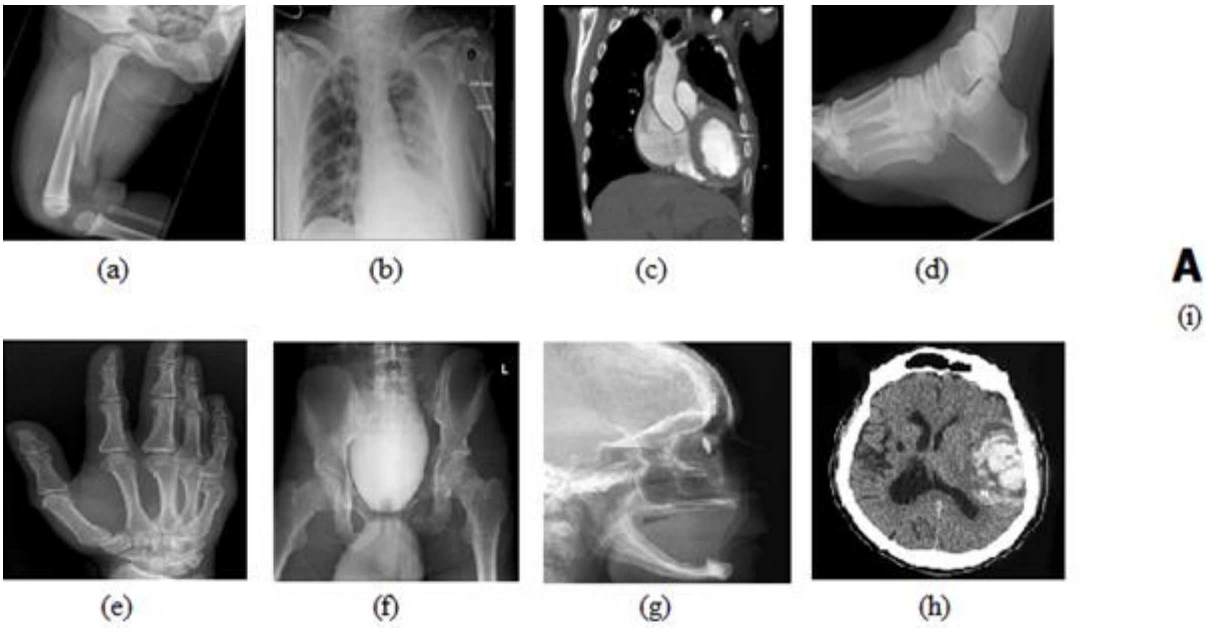
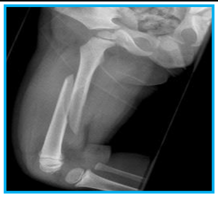
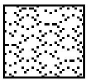
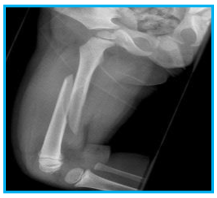
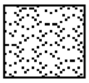


Figure 3.5 (a)-(h) Cover medical images (i) Watermark.

Table 3.1 Example of the realized application executed on image (a) and (b).

<table>
<tr><th colspan="5">Image name: (a)</th></tr>
<tr><th colspan="3">Cover Image</th><th colspan="2">Watermark image</th></tr>
<tr><td colspan="3"></td><td colspan="2"> </td></tr>
<tr><th>Encrypted Watermark Image</th><th>Watermarked Image</th><th>Extracted Watermark</th><th>Decrypted Extracted watermark</th><th>Performance Results</th></tr>
<tr><td></td><td></td><td></td><td> </td><td><em>Embedding Time</em>
<em>1.5288 s</em>
<em>Imperceptibility</em>
<em>PSNR : 43.761 dB</em>
<em>Extracting Time</em>
<em>0.6082 s</em>
<em>NC : 1</em>
<em>SSIM : 1</em></td></tr>
</table>

- Imperceptibility measurement

To evaluate the imperceptibility of the proposed method, we use the PSNR defined via the Mean Square Error (MSE) (detailed in Chapter 1 Section 4). High PSNR value means a higher imperceptibility degree. Table 3.2 presents the obtained PSNR values between the original image and the watermarked image in different medical images. We noticed that the obtained results by our method are very encouraging (e.g. the PSNR values greatly exceed 34db) and helpful in the preservation of the watermarked image quality compared to the original image. The main reason is that the middle band coefficients of blocks are slightly modified to embed the binary watermark data's.

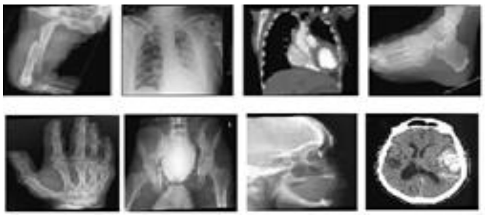
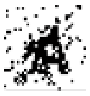
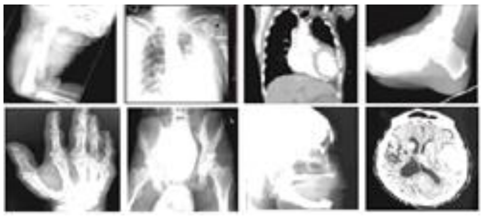
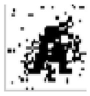
Table 3.2 PSNR values between the original and the watermarked images.

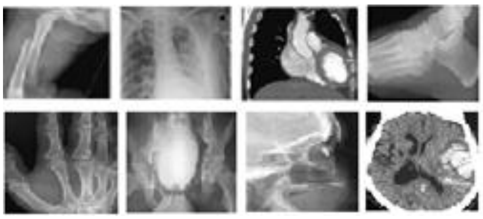
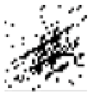
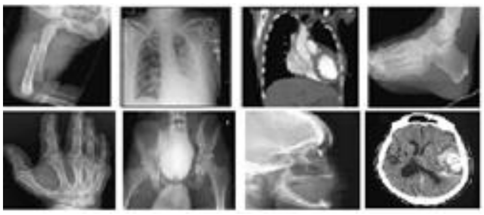
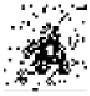
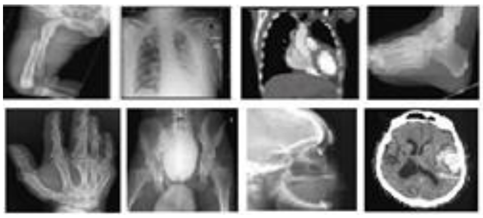
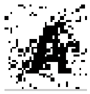
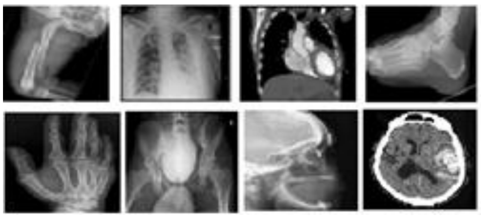
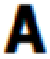
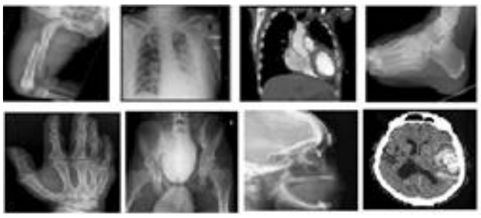
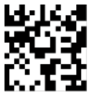
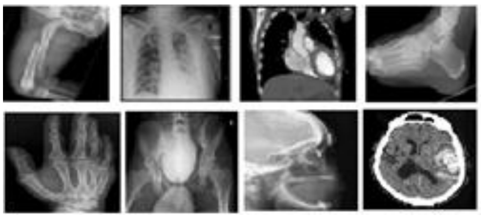
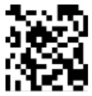
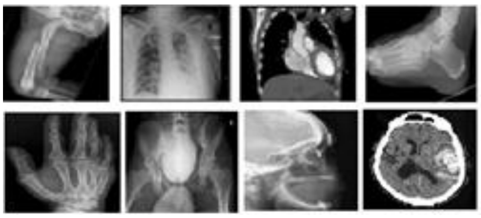
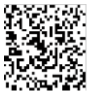
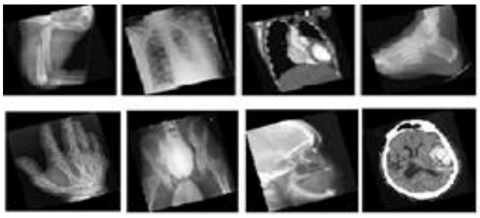
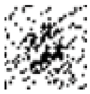
H	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
PSNR (dB)	43.761	44.078	44.098	43.548	45.934	43.463	45.73	43.026

- Robustness measurement

This experiment was designed to evaluate the proposed method in terms the robustness. Using Stirmark benchmark software [63] and MATLAB, we apply different types of attacks on the watermarked images. We calculate the robustness values using the NC/SSIM measures between the original watermark and the extracted one. The averages of the obtained NC/SSIM results are shown in Table 3.3 and Table 3.4. It's clear that the proposed method provides high robustness to the watermark improved by the high values of NC/SSIM except for Rescale (RESC), Remove Line (RML), Random Distortions (RNDDIST) and Translation attacks. These findings are practically significant and accomplish robustness, signify that the orientation (λ) of the coefficients used for embedding the watermark data is slightly changed when the coefficients are modified. So the watermark bit extraction still possible even that the watermarked image is altered.

Table 3.3 The obtained Robustness measurement for the first serie (using Stirmark Benchmark).

	Attacked watermarked images	**Extracted watermark**	**NC**	**SSIM**
AFFINE_2			**0.8688**	**0.6043**
CONV_1			**0.8866**	**0.6474**

CROP_75			**0.9447**	**0.4105**
JPEG_50			**0.9255**	**0.4662**
MEDIAN_3			**0.9276**	**0.6744**
PSNR_0			**1**	**1**
RESC_50			**0.6283**	**0.0305**
RML_10			**0.6859**	**0.0065**
RNDDIST_0.95			**0.6225**	**0.0119**
ROT_15			**0.9285**	**0.4217**

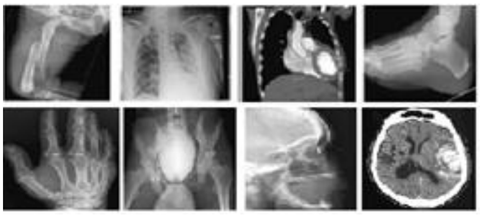
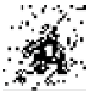
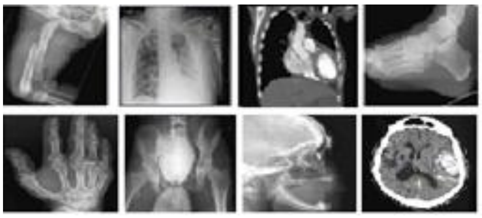
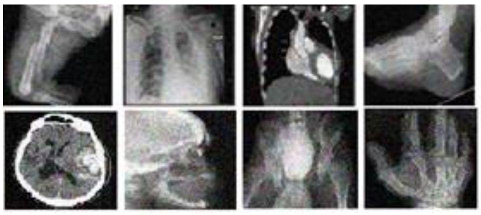
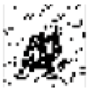
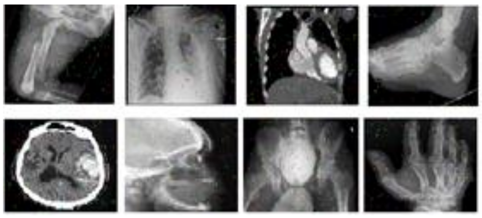
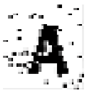
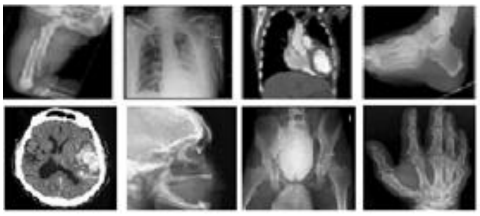
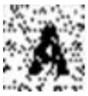
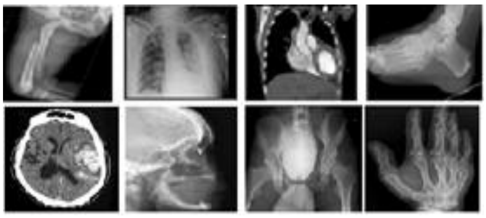
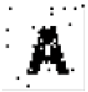
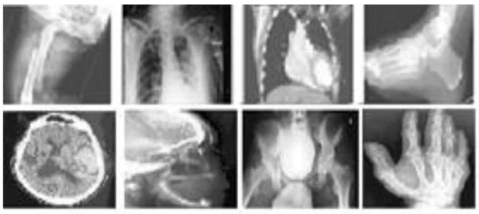
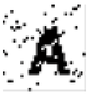
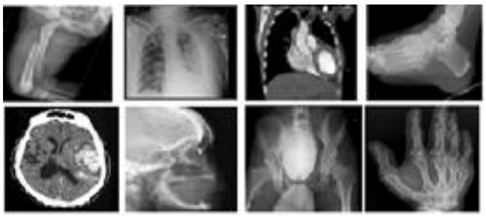
ROTCROP_2			**0.8574**	**0.5468**
SS_2			**1**	**1**

Table 3.4 The obtained robustness measurement for the second serie (Using MATLAB).

	Attacked watermarked Image	Extracted Watermark	NC	SSIM
White-Noise V=0.005			**0.8188**	**0.5044**
Salt & Pepper noise V=0.01			**0.9539**	**0.8022**
Speckle Noise V=0.01			**0.8262**	**0.6157**
Average Filtering[2,2]			**0.9755**	**0.8662**
Histogram Equalization			**0.9559**	**0.7877**

Translation			**0.4167**	**0.092**

- Computational Complexity measurement

All our experiments are realized through a DELL LATITUDE E5410 Laptop/Intel Core i5 2.67 GHz, 4 GB PC using Matlab. Table 3.5 illustrates the execution time needed for embedding and extracting the watermark in different medical images. Experimental results show that our proposed method allows fast execution time (*doesn't exceed 2 second for the embedding process and 1 second for the extracting process*). A fast execution time obtained via a fast technique for embedding/extracting the binary watermark image in/from the medical images.

Table 3.5 Time required for embedding and extracting the watermark.

Images	Embedding time (Second)	Extracting time (Second)
(a)	1.5288	0.6084
(b)	1.5132	0.624
(c)	1.6224	0.5928
(d)	1.5159	0.6148
(e)	1.5912	0.6369
(f)	1.6536	0.6084
(g)	1.7316	0.608
(h)	1.6692	0.651

- Performances comparison

We studied the watermarking techniques' performance and compared them to some other works in order to illustrate the efficiency and the effectiveness of our approach. The different performance measures are determined and the obtained results are shown in Table 3.6, 3.7 and

3.8. Table 3.6 shows the imperceptibility measure compared to some relevant works such as [21] and [64]. Table 3.7 shows the computational complexity results compared with [67]. It's clear that the proposed approach requires low computational complexity than other methods exploited in the spatial domain. Table 3.8 shows the robustness results compared with some works in [65] and [64]. The proposed method allows fast execution time and low computational complexity, preserves medical images quality and gives-better robustness than other works.

Table 3.6 The obtained PSNR values of our method compared with other works [21, 64].

Approach	Approach in [21]	Approach in [64]	Our proposed approach
PSNR (dB)	43.0388	32<PSNR<37	44.306

Table 3.7 The obtained computational complexity of our method compared with [67].

Parameters	**Approach in [67]**	**Our proposed approach**
Cover image size	128x128	256x256
Watermark size	8x8	32x32
Watermark encryption?	No	Yes
Average embedding time	4.5 s	1.603 s
Average extracting time	4.56 s	0.618 s

Table 3.8 Performance analysis under NC values.

Attacks	**Approach [65]**	**Approach [64]**	**Proposed approach**
Salt & Pepper noise (v=0.01)	< 0.8	0.9478	0.9540
Speckle noise(v=0.001)	-	0.9455	0.95197
Rotation 5°	< 0.95	0.9667	0.9673
Median filtering	0.865	0.8663	0.9276
JPEG compression Q=50	0.795	1	0.925

3.2.2 Schur and DCT Decomposition Based Medical Images Watermarking

We present in this section, a new robust semi-blind based watermarking technique for medical images, using Schur decomposition and DCT. The main idea is to embed the watermark derived from the cover image blocks in the DCT middle band coefficient, after carrying out the Schur decomposition on the image's blocks.

3.2.2.1 Digital Imaging and Communication in Medicine (DICOM)

Digital Imaging and Communication in Medicine (DICOM), is a standard designed to cover the whole large aspect of medical images, including data transferring, storing and display protocol built [4, 106].

a) Why DICOM

The principal objectives behind the DICOM developments are [106]:

- Ensure the communication of medical data's regardless the device manufacturer.
- Facilitate the development and expansion of medical data archiving and communication systems.
- Allow the creation of diagnostic information data bases that can be interrogated by heterogeneous devices which are geographically separated.

b) DICOM Basic File structure

The DICOM file is constituted from two principal components (Figure 3.6), namely: Header and Body [4]. The header contains the File Meta information's. While the body contains the medical data's set (a set of data element which constitute the medical image).

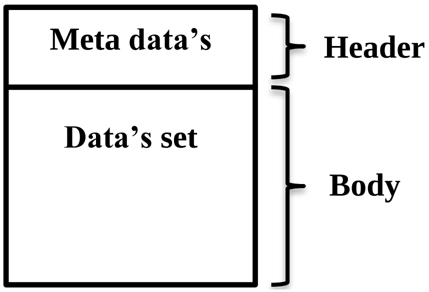


Figure 3.6 DICOM File Basic Structure.

c) DICOM Terminologies

- The header

The header constituted with three essentially components [106]: the file preamble, the DICOM prefix and the File Meta elements (Figure 3.7).

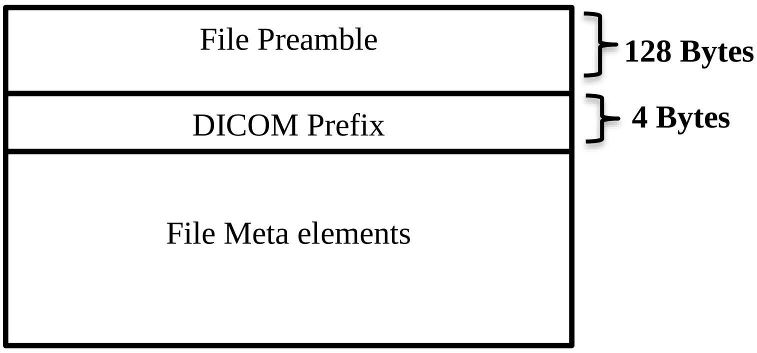


Figure 3.7 DICOM Header elements.

- ✓ *File Preamble*

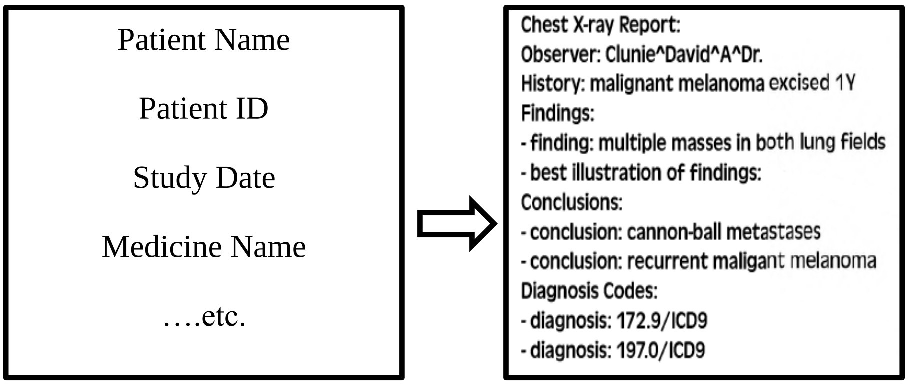
The File Preamble used to facilitate access to the images and other data in the DICOM file by providing compatibility with the image file formats, if it’s not used by an application, all 128 bytes shall be set to 00H, in order to facilitate the recognition that the preamble is used. The File Preamble contains information enabling a multi-media application to randomly access images stored in a DICOM data set, it’s can be accessed in two ways: by a multi-media application using the preamble and by a DICOM application which ignores the preamble.

- ✓ *DICOM Prefix*

The DICOM prefix contains the character string "DICM" encoded as uppercase characters of the ISO 8859 G0 Character Repertoire. This four byte prefix is not structured as a DICOM Data Element with a Tag and a Length.

- ✓ *File Meta Information’s*

This part of header contains the real information’s relative to the medical image (patient, physician, hospital…etc.) (Figure 3.8).


Patient Name
Patient ID
Study Date
Medicine Name
….etc.

Chest X-ray Report:
Observer: Clunie^David^A^Dr.
History: malignant melanoma excised 1Y
Findings:
- finding: multiple masses in both lung fields
- best illustration of findings:
Conclusions:
- conclusion: cannon-ball metastases
- conclusion: recurrent maligant melanoma
Diagnosis Codes:
- diagnosis: 172.9/ICD9
- diagnosis: 197.0/ICD9

Figure 3.8 DICOM Meta information example.

The Meta information's are presented as a set of attribute where each attribute have: a tag, value representation (VR), value length and value field. Figure 3.9 show an example of a DICOM Meta information:

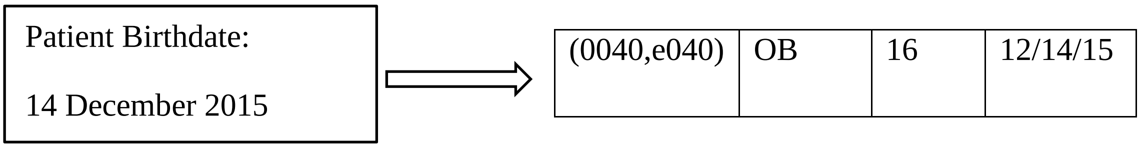


Figure 3.9 DICOM meta information representation.

- The DICOM Data Set (Body)

The DICOM body contain the graphical medical data, which constituted by a set of pixel Cell. The image pixel data's are divided into two regions (Figure 3.10): Region Of Interest (ROI) and Region Of Non-Interest (RONI), the ROI area is depending on the availability of clinical finding and its features in the medical image, it constituted from the significates pixel, while the RONI is the area where there is not any clinical finding (insignificants pixels) [4, 106].

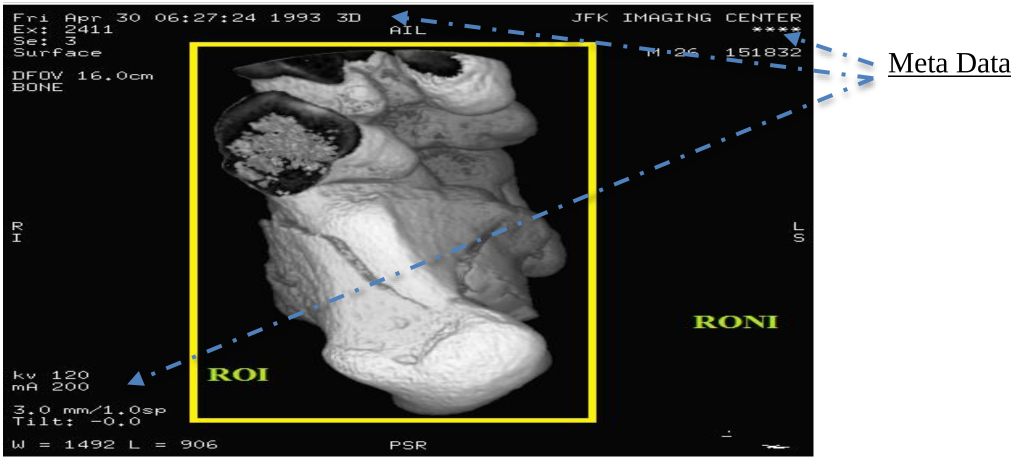


Figure 3.10 DICOM image principal component.

3.2.2.2 Proposed Watermarking Method

The aim of the presented watermarking method is to transmit the watermarked images from sender "A" to remote receiver "B" as is depicted in Figure 3.11. An input image (*cover image*) "*I*" is transmitted over an unsecured communication channel. The watermark embedding process is applied to "*i*" using Schur decomposition and DCT prior to transmission to generate a watermarked image i_w. The watermarked image i_w (potentially attacked) is sent to receiver B, where the attacked watermark image w_a is extracted using the same operation in embedding process *(symmetric operation*). The Watermark embedding/extracting process is detailed in the next sections.

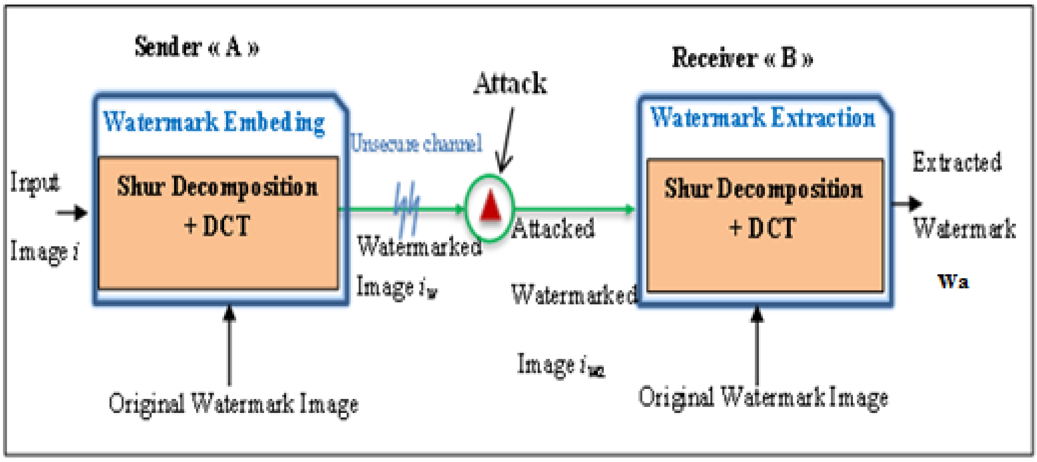


Figure 3.11 General generic model of the proposed method.

- *Watermark embedding process*

The watermark embedding process is based on Schur decomposition and DCT, as illustrated in Figure 3.12 and detailed as follow:

Step1. Decompose up the cover image into 2x2 non-overlapping blocks.

Step 2. Perform Schur decomposition on each block (B_i):

$$Schur(B_i) = [U, V] \qquad (3.8)$$

Step 3. apply DCT on the V matrix obtained bellow and the watermark image.

Step 4. Select a block's coefficients (BC_i) and two watermark DCT coefficients (WC_j and WC_{j+1}), and embed them in the middle band coefficients of BC_i , using scaling factor α as follow:

$$\begin{cases} BC_i(1,2) = BC_i + (1-\alpha) * WC_j \\ BC_i(2,1) = BC_i + (1-\alpha) * WC_{j+1} \end{cases} \qquad (3.9)$$

Where α in]0,1[.

Embedding two watermark DCT coefficients in the middle band DCT coefficients of the V matrix doesn't affect the cover image intensity (Fig 3.13) due to the good characteristics of DCT and Schur decomposition [68,69,71,9, 42].

Step 5. Apply DCT^{-1} on BC_i to obtain the watermarked V matrix (V_W), then perform $Schur^{-1}$ to obtain the watermarked block using the following equation:

$$Schur^{-1} = U * V_W * U^T \qquad (3.10)$$

Step 6. If not all the watermark DCT coefficients are embedded go back to step 4 with i+1 and j+2. Else end.

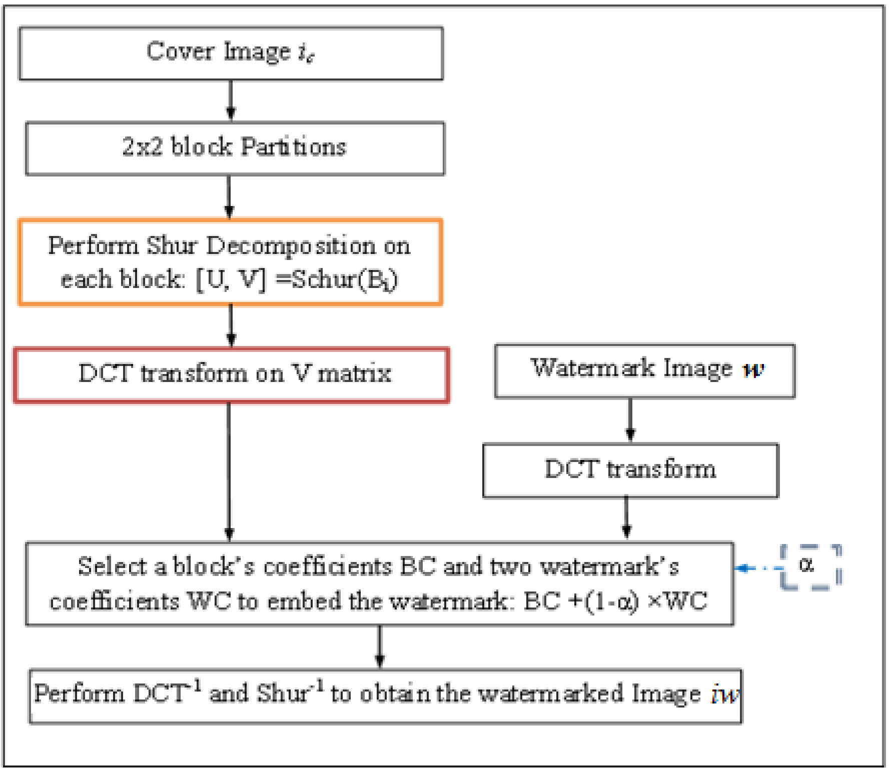

Cover Image i_c
2x2 block Partitions
Perform Shur Decomposition on each block: [U, V] =Schur(B$_i$)
DCT transform on V matrix
Watermark Image w
DCT transform
Select a block's coefficients BC and two watermark's coefficients WC to embed the watermark: BC +(1-α) ×WC
α
Perform DCT^{-1} and Shur^{-1} to obtain the watermarked Image iw

Figure 3.12 Watermark embedding process.

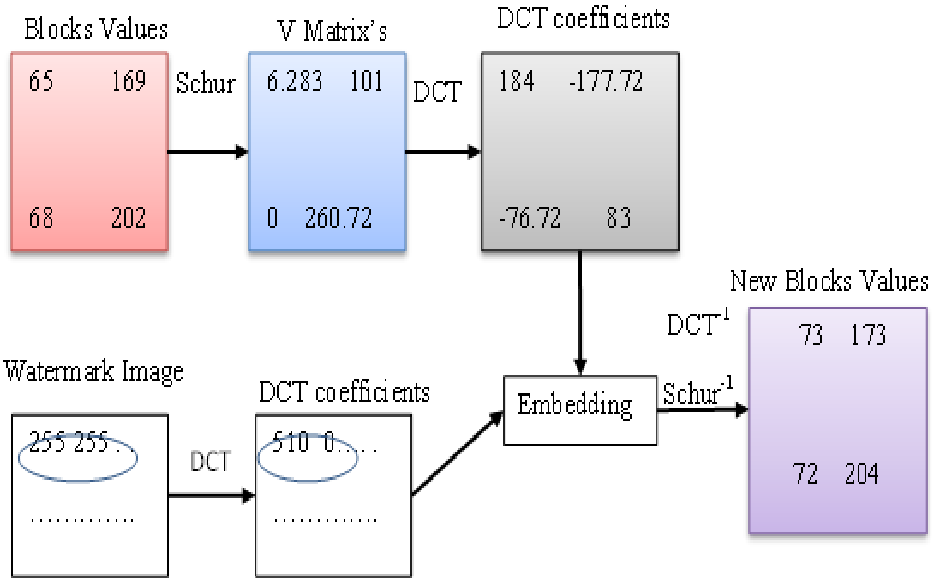


Figure 3.13 Example of new blocks pixel intensity values after embedding of watermark.

- *Watermark extracting process*

The extraction process is semi-blind since it requires the original watermark image. The detailed extraction process is illustrated with a block diagram in Figure 3.14 and discussed as follow:

1. Decompose up the host image into 2x2 non-overlapping blocks.
2. Perform Schur decomposition on each block (B_i) using Eq.3.8.
3. Apply DCT on the V matrix obtained below.
4. Select a block's coefficients (BC_i) and two watermark intensities (WI_j and WI_{j+1}).

And then extract the watermark DCT coefficients as follow:

$$\begin{cases} WC_j = \dfrac{WI_j(1,2)}{\alpha} - \dfrac{1-\alpha}{\alpha} * BC_i(1,2) \\ WC_{j+1} = \dfrac{WI_{j+1}(2,1)}{\alpha} - \dfrac{1-\alpha}{\alpha} * BC_i(2,1) \end{cases} \qquad (3.10)$$

5. If not all the watermark blocks are extracted go back to step 4 with i+1 and j+2. Else Apply DCT^{-1} on the extracted watermark coefficients to get the extracted watermark block.

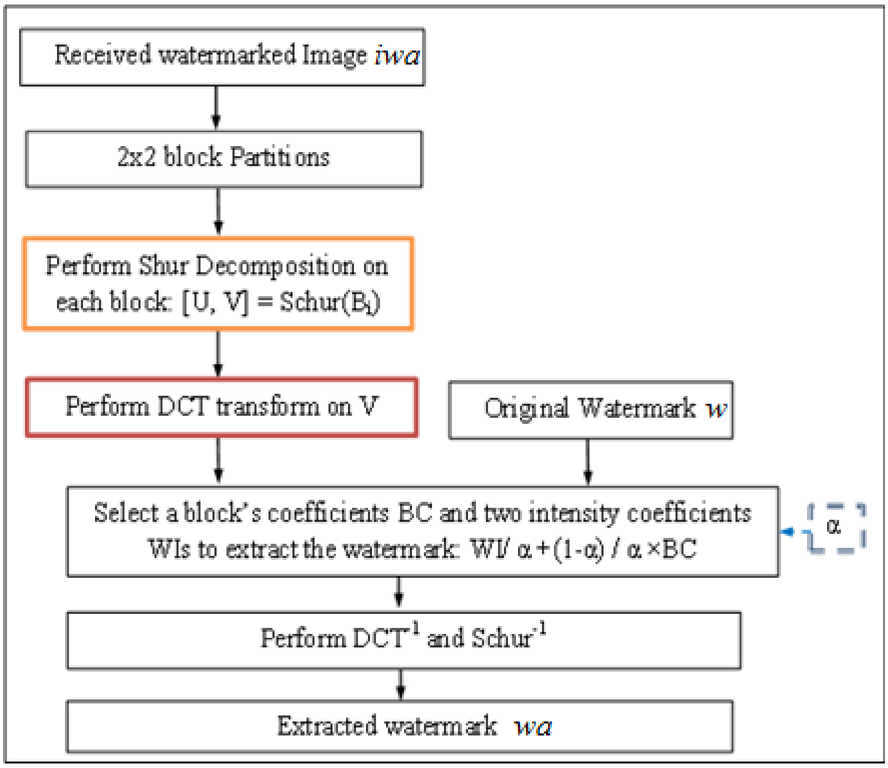

Received watermarked Image iwa
2x2 block Partitions
Perform Shur Decomposition on each block: [U, V] = Schur(B_i)
Perform DCT transform on V
Original Watermark w
Select a block's coefficients BC and two intensity coefficients WIs to extract the watermark: WI/ α+(1-α) / α ×BC
α
Perform DCT^-1 and Schur^-1
Extracted watermark wa

Figure 3.14 Watermark extracting process of the proposed method.

3.2.2.3 Experimental Results

We studied in this section, the technique's performances and compared them to some relevant work results [44, 71, 72] in order to illustrate the effectiveness and the robustness of our approach.

- *Performance evaluation measures and data used*

In order to evaluate the performance~~s~~ of the proposed technique in terms of imperceptibility and robustness, a data set of DICOM images of size 256x256 are used (from [78, 106]), while the watermark image is of size 128x128. We use some similarity measures such as MSE, PSNR, NC, CC and BER. The principles of these measures are well detailed in chapter 1, section 4.

Figure 3.15 illustrates the watermark image used for our experiments, while Figure 3.16 present a sample of tested medical images.

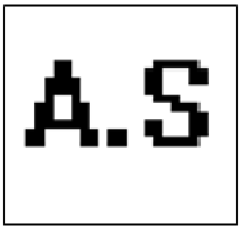


Figure 3.15 Watermark image used in experiment.

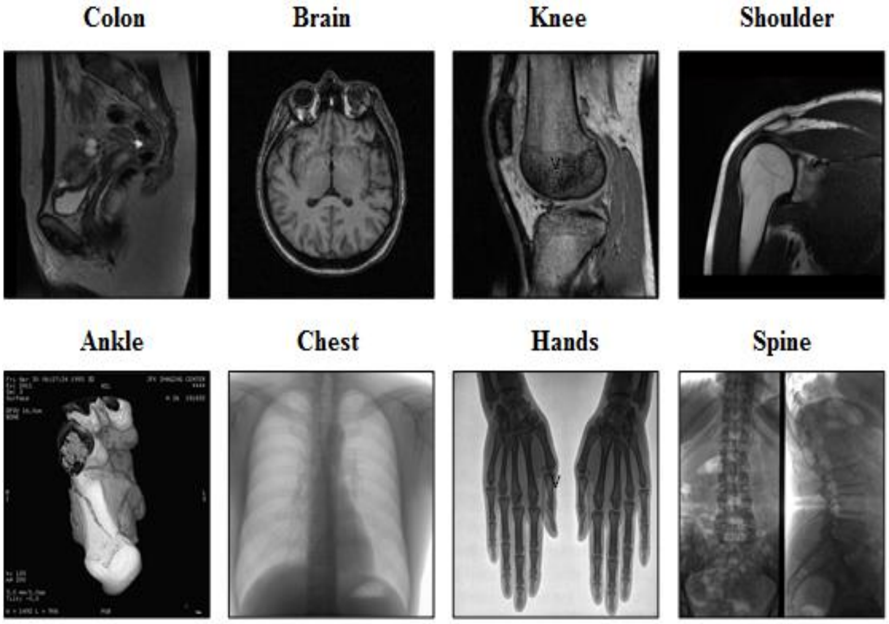
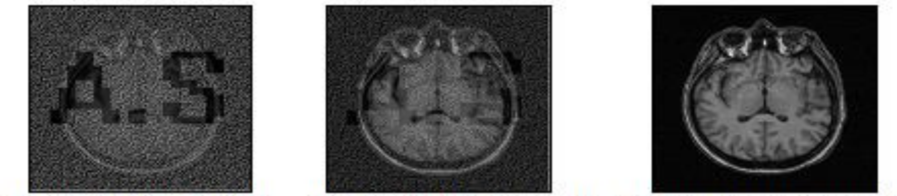


Figure 3.16 Sample of medical images used in experimentation.

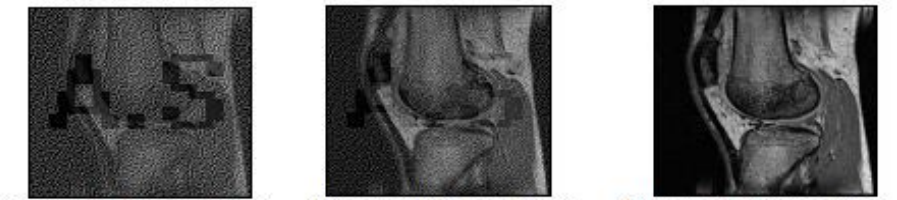
Figure 3.17 presents the watermarked images with different values of alpha α (0.01, 0.5 and 0.98) to achieve visible, semi-visible and invisible watermarking respectively.



Watermarked image (brain) with α=0.1

Watermarked image (brain) with α=0.65

Watermarked image (brain) with α=0.98



Watermarked image (knee) with α=0.1

Watermarked image (knee) with α=0.65

Watermarked image (knee) with α=0.98

Figure 3.17 Watermarked images with different values of α.

In the following, we use a scaling factor α of value 0.98.

- *Imperceptibility evaluation*

The first performance was used to evaluate the proposed method in term of imperceptibility. A higher imperceptibility value means a high similarity between the original image and the watermarked one. This factor α is important on the medical images application, since a mediocre imperceptibility degree means an impracticability of the watermarking method. The quality degradation of medical image implies wrong interpretation from physician, which may direct to wrong diagnosis and treatment. Table 3.9 illustrates the imperceptibility degree in terms of PSNR. PSNR average value of all dataset images was around 41 dB.

Table 3.9 Imperceptibility evaluation of the proposed watermarking method.

Images	**Colon**	**Knee**	**Hands**	**Spine**
PSNR(dB)	40.44	40.47	43.39	40.98

We measured the PSNR values between the proposed approach and the related works [71, 44, 72] as shown in Figure 3.18.

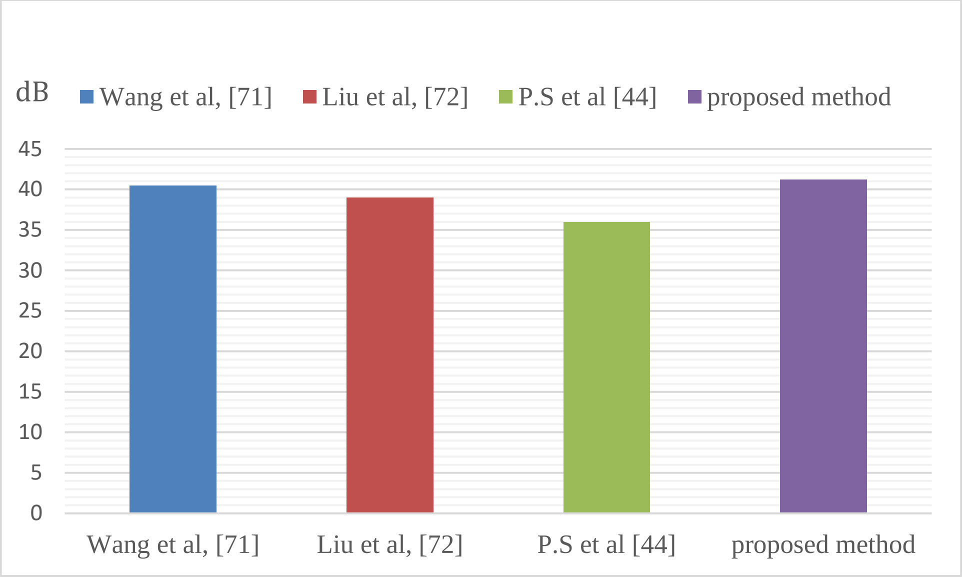


Figure 3.18 PSNR (dB) comparison results with the works described in [71, 44, 72].

The obtained results in Table 3.9 and Figure 3.18 show that the proposed method gives better imperceptibility. These results confirm that by embedding a watermark DCT coefficients involves a little changes in the Schur DCT coefficients of the cover image blocks, Fig 3.13 prove that the proposed method keep a good imperceptibility compared to relevant related works [71, 44, 72].

- *Robustness Evaluation*

The second performance was used to evaluate the proposed method in term of robustness. Robustness is the degree of resistance of an embedded watermark against different attacks performed to remove it or to confuse the image authentication. In our experimentation, we applied some geometric and non-geometric attacks on the watermarked image then evaluate the extracted watermark image using NC, BER and CC measures between the original watermark and the extracted one. Table 3.10 gives the NC values of the extracted watermarks from the attacked watermarked images. Table 3.11 shows the robustness comparison results between the proposed method and the approaches described in [65, 44]. The results show that our approach is more robust against different kind of attacks than other approaches [65, 44]. It’s obvious that the proposed model offers good robustness (i.e. NC and CC values are very close to 1, while BER is close to 0).

Table 3.10 NC values of the extracted watermark from the different attacked watermarked images.

Attacks	**Colon**	**Knee**	**Hands**	**Spine**
Salt & pepper noise v=0.05	0.91	0.91003	0.913	0.91
White noise v=0.05	0.885	0.885	0.887	0.885
DICOM JPEG compression attacks QF=50	0.996	0.996	0.994	0.996
Rotation 45°	0.994	0.994	0.995	0.995
Cropping 10%	0.993	0.993	0.993	0.994
Shearing	0.99	0.9907	0.99	0.99

Table 3.11. Robustness comparisons under NC values between the proposed method and works presented in [65, 44].

Attacks	**Mansoori et al.[65]**	**Prasanth et al.[44]**	**Proposed method**
Salt & pepper noise v=0.01	0.90	0.99	**1**
Salt & pepper noise v=0.05	-	0.91	0.91
White noise noise v=0.01	0.90	0.94	**0.981**
Rotation 5°	0.93	-	**1**
Rotation 45°	0.89	0.90	**0.99**

3.3 Synthesis and discussion

Two new robust watermarking techniques were presented in transform domain. The first efficient technique leverages of the DCT coefficients and Weber descriptors technique, makes it power to offers more significant advantages such as in good imperceptibility and security (e.g. as shown in Table 3.9 PSNR values exceed 41 dB.) and low computational complexity (e.g. as shown in Table 3.5) compared to related watermarking techniques. However, the embedding capacity is limited (a watermark bit is embedded in a block of size 4 × 4, which means a binary watermark of size $N \times N$ necessitates at least a cover medical image of size $4N \times 4N$), and the limited robustness degree with some geometric attacks such as translation, rescale (RESC), remove line (RML) and random distortions (RNDDIST). This is requiring an improvement by enhancing the ideal emplacement for embedding the watermark. To this end, the second enhancement technique of the first one was proposed. This method uses both benefits and features of Schur decomposition and DCT. It achieves better performance in term of robustness compared to the first method (Table 3.10). We noticed also that our second proposed approach ensures good imperceptibility when important amount of data is embedded. However, it requires a high computational complexity and it couldn’t be applied with real time e-health applications. This must be taken in consideration in the future works.

3.4 Conclusion

This chapter presented two contributions in robust medical image watermarking field. The first contribution is a new blind medical image watermarking in frequency domain which means that the embedded watermark could be extracted without the need of the original (i.e., watermark and/or cover) image. This technique based on Weber Descriptors and Arnold Chaotic Map. It provides better performance in terms of robustness compared to other related methods. It achieves a remarkable robustness against several attacks such as JPEG compression, median filtering…etc., and guarantees watermark imperceptibility compared to same related methods. The second contribution is a semi-blind watermarking medical image watermarking based On Schur decomposition and DCT. Embedding two watermarks DCT coefficients in the middle coefficients of the DCT middle band coefficient of the cover image blocks, after carried out the Schur decomposition on the image’s blocks. This gives the possibility to benefits from the good features of Schur decomposition and DCT. Experimental results demonstrate that the proposed scheme not only improve the efficient robustness against many attacks such as *JPEG compression, rotation and noising*, but also ensures a good imperceptibility when embedding an important amount of data.

In the next chapter, we will present our contributions in the semi-fragile techniques.

Chapter 4

Semi-fragile Medical Image Watermarking Techniques

Content

4.1 Introduction………………………………………………………………………73
4.2 Semi-Fragile Watermarking Approach's……………………………….…….........73
  4.2.1 A FAST END EFFECTIVE WATERMARKING METHOD FOR MEDICAL DATA …........73
    4.2.1.1 Proposed Watermarking Method……………………………………......…...73
    4.2.1.2 Experimental Results And Evaluation…………………………….….…......77
  4.2.2 A NOVEL BLIND MEDICAL IMAGE WATERMARKING SCHEME BASED ON SCHUR TRIANGULATION AND CHAOTIC SEQUENCE……………………………………………………….….…..80
    4.2.2.1 Chaotic Sequence……………………………………….....……….…….….…80
    4.2.2.2 Proposed Watermark Embedding And Extracting Processes……….……....80
    4.2.2.3 Experimental Results And Discussion……………………………….….…..85
4.3 Synthesis And Discussions……………………………………………………...….93
4.4 Conclusion……………………………………….………………….…...….…….94

4.1 Introduction

Image watermarking is an effective and powerful solution in multimedia security especially when it comes to data authentication and integrity checking, where the semi-fragile watermarking methods are the ideal tool for that purpose. In the sequel, blind watermarking technique increases the security factor in the medical field, but unfortunately the majority of the proposed watermarking techniques available in literature are semi-blind or non-blind.

This chapter presents two blind semi-fragile watermarking approaches in the frequency domain. The goal is to achieve low computational complexity and good imperceptibility. The rest of the chapter is organized as follows: section 2 focuses on our contribution, i.e., it details the proposed watermarking blind semi-fragile approach. We will present the processes of watermark embedding and the processes of watermark extracting. Section 3 presents a synthesize discussions and comparison between the proposed approaches. Section 4 concludes the chapter.

4.2 Semi-fragile watermarking approach’s

In this section, two semi-fragile watermarking methods in frequency domain. The first is based on DWT combined with Schur Decomposition. While the second scheme based on Schur Triangulation and Chaotic Sequence.

4.2.1 A Fast and Effective Watermarking Method for Medical Data Security

In this section, presented a novel watermarking method to protect the sensitive medical data transmitted through unsecured network. The proposed method benefits from the combination of DWT and Schur decomposition for embedding watermark bits. The proposed technique is blind which means that the data embedded is extracted without the needing of original or watermark images, where experimental results in end of this section, demonstrate the performances of the proposed scheme.

4.2.1.1 Proposed Watermarking method

In this section we describe in detail the proposed watermarking methods.

A. *Embedding process*

The watermark embedding process steps are presented in the Algorithm 4.1 and shown in Figure 4.1.

Algorithm 4.1 Watermark embedding process.

```
Input : Original image, Watermark image, block size.
Output: Watermarked medical image.
Begin
  While not all the watermark bits are embedded Do
    - Decompose the medical image into mxm non-overlapping blocks.
    - Select a block $B_i$ and a watermark bit $W_i$.
    - Scrambling $B_i$ using Arnold chaotic map [1].
    - Apply DWT [6] on $B_i$ then perform Schur decomposition [7] on the LL sub-bands:
          o Schur (LL)=[U,V]          (1)
    - Select the V matrix block (BV) and compute their weight (We) using the following equation:
      $We=\sum_{j=1}^{\frac{m}{2}-1}\sum_{k=1}^{\frac{m}{2}-j}\big(BV(j,k)\big)+\sum_{j=2}^{\frac{m}{2}}\sum_{k=\frac{m}{2}}^{\frac{m}{2}-j+2}\big(BV(j,k)\big)-\sum_{j=1}^{m/2}(BV(j,m-j+1))$          (2)
    - Embed $W_i$ into BV according to We value:
      If We <0 and $W_i$ ==1
        Repeat
            min $(BV(j,m-j+1))+\epsilon$ {j=1:m}          (3)
        Until We>=0
      Else if We >=0 and $W_i$ ==0
        Repeat
            min $(BV(j,m-j+1))-\epsilon$ {j=1:m}          (4)
        Until We>=0
        Where $\epsilon$ is the embedding strength.
    - Apply $Schur^{-1}$ succeeded by $DWT^{-1}$, and descrambling $B_i$ to
  End While
  Return the watermarked medical image.
End.
```

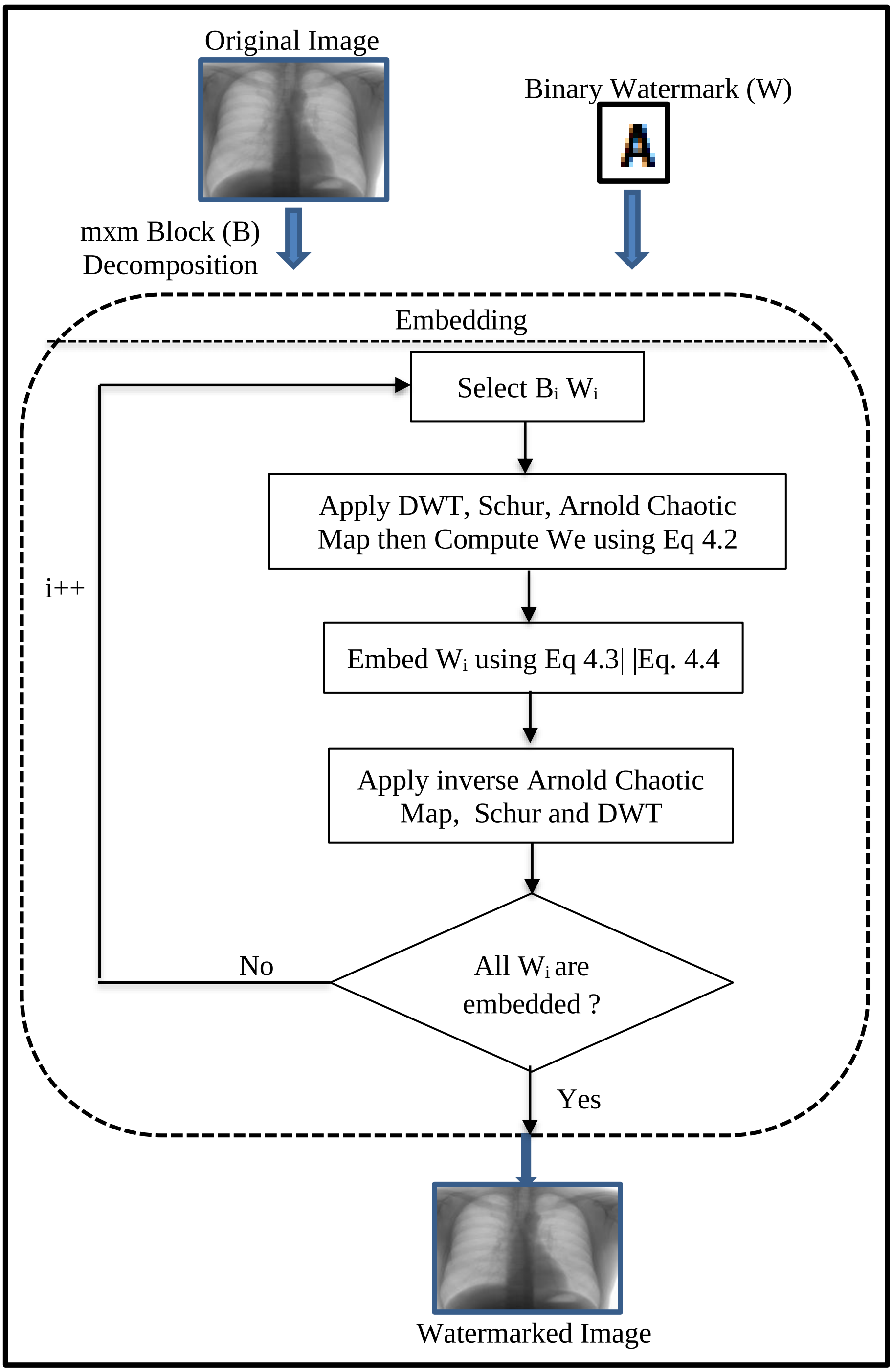

Original Image
Binary Watermark (W)
mxm Block (B) Decomposition
Embedding
Select B_i W_i
Apply DWT, Schur, Arnold Chaotic Map then Compute We using Eq 4.2
i++
Embed W_i using Eq 4.3| |Eq. 4.4
Apply inverse Arnold Chaotic Map, Schur and DWT
No
All W_i are embedded ?
Yes
Watermarked Image

Figure 4.1 Watermark embedding process main steps.

B. *Extraction process*

The extraction process steps are described in the Algorithm 4.2 and described in Figure 4.2.

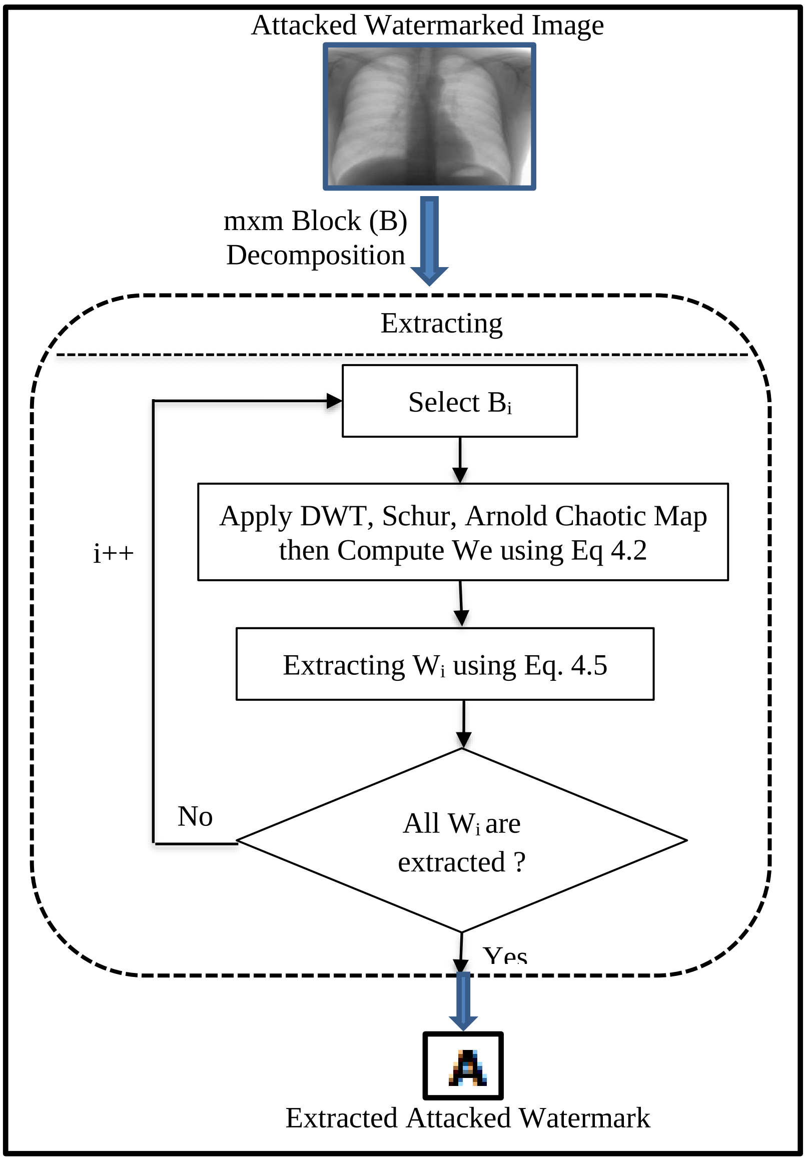

Attacked Watermarked Image
mxm Block (B)
Decomposition
Extracting
Select B_i
Apply DWT, Schur, Arnold Chaotic Map
then Compute We using Eq 4.2
Extracting W_i using Eq. 4.5
i++
No
All W_i are
extracted ?
Yes
Extracted Attacked Watermark

Figure 4.2 Watermarking extraction process main steps.

Algorithm 4.2 Watermark Extraction Process.

```
Input  : Watermarked medical image, block size.
Output: Watermark image.
Begin
  While not all the watermark bits are extracted Do
    -   Decompose the whole medical image into mxm non-overlapping blocks.
    -   Select a block $B_i$ and scramble it using Arnold chaotic map.
    -   Apply DWT [6] on $B_i$ then perform Schur decomposition [7] on the LL
        sub-bands (Eq. 1).
    -   Select the V matrix block (BV) and compute their weights (We) By Eq. 2.
    - Extract the $W_i$ from BV using the following equation:
          $\begin{cases} Wi = 0; \text{if } We < 0 \\ Wi = 1; \text{otherwise} \end{cases}$      (5)
  End While
  Return the watermark image.
End.
```

4.2.1.2 Experimental results and Evaluation

In order to prove the efficiency of the proposed method; a data set of medical images of size 256x256 in DICOM format [79] and watermark of size 32x32 are used (in our experimentation we use a block size of 4x4 and an embedding strength ϵ=5).

Figure 4.3 show a sample of images used in experimentation and watermark, where all images used are from [78, 79].

We evaluate the proposed digital watermarking method in terms of imperceptibility, robustness.

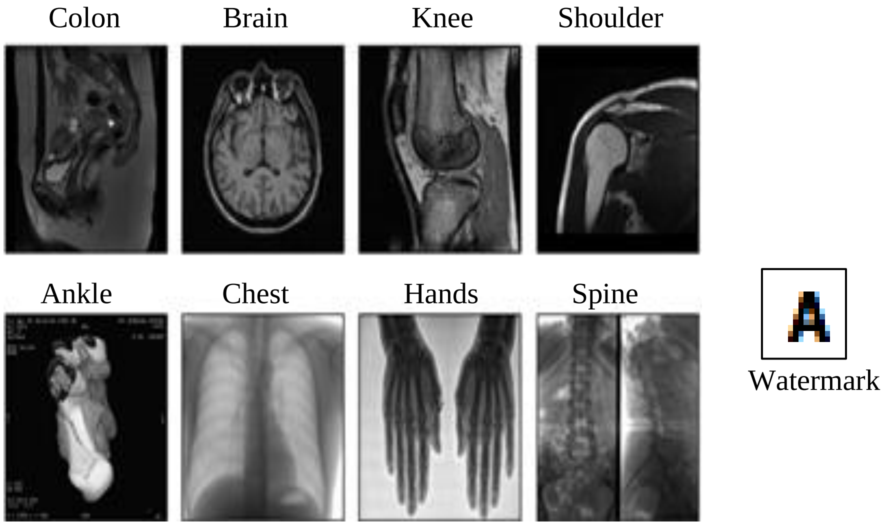


Figure 4.3 Sample of medical images used and watermark used in experimentation.

- *Imperceptibility measurement*

The imperceptibility [74] has a high impact in the medical field, where a mediocre imperceptibility could lead to a serious consequences. Table 4.1 shows imperceptibility degrees of the proposed method in terms of PSNR (dB) [75].

Table 4.1 PSNR (dB) values of the proposed method.

Images	Colon	Brain	Knee	Shoulder	Anckle	Chest	Hands	Spine
PSNR(db)	38.11	36.83	43.17	40.97	37.89	45.13	48.87	43.21

Examining the obtained results in Table 4.1 concludes that the proposed method improves good imperceptibility. The reason is that the embedding of a watermark bit necessitates a small unnoticeable change in the V matrix after Schur decomposition on the LL sub-bands of DWT value of the cover image blocks. To this end, the watermarked images keep the good imperceptibility comparing to the original one.

- *Robustness measurement*

In order to evaluate the robustness [74] of the presented method, some attacks are applied to the watermarked image, and then NC [75] measure is evaluated between the original watermark and the extracted one. Table 4.2 shows the list of attacks used in the experimentation, while tables 4.3 show the NC values of the extracted watermark after attacks listed in table 4.2.

Table 4.2 List of attacks used in experimentation.

Attacks Names	Abbreviations
DICOM JPEG Compression Lossless	DJL
DICOM JPEG Compression Lossy (QF=50)	DJLY
DICOM JPEG 2000 compression Lossless	DJ2L
DICOM JPEG 2000 compression Lossy (QF=50)	DJ2LY
Rotation 0.1°	RT
Salt & Pepper noise V=0.01	SPn
White noise V=0.0001	WN
Speckle noise V=0.0001	SPeN

It's clearly indicated from Tables 4.3 that our technique performs good robustness under different attacks used in experimentation. The reason is that the watermark data is embedded into the ideal location (DWT-Schur coefficients) which makes it robust against these kinds of attacks.

Table 4.3 Robustness measurement under NC values.

Images	DJL	DJLY	DJ2L	DJ2LY	RT	SPn	WN	SpeN
	Attacks							
Colon	0.97	0.978	0.977	0.96	0.668	0.96	0.676	0.716
Brain	0.985	0.984	0.985	0.978	0.64	0.97	0.681	0.742
Knee	0.971	0.97	0.971	0.97	0.646	0.96	0.67	0.743
Shoulder	0.983	0.981	0.97	0.97	0.639	0.97	0.682	0.742
Ankle	0.98	0.984	0.979	0.97	0.642	0.97	0.678	0.732
Chest	0.986	0.986	0.985	0.981	0.651	0.978	0.685	0.74
Hands	0.974	0.971	0.97	0.97	0.624	0.96	0.652	0.74
Spine	0.985	0.981	0.985	0.98	0.642	0.97	0.668	0.741

- *Performances comparison*

In this section, we compare the proposed method with some recent techniques in terms of imperceptibility and robustness. Table 4.4 show the comparison of imperceptibility values (dB) of our approach with work presented in [64, 80, 81]. It's very clear that our approach performs better performances neither with medical images or other images.

Table 4.4 Comparisons of imperceptibility results of our approach with different approaches [64,80,81] using medical images.

Methods	[64]	[80]	[81]	**Proposed method**
PSNR (dB)	44	44	33	**44.5**

Table 4.5 illustrates the performance comparison of the proposed scheme with some recent methods [65, 81, 82] in terms of robustness using NC values.

Table 4.5 Robustness comparison with works presented in [65, 81, 82].

Attacks	[65]	[82]	[81]	Proposed approach
Salt & Pepper noise (v=0.01)	<0.8	**0.96**	0.88	**0.97**
Salt & Pepper noise (v=0.001)	0.96	0.98	**1**	**1**
Rotation 15°	**0.90**	-	-	0.613
JPEG compression Q=50	0.795	-	0.919	**0.97**

It’s clear that the comparison of the proposed technique shown in tables 4.4 and 4.5 proof the superior performances of the proposed method compared to some recent existing watermarking approaches in terms of imperceptibility and robustness. This makes our method legible to be practicable in telemedicine applications.

4.2.2 A Novel Blind Medical Image Watermarking Scheme Based on Schur Triangulation and Chaotic Sequence

In this section, we present a new blind semi-fragile based watermarking technique for medical images using Schur decomposition and chaotic sequence. An efficient chaotic method is exploited to encrypt the watermark image and cover image blocks. A decomposition based on Schur is employed to embed the encrypted watermark bits in the encrypted cover image blocks. Finally, the watermarked image is obtained using the same chaotic sequence used in encryption.

4.2.2.1 Chaotic Sequence

Chaotic sequence is an evolution function that exhibits some sort of chaotic behavior, where each value of the chaotic sequence has a dependency to the initial value [5, 76, 77], and the whole chaotic sequence could be obtained only with the presence of the seed.

The chaotic sequence is used as spread sequence to effectively encrypt and decrypt the watermark embedded in image blocks. The aim is not only to reinforce the security but also mainly to enhance the imperceptibility.

4.2.2.2 Proposed Watermark Embedding and Extracting Processes

Embedding watermark becomes more important to bits into medical images. A highly imperceptible watermarked image is an essential requirement to accurate and assuring quality diagnostics. Schur decomposition is a powerful technique that allows more imperceptibility and provides stronger robustness against some attacks. The proposed watermarking method consists of two processes: the watermark embedding process and the watermark extraction process which are explained as follow:

- *Watermark embedding process*

The watermark embedding steps are illustrated through a block diagram in Figure 4.4 Summarized as follow:

1. Generate a Binary Chaotic Sequence (BCS) from a key K using Algorithm 4.3.

Algorithm 4.3: binary chaotic sequence generation.

```
Input: K Key, n,m watermark size.
Output: BCS binary chaotic sequence.
Begin
  BCS (1:8)= Binary value Of (K);
  b=8;
  For i=2:n*m/8
      BCS(b:i*8)= Binary value Of (K+BCS(i-1));
      b=i*8;
  End For;
Return BCS.
```

2. Encrypt the binary watermark image by performing the XOR operation between the Binary Chaotic sequence generated bellow and the watermark image.
3. Decompose up the encrypted cover image into 2x2 non-overlapping blocks.
4. Generate a chaotic sequence (CS) from a key K using the following equation:

$$\begin{cases} \mathrm{CS}(1,1) = \mathrm{K} \\ \mathrm{CS}(1,\mathrm{j}) = \mathrm{CS}(1,\mathrm{j}-1) + \mathrm{K} \\ \mathrm{CS}(\mathrm{i},1) = \mathrm{CS}(\mathrm{i}-1,1) + \mathrm{K} \\ \mathrm{CS}(\mathrm{i},\mathrm{j}) = \mathrm{CS}(\mathrm{i},\mathrm{j}-1) + \mathrm{CS}(\mathrm{i}-1,\mathrm{j}) - \mathrm{K} \end{cases} \tag{4.6}$$

5. The Chaotic sequence generated bellow is decomposed up into 2x2 non-overlapping blocks.
6. Each Block of the Cover image blocks is encrypted by adding the Chaotic sequence (CS) generated in Step 4 to the pixel intensity of the original image (OI) as follow:

$$Enc(i,j) = mod\left(OI(i,j) + CS(i,j) + K2, X\right) \tag{4.7}$$

Where Enc(i,j) is the encrypted intensity value, X=2^8 for JPEG format image and 2^{15} for DICOM format image.

7. The encrypted watermark bits are embedded in the encrypted medical image blocks using the following sub-steps:

a) Select an encrypted Block Enc$_i$, and compute its weight W(i) using Eq 4.8.

$$W(i)=\sum_{j=1}^{4} Enc(j) \qquad (4.8)$$

Where "*i*" is the block number, and j is the pixel number.

b) Select a Watermark Bit WB$_k$ from the encrypted watermark bits and embed it according to the following cases:

If mod (W(i),2)~=WB$_k$ then

[u,v]=Schur(Enc(i));

Min(v(1,2), v(2,1))= Min(v(1,2),v(2,1))+1 ;

Incrementing minimum (v(1,2) , v(2,1)) modify (increment or decrement) one pixel intensity from the 2x2 block pixel intensities (Figure 4.5). This improve the imperceptibility of the watermark.

Enc(i)=u*v*u^T.

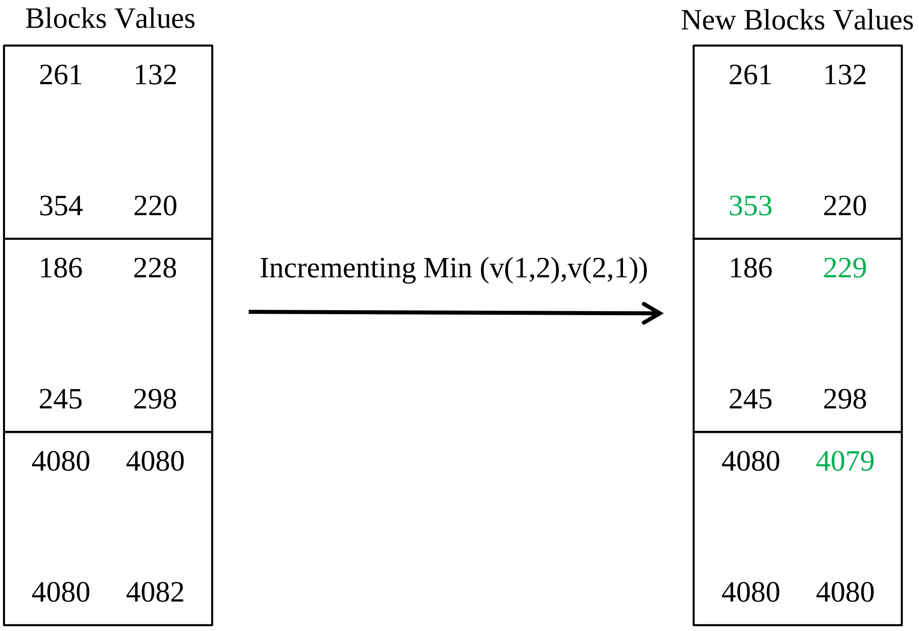
Else go to sub-step c.

c) If all the watermark bits are embedded go to step 8,

else go back to step 7-a with i+1 and k+1.

8. Decrypt the encrypted blocks using the same chaotic sequence to obtain the watermarked image (WI) as follow:

$$WI(i,j)=mod\left(Enc(i,j)+CS(i,j)+K2,X\right) \qquad (4.9)$$



Blocks Values

261	132
354	220
186	228
245	298
4080	4080
4080	4082

New Blocks Values

261	132
353	220
186	229
245	298
4080	4079
4080	4080

Figure 4.5 Example of new blocks pixel intensity values after embedding of watermark bits.

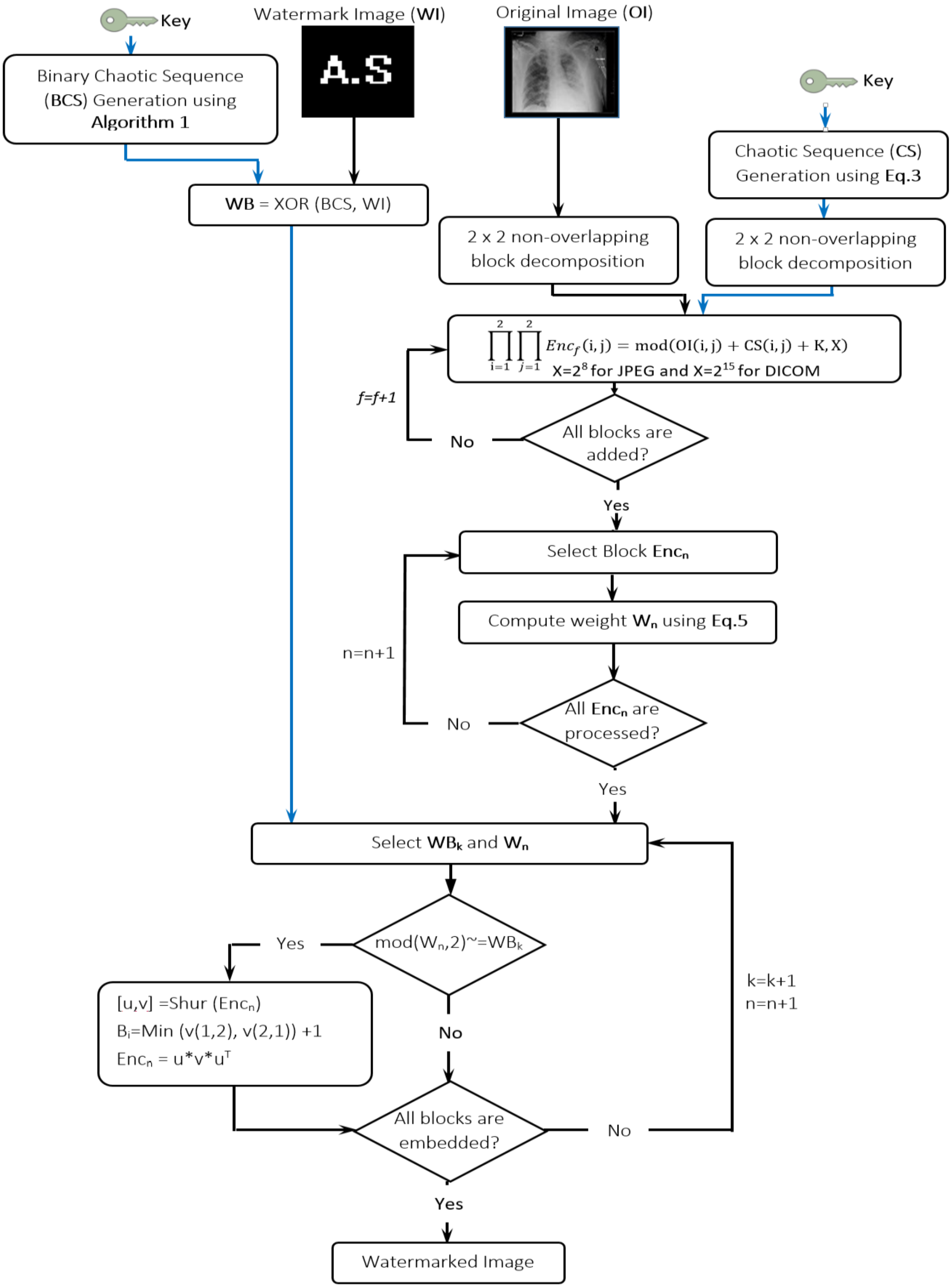

Key
Binary Chaotic Sequence (BCS) Generation using Algorithm 1
Watermark Image (WI)
A.S
Original Image (OI)
Key
Chaotic Sequence (CS) Generation using Eq.3
WB = XOR (BCS, WI)
2 x 2 non-overlapping block decomposition
2 x 2 non-overlapping block decomposition
$\prod_{i=1}^{2}\prod_{j=1}^{2} Enc_f(i,j) = \text{mod}(OI(i,j) + CS(i,j) + K, X)$
X=2^8 for JPEG and X=2^{15} for DICOM
f=f+1
No
All blocks are added?
Yes
Select Block Enc_n
Compute weight W_n using Eq.5
n=n+1
No
All Enc_n are processed?
Yes
Select WB_k and W_n
Yes
mod(W_n,2)~=WB_k
[u,v] =Shur (Enc_n)
B_i=Min (v(1,2), v(2,1)) +1
Enc_n = u*v*u^T
No
k=k+1
n=n+1
All blocks are embedded?
No
Yes
Watermarked Image

Figure 4.4 Watermark embedding process.

- *Watermark Extraction Process*

The extraction process is illustrated with a block diagram in Figure 4.6 This process is described as follow:

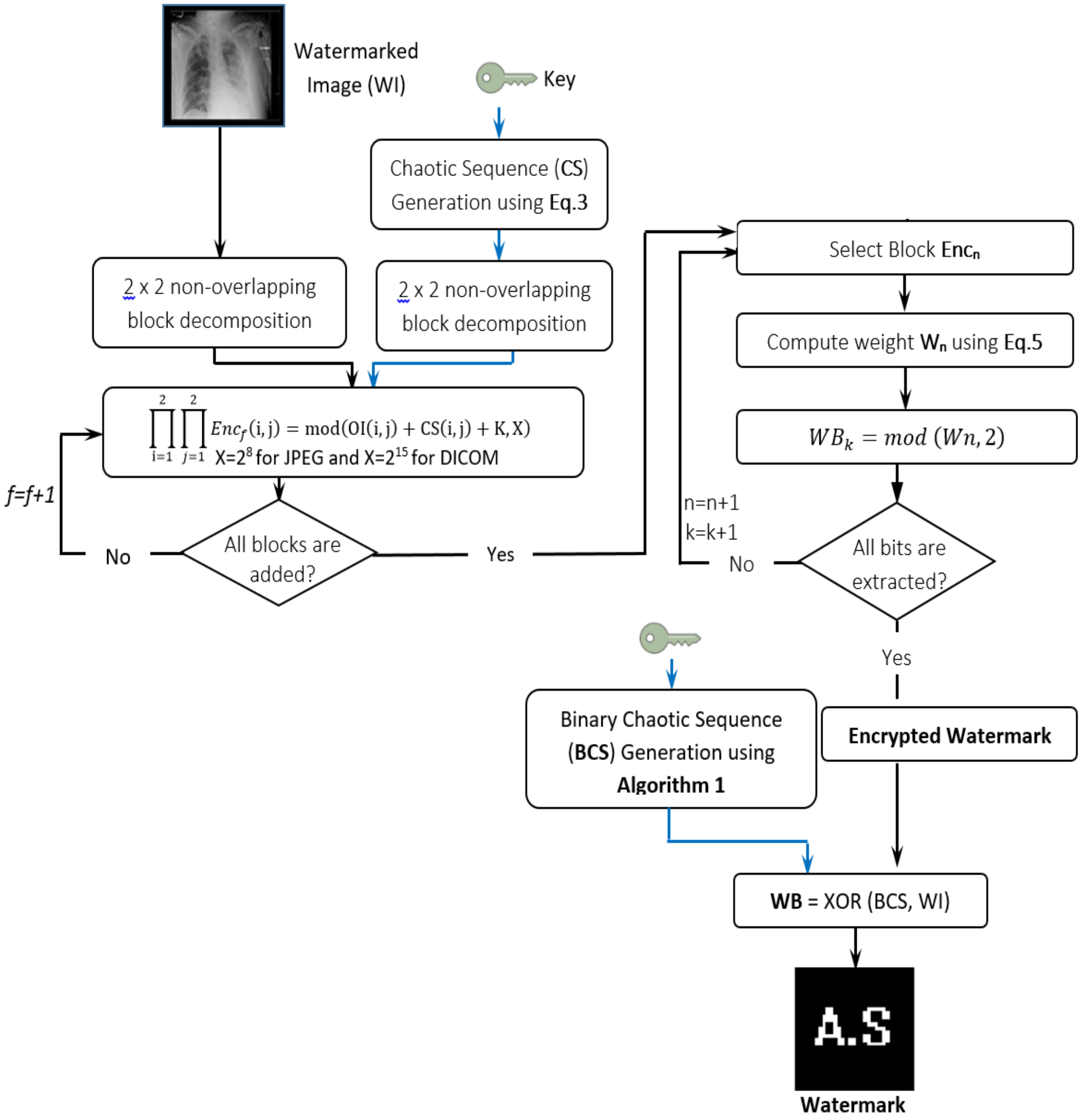

Watermarked Image (WI)
Key
Chaotic Sequence (CS) Generation using Eq.3
2 x 2 non-overlapping block decomposition
2 x 2 non-overlapping block decomposition
$\prod_{i=1}^{2}\prod_{j=1}^{2} Enc_f(i,j) = \mathrm{mod}(OI(i,j) + CS(i,j) + K, X)$ X=2^8 for JPEG and X=2^15 for DICOM
f=f+1
No
All blocks are added?
Yes
Select Block Enc_n
Compute weight W_n using Eq.5
$WB_k = mod\ (Wn, 2)$
n=n+1
k=k+1
No
All bits are extracted?
Yes
Binary Chaotic Sequence (BCS) Generation using Algorithm 1
Encrypted Watermark
WB = XOR (BCS, WI)
A.S
Watermark

Figure 4.6 Watermark extracting process.

1. Generate a binary chaotic sequence (BCS) from a key K using Algorithm 4.3.
2. Decompose up the watermarked image into 2x2 non-overlapping blocks.
3. Generate a chaotic sequence (CS) from a key K2 using Eq 4.6.
4. The Chaotic sequence generated bellow is decomposed up into 2x2 non-overlapping blocks.
5. Each Block of the Cover image blocks is encrypted by adding the Chaotic Sequence generated in Step 4 to the intensity of the watermarked image using Eq 4.7.
6. The encrypted watermark bits are extracted from the encrypted medical image blocks using the following steps:
    a) Select an encrypted Block Enc_i, and compute its weight W(i) using Eq 4.8.

b) A Watermark Bit WB_k is extracted from the encrypted block intensity:

$$WB_k = mod\ \left(W\left(i\right),2\right) \quad (4.10)$$

c) If not all the watermark bits are extracted go back to step 5-a with i+1 and k+1.

7. Decrypt the extracted watermark bits by performing the XOR operation between the Binary Chaotic sequence generated bellow and the extracted watermark image.

4.2.2.3 Experimental Results and Discussion

To evaluate the performance of the proposed technique in terms of imperceptibility and robustness, a data set of DICOM images of size 256x256 provided by [78, 79] are used. All experiments have been performed on a PC with Intel Core i5 2.67 GHz, with 4 GB of RAM, 250 GB hard disk and window 7 64 bits, using MATLAB R2013a.

Figure 4.7 shows the binary watermark image used, while Fig 4.8 gives a sample of tested images in experimentation as host images.

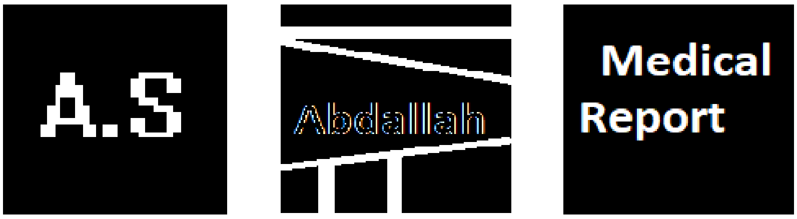
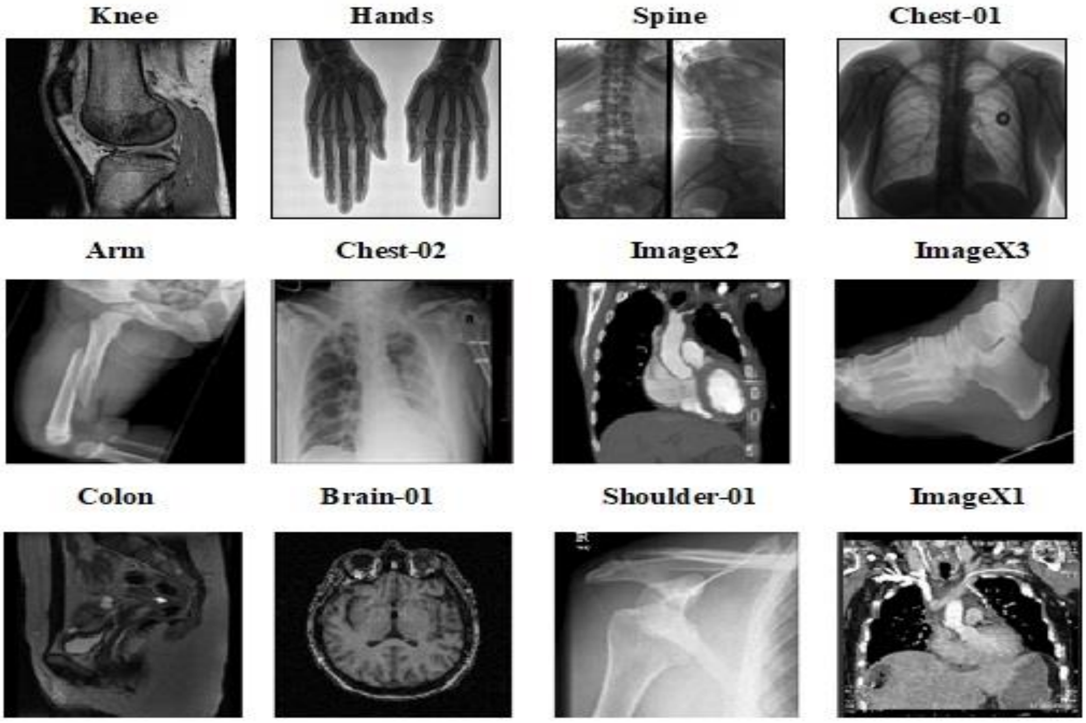


Figure 4.7 binary Watermark image used in experimentation.


Knee Hands Spine Chest-01

Arm Chest-02 Imagex2 ImageX3

Colon Brain-01 Shoulder-01 ImageX1

Figure 4.8 Sample of host images used in experimentation.

- *Imperceptibility Measurement*

Table 4.6 gives the imperceptibility degrees of the the presented scheme in terms of PSNR (dB) for different watermark size.

Table 4.6 PSNR values (dB) using different watermark size.

Images	Watermark Size							
	16x16	**24x24**	**32x32**	**48x48**	**64x64**	**80x80**	**96x96**	**128x128**
Knee	74.110	71.22	68.887	65.41	63.085	61.254	59.66	57.145
Hands	94.185	90.480	88.332	84.705	82.119	80.352	78.689	76.115
Spine	94.365	90.94	88.240	84.660	82.01	80.189	78.651	76.241
Chest	94.842	90.918	88.360	84.842	82.39	80.404	78.870	76.350
Colon	75.415	71.780	69.380	65.730	63.12	61.250	59.620	57.190
Brain01	75.090	71.660	68.159	64.879	63.09	60.959	59.030	57.001
Shoulder01	94.770	92.180	88.357	83.890	82.06	80.413	78.641	76.002
ImageX1	75.190	71.890	70.089	65.110	63.002	60.745	58.050	56.812
Arm	94.690	92.145	88.148	83.810	81.11	79.101	77.090	74.220
Chest02	94.418	90.980	88.200	84.630	82.09	80.250	78.660	76.200
ImageX2	80.453	76.487	71.220	68.112	66.745	62.921	60.812	58.660
ImageX3	89.451	86.745	83.480	80.227	78.5	75.265	72.332	70.154

Table 4.7 depicts the imperceptibility degrees of the proposed scheme according to different watermark sizes in terms of SSIM.

Images	Watermark Size							
	16x16	**24x24**	**32x32**	**48x48**	**64x64**	**80x80**	**96x96**	**128x128**
Knee	0.989	0.982	0.978	0.969	0.954	0.949	0.942	0.939
Hands	0.99	0.982	0.979	0.969	0.954	0.95	0.942	0.94
Spine	0.989	0.982	0.978	0.97	0.952	0.949	0.941	0.94
Chest	0.989	0.982	0.978	0.968	0.954	0.949	0.942	0.94
Colon	0.99	0.982	0.978	0.969	0.954	0.949	0.942	0.939
Brain01	0.981	0.982	0.979	0.969	0.954	0.95	0.942	0.94
Shoulder01	0.988	0.982	0.978	0.97	0.952	0.949	0.941	0.94
ImageX1	0.989	0.982	0.978	0.968	0.954	0.949	0.942	0.94
Arm	0.989	0.982	0.978	0.969	0.954	0.949	0.942	0.931
Chest02	0.989	0.982	0.979	0.969	0.954	0.95	0.942	0.94
ImageX2	0.989	0.982	0.978	0.97	0.952	0.949	0.941	0.94
ImageX3	0.989	0.982	0.978	0.968	0.954	0.949	0.942	0.94

We present the comparison results among various techniques described in [35, 64, 80, 81-83], as shown in Figure 4.9 in terms of PSNR (dB).

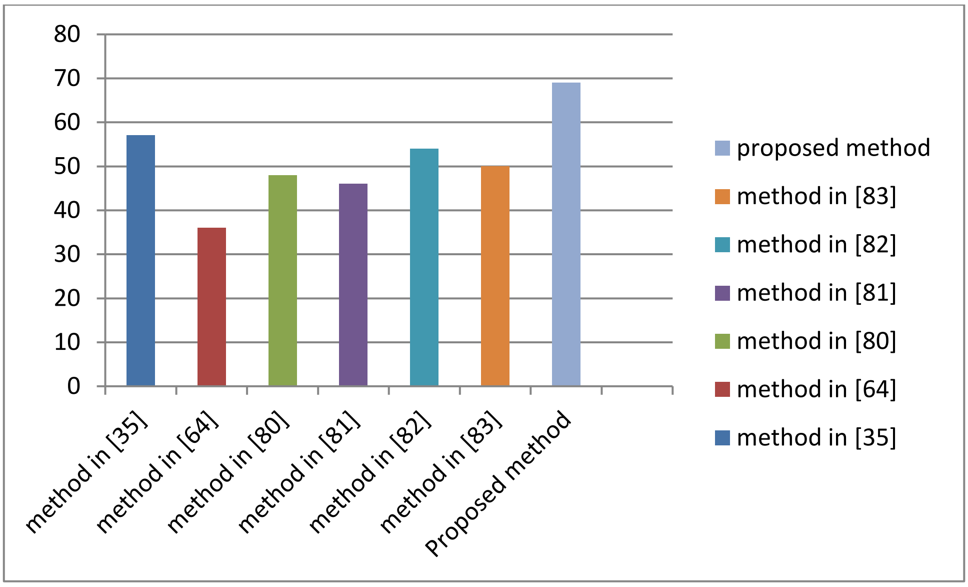


Figure 4.9 Imperceptibility (dB) comparison between the proposed method and methods in [35, 64, 80, 81-83].

As shown in Tables 4.6, 4.7 and Figure 4.9, the proposed algorithm achieves high imperceptibility when embedding a watermark of maximal size (128x128). Is due by embedding of a bit, it need the increment of one-pixel intensity in a block of four pixels.

- *Robustness Measurement*

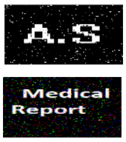
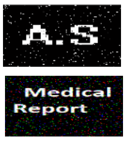
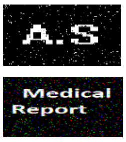
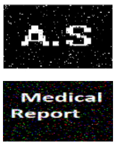
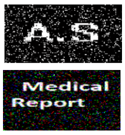
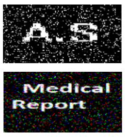
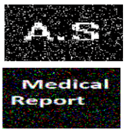
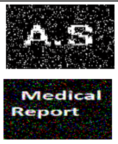
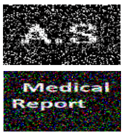
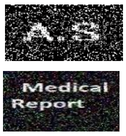
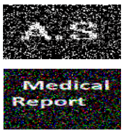
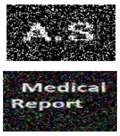
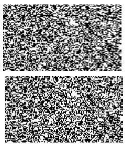
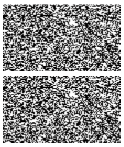
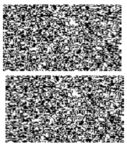
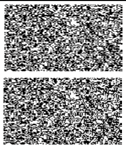
We attempt to evaluate the robustness of the proposed method against various attacks as described in Table 4.8. Normalized Coefficients (NC) and Bit Error Rate (BER) measures are used to evaluate the robustness of the proposed model. Table 4.9 shows the attacked watermarked images and the correspondent extracted watermarks. While Table 4.10 provides the values of NC and BER of the extracted watermarks from the attacked watermarked images when a watermark size is of 128x128.

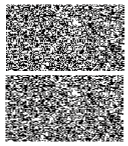
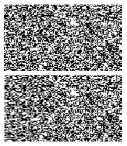
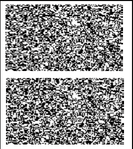
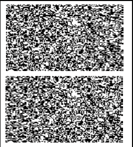
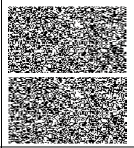
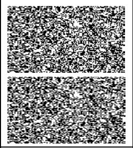
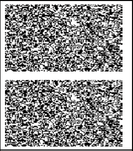
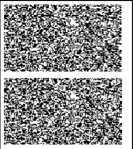
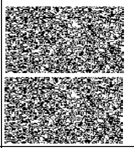
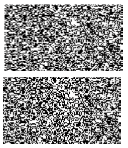
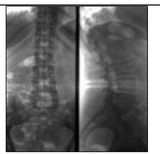
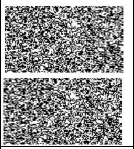
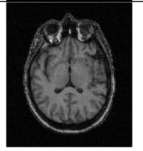
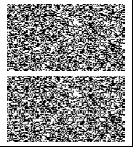
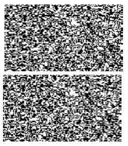
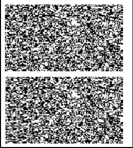
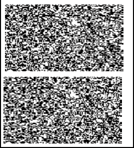
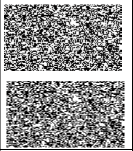
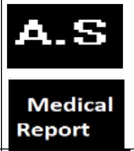
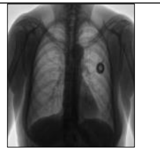
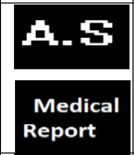
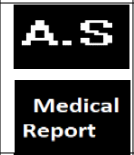
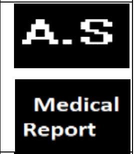
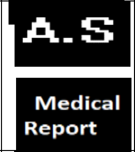
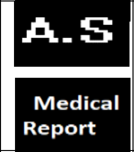
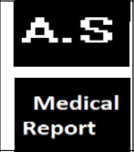
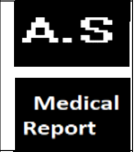
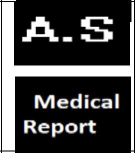
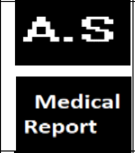
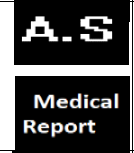
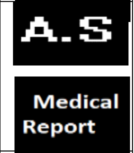
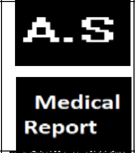
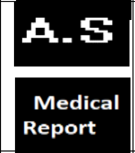
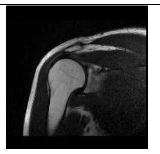
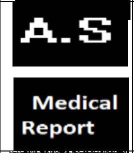
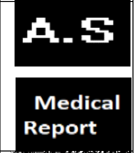
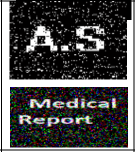
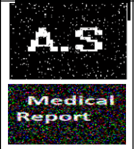
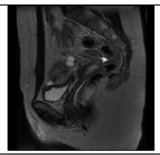
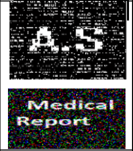
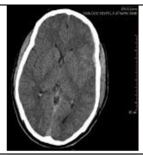
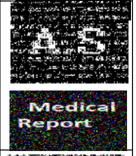
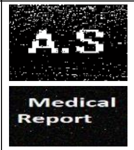
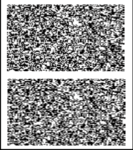
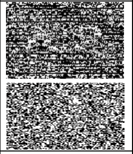
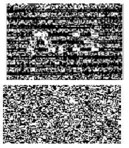
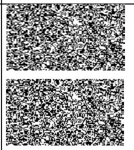
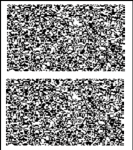
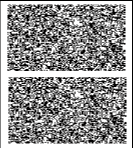
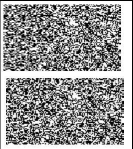
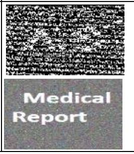
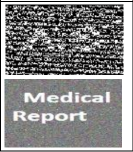
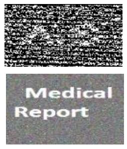
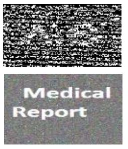
Table 4.8 The Applied attacks names abbreviation.

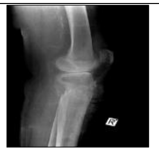
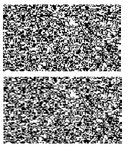
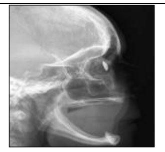
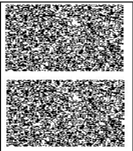
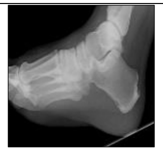
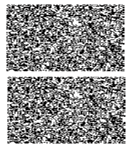
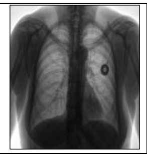
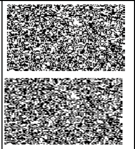
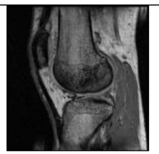
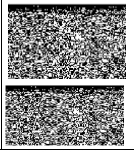
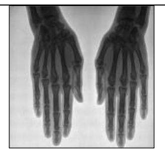
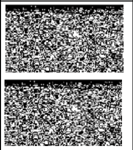
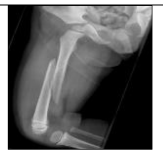
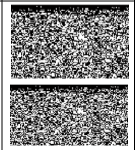
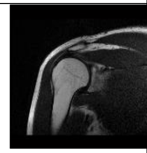
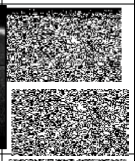
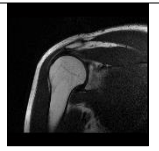
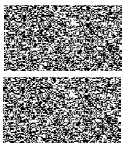
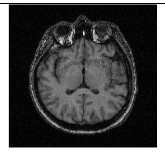
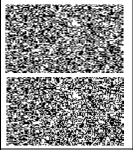
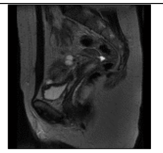
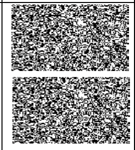
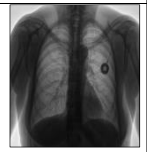
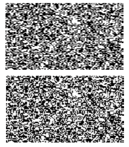
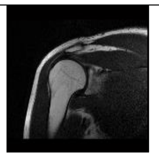
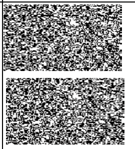
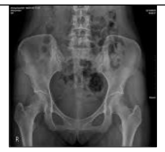
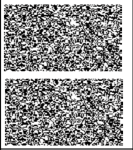
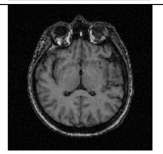
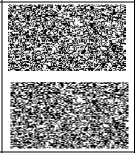
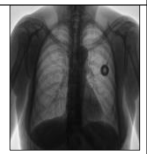
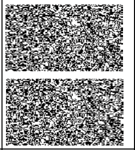
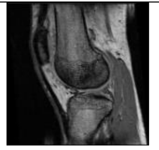
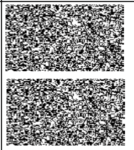
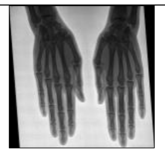
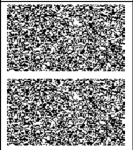
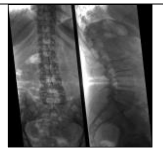
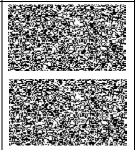
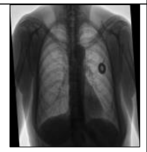
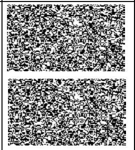
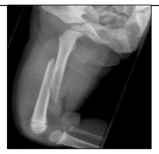
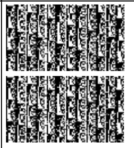
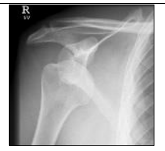
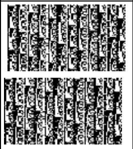
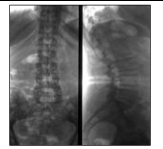
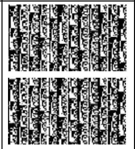
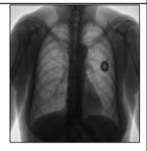
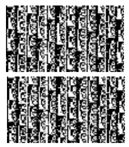
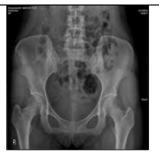
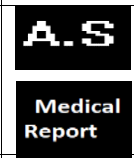
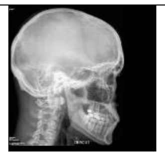
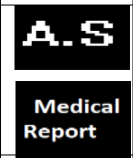
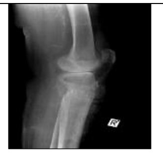
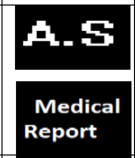
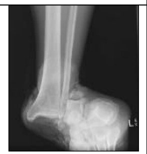
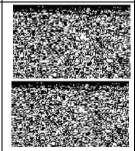
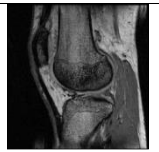
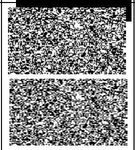
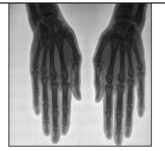
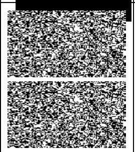
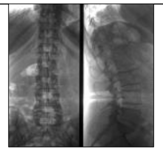
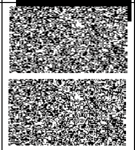
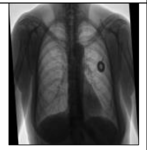
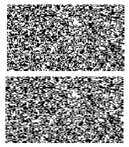
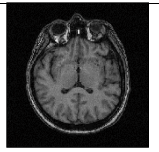
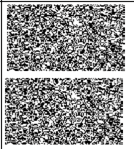
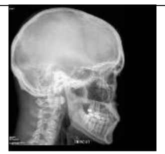
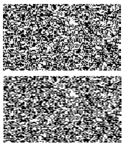
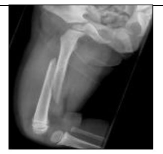
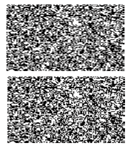
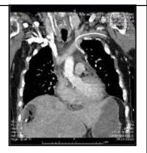
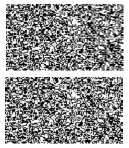
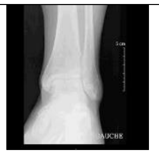
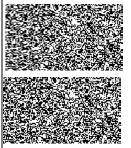
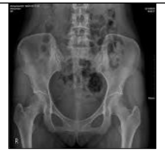
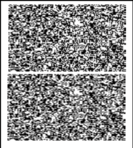
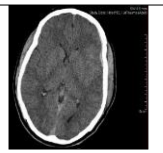
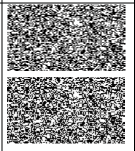
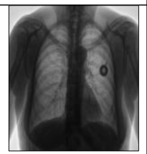
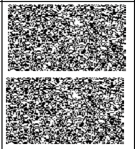
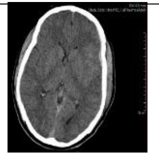
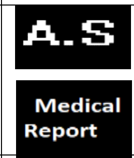
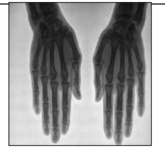
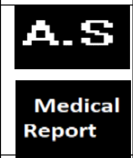
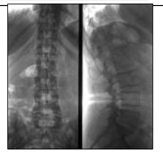
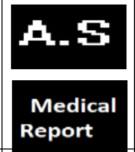
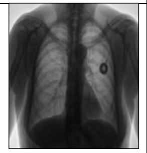
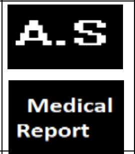
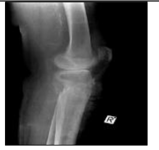
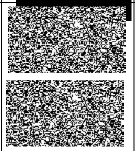
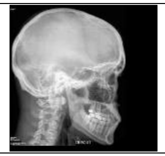
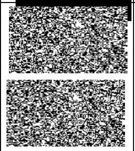
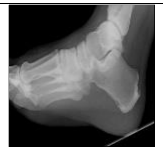
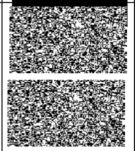
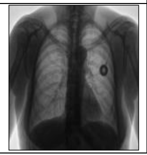
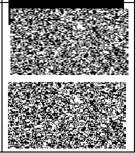
Attacks abbreviation	Attacks names
Sp	Salt & Pepper noise
Gn	Gaussian noise
Sn	Speckle noise
Af	Average Filtering
Mf	Median Filtering

DJL	DICOM JPEG Compression Lossless
DJLY	DICOM JPEG Compression Lossy
DR	DICOM RLE Compression
DJ2L	DICOM JPEG 2000 compression Lossless
DJ2LY	DICOM JPEG 2000 compression Lossy
Rt	Rotation
Gc	Gamma correction
Sc	Scaling
Tr	Translation
Sh	Shearing
Dt	Dithering
Cr	Cropping
WF	Wiener Filtering
HE	Histogram Equalization
RML	Remove Line
RNDDIST	Random Distortion
JPEG-Crop	JPEG Compression combined with cropping

Table 4.9 the attacked watermarked images and the correspondent extracted watermark.

Attacks	Attacked watermarked Img	Extracted watermark	Attacked watermarked Img	Extracted watermark	Attacked watermarked Img	Extracted watermark	Attacked Watermarked Img	Extracted watermark
Sp v=0.01								
Sp v=0.05								
Sp v=0.1								
Gn v=0.001								

Sn v=0.0001								
Sn v=0.001								
A f [2,2]								
Mf [2,2]								
DJL								
DJLY QF=50								
DR								
DJ2L								
DJ2LY QF=5								
Rt 0.1°								
Rt 1°								
Gc γ=0.95								

Gc γ=0.9								
Sc (1,1)								
Sc (2,2)								
Tr (2)								
Sh								
Dt								
Cr 1%								
Cr 10%								
WF [2,2]								
HE								
RML 2								
RNDDIST								

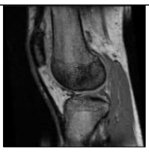
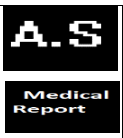
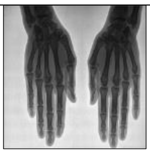
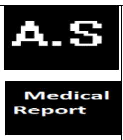
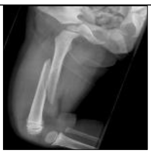
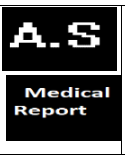
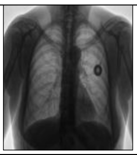
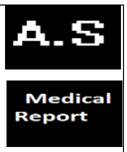
JC (50,1%)								

Table 4.10 The NC and BER values of the extracted watermark from different images.

	Knee		**Hands**		**Spine**		**Chest**		**Baboon**	
Attacks	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Sp v=0.01	**0.980**	**0.002**	**0.99**	**0.001**	**0.99**	**0.002**	**0.98**	**0.002**	**0.95**	**0.009**
Sp v=0.05	**0.930**	**0.008**	**0.93**	**0.008**	**0.93**	**0.008**	**0.92**	**0.009**	**0.88**	**0.014**
Sp v=0.1	**0.850**	**0.160**	**0.85**	**0.15**	**0.86**	**0.150**	**0.84**	**0.170**	**0.81**	**0.240**
Gn v=0.001	0.520	0.460	0.52	0.5	0.5	0.500	0.49	0.490	0.44	0.500
Sn v=0.0001	0.690	0.280	0.69	0.28	0.68	0.270	0.67	0.290	0.60	0.350
Sn v=0.001	0.540	0.500	0.56	0.43	0.56	0.420	0.58	0.450	0.50	0.500
Af [2,2]	0.530	0.490	0.53	0.49	0.52	0.490	0.52	0.490	0.50	0.500
Mf [2,2]	0.540	0.464	0.54	0.45	0.54	0.460	0.54	0.460	0.50	0.500
DJL	**1.000**	**0.000**	**1.00**	**0.000**	**1.00**	**0.000**	**1.00**	**0.000**	**0.88**	**0.011**
DJLY QF=50	**1.000**	**0.000**	**1.00**	**0.001**	**1.00**	**0.000**	**0.99**	**0.000**	**0.91**	**0.007**
DR	**1.000**	**0.000**	**1.00**	**0.000**	**1.00**	**0.00**	**1.00**	**0.000**	**0.81**	**0.019**
DJ2L	**1.000**	**0.000**	**1.00**	**0.000**	**0.99**	**0.000**	**1.00**	**0.000**	**0.81**	**0.019**
DJ2LY QF=50	**0.850**	**0.090**	**0.88**	**0.030**	**0.92**	**0.040**	**0.88**	**0.110**	**0.68**	**0.250**
Rt 0.1°	**0.890**	**0.070**	**0.51**	**0.500**	**0.65**	**0.370**	**0.70**	**0.320**	0.60	0.500
Rt 1°	0.550	0.460	0.48	0.500	0.63	0.400	0.61	0.410	0.50	0.700
Gc γ=0.95	**0.760**	**0.220**	**0.77**	**0.200**	**0.77**	**0.200**	**0.72**	**0.290**	0.60	0.500
Gc γ=0.9	0.530	0.330	0.51	0.500	0.53	0.350	0.53	0.300	0.50	0.510
Sc (1,1)	0.580	0.390	0.6	0.390	0.62	0.350	0.58	0.270	0.50	0.540
Sc (2,2)	0.510	0.470	0.51	0.470	0.51	0.480	0.55	0.300	0.50	0.660
Tr (2)	0.680	0.210	0.55	0.530	0.55	0.520	0.52	0.500	0.50	0.740
Sh	0.510	0.490	0.49	0.500	0.49	0.480	0.50	0.480	0.50	0.530
Dt	0.530	0.450	0.52	0.440	0.52	0.450	0.50	0.460	0.50	0.610
Cr 1%	**0.990**	**0.002**	**0.97**	**0.003**	**0.99**	**0.001**	**0.71**	**0.160**	0.60	0.460
Cr 10%	0.590	0.390	0.59	0.400	0.58	0.390	0.56	0.430	0.50	0.520
WF [2,2]	0.530	0.490	0.53	0.490	0.52	0.490	0.52	0.490	0.50	0.500
HE	0.530	0.330	0.51	0.500	0.53	0.350	0.53	0.300	0.50	0.510

RML2	**0.930**	**0.008**	**0.93**	**0.008**	**0.93**	**0.008**	**0.92**	**0.009**	**0.88**	**0.014**
RNDDIST	0.500	0.490	0.49	0.490	0.50	0.490	0.50	0.490	0.50	0.500
JC(50, 1%)	**0.970**	**0.003**	**0.97**	**0.003**	**0.98**	**0.003**	**0.96**	**0.004**	0.60	0.460

We can notice that the proposed technique presents high robustness against some attacks such: DICOM JPEG compression lossless, DICOM JPEG compression lossy, DICOM JPEG2000 compression lossless, DICOM JPEG2000 compression lossy and salt & pepper noise attacks. This is proved through the good NC and lowest BER values of the extracted watermarks from the attacked watermarked images. Table 4.11 shows the comparison results with some methods presented in [64, 81] in terms of robustness with salt & pepper noise (Sp) attack with different noise density using NC values.

Table 4.11 NC values comparison on different variances between works in [64, 81] and the proposed model for the extracted watermark image after salt & pepper noise attack (Sp).

	Attacks					
Methods	**Sp v=0.001**	**Sp v=0.005**	**Sp v=0.007**	**Sp v=0.01**	**Sp v=0.02**	**Sp v=0.05**
Thakkar et al [81]	-	0.98	0.95	0.88	0.73	-
Singh et al [64]	0.98	-	-	0.76	-	0.61
Proposed	**1**	**1**	**1**	**0.98**	**0.95**	**0.93**

Table 4.12 Show the comparison results with Hernandez et al [84] technique in terms of robustness after DICOM JPEG Compression lossy attack using NC values.

Table 4.12 NC values comparison between Hernandez et al [84] and the proposed scheme for the extracted watermark image after DICOM JPEG Compression lossy attack.

Attacks	**Hernandez et al [84]**	**Proposed scheme**
DJLY (QF=50)	Under 0.98	1

- *Comparison on Extraction mode, Watermark Security and Computational Complexity*

We present a comparison with some recent works described in [35,64, 80-82] in terms of extraction mode, watermark security and computational complexity which are illustrated in Table 4.13.

Table 4.13 Features comparison between works in [35, 64, 80-82] and the proposed method.

methods	Extraction Mode	Watermark Security	Computational complexity
[35]	Non-Blind	No	High
[64]	Blind	Yes	High
[80]	Non-Blind	Yes	High
[81]	Blind	No	High
[82]	Blind	No	Median
Proposed	Blind	Yes	Median

According to experimental results of Table 4.13, the proposed method is more effective and practical rather than other compared techniques. The reasons is that it's blind where in the proposed model the host image blocks and watermark are encrypted. This offers more security contrarily to works presented in [35, 81, 82] where the watermark is embedded without encryption. Finally, the computational complexity required by the proposed method is on average, while it became high in works presented in [35, 64, 80,81].

4.3 Synthesis and discussions

The main objective of the presented blind semi-fragile watermarking methods is to keep high quality watermarked images. The first proposed technique is a blind method that leverages from the good features of the DWT coefficients. Experimental results showed that our proposal method provides high imperceptibility, security and good robustness with attacks of low densities. Furthermore, this method suffers from the important computational complexity, and it's vulnerable against many geometric and signal processing attacks of high densities. For this purpose, we proposed another semi-fragile method as an enhancement for the first one. It ensures the integrity of medical data by preserving the medical image quality. The presented technique preserves a high-quality image (i.e. proved by highest PSNR values when watermark image is in its maximal size (128x128)). However, it also suffers from the high computational (i.e. the computational complexity is on average time (4.5s) in the embedding process and (4s) in the extracting process). Unfortunately, it cannot be applied for real-time e-Health applications due to time constraint.

4.4 Conclusion

In this chapter, we present our contributions in the semi-fragile medical image watermarking field in transform domain. The first method proposed is an efficient blind watermarking technique to ensure the security of medical images transmitted through an untrusted channel. This technique combined the DWT and Schur Decomposition, and it’s used to hide and extract the watermark using a medical image in DICOM format as a cover image. The second contribution presented is a blind approach based on Schur decomposition and chaotic sequence; that enables more embedding capacity by keeping good imperceptibility. Moreover, the proposed method is more imperceptible, secure and efficient compared to some related methods. However, it still needs to be improved in future works in terms of computational complexity.

In the next chapter, we will present our contributions based on fragile watermarking method.

Chapter 5

Fragile Medical Image Watermarking Techniques

Content

5.1 Introduction………………………………………………...…..…………………..96
5.2 Proposed Fragile Medical Image Watermarking Methods…….….…...……….96
  5.2.1 A NOVEL WATERMARKING FOR MEDICAL IMAGES AUTHENTICATION 96
    5.2.1.1 Speed Up Robust Features (SURF) Descriptor And Detector……….…..…96
    5.2.1.2 Watermark Embedding And Extracting Processes………………..……..……97
    5.2.1.3 Experimental And Performance Results…………………………..………..102
  5.2.2 A BLIND FRAGILE BASED MEDICAL IMAGE AUTHENTICATION....………..…......105
    5.2.2.1 Watermark Embedding Phase……………………………………..……....106
    5.2.2.2 Watermark Extraction Phase………………………………………….………107
    5.2.2.3 Experimental Results……………………………………………………….....108
5.3 Synthesis And Discussions…………………………………..…………………111
5.4 Conclusion…………………………………………………...……….……..111

5.1 Introduction

Digital multimedia security has become one of the most crucial issues in most health applications. It contains sensitive data such digital radiography and patient's private information. Therefore, threats on such data may put medical applications holding these digital images at high serious risk. The main aspects that should be considered while protecting health data are image authentication and image tamper identification and localization. To cope with this problem, the fragile image watermarking has recently been proposed. It is an effective and powerful solution in multimedia security, especially when it comes to image tamper identification and authenticity.

In this chapter, the proposed blind fragile watermarking techniques are presented for image authentication and tamper identification. These solutions aim at meeting computational complexity and imperceptibility constraints. The rest of the chapter is organized as follows; Section 2 introduces a blind fragile approach for medical images authentication based on SURF points and Weber Descriptors. Performance analysis and discussions are expatiated in section 3. Finally, conclusions and future works are given in section 4.

5.2 Proposed fragile medical image watermarking methods

We present two fragile methods in spatial domain for image authentication and tamper identification. The first method is a blind fragile watermarking-based for medical images authentication based on SURF descriptor combined with Weber Descriptors (WDs) and Arnold scrambling. The second method is also blind method, but it embeds the watermark in the frequency domain where Schur decomposition coefficients are used basically for that purpose.

5.2.1 A Novel Blind Fragile Watermarking-based for Medical Images Authentication

A blind, fast and secure fragile-based watermarking algorithm in spatial domain for medical images authentication is presented in this section. It's based on SURF descriptor combined with WDs and Arnold scrambling.

5.2.1.1 Speed Up Robust Features (SURF) descriptor and detector

SURF is a fast technique for detection and description of interest points. It is based on the integral images and the convolution operation combined with the Hessian matrix [85].

Hessian matrix is used for determining the location and scale of the point. Hessian matrix H(x, σ) for a point X (x, y) is computed as follows:

$$H(x,\sigma)=\begin{bmatrix} L_{xx}(x,\sigma) & L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma) \end{bmatrix} \tag{5.1}$$

Where σ is the scale of X, $L_{xx}(x,\sigma)$ is the convolution of the Gaussian second order derivative of the image I in point x.

In order to localize interest points in the image, the non-maximum suppression in a neighborhood of 3x3x3 is applied. Next, the found maxima of the determinant of the Hessian matrix are interpolated in scale and image space. The interest points detected by SURF are characterized by their fast computing capacity and good recovery characteristic. A more detailed description of the SURF interest point's extraction can be found in **[85].**

5.2.1.2 Watermark embedding and extracting Processes

This section presents a new watermarking method using SURF points combined with the well-known Weber Descriptors (WDs) and Arnold scrambling. This method seems to be more interesting for reducing the computational complexity without affecting the image quality. In fact, the proposed watermarking framework consists of two processes: the watermark embedding and the watermark extraction (Figure 5.1 and Figure 5.4).

- *Watermark embedding Process*

The used medical images are in grayscale of size 256 × 256. The medical image embedding process is achieved on two main phases, ***preprocessing phase*** and ***embedding phase***. Figure 5.1 illustrates the watermark embedding process.

a. Preprocessing phase

The preprocessing phase is a 4-steps process:

Step .1 Select the Region Of Interest (ROI) from the entire medical image. The reason is that the embedding in Region Of Non-Interest (RONI) offers low security to the watermark [39]; where an attacker could remove the RONI of the watermarked image and put his own RONI which contain another watermark.

Step .2 The SURF Descriptors is applied on the selected ROI to extract the interest points.

Step .3 The 3x3 non-overlapping blocks around each interest point are selected as an embedding area. Each block embeds two watermark intensities (*e.g. two bits*).

Step .4: The Arnold chaotic map is applied to scramble the binary watermark image in order to secure the watermark.

b. Processing phase

This step consists of embedding a binary watermark and generates an authentication key which will be used in data's integrity. Since, using a binary watermark image reduces the computational complexity and offers more embedding capacity (the pixel intensity could take two bits values 0 for black and 1 for white intensities). The processing phase is achieved as the following steps (Figure 5.2).

Step .5 Select a block B_i and compute the orientations (λ1, λ2) as follows:

$$\begin{cases} \lambda 1(B_i) = \text{Arctan}\left|\dfrac{i2-i7}{i5-i4}\right| \\ \lambda 2(B_i) = \text{Arctan}\left|\dfrac{i3-i6}{i8-i1}\right| \end{cases} \tag{5.2}$$

Where i1 to i8 are pixels intensities of the block B_i (see Figure 5.3).

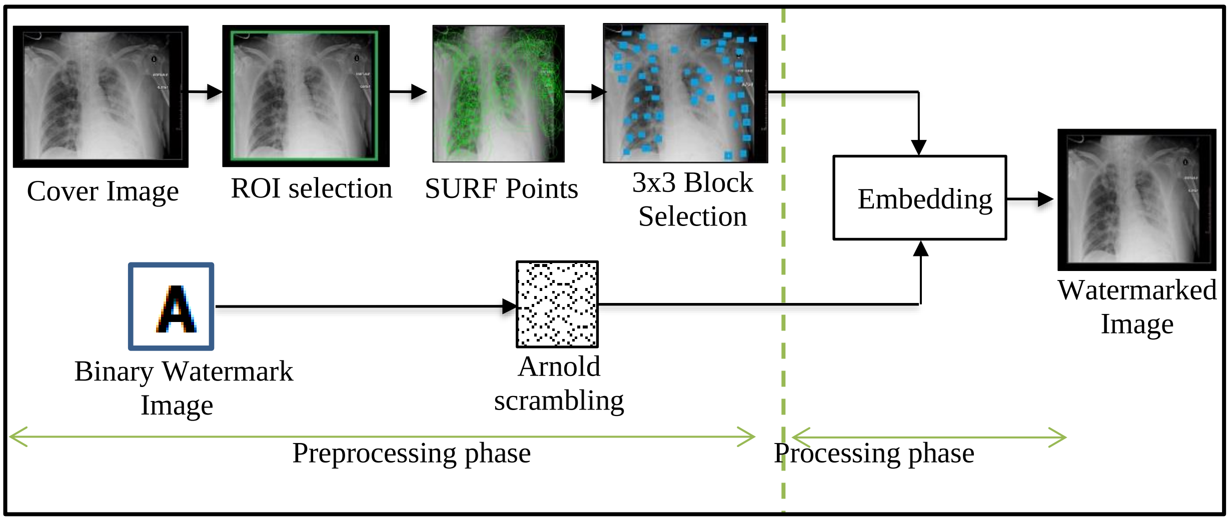


Figure 5.1 Watermark embedding process.

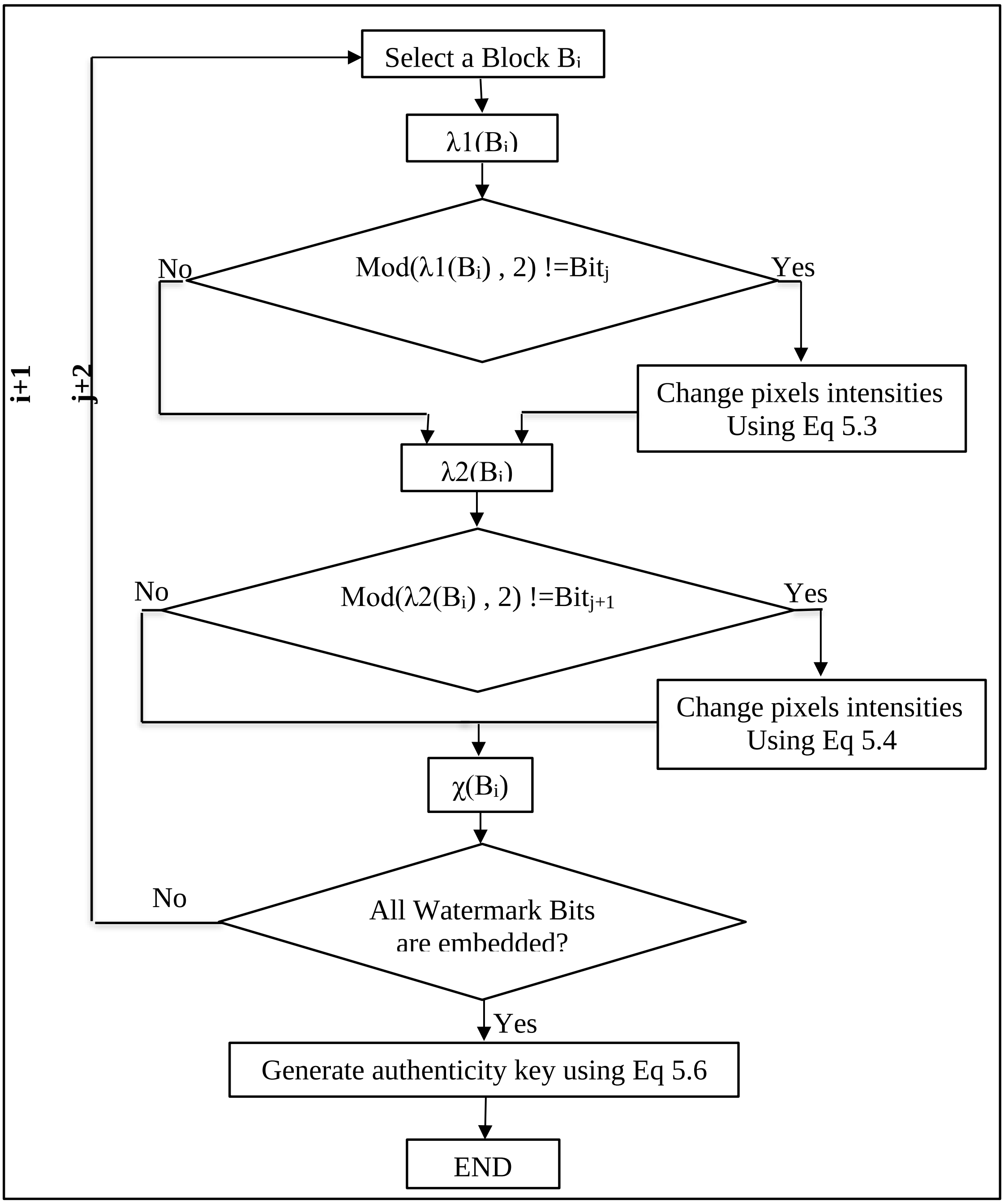

Select a Block Bi
λ1(Bi)
Mod(λ1(Bi) , 2) !=Bitj
No
Yes
Change pixels intensities Using Eq 5.3
i+1
j+2
λ2(Bi)
Mod(λ2(Bi) , 2) !=Bitj+1
No
Yes
Change pixels intensities Using Eq 5.4
χ(Bi)
All Watermark Bits are embedded?
No
Yes
Generate authenticity key using Eq 5.6
END

Figure 5.2 Watermark Bits embedding phase.

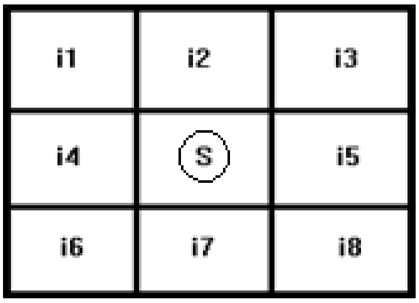


Figure 5.3 3x3 Block illustration.

Step .6 Select two watermark intensities (Bit_j and Bit_{j+1}) from the scrambled binary watermark and embed it on the block B_i according the the following cases:

1. If mod (λ1(B_i), 2) ~= Bit_j , in this case the values of i2, i4, i5, i7 are modified as follows:

$$\begin{cases} i2 = i7, \quad if \quad Bit_j == 0 \\ i2 = i7 + 1, \quad i5 = i4 + 1, \quad Otherwise \end{cases} \tag{5.3}$$

2. If mod (λ2(B_i) , 2) ~= Bit_{j+1} , in this case the values of i1, i3, i6, i8 are modified as follow:

$$\begin{cases} i3 = i6, \quad if \quad Bit_{j+1} == 0 \\ i3 = i6 + 1, \quad i8 = i1 + 1, \quad Otherwise \end{cases} \tag{5.4}$$

Step .7 Compute the block Excitation χ (B_i) of the new intensities values using the following equation:

$$\chi(B_i) = A\text{rctan}(\sum_{k=0}^{8} \frac{i(k) - S}{S}) \tag{5.5}$$

where the i(k) are the neighbors of the SURF point “S” (Fig 5.3).

Step .8 If other watermark bits are needed to be embedded go back to **Step .5** with i=i+1 and j=j+2, else go to step. 9.

Step .9 Compute the authenticity key (AK) using Eq 5.6. The AK is emitted to the receiver side to check if the watermarked image is tampered or not.

$$AK = \sum_{i=1}^{n} \chi(B_i) \tag{5.6}$$

- *Watermark extracting process*

The watermark embedding process is shown in Figure 5.4. The proposed method is blind, meaning that the extraction process doesn’t require any of the original image or original watermark. As and like embedding process, the extracting process consists of two phases, **preprocessing phase** and **extracting phase**.

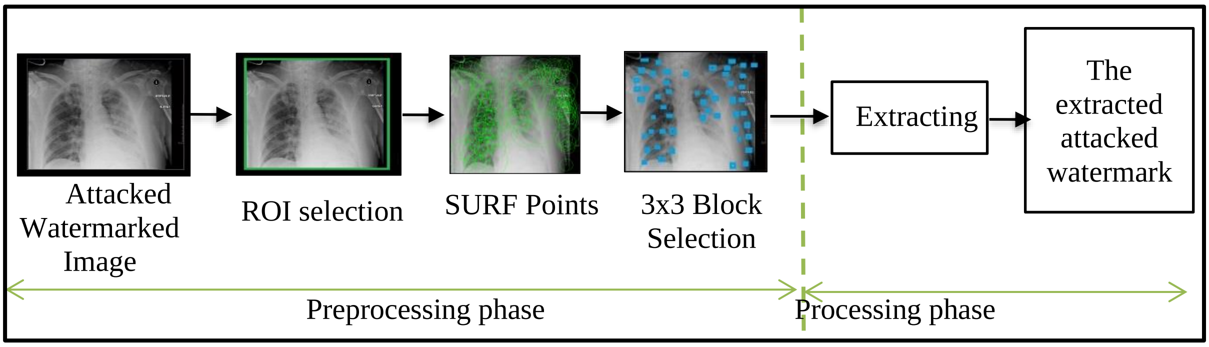


Figure 5.4 Watermark extraction process.

a. Preprocessing phase

The preprocessing phase is achieved as the following steps:

Step .1 Select the ROI from the entire medical image.

Step .2 Apply the SURF Descriptors on the selected ROI to extract interest points.

Step .3 Select the 3x3 non-overlapping blocks around each interest point.

b. Processing phase

Figure 5.5 illustrates the processing phase of the watermark embedding process. It consists to the following steps:

Step .4 Select a block B_i and compute the orientations (λ1, λ2) using **Eq 5.2**.

Step .5 Extract tow bits (Bit_j and Bit_{j+1}) of the scrambled binary watermark as follows:

$$\begin{cases} Bit_j = \mathrm{mod}(\lambda 1, 2) \\ Bit_{j+1} = \mathrm{mod}(\lambda 2, 2) \end{cases} \qquad (5.7)$$

Step .6 Compute $\chi(B_i)$ using **Eq 5.5**.

Step .7 If all the watermark bits are extracted go to **Step 8** else go back to **Step 4** with i=i+1 and j=j+2.

Step .8 Perform the inverse of Arnold scrambling on the extracted watermark to get the original watermark.

Step .9 Compute the Authenticity Key (AK) using Eq 5.6.

Step .10 Checks if the AK computed in the extraction process is equal to the AK computed in the embedding process the image is authorized, else it’s unauthorized.

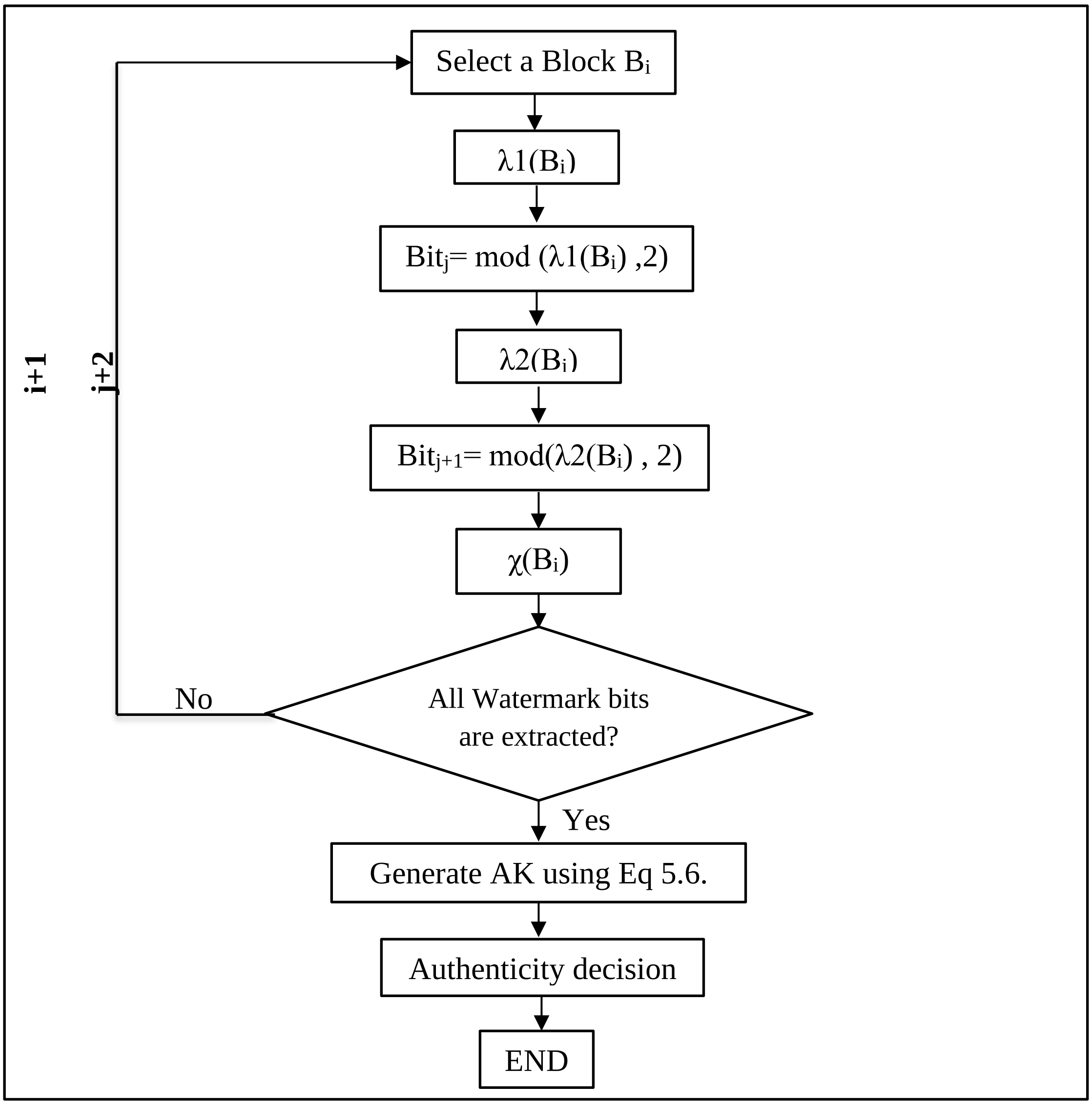


Figure 5.5 Watermark Bits extracting phase.

5.2.1.3 Experimental and performance results

The proposed approach is implemented using the programing language MATLAB. The presented technique improves outcomes and provides helpful for authenticity and integrity in different medical images. We performed our tests on a gray scale medical image of size 256x256 with binary watermark image of size 16x16 where each pixel could take two values 0 or 255 and expressed with 1 bit (*0 for black and 1 for white intensities*). Most of performed experiments use the Peak Signal to Noise Ratio (PSNR) as a metric for imperceptibility evaluation. Figure 5.6 shows the cover images and the watermark used in the experimentation. The tested radiology database is from [**66**].

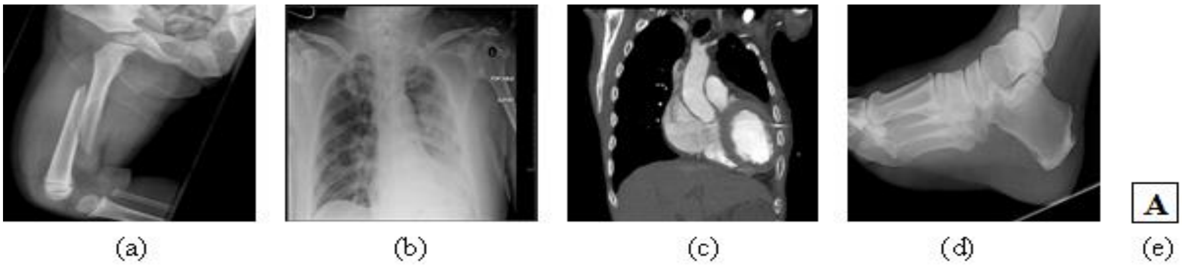


Figure 5.6 (a)-(d) Medical cover image (e) Watermark image.

- *Imperceptibility measurement*

To evaluate the imperceptibility of the proposed method, we measured PSNR (Peak Signal to Noise Ratio). Table 5.1 shows the PSNR values between the original image and the watermarked one. It's clear that the proposed method preserves the quality of the watermarked image compared to the original one. This proposed method can be applied with only slight modification of pixels intensities to embed the binary watermark.

Table 5.1 PSNR values between the original and the watermarked images.

Images	(a)	(b)	(c)	(d)
PSNR (dB)	60.838	61.554	61.099	60.801

- *Computational complexity measurement*

The computational complexity is the execution time needed for embedding and extracting the watermark. Table 5.2 shows the execution time to embed and extract the watermark binary image. The evaluations are performed on DELL LATITUDE E5410 Laptop/Intel core i5 2.67 GHz, 4.0GB RAM. It's obvious that the proposed method ensures fast execution times *(doesn't exceed 1 second for the embedding and extracting processes*). This is due to employ a fast technique to embed and extract the watermark binary image as explained in the proposed system model.

Table 5.2 Time required for embedding and extracting the watermark.

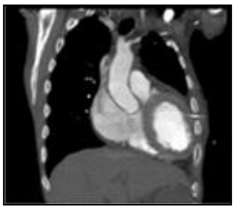
Images	Embedding time (second)	Extracting time (second)
(a)	0.9788	0.6014
(b)	0.9974	0.8124
(c)	0.9481	0.5282
(d)	0.9832	0.6487

- *Authenticity verification*

To prove the efficiency of the proposed technique, we measured the tamper detection precision. The Authentication key (AK) values generated in the embedding process are compared with the AK in the extraction process after minor alteration.

Table 5.3 shows the results of comparison grouped by image type, tamper type and AK in both embedding and in extracting phases that could be compared. We can notice that even the slightest alteration is detectable which prove an accurate and good performance of the proposed technique. Performance refers to alter detection precision.

Table 5.3 Tamper detection precision of our technique.

Images	AK in embedding	Tamper type	AK in extracting
	45.002	Salt & pepper noise V=0.001	63.4349
		White noise V=0.001	210.9638
		JPEG Compression QF=99	557.1027
		Rotation 1°	142.125
	202.8337	Salt & pepper noise V=0.001	2.7169
		White noise V=0.001	2.3454
		JPEG Compression QF=99	1.7974
		Rotation 1°	2.188
	593.1301	Salt & pepper noise V=0.001	126.8699
		White noise V=0.001	247.8337
		JPEG Compression QF=99	628.6678
		Rotation 1°	362.9401
	416.5237	Salt & pepper noise V=0.001	63.4349
		White noise V=0.001	0.5434
		JPEG Compression QF=99	548.6202
		Rotation 1°	262.8750

- *Experimental comparison based on PSNR metric*

The performance of the proposed watermarking approach is evaluated by measuring PSNR, and compared with some other recent proposed methods. Table 5.4 shows the average imperceptibility PSNR value compared with other related work **[43, 86-90]**.

Table 5.4 Comparison of the PSNR between our method and works in [43, 86-90].

Approach's	PSNR (dB)
Approach in **[88]**	51.14
Approach in **[87]**	43.58
Approach in **[89]**	45.69
Approach in **[43]**	<47
Approach in **[86]**	<34
Approach in **[90]**	<60
Proposed approach	**60.323**

5.2.2 A blind fragile based medical image authentication using Schur Decomposition

In this section we propose a new blind fragile watermarking method using Schur decomposition. Indeed, perturbation due to watermark embedding is reduced using Schur decomposition, which can be considered in designing a watermarking approach to enhance imperceptibility and computational complexity. The main idea is to embed the watermark in the Schur decomposition coefficients of the host image using a new embedding technique.

The proposed approach includes two main phases: embedding and extracting. The general structure of the proposed approach is illustrated in Figure 5.7.

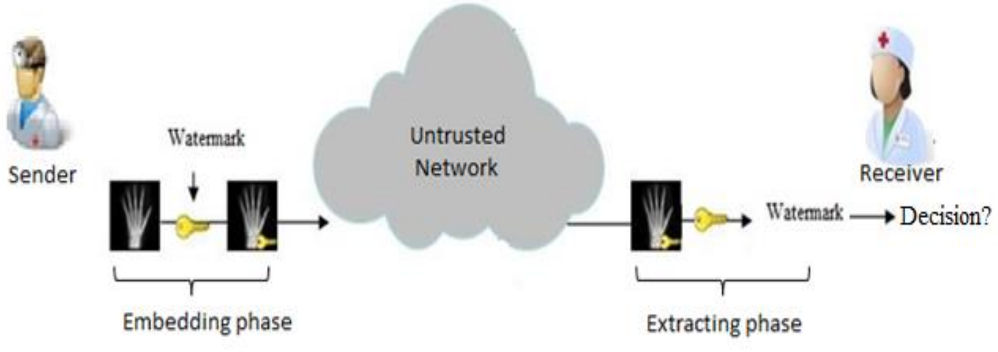


Figure 5.7 Generic model for the proposed method.

5.2.2.1 Watermark embedding phase

The watermark embedding phase is illustrated in Figure 5.8 and detailed below.

Step 1. Apply Schur decomposition on the cover image I:

$$\text{Schur (I)=[U, V]} \qquad (5.8)$$

The reason behind choosing Schur decomposition for watermark embedding is that the perturbation which may result from data embedding in the host image could be reduced when data is embedded in Matrix V. This could improve the imperceptibility significantly.

Step 2. Decompose the V matrix into 2x2 non-overlapping blocks.

Step 3. Select a block's coefficients (BC_i) and compute its weight (Weight (BC_i)) using Equation (2) where I is the block number.

$$\text{Weight } (BC_i) = \sum_{k=1}^{2} \sum_{m=1}^{2} (BCi(k,m) * (-1)^{(k+m+i) mod 2}) \qquad (5.9)$$

Step 4. Select a watermark Bit (WB_i) from the scrambled watermark bits after performing Arnold chaotic map and embed it in BC_i using the following case:

If WB ~= Weight (BC_i) mod 2

Min(BC_i(1,2), BC_i(2,1))= Min(BC_i(1,2), BC_i(2,1))+1 mod S.

Where S is 2^8 for the JPEG format and 2^{16} for the DICOM format.

Note that adding 1 to minimum (BC_i (1,2) , BC_i (2,1)) modifies (increments or decrements) one pixel intensity from the 2x2 block pixel intensities (see Figure 5.9), which could improve the imperceptibility.

Else:

Go to Step 5.

Step 5. If not all the watermark bits are embedded go back to step 3 with i+1 Else go to step 6.

Step 6. Apply Schur^{-1} to obtain the watermarked image.

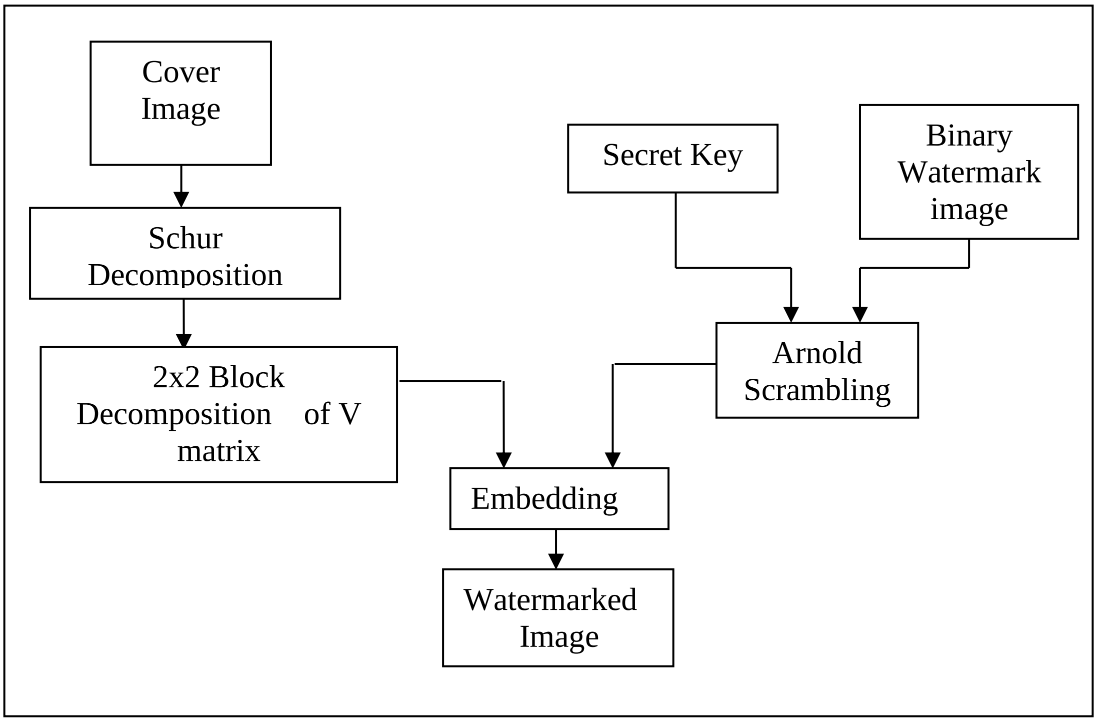


Figure 5.8 Watermark embedding main steps.

5.2.2.2 Watermark extraction phase

The watermark extraction phase is illustrated in Figure 5.10 and detailed below.

Step 1. Apply Schur decomposition on the cover image using Equation (5.8).

Step 2. Decompose the V matrix into 2x2 non-overlapping blocks.

Step 3. Select a block's coefficients (BC_i) and compute its weight using Equation (5.9).

Step 4. Extract a watermark Bit (WB_i) using the following case:

```
If Weight ($BC_i$) mod 2 == 1
        $WB_i$=1
Else
        $WB_i$=0.
```

Step 5. If not all the watermark bits are extracted go back to Step 3 with i+1 Else go to Step 6.

Step 6. Decrypt the extracted encrypted watermark bits, and compare them with the original watermark bits, then decide if the image is authorized.

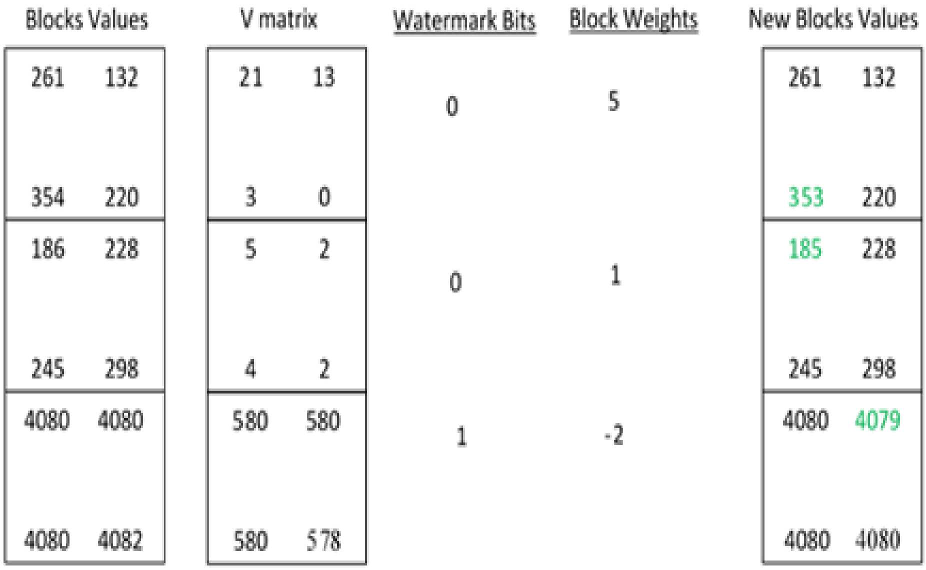


Figure 5.9 Example of new blocks pixel intensities after embedding of bits.

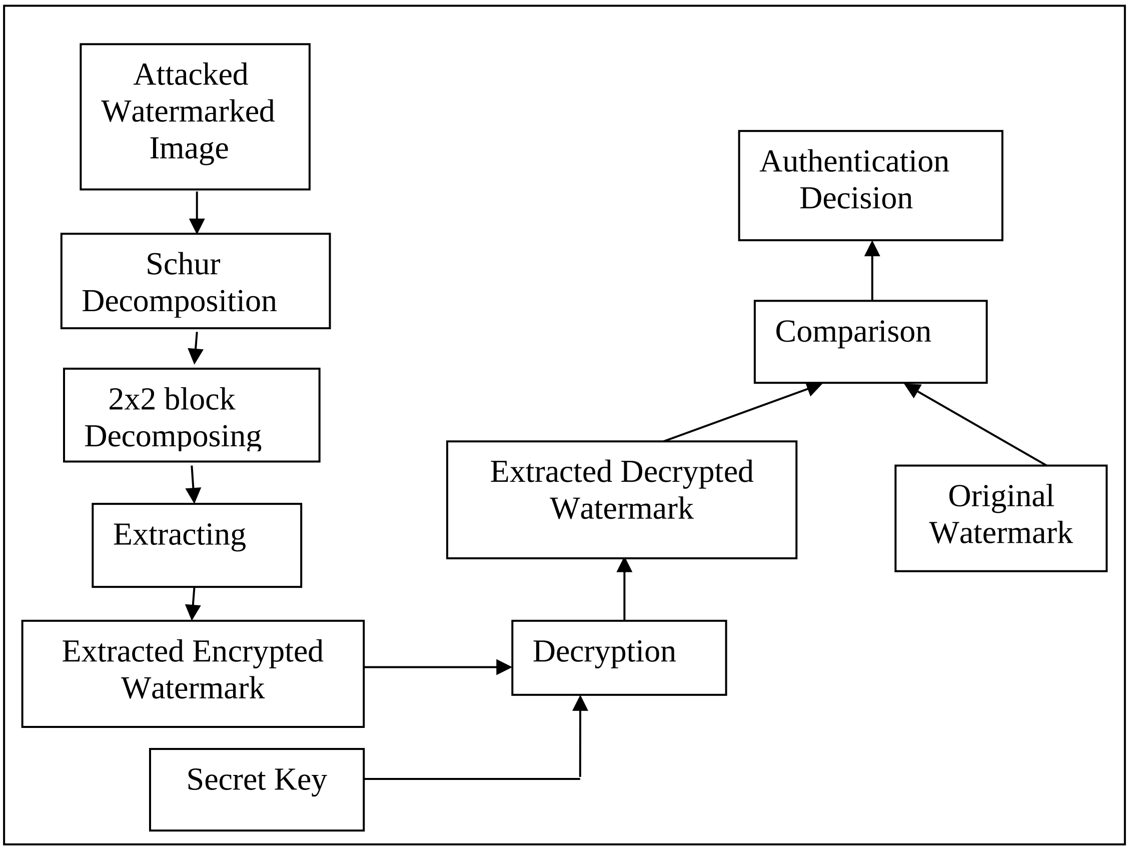


Figure 5.10 Watermark extracting main steps.

5.2.2.3 Experimental results

In order to measure the performance of the proposed technique in terms of imperceptibility and computational complexity, a data set of DICOM images of size 256x256 are used (from [78, 79]), while the watermark image is of size 32x32.

Figure 5.11 shows the binary watermark image used in the experimentation, while Figure 5.12 show a sample of medical images used in the experimentation.

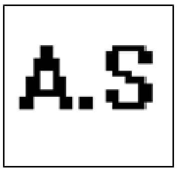


Figure 5.11 Watermark image used in the experimentation.

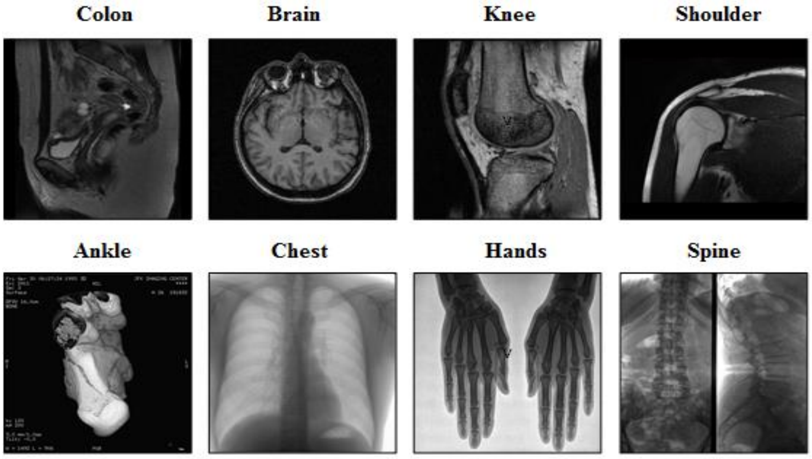


Figure 5.12 Sample of image used in the experimentation.

Table 5.5 shows the imperceptibility degree in terms of PSNR. The PSNR average value of all dataset images is around 54 dB.

Table 5.5 Imperceptibility evaluation of the proposed watermarking method.

Images	**Colon**	**Knee**	**Hands**	**Spine**	**Brain**	**Shoulder**	**Ankle**	**Chest**
PSNR(dB)	53.67	54.96	57.01	57.03	54.02	53.09	54.12	57.03

Figure 5.13 show a comparison of the results obtained with the approaches described in [91-93, 87, 92, 89] and our proposed approach in terms of PSNR (dB).

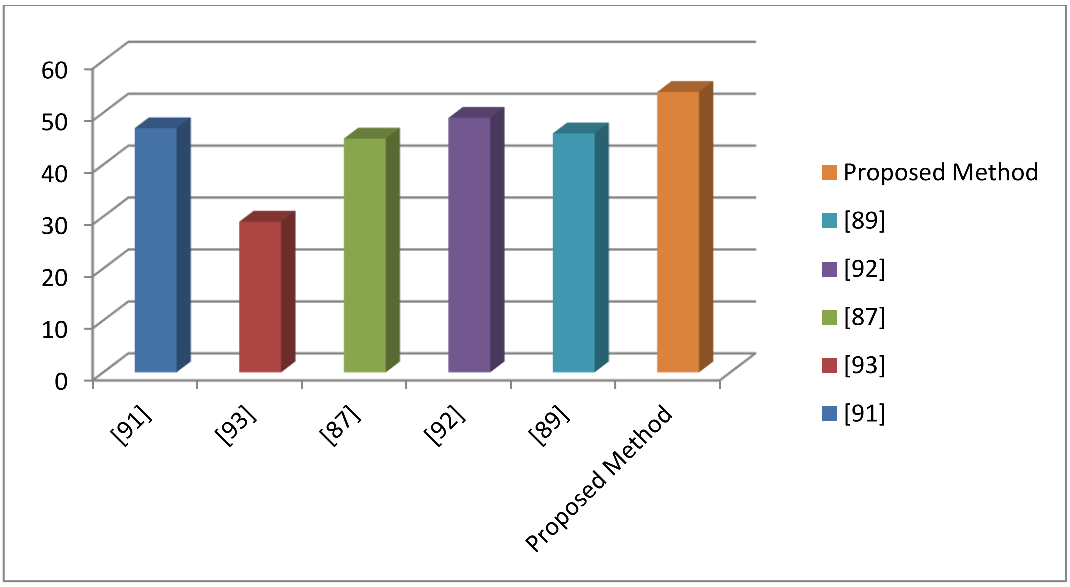


Figure 5.13 Imperceptibility comparison between our proposed technique and methods described in [87, 89, 91-93].

Table 5.6 show the execution time needed to embed and extract the watermark in different medical images.

Table 5.6 execution time measurement.

images	Colon	Knee	Hands	Spine	Brain	Shoulder	Ankle	Chest
Embedding time (seconds)	2.99	2.99	3.48	3.22	3.04	2.96	3.08	3.49
Extracting time (seconds)	2.04	2.05	2.56	2.22	2.19	2.11	2.14	2.59

Clearly, our proposed method yields better imperceptibility. The reason is that the embedding of a watermark DCT coefficient necessitates a small change in the Schur DCT coefficients of the cover image blocks (Figure 5.9). Consequently, the watermarked images keep a good imperceptibility compared to the original ones. This is proved by results described in Table 5.5 and Figure 5.13.

It is also noticed that the computational complexity for the proposed method is acceptable (i.e., about 3 seconds for embedding and 2 seconds for extracting). Such results are obtained on a workstation with the following specifications: DELL LATITUDE E5410 Laptop/Intel core i5 2.67 GHz, 4 GB using MATLAB.

However, the major drawback of the proposed method is the mediocre embedding capacity (a watermark bit is embedded in a block of size 2 × 2, which means a binary watermark of size

N × N necessitates at least a cover medical image of size 2N × 2N). This must be enhanced in future researches.

5.3 Synthesis and discussions

The main objective of the first presented method is to achieve an efficient medical images integrity using SURF Descriptors, WDs and Arnold chaotic map in the spatial domain. We performed the experiments for blind fragile watermarking-based technique and other similar related work for different medical images. As shown in Table 5.1, Table 5.2 and Table 5.3, our technique provides a remarkable imperceptibility, high security level and low computational complexity compared to other recent fragile methods. Moreover, the proposed method achieves good medical image authenticity in terms of identification time (Table 5.4), an efficient tamper identification and localization. This result confirms that by changing a single pixel of the watermarked image. The watermarked image is considered as unauthorized. However, the proposed method offers low embedding capacity, to solving that problem, we propose another fragile blind watermarking method, based on Schur decomposition, that’s gives better embedding capacity and imperceptibility than the first method, however, it require high computational complexity than the first one. To this end, the future researches will focus on developing a technique that can combines the advantages of the two proposed techniques and fell their gaps.

5.4 Conclusion

In this chapter, we present our contributions in fragile medical image watermarking field. For ensuring the integrity and tamper identification. The first technique combines Surf Descriptors, WDs and Arnold chaotic map in the spatial domain. Experimental results on different medical images prove a remarkable imperceptibility, high-level security, low computational complexity compared to other recent fragile/semi-fragile methods and good medical image authenticity. However, the proposed method offers low embedding capacity and still need to be improved in future works. The second technique use Schur Coefficients as an embedding area, it gives better embedding capacity and imperceptibility than the first method, however, it require high computational complexity than the first one. To this end, future works will focus on how benefits from the two method advantages.

General Conclusion

Most of the existing watermarking technique suffer in finding a consensus between the watermarking requirements such robustness Imperceptibility and security. By robustness, we designate a strong visual similarity between the original watermark and the extracted one after being attacked. Imperceptibility means that the watermark should not significantly change the host image and should be invisible. While the security should guarantee the image protection against any kind of attempted modification.

The work presented in this thesis consists in proposing new secure watermarking approaches that provides good robustness (for the robust methods) by keeping good quality of the watermarked image. To this end, we have proposed several watermarking techniques around three main categories: robust, semi-fragile and fragile watermarking.

WORK INTERESTS

The work interests in this thesis are summarized as follows:

1. Developing new watermarking techniques for medical images that offers significant security for the watermark by keeping good image quality.
2. Supporting telemedicine applications in order to implement an effective system for sharing and using medical data in a secured manner.

CONCLUSION

The works presented in this thesis was mainly situated around many objectives such imperceptibility, robustness, semi-fragility, and fragility, embedding capacity and computational complexity. Our mainly goal is to ensure and guarantee the security parameters of medical data by verifying the reliability during the transmission. The proposed solutions are not only to protect medical secret information’s from malicious operations but also used to verify the integrity of images and authenticating the transmitted medical image across unsecured environments.

- The first axe concerns with proposing a new robust watermarking techniques for medical images:

  - A new blind medical images watermarking method based on DCT, Weber Descriptors and Arnold Chaotic Map has been proposed. The cover image is scrambled using Arnold chaotic map and transformed by DCT. The watermark is embedded in the DCT middle-band coefficients using weber law descriptor without any loss by selecting the right coefficients. The proposed method leads to a lower computational complexity, imperceptibility and robustness against various attacks. Moreover, this technique could extract the watermark in a blind manner, and this present a challenge in the watermarking systems.
  - Schur and DCT based medical images watermarking. The Schur method is used to embed the watermark efficiently, on the DCT coefficients. The proposed approach embeds the watermark in many blocks which, guarantee better performance in terms of robustness and embedding capacity than the first method. However, the computational complexity is much higher than the first method. Also, the extracting mode is semi-blind which make it less practicable.
- The second axe consists in proposing new semi-fragile medical images watermarking techniques:
  - A new semi-fragile method based on DWT (Discrete Wavelet Transform) and Schur Decomposition is proposed in order to guarantee the security and preserve quality of medical images. The cover images are watermarked with patient information. The host image is scrambled using chaotic map, then it’s embedded in DWT-Schur coefficients in a blind way. The performance of this method is not more sufficient when it comes to robustness and imperceptibility.
  - A novel blind medical image-watermarking scheme based on Schur Decomposition and Chaotic Sequence has been proposed. The proposed approach exploits the chaotic sequence to encrypt the watermark and embedded in Schur coefficients. This method gives good performance when it comes to imperceptibility, computational complexity, and robustness against some attacks. It is better than the first method.

- The third axe is interested in developing new fragile medical images watermarking techniques:
    - A novel blind fragile watermarking approach based medical images authentication has been proposed. This approach is fast and imperceptible and provide a significant contribution in images authentication. It based on SURF points and weber law descriptors, the method basically define the most robust block to embed the watermark in the area around SURF points. Moreover, this method could detect if the watermarked image is altered or not and consequently deciding about the medical image authorization.
    - A new blind based medical image authentication using Schur decomposition has been proposed. Indeed, perturbation due to watermark embedding is reduced using Schur decomposition, which gives high imperceptibility. The principle of this method is to perform the Schur decomposition coefficients of the host image, then decomposes up the V matrix into 2x2 non-overlapping blocks. Finally, each bit from the binary watermark is embedded in a block using a new embedding technique. The experiments results showed better imperceptibility than the first proposed method. However, it requires higher computational complexity than the first one.

Our contribution either in robust, semi-fragile or fragile are blind, except one which is semi blind. The blind methods are very interesting in e-Health applications. The main advantages of the proposed approaches compared to existing related works are: the less degradation on the watermarked image, as well as, less execution time for embedding and extraction processes, and remarkable robustness.

FUTURE WORKS

The work presented in this thesis has addressed various medical watermarking techniques regarding preserving medical image quality and image authentication through unsecured environment. To this end, some perspectives that seem to be relevant in future in order to improve its performance. These perspectives are:

- **Medical Image watermarking with tamper detection, locating and recovery**

In the medical image. There is a strong need for a watermarking technique which could detect the alteration and locate the tampered area, and then recover it. The reason is that the medical image is very sensitive and could even altered unintentionally (e.g. corrupted data packet through internet), to this end we attempt to use some intelligence techniques to find the most significant features for watermarking embedding, also the proposed work will contain mathematical validation (in terms of robustness) between the original watermark and the attacked one.

- **Watermarking methods for medical video.**

The new telemedicine applications generation use medical video in a large scale. To this end, it necessary to develop a new watermarking approach for video authentication, integrity, alter detection, ownership proofing and protection.

References

[1] A. Poljicak, "Discrete Fourier transform–based watermarking method with an optimal implementation radius", Journal of Electronic Imaging, vol. 20, no. 3, p. 033008, 2011.

[2] A. Khan, A. Siddiqa, S. Munib and S. Malik, "A recent survey of reversible watermarking techniques", Information Sciences, vol. 279, pp. 251-272, 2014.

[3] N. Agarwal, A. K. Singh, P. K. Singh, "Survey of robust and imperceptible watermarking", Multimedia Tools and Applications, pp. 1–31, 2019.

[4] M. Al-shaikh, "Protection des contenue des images médicales par camouflage d'information secrète pour l'aide à la télémédecine", PHD thesis, 2016.

[5] G. Çetinel and L. Çerkezi, "Robust Chaotic Digital Image Watermarking Scheme based on RDWT and SVD", International Journal of Image, Graphics and Signal Processing, vol. 8, no. 8, pp. 58-67, 2016.

[6] M. Islam and U. Chong, "A Digital Image Watermarking Algorithm Based on DWT DCT and SVD", International Journal of Computer and Communication Engineering, vol. 3, no. 5, pp. 356-360, 2014.

[7] V.S. Jabade, S.R. Gengaje, "Comprehensive Survey on Image Watermarking", International Journal of Advances in Engineering & Technology, Vol. 6, Issue 3, pp. 1271-1282, 2013.

[8] S. Dogan, T. Tuncer, E. Avci and A. Gulten, "A robust color image watermarking with Singular Value Decomposition method", Advances in Engineering Software, vol. 42, no. 6, pp. 336-346, 2011.

[9] H. Rahmani, R. Mortezaei and M. Ebrahimi Moghaddam, "A New Robust Watermarking Scheme to Increase Image Security", EURASIP Journal on Advances in Signal Processing, vol. 2010, no. 1, p. 428183, 2010.

[10] S. Jose, R. Cherian Roy and S. S Nambiar, "Robust Image Watermarking based on DCT-DWT-SVD Method", International Journal of Computer Applications, vol. 58, no. 21, pp. 12-16, 2012.

[11] H. Tao, L. Chongmin, J. Mohamad Zain and A. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review", Journal of Applied Research and Technology, vol. 12, no. 1, pp. 122-138, 2014.

[12] I. Ansari, M. Pant and C. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC", Engineering Applications of Artificial Intelligence, vol. 49, pp. 114-125, 2016.

[13] A. M. Ortiz, C. F. Uribe, R. H. Beltran, J. J. G. Hernandez, "A survey on reversible watermarking for multimedia content: A robustness overview", IEEE Access, pp. 1–21, 2019.

[14] D. G. Savakar, A. Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme", Arabian Journal for Science and Engineering, PP 1-14, 2019.

[15] R. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain", Measurement, vol. 46, no. 1, pp. 367-373, 2013.

[16] A. Benoraira, K. Benmahammed and N. Boucenna, "Blind image watermarking technique based on differential embedding in DWT and DCT domains", EURASIP Journal on Advances in Signal Processing, vol. 2015, no. 1, 2015.

[17] Kamran, A. Khan and S. Malik, "A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection", Information Sciences, vol. 256, pp. 162-183, 2014.

[18] H. Liu, D. Xiao, R. Zhang, Y. Zhang and S. Bai, "Robust and hierarchical watermarking of encrypted images based on Compressive Sensing", Signal Processing: Image Communication, vol. 45, pp. 41-51, 2016.

[19] S. Parah, J. Sheikh, N. Loan and G. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing", Digital Signal Processing, vol. 53, pp. 11-24, 2016.

[20] S. Roy and A. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling", Multimedia Tools and Applications, vol. 76, no. 3, pp. 3577-3616, 2016.

[21] S. Roy and A. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks", AEU - International Journal of Electronics and Communications, vol. 72, pp. 149-161, 2017.

[22] S. Yang, Z. Song, Z. Fang and J. Yang, "A novel affine attack robust blind watermarking algorithm", Procedia Engineering, vol. 7, pp. 239-246, 2010.

[23] X. Wang, Y. Liu, H. Xu, A. Wang and H. Yang, "Blind optimum detector for robust image watermarking in nonsubsampled shearlet Domain", Information Sciences, vol. 372, pp. 634-654, 2016.

[24] C. Wang, X. Wang, C. Zhang and Z. Xia, "Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution", Signal Processing, vol. 134, pp. 197-208, 2017.

[25] Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux and J. Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography", Signal Processing: Image Communication, vol. 48, pp. 12-21, 2016.

[26] O. Jane, E. Elbaşi and H. İlk, "Hybrid Non-Blind Watermarking Based on DWT and SVD", Journal of Applied Research and Technology, vol. 12, no. 4, pp. 750-761, 2014.

[27] M. Ming, Q. Zhiguang, L. Fang, "A Digital Watermarking Algorithm against Dithering Attack Based on Watson Perceptual Pattern", In proceeding of the second International Conference on Signal Processing Systems (ICSPS), IEEE, Vol 3, pp. 306-309, 2010.

[28] H. Kandi, D. Mishra and S. Gorthi, "Exploring the learning capabilities of convolutional neural networks for robust image watermarking", Computers & Security, vol. 65, pp. 247-268, 2017.

[29] S. Radharani and D. Valarmathi, "A Study on Watermarking Schemes for Image Authentication", International Journal of Computer Applications, vol. 2, no. 4, pp. 24-32, 2010.

[30] T. Hoang Ngan Le, K. Hung Nguyen and H. Bac Le, "Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools", In proceeding of the Second International Conferences on Advances in Multimedia (MMEDIA), IEEE, pp. 67-73, 2010.

[31] N. Makbol and B. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition", Digital Signal Processing, vol. 33, pp. 134-147, 2014.

[32] S. Lagzian, M. Soryani and M. Fathi, "A New Robust Watermarking Scheme Based on RDWT-SVD", International Journal of Intelligent Information Processing, vol. 2, no. 1, pp. 22-29, 2011.

[33] B. Han, J. Li and L. Zong, "A New Robust Zero-watermarking Algorithm for Medical Volume Data", International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 6, no. 6, pp. 245-258, 2013.

[34] F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes", Pattern Recognition Letters, vol. 35, pp. 120-129, 2014.

[35] M. Arsalan, A. Qureshi, A. Khan and M. Rajarajan, "Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique", Applied Soft Computing, vol. 51, pp. 168-179, 2017.

[36] Q. Su, Y. Niu, Q. Wang and G. Sheng, "A blind color image watermarking based on DC component in the spatial domain", Optik - International Journal for Light and Electron Optics, vol. 124, no. 23, pp. 6255-6260, 2013.

[37] S. Arumugham, S. Rajagopalan, J. B. B. Rayappan, R. Amirtharajan, "Tamper-Resistant Secure Medical Image Carrier: An IWT–SVD–Chaos–FPGA Combination", Arabian Journal for Science and Engineering, Vol. 44, pp. 9561-9580, 2019.

[38] J. Li, C. Zhang, " Blind and robust watermarking scheme combining bimodal distribution structure with iterative selection method", Multimedia Tools and Applications, pp. 1-35, 2019.

[39] S. Mousavi, A. Naghsh and S. Abu-Bakar, "Watermarking Techniques used in Medical Images: a Survey", Journal of Digital Imaging, vol. 27, no. 6, pp. 714-729, 2014.

[40] F. Hsu, M. Wu, S. Wang and C. Huang, "Reversibility of image with balanced fidelity and capacity upon pixels differencing expansion", The Journal of Supercomputing, vol. 66, no. 2, pp. 812-828, 2013.

[41] F. Jiang, T. Gao, D. Li, "A robust zero-watermarking algorithm for color image based on tensor mode expansion", Multimedia Tools and Applications, pp 1-16, 2020.

[42] C. Das, S. Panigrahi, V. Sharma and K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation", AEU - International Journal of Electronics and Communications, vol. 68, no. 3, pp. 244-253, 2014.

[43] B. B. Haghighi , A. H. Taherinia , A. H. Mohajerzadeh, "TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA ", Information Sciences, pp. 204-230, 2019.

[44] P. S. and C. P. V. S. S. R., "A robust semi-blind watermarking for color images based on multiple decompositions", Multimedia Tools and Applications, 2017.

[45] Y. Raghavender Rao and E. Nagabhooshanam, "A NOVEL IMAGE ZERO-WATERMARKING SCHEME BASED ON DWT-BN-SVD", International Conference on Information Communication and Embedded Systems (ICICES), IEEE, pp. 1-6, S.A.Engineering College, Chennai, Tamil Nadu, India, 2014.

[46] S. Pal Singh and G. Bhatnagar, "A Novel Chaos Based Robust Watermarking Framework", In Proceedings of the International Conference on Computer Vision and Image Processing, Advances in Intelligent Systems and Computing, Springer, pp. 439-447, 2017.

[47] H. Agarwal, B. Raman and I. Venkat, "Blind reliable invisible watermarking method in wavelet domain for face image watermark", Multimedia Tools and Applications, vol. 74, no. 17, pp. 6897-6935, 2014.

[48] K. Lakshmi Prasad, T. Malleswara Rao and V. Kannan, "A Novel and Hybrid Secure Digital Image Watermarking Framework Through sc-LWT-SVD", Indian Journal of Science and Technology, vol. 9, no. 23, pp. 1-10, 2016.

[49] D. Singh and S. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection", Multimedia Tools and Applications, 2016.

[50] Y. AL-Nabhani, H. Jalab, A. Wahid and R. Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network", Journal of King Saud University - Computer and Information Sciences, vol. 27, no. 4, pp. 393-401, 2015.

[51] K. Jawad and A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases", Journal of Systems and Software, vol. 86, no. 11, pp. 2742-2753, 2013.

[52] S. William, and W. Stallings, "*Cryptography and Network Security*", Pearson Education India, 2006.

[53] A. N. Akansu, W. A. Serdijn, I. W. Selesnick , "Emerging applications of wavelets: a review", Phys Commun 3(1), PP. 1–18, 2010.

[54] M. Islam and U. Chong, "A Digital Image Watermarking Algorithm Based on DWT DCT and SVD", International Journal of Computer and Communication Engineering, vol. 3, no. 5, pp. 356-360, 2014.

[55] B. W. R. Agung, F. P. Permana, "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression", In IEEE International Conference on Communication, Networks and Satellite (ComNetSat*)*, pp. 167-171, 2012.

[56] S. Bajaj, M. Shukla, "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), 2014.

[57] H. M. Yoo, S. K. Lee, J. W. Suh, "Fragile watermarking based on localized histogram modification", In Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference, IEEE Press,pp. 634-635, 2009.

[58] Z. Fang, Y. Zhao, "Image Watermarking Resisting to Geometrical Attacks Based on Histogram", In IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP'06, pp. 79-82, 2006.

[59] M. Chaumont, "Rotation Based Acceleration of Informed Embedding in DPTC Watermarking Scheme", International Journal of Image Processing and Visual Communication, pp. 19-26, 1(2), 2012.

[60] A. Abrardo, M. Barni, "Informed Watermarking By Means of Orthogonal and quasi-orthogonal dirty paper coding", IEEE Transaction on Signal Processing, 53(2), pp.824-833, 2005.

[61] C. Wang, "An Enhanced Informed Watermarking Scheme Using the Posterior Hidden Markov Model", The Scientific World Journal, pp. 1-13, 2014.

[62] L. Laouamer, M. AlShaikh, L. Nana and A. Pascu, "Robust watermarking scheme and tamper detection based on threshold versus intensity", Journal of Innovation in Digital Ecosystems, vol. 2, no. 1-2, pp. 1-12, 2015.

[63] F. Petitcolas, Watermarking Stirmark, http://w.petitcolas.net/fabien/watermarking/stirmark/, 2012.

[64] A. Singh, M. Dave and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images", Multimedia Tools and Applications, vol. 75, no. 14, pp. 8381-8401, 2015.

[65] E. Mansoori and S. Soltani, "A new semi-blind watermarking algorithm using ordered Hadamard transform", The Imaging Science Journal, vol. 64, no. 4, pp. 204-214, 2016.

[66] M. Lazoff, M. Cadogan. Life in the Fastlane, LITFL Review 236. http://lifeinthefastlane.com/resources/radiology-database/

[67] M. Ghadi, L.Laouamer, L.Nana, A. Pascu, " A novel zero-watermarking approach of medical images based on Jacobian matrix model", Security Comm. Networks, pp. 1-16, 2016.

[68] Q. Su, X. Zhang, G. Wang, "An improved watermarking algorithm for color image using Schur decomposition", soft computing, vol. 24, pp. 445–460, 2020.

[69] GH. Golub, CF. Van Loan CF, "Matrix computations", Johns Hopkins Univ Press, Baltimore, 1989.

[70] J. Makhoul, "A Fast Cosine Transform in One and Two dimensions", In IEEE TRANSACTIONS ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING, VOL. ASSP-28, NO.1, February 1980.

[71] J. Wang and Y. Liu," Schur Decomposition Based Robust Watermarking Algorithm in Contourlet Domain", In Proceeding of the International Conference on Cloud Computing and Security(ICCCS), Part I, Springer, pp. 114-124, 2016.

[72] X.L., Liu, C.C., Lin, S.M., Yuan, "Blind dual watermarking for color images' authentication and copyright protection ", IEEE Transactions on Circuits and Systems for Video Technology, pp. 1-9, 2016.

[73] C. Heil, D. Walnut, "Continuous and discrete wavelet transforms", SIAM Rev. **31**(4), pp. 628–666, 1989.

[74] A. M. Ortiz, C. F. Uribe, R. H. Beltran, J. J. G. Hernandez, "A survey on reversible watermarking for multimedia content: A robustness overview", IEEE Access, pp. 1–21, 2019.

[75] N. Agarwal, A. K. Singh, P. K. Singh, "Survey of robust and imperceptible watermarking", Multimedia Tools and Applications, pp. 1–31, 2019.

[76] P. Stavroulakis , "*Chaos Applications in Telecommunications*",1st ed., Boca Raton, FL, USA, Taylor &Francis, CRC Press,2006.

[77] M. Alshaikh, L. Laouamer, L. Nana, A. C. Pascu, "Efficient and robust encryption and watermarking technique based on a new chaotic map approach", vol. 76, pp. 8937-8950, 2017.

[78] DICOM medical Images sample, http://deanvaughan.org/wordpress/2013/07/dicom-sample-images/ (accessed 03/12/2017).

[79] DICOM Documents, http://dicom.nema.org (accessed 15/10/2017).

[80] A. Ustubioglu, G. Ulutas, "A New Medical Image Watermarking Technique with Finer Tamper Localization", JOURNAL OF Digit Imaging, vol. 30, pp. 665-680, 2017.

[81] N. Falgun. Thakkar, V. Kumar Srivastava, " A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications ", Multimedia Tools and Applications, vol. 76, pp. 3 669–3697, 2017.

[82] S. M. Mousavi, A. Naghsh, A. A. Manaf, S. A. R. Abu-Bakar, " A robust medical image watermarking against salt and pepper noise for brain MRI images ", Multimedia Tools and Applications, vol. 76, pp. 1 0313–10342, 2017.

[83] D. Bouslimi, G. Coaterieux,C. Roux, " A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images ", computer methods and programs in biomedicine, 2012, pp. 47-54.

[84] M. C. Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging", SIViP, pp. 1–16, 2013.

[85] H. Bay, A. Ess, T. Tuytelaars and L. Van Gool, "Speeded-Up Robust Features (SURF) ", Computer Vision and Image Understanding, vol. 110, no. 3, PP. 346–359, 2008.

[86] J. M. Garcia , B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy , C. Cruz-Ramos, " An effective fragile watermarking scheme for color image tampering detection and self-recovery" , Signal Processing: Image Communication, vol .81, pp. 1-20, 2020.

[87] S. A. Pinjari and N. N. Patil, "A Pixel Based Fragile Watermarking Technique Using LBP (Local Binary Pattern)", In: International Conference on Global Trends in Signal Processing, Information Computing and Communication, IEEE, pp. 194-196, 2016.

[88] R. Munir, "A Semi-Fragile Watermarking Method Using Slant Transform and LU Decomposition for Image Authentication", In: International Seminar on Intelligent Technology and Its Applications, IEEE, 2015.

[89] I. Sikder, P. Kumar Dhar, and T. Shimamura, "A Semi-Fragile Watermarking Method Using Slant Transform and LU Decomposition for Image Authentication", In: International Conference on Electrical, Computer and Communication Engineering (ECCE), IEEE, Cox's Bazar, Bangladesh, February 16-18, 2017.

[90] E. Akhtarkavan, B. Majidi, M. F. M. Salleh, J, C. Patra, " Fragile high capacity data hiding in digital images using integer-to-integer DWT and lattice vector quantization ", Multimedia Tools and Applications, vol. 79, pp. 13427–13447, 2020.

[91] M. S. Khalil, F. Kurniawan, M. K. Khan and Y. M. Alginahi, "Two-Layer Fragile Watermarking Method Secured with Chaotic Map for Authentication of Digital Holy Quran", The ScientificWorld Journal, pp. 1-29, 2014.

[92] H. Zhang, C. Wang and X. Zhou, "Fragile Watermarking for Image Authentication Using the Characteristic of SVD", *algorithms*, 10 (27), pp. 1-12, 2017.

[93] C. C. Lin, X. L. Liu, C. H. Lin, S. M. Yuan, "Fragile Watermarking-based Authentication Scheme for Demosaicked Images", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, pp. 97-100, 2015.

[94] J. Liu, J. Li, J. Cheng, J. Ma, N. Sadiq, B. Han, Q. Geng and Y. Ai, " A Novel Robust Watermarking Algorithm for Encrypted Medical Image Based on DTCWT-DCT and Chaotic Map ", Computers, Materials & Continua (CMC), vol.61, no.2, pp.889-910, 2019.

[95] J. Dong, J. Li, Y. Duan and Z. Guo, "A Robust Zero-Watermarking Algorithm for Encrypted Medical Images in the DWT-DCT Encrypted Domain", International Journal of Simulation Systems, Science & Technology (IJSSST), 17(43), pp. 1-7, 2016.

[96] S. A. Ali, M. J. Jawad, M. A. Naser, "A semi-fragile watermarking based image authentication", Journal of Engineering and Applied Sciences, 12(6), pp. 1582-1589, 2017.

[97] X. Hou, H. Yang and L. Min, "An Efficient Semi-fragile Watermarking Scheme for Tamper Localization and Recovery", IOP Conf. Series: Materials Science and Engineering, 322 , pp. 1-5, 2018.

[98] D. Zhao and W. Xie, "A Semi-fragile Image Watermarking Scheme Exploiting BTC Quantization Data ", KSII Transactions on Internet and Information Systems, 8 (4), pp. 1499-1519, 2014.

[99] K. Lakshmi Prasad, T. Malleswara Rao and V. Kannan, " A Hybrid Semi-Fragile Image Watermarking Technique using SVD-BND Scheme for Tampering Detection with Dual Authentication", 6th International Conference on Advanced Computing, IEEE, pp. 517-523, 2016.

[100] A. Zhuvikin, V. Korzhik and G. Morales-Luna, "Semi-fragile Image Authentication based on CFD and 3-bit Quantization", Indian Journal of Science and Technology, 9(48), pp. 1-7, 2016.

[101] Y. Huo, H. He, F. Chen, "A semi-fragile image watermarking algorithm with two-stage detection", Multimedia Tools and Applications, pp. 1-27, 2013.

[102] H. Mazumdar, P. Anand, S. J. Soni, M. Joshi, K. Rajeev, M. Rajak, "Human Visual System Models in Digital Watermarking", International Conference and Workshop on Computing and Communication (IEMCON), pp. 1-7, 2015.

[103] M. Q. Al-Ghadi, "Watermarking approaches for images authentication in applications with time constraints", PhD thesis, 2018.

[104] H. Gao, L. Jia, M. Liu, A Digital Watermarking Algorithm for Color Image Based on DWT, TELKOMNIKA, Vol. 11, No. 6, pp. 3271-3278, 2013.

[105] M. Ghadi, L. Laouamer, T. Moulahi, "Enhancing digital image integrity by exploiting JPEG bitstream attributes", journal of innovation in digital ecosystems, 2, pp. 20–31, 2015.

[106] DICOM medical image sample, http://dicom.nema.org/medical/dicom/current/output/html (accessed 15/10/2017).

[107] Y. Niu , M. Kyan , S. Krishnan , Q. Zhang , "A combined just noticeable distortion model–guided image watermarking", Signal Image Video Process. 5 (4) pp. 517–526, 2011.

[108] D. Ariatmanto, E. Ernawan, "An improved robust image watermarking by using different embedding strengths", Multimedia Tools and Applications, pp. 1-27, 2020.

[109] A. Benhocine, L. Laouamer, L. T. Nana, A. C. Pascu, "New Images Watermarking Scheme Based on Singular Value Decomposition", Journal of Information Hiding and Multimedia Signal Processing 4(N1), pp. 1-10, 2013.

[110] A. Benhocine, L. Laouamer, H. Hadji, "Toward An Efficient Security: A New Methodology For Information Security", J. Econ. Bus, 1(1), 2011.

[111] A. Benhocine, L. Laouamer, L. T. Nana, A. C. Pascu, " Measuring Watermarking Robustness Using Fractal Dimensions", Journal of Computer-Mediated Communication 7, pp. 1548-7709, 2010.

[112] A. Benhocine, L. Laouamer, L. T. Nana, A. C. Pascu, " A New Approach against Color Attacks of Watermarked Images", 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008), Harbin, China, 15-17 August 2008.

List of Publications

Book chapter (2):

1. Abdallah Soualmi, Lamri Laouamer, Adel Alti, " Performing Security on Digital Images", In: Exploring Security in Software Architecture and Design, IGI- Global, pp. 211–246, 2019.
2. Abdallah Soualmi, Lamri Laouamer, Adel Alti, " Medical Data Protection using Blind Watermarking technique", In: Enabling AI Application In Data Science, Springer,2020.

Refereed Journals (7):

1. Abdallah Soualmi, Adel Alti, Lamri Laouamer, " A New Blind Watermarking Technique for Medical Images Based on DCT Transform, Weber Descriptors and Arnold Chaotic Map", Ar. Journal for Science and Engineering, Springer, vol. 43, pp. 7893-7905, 2018.
2. Abdallah Soualmi, Adel Alti, Lamri Laouamer, "Blind Watermarking method for Medical Data Protection ", International Journal of Strategic Information Technology and Applications (IJSITA), IGI-Global, vol. 10, no. 4, pp. 1-15, 2019.
3. Abdallah Soualmi, Adel Alti, Lamri Laouamer, " Robust Medical image Watermarking method based on DFT and QR decomposition", International Journal of Informatics and Applied Mathematics, dergipark, Vol. 2, pp. 1-11, 2020.
4. Abdallah Soualmi, Adel Alti, Lamri Laouamer, "MinEigen Value Features Based Novel Blind Medical Image Watermarking Approach against DICOM JPEG Compression attacks ", multimedia tools applications,1-15, 2021.
5. Abdallah Soualmi, Adel Alti, Lamri Laouamer, "Multiple Blind Watermarking Framework for Security and Integrity of Medical Images in e-Health Applications ", the international journal of computer vision and image processing, IGI,11(1), pp. 1-16, 2021.
6. Abdallah Soualmi, Adel Alti, Lamri Laouamer, "A Novel Blind Fragile Watermarking -Based Medical Images Authentication", accepted to be published in the International Journal of Information Security and Privacy, IGI,2021.
7. Abdallah Soualmi, Adel Alti, Lamri Laouamer, " A Novel Blind Medical Image Watermarking Scheme Based on Triangulation Decomposition and Chaotic Sequence", Submitted to digital libraries, springer, 2021.

Referred International Conferences (5):

1. Abdallah Soualmi,Adel Alti, Lamri Laouamer, " Toward a Secure and robust Medical Images watermarking in Untrusted Environment ", The 3rd International

Conference on Advanced Machine Learning Technologies and Applications (AMLTA) 2018, AISC Springer series, pp. 693-703, 2018.

2. Abdallah Soualmi, Adel Alti, Lamri Laouamer, " Schur and DCT Decomposition Based Medical Images Watermarking", IEEE 6th International Conference on Entreprise Systems, Limassol, Cyprus, pp. 204-210, 2018.
3. Abdallah Soualmi, Adel Alti, Lamri Laouamer, Morad Benyoucef, " A New Blind Based Medical Image Authentication Using Schur Decomposition", The 4th International Conference on Advanced Machine Learning Technologies and Applications (AMLTA), AISC Springer series, pp. 623-632, 2019.
4. Abdallah Soualmi, Adel Alti, Lamri Laouamer, " A Blind Medical Image Watermarking For Medical Data Security", The 4th international Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, IEEE, pp. 1-5 ,2019.
5. Abdallah Soualmi, Adel Alti, Lamri Laouamer, "Robust Medical Image Watermarking Method Based On DFT and QR Decomposition ", The first International Conference on Innovative Trend in Computer Science (CITCS'19), Guelma, Algeria, October 2019.

ملخص

إن حماية السجلات الإلكترونية المخزنة والمنقولة للمرضى، ملزم باحترام عدة شروط مثل السرية، النزاهة والمتانة ضد جميع محاولات الاطلاع غير المرخص أو التخريب. لذلك نقترح العديد من المساهمات في مجال التشفير والعلامة المائية. المساهمة الرئيسية هي اقتراح طريقتين قويتين للعلامة المائية للصور الطبية: واحدة عمياء على أساس تحويل DCT، واصف ويبر وخريطة أرنولد الفوضوية والاخرى نصف عمياء تستعمل مزيج من تحويلات DCT و Schur. المساهمة الثانية هي اقتراح طريقتين جديدتين شبه هشتين لتقليل التعقيد الحسابي وضمان صحة محتويات الصور الطبية. تعتمد الأولى على مزيج من تحويلات DWT وSchur، بينما تعتمد الثانية على تحويل Schur والتسلسل الفوضوي. تتكون المساهمات الأخيرة من مناهج للعلامات المائية الهشة تضمن نزاهة البيانات الطبية، وتم عرض طريقتين: الأولى تجمع بين الواصفتين SURF وويبر وخريطة أرنولد الفوضوية بينما الثانية تعتمد على تحويل Schur.

كلمات مفتاحية: العلامة المائية، حماية الصور الطبية، النزاهة، المتانة، الشفافية، التعقيد الحسابي، هجمات إلكترونية، DICOM.

Résumé

La protection des dossiers électroniques des patients stockées et transmises, nécessite l'intégrité, la confidentialité et la robustesse contre toutes tentatives intentionnelles ou bien non intentionnelles. Pour Cela, nous avons développé plusieurs contributions en crypto-tatouage. La principale contribution est la proposition de deux méthodes de tatouage d'images médicales robustes : la première et aveugle basée sur la transformée DCT, le descripteur Weber et la carte chaotique d'Arnold, et la deuxième et semi-aveugle basée sur les transformées DCT et Schur. La seconde contribution est la proposition de deux nouvelles méthodes semi-fragiles qui réduisant la complexité en termes de temps de calcul et assurant l'authenticité des contenus des images médicales. La première méthode se base sur la combinaison de deux transformées : DWT et Schur, alors que la deuxième méthode se base sur la transformée Schur et la séquence Chaotic. Les dernières contributions consistent à des approches de tatouages fragiles assurant une imperceptibilité et une intégrité des données médicales remarquables. Deux méthodes fragiles ont été introduites : la première combine les descripteurs SURF avec les descripteurs Weber et Arnold alors que la deuxième se base sur la Schur.

Mots clé : Watermarking, Sécurité des données médicale, intégrité, robustesse, imperceptibilité, complexité computationnelle, attaques, DICOM.

Abstract

The protection of the transmitted and stored electronic patient information's; need the ensuring of many criteria such: confidentiality, integrity, and robustness against all intentional or unintentional attempts that used to access or destroy these data. For these purposes, we have brought many contributions in crypto watermarking. The main one is the proposition of two robust methods: a blind medical image watermarking technique based on DCT transform, Weber descriptor, and Arnold chaotic map, and a semi blind technique using DCT and Schur Decompositions. The second contribution is the proposal of two new semi-fragile techniques for medical image authentication with low computational complexity. The first technique combines DWT and Schur transforms, while the second technique combines Schur transform and Chaotic sequence. The last contribution is two fragile watermarking methods, which achieves high imperceptibility and better integrity checking of medical data. The first method combines the SURF and weber descriptors and Arnold chaotic map while the second based on Schur transform.

Key words: Watermarking, Medical Data Security, Integrity, Robustness, Imperceptibility, Computational complexity, Attacks, DICOM.