Medical image content protection by secret information hiding to support telemedicine
Mu’Ath Al-Shaikh

To cite this version:

HAL Id: tel-01477224
https://tel.archives-ouvertes.fr/tel-01477224
Submitted on 27 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Protection des contenus des images médicales par camouflage d'informations secrètes pour l'aide à la télémédecine.
To my wife ESRAA

My son ZIAD

And my daughter LAREEN
ACKNOWLEDGEMENTS

First and foremost I would like to express my special appreciation and thanks to my advisors Professors Laurent Nana, Anca Pascu and Lamri Laouamer, you have been a tremendous mentors for me. I would like to thank you for encouraging my research and for allowing me to grow as a researcher. I would also like to thank my committee members, Professors Ismail Biskri, William Puech, Caroline Fontaine, Gouenou Coatrieux and Antoine Beugnard for serving as my committee members even at hardship. I also want to thank you for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you. I would especially like to thank all of my friends and colleagues at UBO for their supporting and helping during my PhD trip.

A special thanks to my family. Words cannot express how grateful I am to my father, my brothers and my sisters for all of the sacrifices that you have made on my behalf. Your prayer for me was what sustained me thus far. At the end I would like to express appreciation to my beloved wife ESRAA who spent sleepless nights with me and was always my support in the moments when there was no one to answer my queries.
Table Of Contents
Table Of Contents ......................................................................................................................................... 3
List Of Figures .............................................................................................................................................. 7
List Of Tables ............................................................................................................................................. 10
General introduction ................................................................................................................................... 12
FIRST PART ................................................................................................................................................ 17
Chapter 1 Digital Image Watermarking ...................................................................................................... 17
1.1 Introduction ............................................................................................................................................. 17
1.2 Properties of digital image watermarking .............................................................................................. 19
  1.2.1 Robustness ...................................................................................................................................... 19
  1.2.2 Imperceptibility ............................................................................................................................. 20
  1.2.3 Capacity and payload ...................................................................................................................... 20
  1.2.4 Security ......................................................................................................................................... 21
  1.2.5 Computational complexity ............................................................................................................ 22
  1.2.6 Blindness ...................................................................................................................................... 22
1.3 Application of digital image watermarking ............................................................................................. 22
  1.3.1 Copyright protection ...................................................................................................................... 22
  1.3.2 Transaction tracking or fingerprinting ............................................................................................ 23
  1.3.3 Authentication ............................................................................................................................... 23
  1.3.4 Integrity ....................................................................................................................................... 23
  1.3.5 Tamper detection ............................................................................................................................ 23
1.4 Domains of image watermarking ........................................................................................................... 24
  1.4.1 Spatial domain ............................................................................................................................... 25
  1.4.2 Frequency domain ........................................................................................................................ 28
1.5 Visible image watermarking ................................................................................................................... 35
  1.5.1 Visible image watermarking techniques ....................................................................................... 35
  1.5.2 Visible image watermarking applications ..................................................................................... 36
1.6 Digital image watermarking attacks and robustness ............................................................................. 37
  1.6.1 Digital image watermarking attacks ............................................................................................. 37
  1.6.2 Robust image watermarking approaches ....................................................................................... 39
  1.6.3 Fragile image watermarking approaches ....................................................................................... 42
1.7 Image quality measurement .................................................................................................................... 43
  1.7.1 Mean square error (MSE) .............................................................................................................. 44
  1.7.2 Peak signal to noise ratio (PSNR) ................................................................................................. 44
  1.7.3 Structural similarity index measurement (SSIM) ........................................................................ 44
  1.7.4 Bit error rate (BER) ....................................................................................................................... 45
Chapter 2 Digital Image Cryptography ................................................................. 47
2.1 Introduction ........................................................................................................ 47
2.2 Cryptography: definition and principle ............................................................... 48
2.3 Cryptography classification ............................................................................... 48
  2.3.1 Symmetric cryptography .......................................................................... 49
  2.3.2 Asymmetric cryptography ....................................................................... 51
  2.3.3 Hash function cryptography .................................................................... 52
2.4 Cryptographic techniques .................................................................................. 53
  2.4.1 Symmetric encryption algorithms ............................................................. 53
  2.4.2 Asymmetric encryption algorithms .......................................................... 57
2.5 Cryptanalysis ...................................................................................................... 59
  2.5.1 Brute-force attack ..................................................................................... 59
  2.5.2 Birthday attack ......................................................................................... 60
  2.5.3 Meet in the middle attack ....................................................................... 60
2.6 Conclusion ........................................................................................................... 61

Chapter 3 Hybrid Watermarking and Cryptography Techniques ....................... 63
3.1 Introduction ......................................................................................................... 63
3.2 Combined watermarking and encryption approaches classifications .......... 63
  3.2.1 Watermarking followed by encryption (WFE) ....................................... 63
  3.2.2 Encryption followed by watermarking (EFW) ....................................... 65
  3.2.3 Joint watermarking / decryption (JWD) .................................................. 67
  3.2.4 Joint watermarking / encryption (JWE) .................................................. 68
3.3 Conclusion .......................................................................................................... 69

Chapter 4 Digital Medical Image and Telemedicine Security .................................. 71
4.1 Introduction .......................................................................................................... 71
  4.1.1 Digital image ............................................................................................ 72
  4.1.2 Digital medical image .............................................................................. 72
4.2 Picture archiving and communication system (PACS) ..................................... 72
4.3 Telemedicine ...................................................................................................... 73
  4.3.1 Telemedicine and teleradiology .............................................................. 74
4.4 Digital imaging and communication in medicine (DICOM) ........................... 75
4.5 DICOM security profiles ............................................................................... 77
  4.5.1 Secure use profiles ............................................................................... 77
  4.5.2 Secure transport connection profiles ...................................................... 77
  4.5.3 Digital signature profiles ................................................................. 77
List Of Figures
Figure 1.1: Data security system [Mousavi 14] ................................................................. 18
Figure 1.2: Characteristic watermarking system............................................................... 18
Figure 1.3: Example of watermarking imperceptibility .................................................... 20
Figure 1.4: The trade-off between the three properties watermarking ............................. 21
Figure 1.5: Watermarking domains ................................................................................. 25
Figure 1.6: LSB watermarking approach ....................................................................... 26
Figure 1.7: Local Binary Pattern of eight neighbours ......................................................... 26
Figure 1.8: 2-level- DWT decomposition ......................................................................... 29
Figure 1.9: Image DCT frequency coefficients.................................................................. 32
Figure 2.1: The general encryption and decryption diagram .......................................... 48
Figure 2.2: Cryptography main area ................................................................................ 49
Figure 2.3: Encryption and decryption process based on symmetric technique ............. 50
Figure 2.4: Stream cipher diagram .................................................................................. 50
Figure 2.5: Block cipher diagram ..................................................................................... 51
Figure 2.6: Encryption and decryption process based on asymmetric technique .......... 52
Figure 2.7: DES structure ............................................................................................... 55
Figure 2.8: AES-128 bit encryption process ..................................................................... 57
Figure 2.9: General idea of meet in the middle attack ...................................................... 61
Figure 3.1: WFE approach in the case of the embedding- encryption process .................. 64
Figure 3.2: WFE approach in case of the decryption- extraction process ......................... 64
Figure 3.3: EFW Approach in case of the encryption-embedding process ....................... 65
Figure 3.4: EFW approach in case of the extraction-decryption process ......................... 65
Figure 3.5: JWD general diagram .................................................................................... 67
Figure 3.6: JWE general diagram .................................................................................... 68
Figure 4.1: General telemedicine scenario ....................................................................... 74
Figure 4.2: Medical image components .......................................................................... 76
Figure 4.3: NROI & ROI medical image ......................................................................... 76
Figure 5.1: Line diagram of formal concept analysis for images and their features .......... 94
Figure 5.2: Watermark embedding scheme ..................................................................... 96
Figure 5.3: (a) Extraction of four 12 × 12 sub-matrices from i, (b) Decimal representation of each sub-matrix ................................................................. 97
Figure 5.4: 144 × 8 Boolean Matrix for each area picked up ........................................... 97
Figure 5.5: iw and w watermarked and watermark images ............................................. 100
Figure 5.6: Watermark embedding with different values of t .......................................... 101
Figure 5.7: Watermark extraction scheme ..................................................................... 101
Figure 5.8: Attacked watermarked and retrieved watermark images .............................. 103
Figure 5.9: Example of a binary tree graph .................................................................... 110
Figure 5.10: Example of a BDD representing the given function .................................... 111
Figure 5.11: The BDD for a given combination set ........................................................... 112
Figure 5.12: Ordinary binary decision diagram: a) node deletion, b) node sharing ........ 112
Figure 5.13: Reducing ZBDD represented by a given function \( f = \neg x_1 \cap x_2 \) .............. 113
Figure 5.14: ZBDD Map for an item set histogram ......................................................... 116
Figure 5.15: Determination of the image main ROI ....................................................... 119
Figure 5.16: Attacks on the watermarked hand image \( i_{\text{w}} \) and the extracted watermarks \( w_{a} \) in the case of the Boolean function \( F = \neg B \land C \land \neg D \land \neg F \) ................................................................. 121
Figure 5.17: Attacks on the watermarked hand image \( i_{\text{w}} \) and the extracted watermarks \( w_{a} \) in the case of the Boolean function \( F = \neg A \land \neg B \land C \land \neg F \land \neg H \) ................................................................. 121
Figure 5.18: Attacks on the watermarked brain image \( i_{\text{w}} \) and the extracted watermarks \( w_{a} \) in the case of the Boolean function \( F = \neg B \land C \land \neg D \land \neg F \) ................................................................. 122
Figure 5.19: Attacks on the watermarked brain image \( i_{\text{w}} \) and the extracted watermarks \( w_{a} \) in the case of the Boolean function \( F = \neg A \land \neg B \land \neg D \land F \land \neg H \) ................................................................. 122
Figure 5.20: Attacks on the watermarked brain image \( i_{\text{w}} \) and the extracted watermarks \( w_{a} \) in the case of the Boolean function \( F = \neg B \land C \land \neg D \land \neg F \) ................................................................. 122
Figure 5.21: Attacks on the watermarked brain image \( i_{\text{w}} \) and the extracted watermarks \( w_{a} \) in the case of the Boolean function \( F = \neg A \land \neg B \land \neg D \land F \land \neg H \) ................................................................. 122
Figure 5.22: Weber Law description................................................................. 129
Figure 5.23: 3×3 block....................................................................................... 129
Figure 5.24: Original medical images \( i_{\text{w}} \) .......................................................... 131
Figure 5.25: Informed watermark images \( w_{a} \) ............................................... 131
Figure 5.26: Various watermarked images with different values of \( \alpha \) ........ 132
Figure 5.27: The applied attacks and the corresponding PSNR values .......... 132
Figure 5.28: Tampered watermarked images ................................................. 133
Figure 5.29: Differences between watermarked image and tampered watermarked image .......................... 133
Figure 5.30: 2D Medical image wavelet transform with one level decomposition. ................................................................. 135
Figure 5.31: Watermark embedding process .................................................. 137
Figure 5.32: Watermark extraction process ................................................... 138
Figure 5.33: Embedding watermark by linear interpolation with different values of \( t \) (secret key). .. 139
Figure 5.34: Watermark extraction results when \( t=0.98 \) .................................. 139
Figure 5.35: Watermark extraction results when \( t=0.5 \) .................................. 140
Figure 5.36: Watermark extraction results when \( t=0.2 \) .................................. 140
Figure 5.37: Embedding watermark by linear interpolation with different values of \( t \) (secret key). .. 141
Figure 5.38: Watermark extraction results when \( t=0.98 \) .................................. 141
Figure 5.39: Watermark extraction results when \( t=0.5 \) .................................. 141
Figure 5.40: Embedding watermark by linear interpolation with different values of \( t \) (secret key). .. 142
Figure 5.41: Watermark extraction results when \( t=0.98 \) .................................. 142
Figure 5.42: Watermark extraction results when \( t=0.5 \) .................................. 142
Figure 5.43: Watermark extraction results when \( t=0.2 \) .................................. 143
Figure 5.44: Robustness measures in case of SSIM and UQI.......................... 143
Figure 5.45: Robustness measure in case of PSNR................................. 144
Figure 5.46: Imperceptibility results for different values of \( t \) ......................... 144
Figure 5.47: PSNR Comparative results with the works in [Ahmad 14] and [Benrouma 15] .... 145
Figure 5.48: SSIM comparative results with the works in [Ahmad 14] and [Benrouma 15] .... 146
Figure 6.1: The process of the proposed system for images securing exchange between the sender and the receiver. .................................................. 151
Figure 6.2: Proposed system for medical image securing .............................. 152
Figure 6.3: Example for computing the pixel length matrix .......................... 152
Figure 6.4: Results of the bigrams proposed encryption/decryption process .......................... 153
Figure 6.5: Results of the trigrams proposed encryption/decryption ............... 154
List Of Tables
Table 5.1: The images and their features .............................................................................................................. 92
Table 5.2: The relation between Objects and Attributes .......................................................................................... 92
Table 5.3: Formal concepts of data given by the images and their features ................................................................. 93
Table 5.4: PSNR quality measurements for extracted watermark after attacks ......................................................... 104
Table 5.5: NCC results after common image processing attacks .................................................................................. 105
Table 5.6: The bits used for the watermark image ...................................................................................................... 106
Table 5.7: Comparisons of the execution time between the proposed method and the method in [Su 13] ........................................................ .......................................................... 106
Table 5.8: Truth Table for the given Boolean function $F$ .......................................................................................... 110
Table 5.9: Items set histogram .................................................................................................................................. 114
Table 5.10: Item set histogram and binary representation .......................................................................................... 115
Table 5.11: The available spaces for the item set histogram ......................................................................................... 117
Table 5.12: Description of the attack types used ....................................................................................................... 121
Table 5.13: PSNR values between $i$ and $iw$ ............................................................................................................. 123
Table 5.14: Similarity metrics between $w$ and $wa$ in the case of image “hand” ............................................................ 124
Table 5.15: Similarity metrics between $w$ and $wa$ in the case of image “brain 1” ........................................................ 124
Table 5.16: Similarity metrics between $w$ and $wa$ in the case of image “brain 2” ......................................................... 124
Table 5.17: Similarity metrics between $w$ and $wa$ in the case of image “leg” ............................................................. 125
Table 5.18: Comparative study of image quality .......................................................................................................... 125
Table 5.19: PSNR robustness measurements and comparison with the work [Tsougenis 14] ......................................... 126
Table 5.20: CC Robustness measurements and comparison with the work [Shahid 12] ..................................................... 126
Table 5.21: Adaptive watermark image size (bits) and compared with the works [tsougenis 14] and [shahid 12] ................................................................................................................................ 126
Table 5.22: Comparison of the payload and imperceptibility with work in [Walia 13] ...................................................... 134
Table 5.23: Robustness measurements after different attacks ........................................................................................ 143
Table 5.24: Imperceptibility measurement based on PSNR .......................................................................................... 144
Table 5.25: PSNR comparative results ....................................................................................................................... 145
Table 5.26: SSIM comparative results ......................................................................................................................... 145
Table 7.1: The applied attacks descriptions .................................................................................................................. 165
Table 7.2: Similarity measures between $w$ and $wa$ based on PSNR, NCC and SSIM measures ................................. 165
Table 7.3: Comparison of the robustness of our method with some other related works [Guo 15] and [Zheng 13] ....... 166
List Of Publications

General introduction

With the huge developments and rapid growth in the technology field, Internet becomes the main communication media to transmit, share and exchange data between users. Internet provides fast, easy and low cost sharing way. But, it still produces a gap and a lack in the security and privacy issues such as integrity and authenticity. Moreover, the use of Internet as a central communication media of data opens new challenges and opportunities for duplicating, creating and manipulating the visual content of the digital material. Also, it opened new challenges in the field of illegal distribution and copyright issues which must be controlled. The ownership and the authorization to use the digital material also have to be proved.

On the other hand, one of the main concerns in the world is to develop the healthcare quality. The human healthcare is considered as the most important point throughout the world. The information technology contributes to the medical service improvement that is provided to people. Telemedicine represents the use of information and communications techniques to offer the health care where the patients and the physicians are disjointed by physical distance. The modern health care system like Hospital Information System (HIS) and Picture Archiving and Communication System (PACS) provide the health sector with the digital medical information like medical image in an easy and fast ways. The medical image is considered as a main core in telemedicine field. It is used for diagnosis in hospitals. So, any modification, even slight modification, will affect the physician’s diagnosis. Medical images request strong security to guarantee only the events of authentic modifications. Interchange of medical images between clinics situated in different geographic places is a very commonly used way these days. But unluckily, this interchange happens through insecure and open networks, which create a threat of unfavorable acts and finally corrupted or lost data in the results. For these reasons and these threats, telemedicine has to provide security conditions of interchanges in order to guarantee the integrity and authenticity of the medical images during the transmission.

A huge amount of the medical images is captured in hospitals for diagnosis and research goals and are stored in databases. These databases must be protected against intentional and unintentional attacks.
General introduction

and modifications. Such databases make possible to detect the disease and early treatments. Meanwhile, the physician has to be sure that the image is free of manipulations before making the decision. For this goal, the watermarking is proposed as one of solutions to ensure about the medical image authenticity and integrity.

Using the authentication method provided by the watermarking, the physician will be able to detect some intentional alteration of the medical image and will not use such image to build the diagnosis. Nevertheless, if the physician can be able to extract the embedded watermark perfectly, which usually takes a few seconds, he can continue safely with the diagnosis and treatments based on this image. The watermark is not only authenticating the host image, but may also be useful in embedding extra information related to the host image. For example, information correlated to the patient as physician name, hospital and so on, are very useful in the telemedicine scenario.

The protection of digital medical image comprises at least two main aspects: security and authentication. In order to ensure the security, the information has to be protected from the unauthorized users while the authentication confirms that the received data is not affected or modified and is sent by the intended sender (watermarking). The cryptography technique proves the security issues by assuming the intended sender and intended receiver have some security aspects called keys. So, after encryption of the digital material from the sender side, the person who has the key (receiver) can decrypt and access the content of the digital material.

Three main characteristics have to be ensured after the transmission of the medical image: confidentiality, authenticity and reliability. Confidentiality means that an authorized user can access and modify the medical image while an unauthorized user cannot access or take any information about the medical image. The user, at the destination side, who has the key, can decrypt the encrypted medical image and access to the patient information. Cryptography plays an important role to ensure this aspect. Authenticity is a characteristic that requires the fact that the received medical image at the destination is the same as sending from the source and belongs to the certain patient. Watermarking approach can achieve this aspect by a perfect extraction of the embedded watermark from the
General introduction

watermarked image. The third aspect is the reliability. It comprises the integrity and availability. Integrity means that the received medical image must be intact from any modification. This aspect can also be achieved by extracting the exactly embedded watermark from the received image. The availability means that the medical image is available upon the request of the physicians or any medical party.

The cryptography approaches protect the data during the transition. The person who has the secret key and the algorithm can decrypt the data in a useful format. But after the decryption the data are no longer protected. Therefore, it is very hard to verify its integrity and its origin. This kind of protection is called *priori protection methods*. The watermarking approaches came as complimentary protection techniques to prove the data integrity, authenticity and its originality. After the data decryption, we still have the possibility to identify if the data is tampered or is in original form. This kind of protection is called *posteriori protection methods* [Bouslimi 12].

One of the goals of our research is to ensure and to prove the security of the medical image. This includes the authenticity of medical image and the proof of its integrity and its originality (owner). Finally, this research focuses on supporting the health care system in order to implement a secure, robust and privacy system for the intact sharing and usage of the medical image.

In this thesis, we investigated the watermarking, cryptography and combined watermarking and cryptography approaches and apply them to telemedicine.

**Thesis Organization**

The thesis is divided in two parts. The first part includes the main principles and some of the previous studies in the watermarking, cryptography and combined watermarking and cryptography with a focus on the medical image field. This first part comprises four chapters (chapters 1 to 4).

In chapter one, we present the literature review of the digital image watermarking. We are focusing in this review on the robustness, imperceptibility and complexity properties in the existing approaches.
In chapter two, the cryptography approaches are investigated. Our goal is to focus on the complexity and security issues in the existing cryptography approaches.

Chapter three carried the hybrid watermarking and cryptographic existing approaches. Chapter four presents the telemedicine principle and medical image characteristics. Our aim is to show the importance of the medical image security properties and the gap in the existing approaches.

The second part presents our contribution based on robust watermarking in the spatial and frequency domain, informed and symmetric cryptography approach and joined (hybrid) watermarking and cryptography approach. This second part comprises 3 chapters (chapters 5 to 7).

Chapter five comprises five sections. The first one is the introduction. In the second section, we investigate a novel and robust watermarking approach in the spatial domain. Our approach is innovative and based on using Formal Concept Analysis. It proposes the generation of the optimal position for embedding. The watermark is built from some header information of the medical image. It is embedded into the region of non-interest (NROI) of the medical image. Our goal is to provide watermarking solution with low computational complexity, high robustness, high imperceptibility and low degradation. In the third section, another robust watermarking approach is presented in the spatial domain. In this approach, we addressed the problem of generating watermarks as small as possible (small payload) based on ZBDD to adapt the hidden data to the real time applications by maintaining high robustness, high imperceptibility and low complexity within the medical image. The aim is to provide new adaptive watermarking method offering low complexity, high robustness and imperceptible watermarks. In the fourth section, we present a novel semi-blind watermarking technique in the spatial domain. The proposed algorithms covered two security issues: the tamper detection and the watermarking robustness. The approach is based on the Weber differential excitation descriptor. In the fifth section, we propose a new watermarking approach to ensure the CT scan medical image authentication and robustness, which is based on the wavelet transform in the frequency domain. The chapter ends with the conclusion.
General introduction

In chapter six, we present our new informed symmetric cryptography approach. This approach exploits the characteristics of the image to generate the keys for encryption / decryption. It is based on N-gram technique. The main goal is to provide a solution for symmetric cryptography with more secure keys while maintaining low computation complexity.

Chapter seven deals with an innovative hybrid encryption and watermarking approach to improve the security and ensure the integrity of medical image content. It is based on one time pad (OTP) technique and a new formula of the chaotic map which provides a key matrix whose sizes is equal to the image size, where for each image pixel there is a mismatch-specific key value. The generated key stream used for the OTP cryptosystem is based on a new way of applying the chaotic map approach. Here, the initial value of the key stream in the chaotic map is the same as the key used for watermarking. The properties of our chaotic map and OTP approach provided us with a reversible and predictable watermarking system.
Chapter 1 Digital Image Watermarking

1.1 Introduction
Digital Watermarking is the art of hiding secret information in the original data. The original data is readable and visual for all, while the hidden data is readable and changeable by the authorized user. It may be used to verify the authenticity and the integrity of the host signal or to show the identity of its owners. There is another field developed before watermarking for security issues: the steganography. Watermarking is similar to the steganography. Both steganography and watermarking employ stenographic techniques to embed data covertly in noisy signals [Cox 07].

Steganography name is derived from the Greek where the prefix “stegano” means covered and the prefix “graphos” means write. The differences between steganography and watermarking are [Shih 07]: in steganography, the hidden information and cover information are unrelated each other, while in watermarking the cover and embedded data are related to each other. Also, in steganography, the message should be invisible, while in watermarking, it can be visible or invisible. Moreover, in steganography the main aim is to hide the data in a way the intruder cannot detect it, but in watermarking the main aim is to hide data such that the data cannot be removed or replaced by an intruder. So, the watermarking is more appropriate than steganography for preserving the security of digital images, due to its flexibility (choice between visible and invisible watermark, possibility to have a link between the hidden data and the host image) and because it makes it difficult to remove the hidden data. The data can be encrypted before embedding the watermark, as a second layer of protection [Subramanyam 12]. As we illustrate in figure 1.1, the existing data security system is divided into information hiding and cryptography. Information hiding is also divided into watermarking and steganography. Watermarking techniques can be classified based on the human perception (visible or non-visible), based on reversibility (reversible or non-reversible), and based on
the domain (frequency or spatial) [Memon 10]. We will discuss the characteristics and classification of the watermarking system in the depth later on.

Figure 1.1: Data security system [Mousavi 14]

A characteristic watermarking system is shown in figure 1.2 which comprises watermark embedding and watermark extraction. The inputs on the embedding side are the watermark, the host signal content and the secret key. The purpose of this secret key is to enhance the security of the watermarking system. The output of the watermarking embedding is the watermarked signal. Then, the watermarked signal is sent in a noisy transmission medium like the internet. During the transition, there is probably an attack or a modification from unauthorized users. At the extraction (detector) side, the inputs are the watermarked signal, the secret key (similar to the one used at the time of embedding), the original signal and/or the watermark. The detector has to extract the watermark from the watermarked signal and verify the authenticity of the watermark to determine if the extracted watermark is the same as the original watermark.

Figure 1.2: Characteristic watermarking system
Chapter 1: Digital Image Watermarking

In this chapter, in the first section, we discuss the definition of the digital image watermarking, the second section includes the characteristics of the watermarking techniques, the third section talks about the goal and the watermarking application, the fourth section discusses the classification of the watermarking embedding and extraction methods, the fifth section speaks about the visibility watermarking approaches, while the attacks and robustness will be discussed in the sixth section. Finally, the quality image assessments will be discussed in the seventh section.

1.2 Properties of digital image watermarking

The digital watermarking system has important properties which must be achieved in the technique of watermarking. In this section, we discuss in details these properties:

1.2.1 Robustness

The robustness of the watermark is the ability to stand against different kinds of attacks. The common attacks are the image processing operations, like noise and cropping and geometric transformations like rotation and scaling. The attacks can be intentional attacks which try to remove and destroy the watermark in the watermarked image, or unintentional attacks, which are happening to the watermarked image during the transmission without aim to removing or impair the watermarked image. To measure the robustness, the following steps must be performed: apply different attacks to the watermarked image, then extract the watermark image from the watermarked image, and compare the original watermark with the extracted one.

In any attack cases, the robust watermarking approach has to resist and preserve the watermark image quality. These cases are:

1- Removal attacks like compression, which aim to remove the watermark,
2- Geometric transformation attacks like rotation, which aim to destroy the watermark,
3- Cryptographic attacks which aim to destroy the security key of the watermarking,
4- Property attacks which aim to add new watermark to the watermarked image.

The robustness as property is suitable to improve the copyright, the ownership issues and the medical application [Malshe 12].
1.2.2 Imperceptibility
The *imperceptibility* [Shih 07] refers to the quality degradation between the original image and the watermarked image. Normally, the watermarked image should be perceptually similar to the original image. This property is called the imperceptibility or the transparency of the watermarking approach. If in the watermarking process it happens that the original image after the embedding is affected, the whole technique is useless. In some applications which want the watermark to be perceptible for human eyes such as a logo for channels, a name of a person on some material and the other applications that want to show the owner of the materials, the imperceptibility can be low.

To evaluate the imperceptibility aspects in the watermarking system, we measure the fidelity between the watermarked image and the original image. The measurement tools show the degradation that happened to the watermarked image after the embedding. The common algorithms to measure the imperceptibility are Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Structure Similarity (SSIM) and Bit Error Rate (BER) [Malshe 12]. We will discuss these tools in detail later on. Figure 1.3 shows an example of a watermarking approach with high and low imperceptibility.

<table>
<thead>
<tr>
<th>Original Image</th>
<th>Watermark Image</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Original Image" /></td>
<td><img src="image2.png" alt="Watermark Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Watermarked Image (High Imperceptibility)</th>
<th>Watermarked Image (Low Imperceptibility)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3.png" alt="Watermarked Image (High Imperceptibility)" /></td>
<td><img src="image4.png" alt="Watermarked Image (Low Imperceptibility)" /></td>
</tr>
</tbody>
</table>

Figure 1.3: Example of watermarking imperceptibility

1.2.3 Capacity and payload
The *capacity* refers to the available space of embedding in the original image, while the *payload* refers to the watermark size that will be embedded in the original image without noticeable to the
reduction of the image quality and fidelity. The simpler capacity of a watermarking system is obtained with one bit for the watermark (Zero watermarks) [Li 12]. Some of the applications require high capacity and low payload which means the watermark size is low (one bit) but will be embedded many times through the original image [Yaghmaee 15]. There is a trade-off between the capacity, robustness and imperceptibility. For instance, if the capacity is increasing, the robustness will decrease, while the imperceptibility will increase. Figure 1.4 illustrates the trade-off between the three properties. This aspect is very important for medical application, secure media, and other applications that want less capacity properties.

![Figure 1.4: The trade-off between the three properties watermarking](image)

### 1.2.4 Security
A watermarking is secure if it is capable to fight intentional tampering attacks. It would include outstanding security even when the attacker knows the process for embedding and extracting the watermark. The power of the security of the watermark based on the key is selected. Let us consider the following scenario: the hacker attacks the watermark by removing it from the watermarked image and try to embed faked watermark. If the key used is secure, the system is considered as a secure system and it will deny the hacker. The security aspect is different from the robustness aspect. The robustness is surviving the common signal processing attacks. But the security is surviving the malicious modification. Some applications want to be secure while the others do not require it [Mousavi 14]. This property is desirable in multimedia security applications, ownership identification, fingerprint, telemedicine or medical image sharing.
Chapter 1: Digital Image Watermarking

1.2.5 Computational complexity
The watermarking system computational complexity is a very important and critical issue. In a watermarking system the size of the original image as well as the size of the watermark image determines the capacity. The capacity has an indirect influence of the computational complexity. However, the time is the second important parameter of the complexity. The time complexity can be defined in terms of algorithm speed. To have a low complexity in time, the embedding and extraction processes time must be low. Moreover, the memory size of the equipment is important for the complexity. The watermarking algorithm complexity can be obtained by measuring the execution time of the embedding and the extraction processes [Cox 07]. This property is important and has to give a high consideration to the real time applications such as telemedicine, telediagnosis applications and online security application.

1.2.6 Blindness
The blind aspect is considered for the watermarking technique on the extraction side. If the technique requires the original image to extract the watermark, it is called non-blind technique [Maity 14]. But if the technique requires the original watermark to extract the embedded watermark, it is called semi blind [Sulong 13] [Laouamer 15]. The technique of watermarking is blind if it does not require original image or watermark image to extract the embedded watermark [Lin 09] [Bhattacharya 14]. The blind approach needs just the key. The non-blind system is more robust because the original image is available at the extraction process. But the blind system is the common way in watermarking. A blind system needs less memory space than a non-blind system.

1.3 Application of digital image watermarking
The watermarking is applied in many and different fields to achieve and/or to improve the security. The watermarking approach can reach many security goals (copyright protection, transaction and finger print ...). Each goal requires the appropriate properties among those mentioned in the previous section [Jabade 11] [Mousavi 14]. We can classify the most important applications as follows:

1.3.1 Copyright protection
One of the watermarking goals is to provide copyright for media material. It is about embedding the copyright information into the host image. The watermarked image has to resist against different
Chapter 1: Digital Image Watermarking

kinds of attacks (removing, modifying, or adding new watermark). The technique proves the copyright owner into the material to avoid non-owners from claiming to be the legal owners of the data. The owner of the material can extract his/her watermark from the watermarked image to prove the right on the watermarked material. The watermarking approach in this application should be robust and invisible. Moreover, this application will not prevent the user from the copy of the digital image [Kutter 99] [Wang 04 (a)].

1.3.2 Transaction tracking or fingerprinting
Fingerprinting requires the embedding of a different watermark for each customer. The watermark is usually related to the customer information like the customer identity. It makes it possible to track the images and to find where illegal copies are happening. Moreover, it makes it possible to detect the customer who breaks the rules and conditions of the agreements. This kind of application needs robust and invisible watermarking technique [Pankanti 99] [Gunsel 02].

1.3.3 Authentication
The watermark is applied to the host image in order to verify its authenticity. In the extraction phase, the extractor can extract the watermark, then compare the extracted watermark with the original watermark to determine if the received data is authentic or not. These kind of applications deals with fragile and semi-fragile watermarking systems. Moreover, the original watermark it is required during the extraction phase [Kundur 99] [Lu 01].

1.3.4 Integrity
The integrity aspects refer to the image safety. The watermark is embedded into the original host. During the transmission process the watermarked image could be attacked (intentional or unintentional). The extractor will extract the embedded watermark and compare with the original watermark to verify its integrity. Any modification or small change in the watermarked image should be noticeable at the receiver side. This application requires fragile watermarking approach [Coatrieux 13] [Wong 98].

1.3.5 Tamper detection
Tamper detection is very critical in some fields as telemedicine in order to fight against counterfeiting of images. The hacker tries to tamper the watermarked image in unnoticeable way, where the normal
user thinks it is un-tampered. The embedded watermark should be extracted by the authorized user. The user has to know if the image is attacked or tampered and where the tampering happened. It is desirable of the approach to be a reverse approach, which means the technique can recover the original content after the watermark extraction. The watermarking system should be fragile [Tan 11] [Fridrich 98] [Lin 05].

1.4 Domains of image watermarking

**Watermarking based on spread spectrum**

The spread spectrum is a technique that is used in radio telecommunications in particular the military to disperse a signal over a wide band frequency so as to make it discreet and resistant to interference [Wong 09]. It is clear that this model is immediately applicable to multimedia watermark.

We describe the approach proposed by [Bender 96] which is based on a pseudo pre-formatting the data to be embedded by dividing it at the image size. It then generates a random key of the size of the pre-formatted data and then applies a simplistic term binary operator "XOR" of this key and the spread data. It add the result to the host image for a sharp image.

This is particularly interesting because it allows to expose several fundamental concepts of image watermarking algorithms namely the spread spectrum, the fact of using a secret key, amplitude modulation, etc ...

The watermarking system embeds the watermark information into the host image. There are many ways and techniques to embed the watermark or to extract it. Based on the algorithm and the way used to embed the watermark in the host image and to extract the embedded watermark from the watermarked image, we can classify the watermarking techniques into two main categories: spatial domain and transform domain with some of existing techniques as we illustrate in figure 1.5 [Mousavi 14]. In the next section, we will discuss the techniques in each domain.
Chapter 1: Digital Image Watermarking

1.4.1 Spatial domain

The *spatial domain* refers to the fact that the watermark information is embedded directly into the host image pixels. The most common use is to embed the watermark in the least significant bit of the host image. The spatial domain techniques are fast, with low complexity and high capacity. Moreover, it is possible to embed small watermark several times in the original host, so after the attacks, the authorized user can recover the watermark from the other. In case of removing the watermark, the possibility to remove the all watermark is very low [Su 13] [Thanh 14].

The weakness of the spatial domain in geometric attacks, especially in the noisy and compression attacks, is that the watermark can be easily changed by a third party [Su 13]. There are many watermarking approaches applied in the spatial domain. We will review some of the common techniques in the following section.

**1.4.1.1 Least significant bit (LSB)**

Least Significant Bit (LSB) is known in the signal sample. It is exchanged in the input signal by embedding data bit in the least significant bit for the pixels. LSB is unnoticeable by the human eye. The basic idea for LSB, is to present the pixel value into binary representation in 8 bits, then the LSB value is replaced with the watermark value: 0 becomes 1 and 1 becomes 0. Then the modified binary
values are converted into decimal pixel values. In fact, the change is to add or to subtract 1 to the bit value. This change will not affect to the image quality and will not be perceptual. This technique is extremely sensitive to changes and insecure in case of attacks such as noise, rotation, compression or even the act of removing all the least bit [Agung 12] [Chopra 12] [Bajaj 14].

Let us assign the bit position from 1 to N, where N is the number of bits used to represent the data. LSB will be the bit number 1 while the N represents the Most Significant Bit (MSB) as we illustrated in the following figure (figure 1.6).

<table>
<thead>
<tr>
<th>Bit Position</th>
<th>N(MSB)</th>
<th>2</th>
<th>1(LSB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original value (149)$_{10}$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Watermarked value (148)$_{10}$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 1.6: LSB watermarking approach

In [Jain 14], the authors presented an invisible watermarking technique based on the LSB. The approach steps are calculating the height and width of the original image and the watermark image, and then scaling the original with scaling factor. After that, they generate a watermark object. Then embedding the watermark LSB set into the original LSB set.

1.4.1.2 Local binary pattern (LBP)
This approach is used for texture analysis and classification [Ojala 02]. In LBP watermarking, the image is separated into non-overlapping square blocks, then the local pixel difference is obtained by calculating the spatial relative between the significant pixel and its adjacent pixel in each block. The local pixel difference is used for embedding and extraction of watermark and it is considered as the threshold. The advantages for LBP over LSB are the robustness against luminance modification, difference alteration and other attacks, and the weakness to other attacks such as filtering and blurring. LBP can be used in semi-fragile watermarking techniques [Sachnev 09]. Figure 1.7 illustrates the general idea of local binary pattern of eight neighbours. The LBP of $D_s$ is calculated from its neighbours, while the embedding and extraction place is $D_s$.

![Figure 1.7: Local Binary Pattern of eight neighbours.](image-url)
In [Wenyin 11], a framework based on the Local Binary Pattern (LBP) in order to embed multi-level watermarking is proposed. The approach divided the image into non-overlapping 3 by 3 regions. Each local region is divided into three items: a vector containing the central pixel values, a vector containing the magnitude obtained from the differences between the central pixel and its neighbors and a vector of the sign value of the differences. The obtained vector's values are based on the Local Binary Pattern (LBP). The watermark is embedded by changing of the sign vector value in a local region. The approach was robust against some kinds of attacks like noise, contrast adjustment, luminance modification.

1.4.1.3 The histogram modification
This technique extracts the general features of the original image. These features are considered as a watermark to be embedded in the host image. A histogram is built based on pixel values. Following this method, we modify the values between the maximum and minimum points of the histogram to implement the data hiding. It provides an easy watermarking, but the capacity is limited by the number of points that is having the maximum value [Lin 06] [Fang 06] [Yoo 09].

In [Pun 14], Pun et al. proposed a geometric watermarking approach based on the histogram modification. They extracted the reliable features from the original image using the Adaptive Harris Detector with Simulated Attacks (AHDSA) method. They applied simulated attacks to the original image to obtain the attack simulated image. Then, they determined the response threshold value in order to extract others features. The threshold was 20. AHDSA also provided them with the information about the location where the watermark should be embedded. This information is used as a key during the extraction process to determine the watermarking location. The extracted features and the watermark image have been embedded and extracted using a histogram based algorithm. The approach survived to geometric attacks like rotation, scaling, compression with low percent, cropping with percent up to 36%. The approach provided them with a capacity up to 128 bits. The image quality was decreased with the increasing of the capacity.
1.4.2 Frequency domain
The frequency watermarking techniques are considered more robust than spatial watermarking
techniques. Frequency domain or transform domain is more complex in computational complexity
than spatial domain. The embedding and extraction process of all watermarking approaches in the
frequency domain can be described as follows:

- The embedding process includes the image decomposition, watermark embedding and reversible
  image decomposing.

- The extraction process includes the image decomposition, watermark extraction and reversible
  image decomposition.

Among the frequency domain watermarking techniques, we can mention Discrete Wavelet Transform
(DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) as the most known
methods in the frequency domain. In the following section, they will be discussed in details.

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

For one level DWT, the image is decomposed into four sub-bands: Low-Low (LL), Low-High (LH),
High-Low (HL) and High –High (HH). In the case of two levels DWT decomposition, it produces
another four sub-sub-band from the sub-band. We can reverse the approach by applying the inverse wavelet decomposition (IDWT). Figure 1.8 presents the general diagram of the second level wavelet decomposition.

![Figure 1.8: 2-level- DWT decomposition](image)

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

\[ i_{w_n} = i_n + s \cdot i_n \cdot w_n \]  \hspace{1cm} (1.1)

where \( n \) is the watermark strength factor, \( s \) is the watermark embedding position, \( i_{w_n} \) is the watermarked image, \( i_n \) is the original image and \( w_n \) is the watermark image.

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

In [Ahmad 14], Ahmad et al. proposed non-blind watermarking techniques in the frequency domain in three levels DWT. The watermark is embedded in the low frequency sub-band using blending technique. In the embedding phase, three level DWT is applied to the original and the watermark image. Then, they embed the watermark in the original image by using the linear interpolation (1.2)

\[ i_{w_{13}} = k \cdot i_{13} + q \cdot w_{13} \]  \hspace{1cm} (1.2)

where \( i_{w_{13}} \) is the third level DWT watermarked image, \( k \) and \( q \) are factors, \( k, q \in ]0,1[ \), \( i_{13} \) is the third level DWT watermark, \( i_{13} \) is the third level DWT original image.
Chapter 1: Digital Image Watermarking

The inverse DWT (IDWT) is applied to obtain the watermarked image. In the extraction phase, three level DWT is applied to the watermarked image and the original image. Then, by using the linear interpolation 1.3 can retrieve the embedded watermark or by 1.4 to retrieve the original image.

\[ R_{wl3} = i_{wl3} - k * i_{l3} \]  \hspace{1cm} (1.3)

\[ R_{l3} = i_{wl3} - q * w_{l3} \]  \hspace{1cm} (1.4)

where \( R_{wl3} \) and \( R_{l3} \) are the low frequency retrieved watermark, low frequency retrieved original image, respectively.

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

In the work of [Basheera 11], it is proposed a blind watermarking technique. The watermark is embedded as a secrete medical information into host color image using DWT. The watermark is embedded in the low level (LL) sub bands of the blue channel of the original image. The embedding process is: decomposition of the host image into three color channels, embedding of the watermark into the LL sub band of the blue color channel of the host image based on discrete wavelet transforms (DWT) three levels. Then, they compressed the data with Zigzag techniques to convert two dimensions to one dimension image. Finally, inverse DWT is applied to obtain the perceptual watermarked image. In the extraction process, the watermarked image is decomposed based on DWT, the LL sub-band is divided into three color channels. The blue channel is chosen. Then inverse Zigzag technique is applied to obtain two dimension blue channel image. Finally, inverse DWT is applied to achieve the watermark image. The experimental result shows that the method is imperceptible and gives a high quality without attacks. But it also shows that the method has a low robustness against cropping, filtering and noising attacks.

[Maneesha 15] proposed a digital image watermarking technique in the frequency domain based on DWT. The original image and the watermark image are decomposed into two levels DWT. Then, they
calculated the image feature matrix and applied hash function for each sub-bands (LL, LH, HL, HH). Then, based on XOR function, they embedded the watermark into the original image. Finally, the inverse DWT is applied. The image features are analyzed into its factored form using DWT. The produced coefficient data are quantized to obtain the image hash. The proposed approach achieved high PSNR (good quality) with low computational complexity and execution time.

1.4.2.2 Discrete cosine transform (DCT)
DCT transforms a signal from the spatial domain to frequency domain [Paunwala 12]. It provides a high robustness against the JPEG standard for image compression [Tataru 12]. It transforms the image into non-overlapping m × m blocks where the left top coefficient is DC coefficient value and the others are AC coefficients [Laouamer 12]. Normally, the block size is 8 by 8 items. The human eyes are more sensitive to low frequencies than high frequencies. DCT splits the image into three different frequency bands: low, middle and high frequency. The low frequency contains the major information about the image while the high frequency contains the image details. If the watermark is inserted in the low frequency, the watermark will be robust but visible. Meanwhile, if it is inserted in the high frequency, the watermark will be invisible but less robust. So, the appropriate band is to embed the watermark in the middle frequency to avoid the image degradation and swap between the imperceptibility and robustness [Laouamer 15].

The DCT coefficient transformation of the signal is represented in the equation 1.5, while the inverse discrete cosine transform is represented in the equation 1.6 [Laouamer 12]

\[
F(u, v) = \frac{2}{N} c(u)c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x, y) \cos \left( \frac{\pi}{N} u(x + \frac{1}{2}) \right) \cos \left( \frac{\pi}{N} v(y + \frac{1}{2}) \right) \tag{1.5}
\]

\[
f(x, y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u)c(v)F(u, v) \cos \left( \frac{\pi}{N} u(x + \frac{1}{2}) \right) \cos \left( \frac{\pi}{N} v(y + \frac{1}{2}) \right) \tag{1.6}
\]

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

Figure 1.9 illustrates the general idea of the obtained image matrix after applying the DCT transform.
Chapter 1: Digital Image Watermarking

The DWT transform is more suitable to human visual system than DCT transform. Also, DWT provides a multi-resolution decomposition, which can be shown at different levels of resolution and sequential procedures from low to high resolution. The DCT is based on a block which is not the case for DWT. Whereas, a higher compression ratio will affect in the blocks, and the visual artifacts are less evident in DWT than DCT. Meanwhile, DCT is a fully transforms frame which means any modification will be noticeable through the whole image while in DWT it is noticeable only locally [Potdar 05].

The work in [Li 12] proposed a blind zero watermarking approach on the medical image features based on DCT. In the process the original image is transformed to DCT coefficients, then the 9 lowest frequencies are chosen: F(1,1),...,F(1,9). The value of low frequency coefficient is changed after attacks, but the vector of the signs of the coefficients remained unchanged even with strong geometric attacks. The feature vector is then generated. After that, watermarking and feature vector are used to generate the key sequence. The binary key sequence is computed by a HASH function. The key should be stored for using in the extraction process. One is used to represent positive or zero coefficient value while zero is used to represent a negative value for coefficients. In the extraction phase, the feature vector is generated. It consists of the signs sequence of the DCT coefficients. Then, the watermark is extracted by using the embedding key is extracted.
Chapter 1: Digital Image Watermarking

The experimental results prove that the algorithm was robust and could detect the watermark without attacks, and with some common attacks (non-geometric attacks). But in the case of noise attacks, the image quality is not acceptable where the PSNR is around 10. In case of the filter attacks, the PSNR is around 20. Also, for JPEG attacks the PSNR is around 20. In geometric attacks, such as rotation and translation attacks PSNR are respectively around 12 and 13 dB. Moreover, the method provides a satisfying capacity; the computational complexity and the memory use are low.

The authors in [Lin 09] proposed a novel blind watermarking technique based on the DC components in the spatial domain. They merged the frequency and spatial domains in order to get better robustness and security for color host image. The proposed algorithm keeps the distribution features of the frequency coefficients and it has avoided the error resulting from the frequency transformation. The embedding steps were converting the image from RGB color into YCrCb color. Then, after obtaining the luminance Y of the YCrCb, dividing it into overlapped 8 × 8 pixel blocks. The method computes the DC coefficient $C_{i,j}(0,0)$ of each block. Based on the watermark information it decides the modifying magnitudes $T_1$, $T_2$. The possibility quantization can be computed by modifying magnitude $T_1$, $T_2$ and calculating the value for watermark embedding in DC coefficients for each block. Finally, the watermarked image is converted from YCbCr color into RGB color. In the extraction phase, the watermarked image is converted into YCrCb. Then, the luminance Y is obtained, and divided into $8 \times 8$ blocks. Next, the DC coefficient is obtained and the watermark value is computed. Finally, the inverse Arnold transform is applied to obtain the extracted watermark image. SSIM is used to measure the imperceptibility between the host image and the watermarked image (HVS). The proposed algorithm had high watermark invisibility and robustness against non-geometric attacks like JPEG compression and filter and geometric attacks like cropping, scaling, and rotation.

1.4.2.3 Singular value decomposition (SVD)

Singular Value Decomposition SVD is another frequency transformation method. It is a linear arithmetical implementation to decompose a matrix into its eigenvectors and eigenvalues. It has been widely used in the compression field cause its capability to provide the low rank calculation by alteration of an image into a new representation [Ranade 07]. The SVD can decompose a set of
connected variables into unconnected variables. Moreover, singular values of an image are satisfying constancy, that is, when a small degradation is added to an image, it SV’s do not modify significantly; and SV’s represent mainly algebraic image features [Liu 02].

Let us denote the image as $I$. $I$ is a square image, $N$ and $M$ are the image dimensions. The SVD of $I$ is defined as:

$$I_{N \times M} = U_{N \times N} \ast S_{N \times M} \ast V_{M \times M}^T \quad (1.7)$$

Where $U$ and $V$ are orthogonal matrices and $S$ is a diagonal matrix.

The matrix $U$ contains the left eigenvalues (left SVs) and the matrix $V$ contains the right eigenvalues (right SV’s), while the $S$ matrix contains the eigenvalues (SVs). These singular values are arranged on the diagonal by a descending order where the highest value is the top left of the matrix while the lowest value is right down of the matrix. In watermarking schemes, after decomposition by SVD and embedding the watermark in a chosen matrix, the inverse SVD is applied to get a meaningful image.

In [Lei 14], the authors proposed a blind reversible watermarking scheme in order to ensure copyright protection of medical images. The approach uses the Recursive Dither Modulation (RDM) and the Differential Evolution (DE) optimization. They inserted double watermark into the original image. Watermark embedding steps divide the original image into blocks. Then, scrambling algorithm is applied to both signature and logo data with an encryption algorithm to produce encrypted watermark text. Two levels wavelet transform were applied to each block and selected the low frequency coefficients. SVD was applied into low frequency wavelet coefficient for each block. The watermark was embedded by quantization using the RDM approach. After the embedding, inverse SVD and inverse DWT were applied to obtain the watermarked image. In the extraction phase, the watermarked image was divided into blocks. Then, two level DWT was applied. SVD algorithm was applied in the low frequency blocks to generate the singular values. Later, the singular values are normalized and the message shuffled, reshuffling the extract shuffled message. This last one was applied to obtain the watermark. The authors achieved a good balance between robustness, imperceptibility and capacity. The algorithm has a high computational complexity.
Chapter 1: Digital Image Watermarking

Benhocine [Benhocine 13] proposed a new implementation of the SVD technique in the embedding and extraction process of an image watermarking approach. The authors purposed it to achieve a high robustness against geometric and non-geometric of attacks. They embedded the watermark in three cases of SVD. The first case was embedding the watermark in the three SVD matrices (U, S, V). The second case was embedding the watermark in U and V matrices. The third case was embedding the watermark in S matrix. The embedding is done using the linear interpolation 1.8

\[ SVD_{tw} = (1 - t)SVD_w + t * SVD_i \]  

where SVD represents the S, V and U matrices of the watermarked image, SVD\textsubscript{w} represents S, V and U matrices of the watermark image. SVD\textsubscript{i} represents S, V and U matrices of the original image. \( t \in ]0,1[. \)

For the extraction process, it was done using the following linear interpolation (1.9)

\[ SVD_{wa} = \frac{1}{t}SVD_{wi} - \frac{1-t}{t}SVD_{twa} \]  

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

Some of the research works hybrid the techniques in the same domain or in different domains. For example, [Nema 14] and [ElGamal 13] hybrid DWT and DCT in the transform domain. The work of [Jose 12] combines DWT, DCT and SVD, while the works in [Lenarczyk 13], [Oueslati 13] combined the spatial and frequency domain into image watermarking approaches.

1.5 Visible image watermarking

1.5.1 Visible image watermarking techniques

The watermarking techniques can be classified based on the human visual perception. The watermark can be embedded in a visible or in an invisible way. In some applications, two watermarks are...
embedded in the host image, one in a visible way and the other in an invisible way. This technique is
called a dual watermark technique. One interest of this technique is that, if the visible watermark is
attacked, the authorized user can retrieve the invisible watermark. Some applications require the
watermark to be visible. This is for example the case of a logo of T.V. channel. The embedding
visible watermark in the host signal will affect and degrade its quality. So the reverse watermarking
technique is advisable with the visual watermarking in order to allow the authentic user to remove the
embedded data and reestablish the original data. The main goal of the visual watermarking approach
is to identify the ownership and the rights [Mousavi 14].

1.5.2 Visible image watermarking applications
In this section, we are reviewing some visible watermarking techniques. The visible watermark is
desirable for fragile and semi fragile watermarking approaches. Moreover, it is used to improve the
integrity, ownership, authenticity and tamper detection

The authors in [Hsu 14] proposed a visible reversible watermarking technique. The watermark is a
binary image while the original image is a grayscale image. They add to the original pixel values the
watermark values directly. Then, the watermark information is hidden in the gray scale (watermarked)
image in an invisible reversible steganography method. In extraction and reconstruction phase, the
embedded watermark information is extracted and the watermarked image is reconstructed from the
received image. After that, the watermark information is used to recover the original image. The
authors provided double watermarking at the technique, the first one to watermark the original image
in a visible way and the second one to hide the watermark information in an invisible way in order to
recover the original image. In order to reduce the image size the authors compressed the first
watermarked image before doing the invisible hiding steganography. The experimental results show a
tradeoff between the watermark size and image distortion.

In [Weng 13], it is proposed visible reversible watermarking approach in order to protect the content
integrity. The watermark is divided into many sub watermark images and the original host is a group
of dynamic images. In steps are a capture of images, division and embedding of the watermark,
generation of identification information and recovers and detects of the image. The generation of
identification information can be used to produce the hash value avoiding tampered watermarks. Moreover, the recovery and detection of image steps are used to ensure that the watermarked is recovered lossless and that the watermark is completely extracted. The proposed approach is a desirable solution for copyright protection and tamper detection. It can confirm the data integrity.

The work in [Tsai 10] presents a visible reverse watermarking approach in order to improve the original data authenticity and transparency. The approach comprises three stages: visible watermarking, protection and transparency compromise and reversible data embedding. In the visible watermarking, the watermark is embedded in the original image based on the pixel value mapping function. In protection and transparency compromise, the hash value of the original image is encrypted by the secret key. Then the generated sequence integer which is built from the zero mean and distinction variance is added to the visible watermark. The integer sequence avoids repairing an original image also it overrides the trade-off between transparency and robustness. In reversible data embedding, the authors embedded the recovered data and the authentication data based on the current reversible data embedding system. The authorized user can retrieve the original image while unauthorized user will retrieve the image with the added integer values noise.

1.6 Digital image watermarking attacks and robustness
The robustness is the strength of the watermarking approach against the general attacks. The robust watermarking preserves the watermark through the transmission process. If intentional or unintentional attacks are happening, the authorized user can retrieve the watermark with high quality. This aspect is necessary in copyright application, the ownership issues and the medical application. The common and image processing attacks will be discussed. Moreover, some of the watermarking approaches that focus on robustness will be presented.

1.6.1 Digital image watermarking attacks
The attack is this process aiming at destroying, manipulating and impairing the detection of the embedding watermark. Watermark attacks include unauthorized embedding, unauthorized detection, unauthorized removal and system attack. Known Original Attack (KOA) happens to watermarked and
original content. Known Message Attack (KMA) happens to watermark contents and hidden messages. Watermark Only Attack (WOA) happens to watermarked contents [Kavadi 12], [Voloshynovskiy 01], [Malshe 12], [Song 10] classified the watermark attacks into four categories explicitly Removal Attacks, Geometric attacks, Cryptographic attacks and Protocol attacks.

Removal attacks are those removing the watermark from the watermarked image, but they do break the security of the watermarking algorithm. Also, they preserve the content so the cover image is still available after the end of the attacks. After a removal attack are cannot rebuild the watermark image from the attacked watermarked image. Examples of these kinds of attacks are noisy (Gaussian, Salt and Pepper, uniform), compression (JPEG, JPEG 200), filtering (Mean, Median, Gaussian), histogram and sharpness attacks.

Geometric attacks are different from the removal attacks. Geometric attack aims to destroy the watermark image rather than to remove it from the watermarked image using the geometric distortion. It is still possible to rebuild the watermark after the geometric distortion if the detail of the attack can be built. The method to correct this kind of attacks is called synchronization. Examples of these kind of attacks are cropping, rotation, translation, skewing.

Cryptographic attacks aim to destroy the security feature in the watermarking system, then to find how to remove the watermark embedded and try to embed a deceptive watermark. The example of this kind is the brute-force search method which tries to break the watermarking security by using a large amount of the possible meaningful security information. Another example is an Oracle attack which is trying to create a non-watermarked image at the decoder side if the decoder policies are accessible.

The protocol Attacks are aiming to add the attacker watermark in the watermarked image rather than to destroy or remove the watermark image and it will give the attacker the right in the ownership of the cover image. Moreover, it can estimate the watermark image from the watermarked image and copy it to another data called target attack.
Chapter 1: Digital Image Watermarking

There are different software in order to apply different kinds of attacks, especially geometric and non-geometric attacks such as Checkmark [Voloshinovskiy 01], Optimark [Solachidis 01], Certimark [CER 00], ….. The most known and used is Stirmark [Petitcolas 98, Kutter 99].

1.6.2 Robust image watermarking approaches

In [Subramanyam 12], Subramanyam et al. proposed a robust watermarking of compressed media for tamper detection, ownership declaration, or copyright management purposes. The proposed technique is dividing the input image into non-overlapping rectangular tiles. Then, it is applying the DWT technique. In result, multiple levels of DWT give a multi-resolution image, the lowest resolution contains the low-pass image, higher resolution contains the high pass, the resolution is divided into smaller blocks known as code-blocks, and each code encodes independently. The extraction of the watermark was done after decryption of the image. They analyzed payload capacity and quality of the image for different resolutions. The experimental results showed that the higher resolution carries a higher payload capacity without affecting too much the quality, and middle resolutions carry lesser capacity and leads to more degradation in the quality. This approach is weak against noise and filtering attacks.

In [Moghaddam 13], the authors applied new robust blind watermarking techniques based on an imperialist competitive algorithm (ICA) in the spatial domain. Firstly, the approach determines the location in the host image to be selected based on modified ICA. Secondly, 5 by 5 neighbors of the modified block are chosen and the least significant color in the neighborhood of each pixel is selected for embedding, then the best neighborhood which will increase the quality of the watermarked image is selected. The proposed approach is applied in the spatial domain in order to find the optimal position of embedding. It is robust against some kinds of attacks, but it is still weak against compression and sharpening attacks.

Wang et al. [Wang 14] improved the sample projection approach in order to achieve copyright protection. In this approach, they produced the enhancement of the code lines by inverting the sample projection approach. The improvements considered two aspects: lower distorted code lines and constructing long line segments. Lower distorted code line purpose is to reduce the distortion during
the embedding process, while constructing the long line segments provides more robust and secure to prevent the unauthorized user from guessing the watermark. This approach was developed from a previous approach of sample projection. It is considered better in robustness against Gaussian, filter and compression, but weak against rotation salt and pepper noise, and AWGN noise.

The work in [Gu 13] proposed new reversible and robust watermarking approach. They used the chaotic map scheme in order to find the optimal embedding position in the original image and also to find a threshold space of reversibility. These threshold works as adaptability between reversibility and robustness aspects. The approach crops the original image into a smaller image. The obtained image is divided into non-overlapping blocks with size $6 \times 6$. The chaotic map is iterated using equation 1.10 to avoid the damaging result algebra fraction operation

$$x_{n+1} = 4x_n(1 - x_n)$$  \hspace{1cm} (1.10)

where $x_n$ is the parameter of $n^{th}$ iteration and $x_0$ is given.

The integer wavelet decomposition (IWT) one level is applied. The low level sub bands with size $3 \times 3$ for each block are chosen and the number of the optimal position in the LL is obtained using the equation 1.11:

$$n = \text{mod}(x_n \times 10^{14}, 9) + 1$$  \hspace{1cm} (1.11)

where $n$ starts with 5 which is considered the central pixel of the LL block. After finding the embedding position, the watermark is embedded. Then, inverse integer wavelet transform is done for each block with the new value of the LL sub band. The watermarked image is gotten. In the extraction phase, the initial values of the $x_0$ in the chaotic map and the chaotic map are assigned and they are the same value that is used in the embedding phase. Repeating the embedding steps including the cropping of the watermarked image, smaller image is obtained by applying IWT to get $3 \times 3$ low level blocks. The optimal numbers of $n$ are found and the embedding position is gotten. Then, extract the watermark from the obtained position. The approach achieved a balance between the reversibility and the robustness. Moreover, the threshold values control the robustness and reversibility, but if the
threshold is equal to 40 the approach is not reversible. The highest robustness is obtained when the threshold is equal to 12.

In [Thabit 14], the authors are presented a robust and lossless watermarking approach. The approach is based on the Slantlet Transform (SLT). After the modification of the sub band coefficient, the watermark will be embedded in the high frequency sub band. The approach is applied in the color medical image, general image and synthetic aperture radar image domain. The watermark can be embedded in three channels of image colors in order to achieve enough capacity. The embedding steps are the following: divide the original image into blocks. Then, apply the SLT decomposition for each block using the equation 1.12:

\[ S = SLT_N \times SLT_N^T \]  

(1.12)

where \( s \) is the original image dimension, \( S \) is the SLT decomposition, \( SLT_N \) is \( N \times N \) SLT matrix.

After the SLT decomposition, the high frequency (low-high and high low) sub band is chosen. After, calculating the mean value for each sub band, they modified the difference between the mean values of the SLT coefficient in the high frequency band. The watermark was a bit and when the value of this bit is 1, the mean value of the high-low sub band SLT coefficient is more than the mean value of the low-high SLT coefficient. While the value of the watermark is 0, the mean value of the low-high SLT coefficient is more than the mean value of the high-low sub band SLT coefficient. Then, the inverse SLT is applied to get image block and pixel adjustment to obtain the watermarked image. In the extraction process, the watermarked image is divided and the SLT decomposition is applied. Calculate the mean value for each block of the coefficient in the high frequency. Then the watermark will be extracted based on the mean value of the SLT coefficients. If the mean value of the SLT coefficient of the high-low sub band is larger than the mean value of the SLT coefficient of the low-high, the watermark will be one. But if the mean value of the SLT coefficient of the low-high sub band is larger than the mean value of the SLT coefficient of the high-low, the watermark will be zero. The proposed approach provided high quality, capacity, imperceptibility and robustness against intentional and unintentional attacks.
1.6.3 Fragile image watermarking approaches

A fragile watermarking is a watermarking which cannot accept the modification or the changing of the image, and for which the watermark is destroyed in case of a modification. It is used for content authentication, integrity and tamper detection applications. We can classify the fragile watermarking into: hard and soft authentication. The hard authentication doesn’t allow the changing even if it is occurring from the authorized user and the watermark will be broken. While the soft-authentication accepts slight modification from the authorized user, but the watermark is broken and damaged against intentional and dangerous attacks. Semi-fragile watermarking is also called a soft authentication [Mousavi 14] and [Malshe 12].

In [Walia 13], proposed a watermarking technique in the spatial domain is presented. The work is based on Weber law and its two properties: differential excitation and orientation. The authors divided the image into $3 \times 3$ blocks. Then, they computed the differential excitation of the center pixel with its 8 neighbors. The positive excitation value of the neighbor’s pixel is selected. Finally, the watermark is inserted and the selected pixel intensity is modified.

The proposed technique has a high imperceptibility; it is sensitive to noise attacks like a Gaussian. It can tolerate compression attacks (JPEG) which are less than 15% compression rate. The localization of the altered region by cut and paste attack was satisfying. It is useful in the hard authentication application.

The authors [Al-Otum 14] have proposed a semi fragile watermarking technique for authentication and tamper detection of gray scale images. The proposed approach is based on a discrete wavelet decomposition algorithm modification. The modification is based on expanded bit multi-scale quantization. The watermark is a random bit sequence and it is expanded into three same watermark values to be embedded in three different spaces. Two level DWT is applied and the low frequency sub band is chosen. The watermark is embedded into $LL_2$, $LL_{HL_1}$, $LL_{LH_1}$. The embedding steps are the following: The original image is divided into $4 \times 4$ blocks using wavelet decomposition. A second decomposition level of wavelet transform is applied in order to build the host matrix. Then, a quantization function is applied for each matrix to obtain the quantization value for each matrix. The
watermark is embedded in the host matrix. In the extraction phase, the same embedding
decomposition is applied to the watermarked image. Then, the watermark is extracted. The proposed
approach is a suitable for the tamper detection and perfect authentication. It can find the tampered
blocks and then location. The approach doesn’t cite the geometric attacks.

1.7 Image quality measurement
The objective image quality metric shows a difference of roles in image processing uses. Firstly, it
may be used to monitor and regulate image quality, such as to evaluate the transmitted image through
the internet to control and allocate the resources. Secondly, it may be used to optimize the process and
settings of image processing methods. For instance, the evaluation metric can support the optimal
design of pre filtering and bit task algorithm at the encoder. Meanwhile, it supports the decoder in
optimal reestablishment, error hiding and post filtering system. Finally, It may be used to benchmark
the image quality processing approaches and algorithms [Wang 04].

The image quality can be measured for the watermark or the original image in order to assess the
watermarking system. Image quality can be valuated using different methods. The optimal manner to
make the visual experiment under controlled conditions is such that the human viewers can note the
image quality degradation. Image quality assessment evaluates the original image by comparison with
the watermarked image in order to see how the embedding effect on the image quality. Moreover, the
assessments evaluate also the extracted watermark by comparing with the original watermark to
measure the approach robustness [Dumic 14].

The objective quality assessments can be classified according to the reference image into three
categories: full reference, non-reference and reduce reference. The full reference is the reference
following which the evaluated image exists during the evaluation. If the evaluation is done without
the original (reference) image, the evaluation is called non-reference or blind. In reduce reference, the
original or reference image does not exist, but the extracted features information about the reference
image is offered during the evaluation [Wang 04].
In the evaluation way, some of the existing techniques are based on pixel evaluation are: Mean Square Error (MSE) [Wang 09] [Tan 13], Peak Signal to Noise Ratio (PSNR) [Tanchenko 14] [Chauhan 13]. Some of them are based on the structural distortion like Structural Similarity (SSIM) [Rehman 12] [Zengzhen 14] [Tan 13]. In the following section, we are reviewing the most common algorithms in the watermarking image quality measurements.

1.7.1 Mean square error (MSE)
The mean square error is the average of the squared intensity differences between the original image and the watermarked image or between the extracted watermark and the original watermark. It is commonly used in the image quality measurements, because it provides a good approximation of the image quality degradation, it is fast in applying and easy in computing. To compute the MSE between two images, the following equation is used:

\[
MSE(I, I_w) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I_w(i,j))^2
\]

where \(I\) and \(I_w\) are the original image and the watermarked one, respectively. \(m\) and \(n\) are the images size [Wang 09].

1.7.2 Peak signal to noise ratio (PSNR)
The PSNR is a distortion measure used in digital image, specifically in any image compression. It consists in quantifying the performance of the encoder by measuring the quality of reconstruction of the compressed image compared with the original image. PSNR is defined by:

\[
PSNR(I, I_w) = 10 \log_{10} \left( \frac{P}{\text{MSE}} \right)
\]

where \(P\) is the image depth. PSNR is depending on the MSE value of the reference image and the watermarked image. If the PSNR value is greater than 30 dB, the image quality is acceptable. A higher PSNR value means that the similarity and fidelity between the two images are better and the degradation and the distortion are lower [Tanchenko 14].

1.7.3 Structural similarity index measurement (SSIM)
PSNR and MSE quality measurement tools are based on the bit errors between the original and distorted images. There are full reference tools and statistical average in the evaluation, where the evaluation is obtained to be closer to the human visual system (HVS). SSIM is a quality measurement
tool based on the structural similarity. The system of similarity measurement is comparing three components of each signal the luminance \( l \), contrast \( c \) and structural \( s \) [Wang 04].

The luminance \( l \) is computed based on the following equation:

\[
l(m, n) = \frac{2\mu_m\mu_n + C_1}{\mu_m^2 + \mu_n^2 + C_1} \quad (1.15)
\]

where \( m \) and \( n \) are two nonnegative images. \( \mu_z \) is the mean intensity of the image \( z \) and \( C_1 \) is small contrast and very close to zero.

To compute the second comparison of the structural similarity, the contrast of each image is calculated as the following equation:

\[
c(m, n) = \frac{2\sigma_m\sigma_n + C_2}{\sigma_m^2 + \sigma_n^2 + C_2} \quad (1.16)
\]

where \( \sigma_z \) is the standard deviation of the image \( z \), \( C_2 \) is small contrast and very close to zero.

The structural comparison is defined by the following equation

\[
s(m, n) = \frac{\sigma_{mn} + C_3}{\sigma_m\sigma_n + C_3} \quad (1.17)
\]

where \( \sigma_{mn} \) is the covariance between image \( m \) and image \( n \), \( C_3 \) is small contrast and very close to zero.

After calculating the three components, we combine them and the SSIM is defined as follows:

\[
SSIM(m, n) = l^\alpha . c^\beta . s^\gamma
\]

\[
SSIM(m, n) = \left(\frac{2\mu_m\mu_n + C_1}{\mu_m^2 + \mu_n^2 + C_1}\right)^\alpha \cdot \left(\frac{2\sigma_m\sigma_n + C_2}{\sigma_m^2 + \sigma_n^2 + C_2}\right)^\beta \cdot \left(\frac{\sigma_{mn} + C_3}{\sigma_m\sigma_n + C_3}\right)^\gamma \quad (1.18)
\]

where \( \alpha > 0 \), \( \beta > 0 \) and \( \gamma > 0 \) are the parameters to control the relation importance of the three components.

1.7.4 Bit error rate (BER)

Bit error rate also called bit error ratio is the number of receiving bits that have been altered, modified or even destroyed during the transmission process, divided by the total number of transmitting bits. Normally, it is expressed as a percentage. The low percentage value refers to a high quality and low degradation of the received data [Zhang 13].

BER is an efficient measurement tool in signal processing. It is widely used in the watermarking field. BER measures the extracted watermark by correlating to the original watermark to prove the
robustness of the watermarking method, or it measures the recovered image by correlating with the original image. The reliability of the watermark is correlated with the robustness and capacity aspects [Zhang 07].

In the watermarking approach, one measures the extracted watermark bits by correlating to the original watermark bits, in order to determine the degradation percentage in the received data using the following equation:

\[
BER(w, w_a) = 0.5erfc \left( \frac{C_w}{\sqrt{V_{w_a}}} \right) \quad (1.19)
\]

where \(erfc\) is the error function, \(C_w\) is the original watermark and \(V_{w_a}\) is the attacked watermark.

1.8 Conclusion

In this chapter, we have presented a state of the art of the techniques currently used in digital image watermarking. These techniques can be classified according to the method used for the embedding of the watermark or following the embedding area. Depending on the way of embedding, the techniques are considered as belonging either to the spatial domain or to the frequency domain. This state of the art has enabled us to identify the main lines leading to the design of a watermarking system and revealed the diversity of techniques used. However, the robustness of the watermarking is mainly checked visa-a-visa the existing standard attacks. Most efforts have been done towards an adequate management of compromise between robustness and visibility. Moreover, the notion of similarity has been introduced to measure the degree of resemblance between the original watermark and the one extracted after an attack and that allows determining the robustness of watermarking schemes. These measures are often metrics that quantify the proximity of spatial images in their characteristics.

The analysis of previous watermarking approaches has led us to the conclusion that the watermarking approaches in frequency domain still present some gaps against some scenarios of attacks, and also for the imperceptibility which remains a negotiate issue. However, the existing solutions based on spatial domain provide not enough robustness against attacks with high watermark payload. Moreover, the computational complexity in watermark embedding/extraction has to be taken into account especially for a real time application.
Chapter 2 Digital Image Cryptography

2.1 Introduction
The protection of digital information comprises at least two featured problems: security problem and authentication. In the security problem the information has to be protected from the unauthorized users while the authentication confirms that the received data is not affected or modified and original as the intended sender. The cryptology technique proves the security issue by assuming the intended sender and intended receiver has some security aspects called keys. These keys can be the same with the sender and receiver sides (symmetric) or can be different which means the key used at the sender side is different from the key used on the receiver side (asymmetric). The algorithm used in the symmetric encryption is known as a cipher. Encryption algorithms are classified into block and stream cipher depending on the way the data are processed. Moreover, cryptography ensures the security issues such as confidentiality, authentication and reliability. Confidentiality aspect refers to the user who can access to the data, the authorized user who can read the data and the unauthorized user who does not have the permission and the access possibilities to the electronic data. The confidentiality is maintained under using the secret key, so the person who has that key will be able to read the data [Zhu 14] [Eslami 13]. While, the authentication is the action of confirming that the received message is the unaffected and the original sending messages from the sender. The authentication of the digital message proves there is no modifying or altering through the transmission process and received without any tampering [Gong 13] [Rajput 12].

Furthermore, the reliability comprises the integrity and the availability. The integrity is the ability of the authorized user to modify, insert, delete and update the data and detecting the modification happened by the sender or the receiver. So, for each different message there is a different fingerprint encrypted by the secret key. The availability is the property that data can be available for the authorized user to be usable and accessible [Bouslimi 12] [Ran 14].
2.2 Cryptography: definition and principle

Cryptography is the art of encryption and decryption data in order to protect them during the transmission or the storage. The cryptanalysis is the art of studying and analyzing the cryptographic approach [Mel 01]. The cryptography and the cryptanalysis have a robust relative. In the next section, we will discuss the encryption and decryption phases in cryptography domain.

The main goal from the encryption is to insure the security of the sending message by reproducing the message in an unreadable way and sending it in the unsecure channel. The decryption phase consists in rebuilding the original message from the encrypted one. The general encryption and decryption scheme can be summarized in two phases as shown in figure 2.1: the encryption is denoted by \( E \) and the decryption \( D \), where \( D \) is the reverse of \( E \). The sender encrypts the original data \( P \) (the plain text), then transmits the encrypted data.

![Figure 2.1: The general encryption and decryption diagram](image)

By \( C \) we denoted the cipher text through the channel where \( C = E(P) \). At the receiver side, the receiver decrypts the cipher text \( C \) to rebuild the original message \( P \) where \( D(C) = P \).

2.3 Cryptography classification

Cryptographic approaches can be classified into three main categories: symmetric, asymmetric and hash function. All of them depend on certain factors called keys [Kotulski 97]. The symmetric encryption uses one key called private key, for both encryption and decryption processes. The asymmetric encryption uses two keys: one of them, called public key is used through the encryption process, the other called the private key, is used through the decryption process. Symmetric encryptions can be divided into two categories: block cipher and stream cipher encryption. The hash
function encryption can be divided into: *keyed hash function* and *un-keyed hash function*. In the cryptography classification section, we will discuss the encryption algorithms categorization in detail.

We present, according to [Menezes 97], the three categories: symmetric, asymmetric and hashed key as shown in figure 2.2.

![Figure 2.2: Cryptography main area](image)

### 2.3.1 Symmetric cryptography

Symmetric cryptography is also called single key because it uses one key in both the encryption process and the decryption process [Kahate 13]. Figure 2.3 illustrates the general process of encryption and of decryption based on symmetric technique. The sender encrypts the plain text using the encryption algorithm and the secret key to provide the ciphered text, while the receiver decrypts the ciphered text based on the decryption algorithm and the same secret key to get the original text. In the symmetric technique, the secret key that is used for the encryption and the decryption processes is the same. The security in the symmetric cryptography is based on the algorithm and the shared key [Mel 01]. The drawback in the symmetric techniques is that it is difficult to share the key in a secure way. The most known examples of the symmetric techniques are DES [Standard 99], AES [Chown 02], IDEA [Leong 00], RC4 [Gupta 14]. The general diagram of the symmetric encryption and decryption process can be summarized in the following equations:

\[ E_k(P) = C \quad (2.1) \]

\[ D_k(C) = P \quad (2.2) \]
where $E$ is the encryption algorithm, $P$ is the plain text, $C$ is the ciphered text, $k$ is the secret key and $D$ is the decryption algorithm.

The symmetric techniques can be divided into two categories: stream cipher and block cipher.

### 2.3.1.1 Stream cipher
In the stream cipher, the plain data will be a stream of data like bit or byte. It encrypts one character at the same time [Kotulski 99]. Normally, the key is a pseudorandom number sequence applied to the plain text to generate the cipher text and that sequence will be applied to the cipher text to produce the plain text. This method is suitable for simple and fast application encryption because it uses small storage and buffer during the encryption and decryption process. Meanwhile, it takes long time for the huge data encryption application since it doesn’t deal efficiently with the real time applications [Golić 97] [Gupta 14]. Figure 2.4 illustrates the general encryption and decryption diagram of the stream cipher. In this figure $A_1, A_2, ..., A_n$ represent the original text and $B_1, B_2, ..., B_n$ represent the ciphered text.

![Stream cipher diagram](image)

The most known techniques in the stream cipher are Rivest Cipher 4 (RC4) [Gupta 14] and one time pad (OTP) [Rubin 96].
2.3.1.2 **Block cipher**
The block cipher is an encryption way applied to a block of text using a secret key. In general, it takes less time than stream cipher and more storage during the encryption and decryption process, but it is suitable for large data encryption application [Kotulski 99]. Figure 2.5 illustrates the general encryption and decryption diagram of the block cipher. In this figure, \((A_1, A_2, \ldots, A_n)\) represent the original text and \((B_1, B_2, \ldots, B_n)\) represent the ciphered text.

![Block Cipher Diagram](image)

Figure 2.5: Block cipher diagram

The most known techniques in the block cipher are DES [Standard 99] and AES [Chitu 05]. In the next section we will discuss deeply the symmetric encryption techniques.

2.3.2 **Asymmetric cryptography**
Asymmetric cryptography is also called public key or two key encryption methods. In 1976, Diffie and Hellman published the first paper about the public key encryption. In that research, the authors formulated and introduced a new contribution in the cryptography field [Diffie 76]. Normally, the first key is called *public*; it is used in the encryption phase, while the other key called *private* is used in the decryption phase or conversely, the private to encrypt and the public to decrypt [Bellare 95]. The sender encrypts the message (plain text) using the encryption algorithm and the public key to generate the cipher text. At the receiver side, it decrypts the cipher text using the decryption algorithm and the private key to get the original text as in figure 2.6. If the receiver can understand the decrypted message, the message is an authentic message and the receiver assumes the message encrypted using the public key of the sender. Else, the receiver drops the decrypted message and he will know that it is an inauthentic message.
The advantage of these techniques is that they do not require a security in transmission channel but they have major problems, particularly in term of calculation time. The general diagram of the encryption and decryption process of the asymmetric technique can be summarized in the following equations:

\[ E_{k_1}(P) = C \quad (2.3) \]
\[ D_{k_2}(C) = P \quad (2.4) \]

where \( E \) is the encryption algorithm, \( P \) is the plain text, \( C \) is the cipher text, \( k_1 \) is the public key, \( k_2 \) is the private key and \( D \) is the decryption algorithm.

In the asymmetric technique, the sender and the receiver have to generate a key, one of them will be shared during the transition process while the other will be hidden and secure from the hacker and unauthorized user [Menezes 97]. The security of the asymmetric technique is based on the algorithm used and on the two keys especially the private key. The most known techniques based on the asymmetric technique are RSA [Harn 13], DSA [Kim 13], ELGAMAL [Khedr 14].

### 2.3.3 Hash function cryptography

Hash function is used to generate the hash value of a given text for cryptography requests like text integrity, text authentication, and other security facilities [Mel 01]. Hash function agrees variable input message sizes and generate static size output. It is called the hash code. Any slight change or
modification in the input text will provide us with a different text as output, which is farthest from the previous one [William 06].

The hash function is a one way function. It generates a fixed message size from variable message size. It is hard to find the plain message from the given hash message [Ferguson 01].

The hash function can be classified into two main categories depending on the use or not of a key: hash function which depends on the secret key called *keyed hash function* and hash function which does not depend on a secret key called *un-keyed hash function*. An example of this type is Message Authenticate Code (MAC) [Procter 14]. The un-keyed hash functions [Menezes 97] are the Message Digest 4/5(MD4, MD5) [Gupta 14 (a)] and Secure Hash Algorithm 0/1(SHA-0,SHA-1) [Biham 15]. The hash function is recognized as message abstract, hash code, digital fingerprint and checksum [Chakraborty 14].

Hash functions can also be classified in two categories depending on the strength of the one way function. Indeed, there are two types of one way function: *weak function* and *strong function* [Chakraborty 14]. Weak one way function is easy to calculate, however, it is hard to get the inverse from the given hash value. The strong function is complicated to calculate, but it's impossible to find the inverse message from the given hash value. Using hash function in the cryptography means one way function applying which is unable to derive the original message from the given hash value [Schneier 07].

2.4 Cryptographic techniques
In this section, we will present the most known techniques in the symmetric and asymmetric domains.

2.4.1 Symmetric encryption algorithms

2.4.1.1 One time pad encryption (OTP)
OTP is a stream cipher symmetric encryption technique. The general idea of OTP is to use a unique key for each letter or number. The key is used to encrypt letters or numbers in the plain text. The key didn't repeat again in the encryption keys at that time (one-time). The sender and the receiver must have a copy of the pad. In the encryption phase, the original message (plain text) is merged with the random strings using an XOR process, while the receiver decrypt the cipher text based on the same
Chapter 2: Digital Image Cryptography

encryption key and reversing the encryption process. Theoretically, OTP is hard to break because for each string we use a unique and not repeated key. It is difficult to use since both the sender and the receiver must have the copy of the pad. Moreover, the key length has to be the same length as the plain text which is impractical and inefficient for large data encryption system [Dube 08]. The following equation explains the general idea of OTP encryption and decryption process:

\[ C_i = E(P_i, K_i) \quad (2.5) \]
\[ D_i = D(C_i, K_i) \quad \text{for } i = 1,2,3,\ldots,n \quad (2.6) \]

where \( C_i, D_i \) are the cipher and the decrypted text, respectively; \( E \) and \( D \) are the encryption and decryption operations; \( P_i \) is the plaintext; \( K_i \) is the key stream that is used for encryption and \( i \) is the text position. The condition: \( K_{i-1} \neq K_i \neq K_{i+1} \) [Rubin 96].

2.4.1.2 Data encryption standard (DES)

Data Encryption Standard (DES) is a block cipher symmetric technique. It consists in encrypting 64 bit plain text to generate the same size of the ciphered text using 56 bit secret key size [Standard 99]. This method has been established by IBM to resolve the need for the data security in their products and it is confirmed by the National Bureau of Standard [Biham 91]. The main idea of the DES is based on the product cipher and Feistel cipher. The product cipher executes several operations to produce a complex encryption function. The internal function of the DES is called a round function which iterates a number of times serially, while the Feistel cipher is the iterated cipher which maps the plain text into the cipher text [Menezes 97]. Figure 2.7 illustrates the working of DES technique.

In the encryption phase, the plain text process through 16 circles and each circle has a sub key of size 48 bits. This sub key is generated from the secret key of the size 56 bits. The plain text is divided into two values with the same size (32 bit). In the decryption process, there is the same number of iterations, but with the reverse order of the key (from \( K_n \) to \( K_1 \)).
where a, b, c, ..., n are the 32 bit input; A, B, C, ..., N are the 32 bit output; K₁, K₂, ..., Kₙ are the secret keys.

F is the function in the various rounds, n = 8.

The DES is used in wide encryption applications. The first version to reduce DES to eight rounds was in [Biham 91]. After that, many other authors proposed approaches for designing DES secret attack to find all the key possibilities within a short time [Wiener 94], [Rouvroy 03], [Quisquater 05].

2.4.1.3 Advanced encryption standard (AES)

After the DES algorithm, at the end of the 1990s, the National Institute of Standards and Technology (NIST) declared the need to improve and implement new encryption techniques. A lot of algorithms were suggested. In 2000 the Rijndael algorithm was chosen [Chitu 05]. The algorithm is a block cipher algorithm and it is based on symmetric technique. There were editions AES-128, AES-192 and AES-256 where the block size and the key size of AES-128 is 128, 192 for AES-192 and 256 for AES-256. It is based on the repeated round process. During the round, many operations are performed on the block of data. AES encryption consists of 10 rounds of process for 128 bits, 12
rounds of process for 192 bits and 14 rounds of process for 256 bits [Menezes 97]. This method is very simple and fast. Meanwhile, it has a resistance against different known attacks. It is also appropriate for varied kinds of hardware and software applications.

In the figure 2.8, we illustrate the AES-128 bit. Firstly, find the round sub key from the shared secret key based on the Rijndael key and load the state array values. Each round sub key is XOR with a byte of the state [Rhee 03]. Therefore, four operation functions are applied (SubBytes, ShiftRows, MixColumns and AddRoundKey) for each round. SubBytes update the value of state array based on Rijndael S-box. ShiftRows updates the value of the state array by shifting it to the left each row, by altering amount based on the number of the rows. MixColumns multiplies four vertical values of the state array by static polynomial. In AddRoundKey, the sub key is mixed with the state array. The ShiftRows and MixColumns are planned to support high transmission to the cipher text. In the last round, all the processes are performed except MixColumns process which unloads the state array as cipher text. In decryption phase, the same process is applied in the inverse round order, and using the same encryption key to decrypt the cipher text. AES is attacked with six rounds in [Daemen 99] and with seven rounds attacks in [Gilbert 00]. In 2000, the Rijndael cryptanalysis is improved with eight rounds of the AES-198 and nine rounds of the AES-256 [Ferguson 01].
2.4.2 Asymmetric encryption algorithms

2.4.2.1 Rivest-Shamir-Adleman (RSA)
In 77, the new asymmetric algorithm is proposed based on a public and private keys cryptography algorithm, the Rivest-Shamir-Adleman (RSA) algorithm. RSA uses variable input message length and variable secret key length where the key is derived from the very large number, which is the product of two large primary numbers selected based on specific instructions [Rivest 78].

The encryption key is public and it is different from the decryption key (private). The public key is generated from the two primary numbers and it is shared while the private (primary numbers) is kept in hidden way. The user can use the public key for the encryption process, but the user who has the primary numbers can decode the cipher text.

Figure 2.8: AES-128 bit encryption process
Chapter 2: Digital Image Cryptography

RSA algorithm comprises the three well known processes: key generation, encryption and decryption. During the key generation, two keys are provided: one of them is public, it can be known by anyone and it is applied through the encryption process. The decryption process is done using the private key. In encryption phase, the sender shares the public key with the receiver while the sender keeps the private key secret and performs the encryption process as shown in the following equation:

\[ c(m) = m^{k_1} \mod k_2 \quad (2.7) \]

where \( c \) is the cipher message, \( m \) is the plain message, \( k_1 \) and \( k_2 \) are the public keys.

In the decryption phase, the private key has to be provided by the authentic user, and the module base is still the same encryption module base. The process is done as the following equation:

\[ m(c) = c^{k_3} \mod k_2 \quad (2.8) \]

where \( k_3 \) is the private key.

2.4.2.2 ElGamal encryption

ElGamal encryption is an asymmetric technique based on Diffie-Hellman technique. It is defined by Taher in [ElGamal 85]. It has come to solve the difficulties of computing discrete logarithm over limited domain. This method is applied in many cryptography fields. One of them is a digital signature approach. The general diagram of the ElGamal scheme comprises three steps: key generation, encryption and decryption. The key generation phase generates two keys: one of them is public and the other is private which must be kept secret with the sender [Menezes 97].

In digital signature approach, the public file contains the public key which is provided to any user. To sign the document, a user has to use the secret key. Any user can verify the authenticity using the public key, but the authentic user can forge the signature. The signature builds based on the following equation:

\[ \alpha^m = y^r \cdot c \mod p \quad (2.9) \]
where $\infty$ is the signature, $m$ is the message to be signed, $y$ is the public key, $p$ is a large prime number, $r$ and $c$ is the pair (private and public) keys of $m$ where $0 \leq r, c \leq p - 1$.

In the verification phase, we verify the authenticity of the message signature by computing the both sides of the previous equation.

ElGamal has some specific properties. It is a randomization encryption operation. The cipher text for a certain message is not repeated, encrypting the same message twice provides us different cipher messages. The specific structure of the approach is that there is no clear relation between the approach functions [ElGamal 85].

### 2.5 Cryptanalysis

Cryptanalysis is both the art and science of the break of the cipher message without knowing the keys. It tests the algorithm robustness against attacks, or from unauthorized user to deciphering the secure message. The process depends on the nature of the technique and on knowing the properties of the original message and the cipher message. From the available information about the properties the user tries to achieve the key. MAC algorithm needs more cryptanalysis offers. In the hash function, the cryptanalysis center is on the inside structure of the compression technique [Chakraborty 14].

Differential cryptanalysis is a technique for breaking the cryptosystems. It was designed in 1990 by Eli Biham and Adi Shamir [Biham 91]. Differential cryptanalysis is effective when the cryptanalyst can select plaintexts and obtain ciphertexts. The process searches for plaintext, ciphertext pairs whose difference is constant, and considers the differential performance of the cryptosystem. The difference of two elements $P_1$ and $P_2$ is defined as $P_1 \ XOR \ P_2$ for DES [Biham 12]. The difference may be defined in a different way if the process is applied to some other cryptosystem.

Several attacks have been applied to cryptography algorithms. In the next section, we will discuss the most known of them.

#### 2.5.1 Brute-force attack

Brute-Force attack is one of the attacks whose purpose is to break the cryptography algorithm by searching all the possibilities for the used keys till achieving the correct one. The resistance of any
cryptography techniques against brute force attacks depends on the key length as more is the time to find the possible key from the existing information. It means the key size plays an important role and that the longer key size is more difficult to achieve. Any system that can discover the secret key faster than the brute force attack is measured an effective attack [Kahate 13].

In the hash function cryptography technique, the robustness of the algorithm against the brute force attack is very weak, because the number of the inputs and the outputs of the hash function are infinite. Moreover, the hash function requires to find two messages of changed lengths which hash to the similar hash value [Gupta 14]. [William 06] produced brute force attacks which applied to MD5 cryptographic algorithm. The author concluded for hash code of size 160 bits, that’s the time to find the required collision is over four thousand years. The collision is to find two different length message with the same hash value [William 06]. However, the hash function is never allowed collision and the strength of the hash function depends on the length of the hash function technique.

2.5.2 Birthday attack
This attack is based on the birthday problem concept. The birthday problem is the probability of finding at least two similar values within the same set of values [Das Gupta 05]. For a set that contains 40 people, and those sharing their birthday, the probability of someone having the same birthday are 40/365 which is approximately equal to 11%. This attack aims to find two different input values \( n_1, n_2 \) with a given function \( f(n) \) which generate the same output value \( f(n_1) = f(n_2) \). It is known as collision where the fastest method to discover a collision is the birthday attacks [Ferguson 01]. We can say the algorithm is collision resistant if it is complex computationally to find two different inputs that have the similar and equals outputs. Birthday attacks in hash function cryptography require around \( 2^{f/2} \) processes where \( f \) is the size of the hash value in bits. For SHA-1 of 160 bits, birthday attack needs \( 2^{160/2} \) \( (2^{80}) \) hash processes.

2.5.3 Meet in the middle attack
Meet in the middle attack is used to realize dual encrypted secret key of block cipher technique. The attacker is expected to access the plain message and the cipher message. He tries to encrypt the plain message by different keys. Meanwhile, it decrypts the cipher message in different keys in order to
find the middle value of the encrypted plain message and the decrypted cipher message. Figure 2.9 illustrates the general diagram for meet in the middle attack.

![Figure 2.9: General idea of meet in the middle attack](image)

Alice sends the value $A = K^n$ and Bob send the value $B = K^m$. Eve computes the value of $E = K^d$ by using her own secret key and instead of transfer $A$ to Bob and $B$ to Alice, she sends $E$ to Alice and Bob. Meanwhile, Eve interchanges $A$ with Alice and $B$ with Bob. In that case, they consider the values have exchange with each other [Buchmann 13].

### 2.6 Conclusion

In this chapter, we have presented the main concepts and principles of cryptography field. Cryptography area comprises: symmetric (private), asymmetric (public) and hash function techniques. Symmetric techniques are divided into stream cipher such as RC4 and block cipher such as DES. The symmetric approaches have a gap in the security issue of sharing the key while the asymmetric approaches take a long execution time. On the other hand, the symmetric techniques allow achieving less computational complexity compared to asymmetric techniques while the latter provides a more secure key.
Chapter 3 Hybrid Watermarking and Cryptography Techniques

3.1 Introduction
The cryptography approaches protect the data during the transition. The person who has the secret key and the algorithm can decrypt the data into a useful format. But after the decryption, the data are no longer protected and it is very hard to verify its integrity and its origin. This kind of protection is called *priori protection methods*. The watermarking approaches came as a complementary protection techniques to prove the data integrity, authenticity, its originality, availability, etc….. After the data decryption, we still have the possibility to identify if the data is tampered or if it is in original form. This kind of protection is called *posteriori protection method* [Bouslimi 12].

We discussed in the previous chapters the security issue for watermarking and cryptography separately. In this chapter, we will discuss the combination of watermarking and cryptography together. The encryption is a common way to secure and prove the data confidentiality. The second section presents the four known ways to combine the watermarking and encryption approach classifications.

3.2 Combined watermarking and encryption approaches classifications
The combinations of watermarking and encryption techniques are well-known. They can be classified according to the approach of combination as follows:

3.2.1 Watermarking followed by encryption (WFE)
In these kinds of approaches, the watermark is embedded in the host data, then the watermarked data are encrypted. On the receiver side, the watermarked encrypted data are decrypted, and after that the watermark data are extracted. Figure 3.1 illustrates the general diagram of WFE embedding-encryption processes. Figure 3.2 illustrates the WFE decryption-extraction processes [Bouslimi 14].
Chapter 3: Hybrid Watermaking and Cryptography Techniques

Figure 3.1: WFE approach in the case of the embedding-encryption process.

Figure 3.2: WFE approach in case of the decryption-extraction process.

here, \( i, w, s \) are the original data, the watermark data and the secret key in the embedding/extraction algorithm, respectively. \( i_w \) is the watermarked data. \( k \) is the secret key in the encryption/decryption algorithm. \( E_iw \) is the encrypted watermarked data. \( D_iw \) is the decrypted watermarked data.

In [Taneja 13], the authors proposed watermarking and encryption approach. The watermarking is done based on the Wavelet Packet Transform (WPT) and Singular Value Decomposition (SVD) methods, while the watermarked data is encrypted based on Set Partitioning in Hierarchical Trees (SPIHT) provided by developing the framework JSON Web Encryption (JWE), in order to ensure the data confidentiality and the content ownership.

In [Kannammal 14], the authors also proposed a dual watermarking and encryption approach in order to prove the authenticity and integrity of medical images. Two levels DWT transform is applied to the original data. The watermark is embedded in the low-high sub-band based on the Least Significant Bit (LSB) where low-high sub band is divided again into many blocks, then the medical information (as a second watermark) is embedded into these blocks also based on the LSB technique. The watermarked image is encrypted using the RSA, AES and RC4 algorithms.
3.2.2 Encryption followed by watermarking (EFW)
In this approach, the encrypted watermark is embedded into the encrypted original data. It comes with the benefit of homomorphism encryption [Bouslimi  14]. This operation is to be conducted in the encryption domain. On the other side, the decoder has to extract the encrypted watermark and encrypted original data then decrypt them. The general diagram of the processes is shown in the figure 3.3 and figure 3.4.

![Figure 3.3: EFW Approach in case of the encryption-embedding process.](image1)

![Figure 3.4: EFW approach in case of the extraction-decryption process.](image2)

In, the figure 3.3 and the figure 3.4 $E_i$ and $E_w$ are the encrypted original data and the encrypted watermark data.

In [Subramanyam 12], Subramanyam presented an encryption and a watermarking technique for JPEG images in order to preserve the confidentiality of the content. The authors applied asymmetric stream cipher technique for encrypting. The obtained encoded stream cipher was embedded in the host image coefficients based on Discrete Wavelet Transform. The watermark can be extracted from encrypted image or from decrypted image. In this research, the authors applied various watermarking approaches like Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM) and Rational Dither Modulation (RDM).
Solanki in [Solanki 14], proposed another encryption / watermarking approach in order to protect the patient information that are stored in the medical images (CT scan or MRI images). In encryption / embedding phase, watermark image is encrypted using the RSA algorithm while the original medical image is enhanced founded on the threshold of the high intensity area. The insertion is done based on the Haar DWT algorithm. During the extraction / decryption phase, they decomposed the original image and watermarked image based on HAAR DWT, then they decrypted the watermark using the RSA algorithm.

In [Saha 14], a hybrid encryption and watermarking image approach is proposed in which the encryption is done using One Time Pad (OTP) method while the watermarking is done based on discrete wavelet transforms. The key was built from each 8 by 8 block of the image. The watermark is encrypted using the XOR, then they embed the encrypted watermark in the original image in the middle frequency sub-band of the DWT coefficients. The weaknesses in this technique are the following: the key is extremely large to share, the way to produce the key is fragile, and the imperceptibility results are unacceptable. Moreover, the authors didn’t measure the robustness of their watermarking algorithm and also didn’t test it against attacks.

In [Pradhan 12], the authors proposed a watermarking scheme based on the Discrete Wavelet Transforms (DWT) applied to an image. The original image is decomposed using DWT and the medium frequency sub-bands are chosen for embedding. Then, Arnold transformation and Cross chaotic sequence are used to encrypt the watermark. The DWT transformation is applied to the encrypted watermark image and the medium frequency coefficients of the encrypted watermark image are embedded in the medium coefficients of the original image. The complexity of the proposed approach was very high due to the dual encryption on the watermark image. Also, there is a remarkable degradation of the retrieved original image after applying attacks.

The work in [Zhang 11], the authors provided a novel and reversible watermarking approach for the encrypted image. After encrypting the whole data of an image based on a stream cipher way, the watermark information is inserted into the image by adapting a slight quantity of encrypted image. At
Chapter 3: Hybrid Watermaking and Cryptography Techniques

the decryption side, the encrypted watermarked image is decrypted by using the encryption key. While the watermark key is obtained by support of spatial relationship in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

The authors in [Wu 14] proposed reversible data hiding in the encrypted domain approach. The authors used two reversible data hiding techniques in encrypted images, called a joint approach and a separable approach. The approaches have been introduced by assuming prediction error. In the joint approaches, the extraction and image rebuilding are made at the same time. The reversibility provided by the number of incorrect extracted bits while the approach achieved good visual quality of recovered data, particularly when embedding amount is high. In the separable approach, the extraction and the recovery of the image are disjointed. The separable approach provided enhanced reversibility and good visual quality of recovered image for high payload embedding.

3.2.3 Joint watermarking / decryption (JWD)
The method is considered as a secure embedding, where the watermarking technique is applied to the decrypted data on the receiver side. The sender encrypts the data and transmits them through the internet, the receiver receives the encrypted data and the unique specific information about the decrypted key (Client Specific Decryption Key (CPDK)). The decryption process and the watermarking process are convoluted and done at the receiver side, which means the decrypted result with the specific CPDK of the receiver produces content copy personalized of the receiver. JWD limits the bandwidth usage, reduces the server (sender) complexity. Moreover, it is useful in forensic tracking, fingerprinting and ownership identity applications [Celik 07].

The JWD general diagram is illustrated in the figure 3.5

\[ \text{Figure 3.5: JWD general diagram} \]

where \( CPDK \) is the unique specific decryption key and \( D_w \) is the decrypted watermarked data.
In JWD approach, the sender generates different and unique key for each receiver that is used to decrypt and to embed the watermark. After the decryption, the watermark is embedded into the decrypted data (plain data) to obtain the watermarked data.

In [Kundur 04], the authors proposed video fingerprinting and encryption approach for digital rights controlling. They encrypted the sign of all the significant Discrete Coefficient Transform (the middle frequencies) for each frame, while they provided each user with a private decryption key to decrypt just the subset of these coefficients. The remaining coefficients knotted the form of the fingerprint. The approach was perfect in its encryption phase, but the lack of effective discovery tools and security procedures limit its prospective using.

Bouslimi et al in their work [Bouslimi 14], presented a novel cryptography and a watermarking approach for medical image securing. They proposed a pair of existing watermarking technique based on Quantization Index Modulation and JWD approach. They insert dual watermark, one of them before the encryption includes the reliability evidence, and the other during the decryption process (JWD) includes traceability evidence. The authors’ goals are to guarantee the confidentiality, the reliability and the traceability to identify the origin of the unlawful distribution of the medical images.

3.2.4 Joint watermarking / encryption (JWE)

In this way, the watermark is embedded through the encryption process which means merging the watermarking and encryption together at the sender side. In JWE, the watermark can be extracted in the spatial domain after the decryption, or in the encrypted domain from the encrypted image, or both of them [Bouslimi 12]. The general diagram of JWE is illustrated in the following figure.

![Figure 3.6: JWE general diagram](image-url)
Bouslimi, [Bouslimi 12] proposed a combination watermarking and encryption approach in order to prove the medical image integrity and to verify its originality and reliability in the spatial domain and encrypted domain. The watermarking technique is based on quantization index modulation, where the encryption techniques are based on the both of stream ciphers (RC4) and block cipher (AES) algorithms. They inserted two messages containing authenticity code (AC), which will be accessible in the spatial and encrypted domains. The embedding and the extraction depend on two watermarking keys. One of them is used within the encrypted domain while the other is used in the spatial domain. The experimental results showed a low image distortion and sufficient capacity to embed a reliability evidence. Its approach is slower than image encryption algorithms, but the execution time for the decryption process is not impacted. Another watermarking and encryption approach was proposed also by Bouslimi et al in [Bouslimi 12 (c)]. The watermarking algorithm comprises two watermarking approaches: least significant bit and quantization index modulation, while the encryption algorithm is based on stream cipher RC4.

3.3 Conclusion
In this chapter, we presented the combined watermarking and cryptography approaches. The joined watermarking and cryptography approaches are aimed to increase the security issue in the digital material. Cryptography is a way to secure the digital material, but the data are no longer protected after the decryption. So, the watermarking approach is a complementary security technique to ensure the security of the digital material. The watermark can be extracted any time to prove the ownership of the digital material. However, posterior protection aims to combine two techniques (cryptography and watermarking) to prove the integrity and authenticity of the digital material. In the literature, there are four know classifications of the combined watermarking and cryptography approaches based on the way of applying the techniques. We have illustrated them in section two in details.
Chapter 4 Digital Medical Image and Telemedicine Security.

4.1 Introduction
In this chapter, we will discuss the definition of telemedicine and medical image, the existing medical systems for storage and transfer (like HIS and PACS), the security characteristics in the medical image. Also, the medical image security applications will be presented.

The research and scientific concerns at the present time are focused to serve and develop the medical sector and make this service available for all. Traditionally, the patient has to visit the physician to get the diagnosis. Sometimes, the physician is too far physically from the patient and the patient’s health doesn't allow him/her to move.

However, the main concern in the world is to develop the healthcare quality. The human healthcare is considered as the most important point throughout the world. Information technology has come to get rid of these problems and to contribute in the medical service improvement that is provided to people.

Telemedicine is the use of information and communications techniques to offer the health care where the patients and the physicians are disjointed by physical distance. The word telemedicine is a word combined from the prefix ‘tele’ derived from the Greek and it means the distance, which means telemedicine is a medicine in the distance. The modern health care system like Hospital Information System (HIS) and Picture Archiving and Communication System (PACS) provide the health sector with the digital medical information in easy and fast ways.

Telemedicine back to the 1920s: the radio signals have been used to link public health physician’s station of ships at sea with medical emergencies. Telemedicine revolution was in the 1970s: scientific revolution occurred based on the ATS-6 satellite techniques project, wherein, the clinical staff in remote Alaskan and Canadian villages was linked with the main hospitals in distant cities or capitals [Krol 97].
Ledley is one of the famous researchers who employed the digital computer for the medical goals [Ledley 90]. In the United States in the 1950s, Ledley provided computer applications for dental projects at National Bureau of Standards. He conducted many projects to provide the medical sector with a high capability using computer applications, like Standard Eastern Automatic Computer (SEAC). One of the leading expert system was MYCIN, a system for computer based medical consultation application, which was implemented by Stanford University in 1976.

### 4.1.1 Digital image

A digital image is a two-dimensional array of positive integer values \( f(x, y) \), where \( 1 \leq x \leq M \) and \( 1 \leq y \leq N \), and \( M \) and \( N \) are nonnegative integer values representing the number of row and column, respectively. The coordinate \( (x, y) \) represents the image pixel position. \( f(x, y) \) represents the image pixel values. In the case of a three-dimensional image, \( f(x, y, z) \) is used where \( 1 \leq z \leq Y \), and \( Y \) is a nonnegative integer [Huang 11 (a)].

### 4.1.2 Digital medical image

The normal method to generate digital medical image is to capture the image on X-ray films or radiographs, computed radiography (CR), and digital radiography (DR) techniques [Huang 11 (a)].

Medical imaging examinations include computed tomography (CT), X-ray computed tomography (XCT), nuclear medicine (NM), positron emission tomography (PET), single photon emission computed tomography (SPECT), ultrasonography (US), magnetic resonance imaging (MRI), digital fluorography (DF), and digital subtraction angiography (DSA) [Huang 11 (a)].

### 4.2 Picture archiving and communication system (PACS)

PACS is considered as the server of the medical images. It receives and archives images from devices such as Hospital Information System (HIS) and Radiology Information System (RIS). PACS are taken into account the different radiological imaging modalities, including patient data, study support information about the patient, a description of the patient case. PACS consists of two components: database server and archiving system.
After the examinations images are done, the HIS and RIS send the examinations image to the PACS server. The PACS extracts the descriptive information from the DICOM header. Then, update the database system and limit the target of the newly generated data. In the case of a huge amount of data, PACS compress them and store or update the database system.

PACS can be integrated with the Teleradiology system in the medical field. It can support the clinic with the necessary data about the patient. At the same time, it is used as a server containing the database for the hospital medical images. PACS can import medical image from the outside imaging center, then PACS sends the reports to the HIS and other medical expert system of the hospital. Also, the image center can send it to the expert system as in the Teleradiology model.

Moreover, PACS has many advantages regarding to Telemedicine sector. In case of PACS server down, imaging devices can send the images directly to the destination. However, PACS is less risk of losing the image data, because PACS considers multi copies broadcast distribution. Furthermore, the destinations of PACS have local storages, these storages keep the historical data for time, it means the data is still available for a longer time at the system. Another advantage of PACS is that it allows to modify the header of a DICOM image which has been stored in the system. Also, PACS is less liable for any modification of the network performance. [Huang 11 (b)].

4.3 Telemedicine

Telemedicine is the delivery of health care using telecommunication, computer and information technology, which includes medical images. Using only one part of the previous components does not consider Telemedicine. For example, using a telephone conversation would not be considered as telemedicine because of the absence of computer and information technology [ATA 13].

Telemedicine can serve three models in the medical field: telediagnosis (store and forward), teleconsultation (just in time) and telemanagement (real time). In telediagnosis model, the patient examination and images are done by the referring physician site, while the results and images are transmitted to the professional physician side to get the diagnosis and treatments about the case. There is a delay in the time in this scenario. The second model is teleconsultation, the referring
Chapter 4: Digital Medical Image and Telemedicine Security

Physician site sends the results and the examination of the patient to the professional physician site to get the diagnosis and treatments about the case, while the patient is still awaiting the results. The third model is telemanagement, the professional physician site is connected with the patient in the examination room, and the medical management care is immediate. In this case, the patient will get the diagnosis from the expert physician directly after the examinations and images. For each model, different tools and information technology technique are required. [Cavaro 13].

Figure 4.1 represents the general idea of using the telemedicine between referring site which involves the physical hospital, laboratory, IT tools and the patient (transmitter). The transmitter side converts and prepares the data and information from the referring side into a signal which can be sent via the network. The transmission part includes the network and the internet that carries the signal between the other two parts. Whereas, the expert side receives the patient information from the internet. Then, convert the data from the signal to usable and readable information. The expert physician does the treatments and diagnosis of the case and the physician resend the report to the referring side using the internet and the network.

4.3.1 Telemedicine and teleradiology
Teleradiology is a subcategory of telemedicine. It is transmitting the medical image of the patient from the examination side to treatment and diagnosis at the expert side using the telecommunication tools and technology. The technology that is required in the teleradiology is stricter than the technology in the telemedicine. Normally, the computer contains the patient information, examination results and images are enough to build basic telemedicine system on the referring site.
Chapter 4: Digital Medical Image and Telemedicine Security

Then, transmitting the data using telecommunication system. Meanwhile, at the expert side, the computer to display the received information is required. All the patient information has to meet the requirements of the hospital information system (HIS) or clinical management system (CMS), these requirements include data format and real time constraints. [Huang 11 (c)].

Teleradiology is more close to PACS functions in technology terms. But PACS deals with the DICOM image using the LAN network, while teleradiology uses the WAN network. Moreover, if the data is huge, the PACS will compress it in the system. But the teleradiology is compressing the data even if it is not huge to achieve high speed and low cost using the WAN through the transmission [Huang 11 (c)].

Teleradiology can capture the image and digitize it in a high quality, reformatting the data to be in standard medical image formatting (DICOM), transmitting the image, reporting, storage and display the medical image [Huang 11 (c)].

4.4 Digital imaging and communication in medicine (DICOM)
The integration of different digital products, modalities, archiving and information medical systems terms demanded to generate a standard format for medical images. Digital Imaging and Communications in Medicine (DICOM) established to be the standard format of medical image in order to store, transmit, save, and use it. DICOM was developed by the corporation between The American College of Radiology (ACR) and National Electrical Manufactures Association (NEMA) to produce standard for data transfer in 1983. In 1985, the ACR-NEMA standard versions 1 published and improved the way to store and transfer the data in a non-proprietary form. The second version enhanced the achievement of the standard definition, data structure and encoding. DICOM version 3 was in 1993, the main difference was based on network protocol by TCP/IP protocol. The data structure model was based on a unique definition for services and objects such as image objects, patient objects, etc.

The DICOM’s header contains the patient information, physician details and hospital information, where they are known as information object definition IOD. All of these objects in the header have a
meaning. The data is divided into several groups, each group contains connected data, such as group 10 which contains the data of patients, the unique identifiers (UID) in terms of technology details in the image such as X-Ray exposure.

The DICOM’s body contains the important information about the patient case, we can classify the body into the region of interest (ROI) which is normally at the center, and the region of non-interest (RONI) which is the border of the image. Figure 4.2 and 4.3 illustrate the medical image parts [Bairagi 11].

![Figure 4.2: Medical image components](image1)

![Figure 4.3: NROI & ROI medical image](image2)

The research is developing and improving the services of DICOM. In Europe, the main companion of the DICOM team is OFFIS (Oldenberger Forschungs und Entwicklungsinstitut Für Informatik The Oldenburger Institut). It is Germany institution located in Oldenburg. It was created in 1991. The institution is interesting in three research domain: Energy, Health and Transportation [OFFIS].
4.5 DICOM security profiles
DICOM is a standard of the medical image. It has addressed the security issue in its part number 15 (PS 3.15-2001) [McAuliffe 01]. In part 15 of DICOM, four security profiles have been added: secure use profiles, secure transport connection profiles, digital signature profiles and media storage secure profiles [McAuliffe 01]. These security profiles treat the attributes using, associations’ security, objects authentication and file security. The next section presents these security profiles in detail.

4.5.1 Secure use profiles
Secure use profiles provide a guide to use the attributes and other security profiles in a certain mode. The profiles include the safe use of online electronic storage, bit maintaining and electronic signatures.

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

4.5.3 Digital signature profiles
Digital signature profiles support tools for the integrity checks using digital signatures. Digital signature lets validation of the identity structure, which is generated, approved or altered a DICOM data. The digital signature generator has to identify the DICOM data set, then calculate the MAC and the hash value. After that, embed the MAC value into the digital signature. While the receiver can verify the authenticity and integrity of the received data by recalculating the MAC value and compare it with the embedded MAC value. The profiles provide three potential ways of digital signature implementation (base, creator and authentication), depending on the content that will be embedded into DICOM.
4.5.4 Media security profiles
The media security profiles support a secure tool to protect the DICOM data against unauthorized access of the information. The profile defines a structure of the DICOM protection exchanging by compressing the data with a cryptographic wrapper. These security way is considered as an application of the asymmetric cryptography techniques.

These security profiles allow encrypting the image using the DES, DSA and other exciting encryption techniques. Whereas, the information after decrypting will not be protected. So, it is difficult to verify its integrity, authenticity and reliability [Bouslimi 12 (b)]. Also, the DICOM security standard does not preserve the confidentiality and integrity of the medical image data. Whereas, its header can be easily removed and regenerate a fake header by the attacker. So, watermarking is a solution to ensure the image security through the storage and transmission. This way it can provide a standing guarantee of confidentiality and integrity of the data [Huang 11 (d)]. Moreover, to increase the medical image security, the watermarking and cryptography techniques are applied to medical data. The general illustration of the encryption and embedding methods are applied at the sender side as follows:

- Image preprocessing: to segment and extract the relevant patient information from the DICOM header.
- Data encryption: to encrypt the medical data and produce ciphered data form.
- Data embedding: to embed the secret information in the medical data.

Where extraction and decryption process are applied at the receiver side, these steps are:

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

4.6 Medical image security requirements
Medical image security is required by the health insurance portability and accountability act (HIPAA) to guarantee that the patient information privacy are protected [Act 96]. DICOM standard provides an optional guide for medical image production. However, in telemedicine, the medical image transmits
between the referring site and expert site using the network. The security term becomes very
important and critical issue is not just for storing the data in the medical system, but also during the
transmitting operation over the network in telemedicine. That is to keep the patients’ information in
term of privacy, authenticity and integrity security characterization. These characterizations can be
described as follows: Confidentiality means rejection of access to the patient information by
unauthorized users. While the integrity refers to medical image safety through the transmitting from
any tampering, changing or modifying. Moreover, the authenticity is to validate the image source and
the image belongs to the correct patient [Bouslimi 12 (a)].

A lot of work is done in this field in order to achieve the highest security level of patient information,
medical image and other information related to the patient. In the next section, The characteristics of
the medical image confidentiality, integrity and authenticity are discussed.

4.6.1 Medical image confidentiality
The confidentiality means the authorized users can access, modify, or do any other allowed process at
the patient information, while preventing the unauthorized user from the access to them or from the
editing. It is considered the first step to guarantee the security issue of the patient information privacy
[Al-Haj 14].

The Patient information has to stand up the law and ethics requirement of confidentiality. The
information must have the critical and important quality of confidence about it. Moreover, the
confidentiality of the information must be guaranteed during the transition. Also, The information
using must keep the patient information security inside the responsible team like the physician, the lab
worker and so on [Abbing 14].

There are two allowed reasons of public law for breaking confidentiality: the first situation, if the
patient is accepted to reveal his/her information. The second situation, if it will improve and serve
the public health sector [Klutas 77].
4.6.2 Medical image integrity
A code of ethics for health Informatics Professionals (HIPs) has provided us with the guidance and the principles of the health information protection [IMIA]. One of the critical and important point is the integrity. The patient information integrity means the data is intact from any intentional or unintentional modifying from unauthorized person. So, if an attack is happening from an unauthorized person, the person in charge of the medical information in the telemedicine system has to detect that.

4.6.3 Medical image authentication
Medical image authentication aims to identify the image source, the ownership and it is an origin as sending from the source. Which means there is no falsification happening through the transmitting process? The Medical image authentication is used to improve the tamper detection and tamper recovery. The authentication and the integrity are very close together [Al-Haj 14].

The general scenario to the medical image authentication is inserting data from the source side in the cover host image. Then send these images to the receiver. At the receiver side, the receiver has to extract the embedded data in the host image and verify if it is authenticated or not.

The medical image authentication schemes can be classified into: A digital signature (meta data) based and watermarking based. In the digital signature, the header data or physician digital signature that is stored along with the medical image is used to verify the data authenticity [Schneider 96] [Umamageswari 14] [Lo 14]. In watermarking, embedding invisible information in the host data, then it extracts and verifies the authenticity. The watermarking approach is widely used for the security goal. [Vellaisamy 14] [Memon 14].

4.7 Medical image security applications
Many works in the medical image watermarking and cryptography techniques for security issue are proposed in the literature. We have presented in this section the most significant and important approaches of the watermarking and cryptography applications in the medical sector. Some of them presented the watermarking approaches in the frequency domain, while there are many works in the spatial domain. Based on previous studies, the frequency domain is better than the spatial domain in robustness security issue. But, spatial domain is better than the frequency domain in the complexity
issue. Since we work with the real time applications (Telemedicine), our contribution focus in the spatial domain for less complexity goal, and improvement of the compromise between robustness, capacity and imperceptibility requirements.

In this section, we divided the existing security applications in the medical sector into two categories. The first category is the pure watermarking techniques that are applied in the frequency and spatial domains. While the second category is the medical image application based on cryptography and watermarking techniques.

4.7.1 Pure watermarking applications in the medical image

In [Kannammal 11], the authors presented multiple and fragile image watermarking of DICOM medical image based on Haar-DWT frequency domain of four levels. The approach addressed the problem of the source authentication, the medical information authentication and transmission of patient analysis details. Multiple watermarks are also used: the reference watermark, Tamper Assessment Factor (TAF), and physician's signature. When using the Haar wavelet technique, the authenticity was satisfied against some kind of attacks, but for other attacks such as rotation and cropping, contrast, flip, blurring, sharpening, salt and pepper noise, and Gaussian noise, we note a remarkable loss of the embedded data.

Another watermarking approach in the frequency domain is presented in [Fakhari 11]. A new and robust technique is proposed for medical image. The approach aimed to protect the copyright of the content and ensure the authenticity of the patient information. It consists to divide the image into three wavelet transform by using a graph theory approach to find optimal places to embed the watermark key. The algorithm ensures a good invisibility and robustness, especially against LSB attacks and is reliable enough for tracing the intruder.

In [Dong 12], The authors presented a zero watermarking blind technique using both DWT and DCT in order to enhance the robustness against common and geometric attacks and the invisibility of watermark. Also, the approach aimed to provide a confidential and integrity (privacy) security issues of the medical information through the transmission between the hospitals. The technique had improved the process of choice of regions of interest (ROI). The embedding process consists to apply Arnold
transform to the binary watermarking image, then decompose the image into one layer DWT, after that compute the DCT for the whole LL part to get featured vector. The lowest frequency in feature vector is chosen and one gets the sign sequence. The experimental result shows a good robustness against different attacks and high weakness when applying JPEG compression and Median Filter attacks.

[Coatrieux 13] proposed a medical image system to verify the image integrity. The system extracts the signature information from the ROI or from the pixel blocks of the Region of Interest (ROI). Then, the extracted signature is embedded in the no significant part of the image Region of Non Interest (RONI). At the verification side, the extracted signature is compared with the recomputed signature at the three level protection L1, L2 and L3. For each integrity level, there is an independent and specific signature. The level one is focused on the detection, while the level two is imported in the localization, and the level three are focused on the approximation of the image degradation. The system has limited with some kinds of degradation and alteration like compression, filtering, rotation, and brightness. But it did not cover the other kinds of attacks. It is not global over all the images tampering.

In [Li 12], the authors presented a blind zero watermarking approach in the frequency domain. The approach is applied in the medical image and based on Discrete Cosine Transform (DCT). The scheme is merging the visual feature vector with encryption technique. Firstly, DCT technique is applied to the medical image and 9th lowest frequency coefficients are chosen. After that, obtained the sign sequence of low frequency coefficients. By using the watermark information and the feature vector, they compute the key sequence based on the HASH function cryptography. The algorithm is given a full consideration of the visual properties of the watermark embedding, which means a low degradation in the watermarked image. The approach provides acceptable capacity and low in complexity. Also, it has a strong robustness against cropping and scaling attacks. But, the quality of the extracted watermark image is very low after noise, compressions, rotation, rotation and translation attacks.
Chapter 4: Digital Medical Image and Telemedicine Security

In the literature review, a lot of watermarking works are applied to the medical image either in the frequency or spatial domains. We have presented some of them. Other works are presented in [Arsalan 12], [Badshah 15], [Bhalerao 13] and [Lei 14].

4.7.2 Cryptography and watermarking applications in the medical image

In this type of approaches, cryptography and watermarking techniques are combined to reinforce the security requirements [Puech 08]. [Ribeiro 14] proposed software to outsource the medical image in the Cross-Enterprise Document Sharing (XDS). XDS’s combination outline offers an essential guideline for sharing the healthcare documents through the medical society. The authors’ outcomes are the confidentiality, interoperability and search ability of the medical information in XDS system. The proposed approach is based on the new searchable encryption system (PPSE). They tried to improve and guarantee the healthcare data protection in the cloud domain.

In [Umamageswari 14], the authors presented encryption and watermarking approach in order to achieve high confidentiality, authenticity and reliability of the medical image. The hash value of the medical image is computed, then the extracted message is encrypted using the RSA technique to get the digital signature. The digital signature and patient information obtained are considered as the watermark. They are embedded in the host image using the reversible watermarking technique. At the receiver side, The receiver extracts the patient information and the digital signature to check its authenticity and integrity also to achieve high confidentiality. The embedding and extraction process based on the secret key to achieve higher authenticate level. The technique provided high capacity (embedding large data) into the medical image. The degradation and the distortion of the medical image data is happening after a compression like JPEG.

The authors in [Kobayashi 09] presented encryption technique of the DICOM images. The original pixel data is encrypted and the encrypted version is stored instead of the original data. The techniques based on three entities: the header data to identify the patient data. The pixel data to validate the image itself. And the authentication entity data to improve the authorship of the image. On the verification side, the authenticating entity has to deal with the stored security data in the header and the pixel data, then the encrypted data has to be decrypted using the security data to determine the
image integrity. The proposed technique provided robust reliability for medical image without any degradation in its quality. The encrypted data frame is similar to the original data frame. Also, the technique has to be improved in order to shrink the time required to encrypt and decrypt huge images.

In [Bouslimi 12 (a)], the authors presented a joint encryption and watermarking approach. The approach aimed to verify the integrity and authenticity of the medical image in the spatial domain as well as in the encrypted domain during the transmission and storage. The technique is based on the quantization index modulation (QIM) with encryption algorithm, encryption algorithm can be a stream cipher RC4 or a block cipher AES. The approach conducted two main processes: protection and verification. Protection phase consists in the watermarking and encryption of the medical image. It embedded two messages by using two keys. Each message contains a security information called authenticity code (AC) which proves the image originality and integrity. In the verification phase, one message has to be extracted from the watermarked image using one key, while the other message has to be decrypted from the encrypted image using the second key. The reliability decision is conducted based on the two messages reliability. The performance evaluation of the Peak Signal to Noise Ratio (PSNR) achieved is around 49 dB without applying attacks. The experimental result shows that the quality is acceptable and the capacity is sufficient for embedding. Similar work is presented in [Bouslimi 12 (b)]. The authors combined the RC4 stream cipher and two replacements watermarking variations: Least Significant Bit approach and the Quantization Index Modulation.

A hybrid watermarking and encryption algorithm is also presented in [Kannammal 14]. The watermarking technique is performed based on symmetric matrix to build the new non-tensor product wavelet filter banks, where it provides the capability to disclose the singularity in several situations. While the encryption is performed based on three encryption techniques RSA, AES and RC4. The original image is natural image and the medical image is the watermark image. After one level wavelet decomposition, the medical image is embedded in the low high sub-band coefficient of the original image. The embedding is done by using least significant bit approach, then inverse decomposition is done to obtain the watermarked image. The watermarked image is encrypted by using RSA, AES and RC4. At the decryption/ extraction phase, the encrypted watermarked image is
decrypted using RSA, AES and RC4 in order to obtain the watermarked image, then, wavelet
decomposition one level is applied to the watermarked image to get the four sub-bands (LL, LH, HL
and HH). The LH sub-band is considered to extract the embedded watermark image, and inverse LSB
is applied to obtain the medical image (watermark). The scheme applied three different cryptography
techniques with the watermarking technique. The encryption / decryption time was less for RC4 than
for AES and RSA. Also, the performance and speed of RC4 were better than AES and RSA. The
correlation value was around 1 for AES and RSA while it was around 0.9 for RC4, which means the
image quality by using AES and RSA is better than by using RC4. The PSNR values were better by
applying RC4 than AES and RSA (lossless). The approach has the ability to resist to different attacks
like noise, rotation, contrast and brightness attacks, where the PSNR was around 91 dB after different
attacks.

The authors in [Al-Haj 15 (a)] proposed cryptography algorithm and digital signature approach in
order to prove the confidentiality, authenticity and integrity of the pixel data medical image as well as
for the header. The cryptographic key and the signature are created from the header and pixel data,
which has established a strong connection between the medical image data and security data applied
in the algorithm. The scheme is based on asymmetric and symmetric data encryption to offer the
confidentiality, integrity and authenticity of DICOM’s header and pixel data. To attain the
confidentiality, the pixel is encrypted, while the authenticity and integrity is attained by applying the
digital signature. The approach is considered as two processes: encryption and signature generating
process, decryption and confirmation process. At the encryption and signature generation process, the
header and data pixel are encrypted using hash function and the output is divided into two parts. First
part is used as encryption key while the second part is used as the initialization vector. The encryption
key and the initialization vector are used to encrypt the confidential attributes of the header and data
pixel based on AES-GCM. Then, by using CDSA, embedding the authentication tag of the header
with the private key of the sending object and save the result as a digital signature in the header. The
approach is robust against statistical attacks and it achieved acceptable encryption and decryption time
performance (low in encryption and decryption time). But, the entropy was around 7 bits/pixel, also, the PSNR was around 11 dB.

A lot of techniques merging watermarking and cryptography are proposed in previous studies. We have presented some of them. Other works can be found in [Bouslimi 15], [Guo 15] and [Al-Haj 15 (b)].

4.8 Conclusion
The medical image is one of the most important elements in the telemedicine and the health care sector. Therefore the security of medical image is very important to prevent the intentional or unintentional distortion. Meanwhile, the confidentiality, the authenticity and the integrity are working together. You cannot separate one from the others and each one depends on the others. In the literate review, there are two ways to obtain the security of medical images: watermarking and meta data (digital signature). Encryption technique can also be used to increase the security level.

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

Our work aims at filling some of the gaps of the previous solutions and to ensure the security of the medical image during the transmission and storing by providing watermarking solutions with better compromise between the watermarking requirements and cryptography solutions ensuring symmetric key security with less complexity.
SECOND PART

Our contributions are presented in this part. Chapter 5 includes pure watermarking approaches in the spatial and frequency domain, while chapter 6 presents a pure cryptographic approach. Also, we present a hybrid cryptographic and watermarking approach in chapter 7. All of these contributions are published in international journals or conferences.

In chapter 5, we aim at providing watermarking solutions to meet the real time requirements of telemedicine, namely execution time and memory space constraints. As we mentioned in the first part, robustness is another critical issue in telemedicine. Based on the previous studies, the frequency domain is better than the spatial domain in robustness security issue. The spatial domain is better than the frequency domain in the complexity issue. To meet real time constraints (less complexity as far as execution time and memory space are concerned) and improve the barter between robustness, capacity and imperceptibility, we have proposed the following solutions:

- An approach based on FCA which provides the way to find a distribution of the embedding area in order to improve the robustness and imperceptibility. The payload of the watermark is not that large since it is generated from the header information of the DICOM image. Moreover, the complexity of our approach is not huge.

- An approach based on ZBDD. We investigate the way to generate adaptive and informed watermark based on ZBDD rules, which has an impact on the storage space.

- An approach based on Weber’s law which provides high robustness. Indeed, it generates informed watermark based on Weber differential excitation and the informed watermark gives the ability to detect the tampered zones.

- An approach in frequency domain based on DWT. It provides more robustness, high imperceptibility as well as low complexity in comparison to existing approaches.

We can summarize the achieved goals of our work in watermarking part as follows:
<table>
<thead>
<tr>
<th>Our approach</th>
<th>Domain</th>
<th>Robustness</th>
<th>Imperceptibility</th>
<th>Payload</th>
<th>Less complexity</th>
<th>Other advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCA</td>
<td>Spatial</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Reversibility and tamper detection.</td>
</tr>
<tr>
<td>ZBDD</td>
<td>Spatial</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Adaptive watermark and lossless</td>
</tr>
<tr>
<td>Weber</td>
<td>Spatial</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Tamper detection</td>
</tr>
<tr>
<td>DWT</td>
<td>Frequency</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>-</td>
</tr>
</tbody>
</table>

In cryptography part (chapter 6), we investigated two security issues: key exchange in secure way and less complexity. N-gram provides a way to generate symmetric key. The relation between the key and the image content increases the robustness of the technique and the security issue. Moreover, this relation provides some predictability which is useful in case of attack. Indeed, part of the key or the entire key can be reconstructed in case of attack. The complexity of the proposed technique is less than that of the classical approaches, while the obtained decrypted image has high fidelity by comparing it with the original image.

In combined watermarking and cryptography part (chapter 7), we are aiming to increase the security level of the digital material by taking the advantages of the two techniques with high concentration about complexity and reversibility aspect.
Chapter 5: Watermarking Approaches

5.1 Introduction
In this chapter, we will present our contributions in watermarking domain. These solutions aim at meeting real time constraints (less complexity as far as execution time and memory space are concerned) and improving the barter between robustness, capacity and imperceptibility in telemedicine. The remaining of the chapter is organized as follows.

In the second section, we present our approach based on formal concept analysis to improve robustness of medical image watermarking scheme in the spatial domain. The third section deals with our watermarking approach which generates an optimal informed and adaptive watermark image based on Zero-Suppressed Binary Decision Diagram for medical images. The fourth section is dedicated to novel robust informed watermarking approach and tamper detection based on Weber Differential Excitation descriptor. The approaches presented in section 5.2, 5.3 and 5.4 are watermarking approaches in spatial domain. The last section presents a novel watermarking approach in the frequency domain, namely CT scan images watermarking scheme in DWT transform coefficient.

5.2 Formal Concept Analysis to Improve Robustness on Medical Image Watermarking Scheme in the Spatial Domain.
In this section (5.2), we present a novel robust approach for medical image watermarking in the spatial domain based on the Formal Concepts Analysis (FCA) model [Ganter 12]. The FCA allows us to find an optimal insertion position in the non-region of interest (NROI) of medical images. We extract the watermark information from the header of medical image information (IODs). The watermark information is defined by Patient Name, Patient Date Of Birth, Patient Age and File Modified Date information. There are relations between these types of watermark information that can help us to know if any (cutting, adding, replacing) attacks have happened (Tamper Detection). Our experimental results show that we extract the embedded watermark image with high quality, low payload and low computational complexity from the attacked watermarked image after attack scenarios.
This part is organized as follows: in the second section, we present the FCA model, definitions and domains of application. The third section is dedicated to the proposed approach (embedding and extraction phase). Fourth section shows the experimental results (robustness, capacity, and complexity and tamper detection). The conclusion is presented in the fifth section.

5.2.1 Formal concept analysis (FCA)
FCA was initially developed in data analysis, knowledge representation and knowledge discovery in databases (KDD) [Alqadah 11]. The FCA can provide a support for processing large dynamic, complex data sets with additional knowledge. It is a sub field of applied mathematics based on the lattice theory. Starting from a formal context built by a set of objects that share a number of properties, this method returns a lattice with a special property, the Galois property. The objects, and the properties which are also called attributes, can be more or less abstract depending on the type of application. In different applications, the appropriate choice of the context allows to obtain more information from the lattice. The FCA has been applied in various fields such as data mining, conceptual modelling, social networks and the semantic web [Alqadah 11] and [Wille 92]. For FCA in ontology engineering, the paper of Richard [Richards 97] was the first paper using FCA in combination with ripple-down rules to extract ontological vocabulary from knowledge bases. FCA played the role of a tool for ripple down rules (RDR), performing the derivation of concepts and the relation between them. The authors in [Jiang 03] combined FCA with natural language processing for building ontology in the field of cardiovascular medicine. In our paper, this theory is applied with an appropriate choice of objects and attributes in order to determine the region of encryption of the watermark. Let us do a short presentation of the FCA.

5.2.1.1 FCA definition
The basic notions in FCA are: a formal context that is a triple set $\mathcal{B} = (G, M, I)$, where $I \subseteq G \times M$ is a binary relation. This triple set can be represented by a cross table, as a set of rows $G$ (formal objects) and a set of columns $M$ (formal attributes); the points where they cross represent the relation $I$. The notation $gI\!m$ stands for $(g, m) \in I$, which is read as: the object $g$ has the attribute $m$ [Ganter 12].
Two sets $X'$ and $Y'$ are defined:

For $X$ a subset of attributes, $X' = \{ g \in G | g \text{Im for all } m \in X \}$  \hspace{1cm} (5.1)

the set of all objects in $G$ sharing all attributes in $X$

For $Y$ a subset of objects, $Y' = \{ m \in M | g \text{Im for all } g \in Y \}$  \hspace{1cm} (5.2)

the set of all attributes in $M$ falling under all objects in $Y$

A formal concept is considered to be a unit of two parts: the Extent (a set of objects), and the Intent (a set of attributes) such that all the objects in Extent have all the attributes in Intent and conversely i.e. all the attributes in the Intent fall under all objects in Extent.

5.2.1.2 Sub-concept relation, Super-concept relation

The concept $(A_1, B_1)$ is a sub-concept of the concept $(A_2, B_2)$ if $A_1 \subseteq A_2$ or $B_2 \subseteq B_1$. So $(A_2, B_2)$ is a super-concept of $(A_1, B_1)$. The relation sub-concept–super-concept is denoted by $\leq$. Being a sub-concept of a super-concept means that the extension of the sub-concept is contained in the extension of the super-concept, which is equivalent to the relationship where the intention of the super concept contains the intention of the sub-concept [Zenou 04].

FCA can be illustrated more clearly through an example. Let us suppose we have records for a set of images. For each image, there is a set of its features. We note the features $(M)$, $M = \{1, \ldots, 8\}$, as shown as follows:
Chapter 5: Watermarking Approaches

Table 5.2: The relation between Objects and Attributes

<table>
<thead>
<tr>
<th>Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Grayscale</td>
</tr>
<tr>
<td>B</td>
<td>Color</td>
</tr>
<tr>
<td>C</td>
<td>Smooth</td>
</tr>
<tr>
<td>D</td>
<td>Nature</td>
</tr>
<tr>
<td>E</td>
<td>Flat</td>
</tr>
<tr>
<td>F</td>
<td>Attacked</td>
</tr>
<tr>
<td>G</td>
<td>Watermarked</td>
</tr>
<tr>
<td>H</td>
<td>YCbCr</td>
</tr>
</tbody>
</table>

Table 5.1: The images and their features

<table>
<thead>
<tr>
<th>Objects(G)/Attributes(M)</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.2: The relation between Objects and Attributes
Table 5.3: Formal concepts of data given by the images and their features

<table>
<thead>
<tr>
<th>C1</th>
<th>&lt;A1,B1&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0</td>
<td>&lt;{}, {A, B, C, D, E, F, G, H}&gt;</td>
</tr>
<tr>
<td>C1</td>
<td>&lt;{1, 5, 9, 11}, {A, B, C, E}&gt;</td>
</tr>
<tr>
<td>C2</td>
<td>&lt;{2, 4, 12}, {A, B, F, H}&gt;</td>
</tr>
<tr>
<td>C3</td>
<td>&lt;{3, 6, 7}, {B, E, G}&gt;</td>
</tr>
<tr>
<td>C4</td>
<td>&lt;{3, 6, 7, 8, 10}, {G}&gt;</td>
</tr>
<tr>
<td>C5</td>
<td>&lt;{1, 3, 5, 6, 7, 9, 11}, {B, E}&gt;</td>
</tr>
<tr>
<td>C6</td>
<td>&lt;{1, 2, 4, 5, 9, 11, 12}, {A, B}&gt;</td>
</tr>
<tr>
<td>C7</td>
<td>&lt;{1, 2, 3, 4, 5, 6, 7, 9, 11, 12}, {B}&gt;</td>
</tr>
<tr>
<td>C8</td>
<td>&lt;{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}, {}&gt;</td>
</tr>
</tbody>
</table>

In table 5.1, we have 12 images (G), G= {1,….., 12}. Our example describes the images and their features in 12×8 binary matrix I (table 5.2). In the following, C refers to a concept, and A and B are extent and intent, respectively.

In table 5.2, the first formal concept, C0, contains zero object (extent) with all attributes (intent), which means no image contained all the descriptions. For the second formal concept, C1, the images 1, 5, 9 and 11 contain features 1,2,3,5. In the last concept, C8, it means that there is no feature contained in all the images from 1 to 12. The first concept includes zero object with all attributes and the next concept includes the sharing objects with their attributes and so on to the last concept. We denote the extent is increasing and the intent is decreasing until the intent is empty intent=∅ (Incrementing way). In the same way, if we take a look at the concepts from C0 to C8, we note that the concept C8 includes all its extent (objects) with empty intent (attributes) and that the previous (C7) concept decreases the extent and increases the intent until the extent becomes the empty set extent=∅ (Decrementing way). Figure 3 illustrates the lattice called also formal concept analysis line diagram between the images and the features they contain.
Chapter 5: Watermarking Approaches

5.2.2 FCA domains
The FCA application is very diverse, since FCA has been applied with some disciplines such as software engineering, knowledge discovery and information retrieval. The work presented in [Krone 94] was the first research applying the FCA in software engineering. It consisted in applying the FCA for analyzing the relationships between source code and preprocessor variables in UNIX system software. The authors extracted configuration structure from existing source code to build the concept lattice.

The second domain of FCA application is web mining. FCA is applied in order to improve the quality of web search. The first application of the FCA to internet data is [Krohn 99]. It analyzed the relationship between keywords used by users to retrieve domain-specific documents. FCA was employed to derive a concept lattice from the usage of a group of users and seeing how documents are related to one another to get a meaningful context for enhancement and find more interesting links for the user searching. Another approach in web-mining based on FCA is available in [Cole 01]. It was browsing web-documents. The authors presented how one can use a Web-based FCA system for classification of real estate properties. The authors in [Cole 00] built the Conceptual email manager (CEM) system, which stored its email in a concept lattice to browse through email collections and

Figure 5.1: Line diagram of formal concept analysis for images and their features
Chapter 5: Watermarking Approaches

retrieve the stored email. In [Carpineto 05] FCA was used to build the lattice for contextual information retrieval (IR) in applications for mining the web results returned by a search engine. It is used in a Meta search engine in the CREDO system.

The third domain of FCA applications is text mining and linguistics. In [Priss 96], the authors described an FCA application to lexical databases and faceted thesauri structures. In [Hotho 02], the authors presented a new approach of knowledge preprocessing to improve clustering results based FCA.

The fourth domain is FCA-based knowledge discovery in biology and medicine field. The paper of Cole and al. [Cole 96] is the first one which applies FCA in combination with the medical nomenclature system for analyzing a large collection of medical discharge summaries. The authors used a set of patient medical data as a set of training. The lattice concept’s structure captures the specialization/generalization information are presented in SNOMED and combinations concepts appearing in the documents. These documents were considered as formal objects and the medical concepts contained in SNOMED were considered as formal attributes. The paper [Schnabel 02] applied FCA to analyze diseases, treatments and symptoms to find implications and relationship hidden in the data, FCA applied to be expert system in medicine.

For ontology engineering based FCA, the paper [Richards 97] was the first one to use. FCA in combination with a ripple down rules to extract ontological vocabulary from knowledge bases. FCA played as a tool into ripple down rules (RDR) and supported the derivation of concepts and the relation between them. In [Jiang 03], we can find a combination of FCA with natural language processing for building ontology in the cardiovascular medical domain.

We apply the FCA principle in the watermarking techniques to determine an optimal position of embedding, in order to obtain low complexity, low capacity, high robustness and high imperceptibility for the embedding and the extraction process. The optimality is considered here according to watermarking requirements.
5.2.3 The proposed approach

5.2.3.1 Embedding phase

Figure 5.2 illustrates the watermark embedding scheme. Our embedding steps can be summarized by the following:

1- We generate out the watermark information from the header of the medical image. The watermark information includes the Patient Name (PName) in the first watermark ($w_1$), Patient Date Of Birth (PDOB) in the second watermark ($w_2$), Patient Age (PAge) in the third watermark ($w_3$) and File Modified Date (FMD) in the fourth watermark ($w_4$), as illustrated in the algorithm I. We have chosen these four watermark information from IOD’s because there is a relation between them and, then, we can verify if the relation is kept. In our approach we calculated, from FMD and PDOB, the age and we compared the result with the watermark age.

$$w = \{w_1, w_2, w_3, w_4\} \in IODs$$

The building of the watermark from the DICOM header can be summarized as follows:

**Algorithm I**

**INPUT:** DICOM Image  
**OUTPUT:** $w_1, w_2, w_3, w_4$ (watermarks) // as four JPEG images
Chapter 5: Watermarking Approaches

Read DICOM image
Extract the PName, PDOB, PAge and FMD

\( w_1 \leftarrow \text{JPEG conversion of PName.} \)

\( w_2 \leftarrow \text{JPEG conversion of PDOB.} \)

\( w_3 \leftarrow \text{JPEG conversion of PAge.} \)

\( w_4 \leftarrow \text{JPEG conversion of FMD.} \)

end

2- We isolated the zero area and started the extraction from the data area in NROI. We extracted a four 12 × 12 sub-matrices from the original image \( i \): Left-Up, Left-Down, Right-Up, Right-Down, as we can see in figure 5.3. Then, we converted the pixel values to the binary form and the result gave us a four 144 × 8 Boolean matrices, as we can see in figure 5.4.

\[
\begin{align*}
\text{Left - Up} &= \begin{pmatrix}
(0,0) & (0,1) & \ldots & (0,j-1) \\
(0,1) & \ldots & (0,1) \\
\vdots & \ddots & \ddots & \ddots \\
(i-1) & \ldots & (i,0) \\
\end{pmatrix} \\
\text{Right - Up} &= \begin{pmatrix}
(0,0) & (0,1) & \ldots & (0,j-1) \\
(1,0) & \ldots & (1,0) \\
\vdots & \ddots & \ddots & \ddots \\
(i-1) & \ldots & (i,0) \\
\end{pmatrix}
\end{align*}
\]

\[
\begin{align*}
\text{Left - Down} &= \begin{pmatrix}
(0,0) & (0,1) & \ldots & (0,j-1) \\
(0,1) & \ldots & (0,1) \\
\vdots & \ddots & \ddots & \ddots \\
(i-1) & \ldots & (i,0) \\
\end{pmatrix} \\
\text{Right - Down} &= \begin{pmatrix}
(0,0) & (0,1) & \ldots & (0,j-1) \\
(1,0) & \ldots & (1,0) \\
\vdots & \ddots & \ddots & \ddots \\
(i-1) & \ldots & (i,0) \\
\end{pmatrix}
\end{align*}
\]

(a) (b)

Figure 5.3: (a) Extraction of four 12 × 12 sub-matrices from \( i \), (b) Decimal representation of each sub-matrix

\[
\begin{align*}
\text{Left - Up} &= \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\end{pmatrix} \\
\text{Right - Up} &= \begin{pmatrix}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
\end{pmatrix}
\end{align*}
\]

\[
\begin{align*}
\text{Left - Down} &= \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & 0 & 0 & 0 \\
\end{pmatrix} \\
\text{Right - Down} &= \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & 0 & 0 & 0 \\
\end{pmatrix}
\end{align*}
\]

Figure 5.4: 144 × 8 Boolean Matrix for each area picked up

3- We built the FCA concepts for Left-Up, Left-Down, Right-Up, and Right-Down Boolean matrices. All the process of transformation of matrices Left-Up, Left-Down, Right-Up, Right-Down to obtain
Chapter 5: Watermarking Approaches

their FCA concepts is given by Algorithm II. We choose the row numbers as formal objects and the column numbers as formal attributes.

Matrices LUcon, LDcon, RUcon, RDcon, here below, contain all formal concepts built by FCA for Left-Up, Left-Down, Right-Up, Right-Down. The first group represents the extent and the second represents the intent. Because of the length of the concepts we could not list all elements of their extent and intent:

\[ LUcon = \langle \{133,160,176,\ldots\},\{9,10,11,12,\ldots\} \rangle, < \cdots > \]

\[ LDcon = \langle \{403,412,43\ldots\},\{12,15,17,21\ldots\} \rangle, < \cdots > \]

\[ RUcon = \langle \{133,137,152,\ldots\},\{494,498,500\ldots\} \rangle, < \cdots > \]

\[ RDcon = \langle \{399,442,446,\ldots\},\{496,499,500\ldots\} \rangle, < \cdots > \]

4- We built the FCA matrix positions for each region. The matrix position is a matrix built based on the extent \((A)\) and the intent \((B)\) as the pair \((A, B)\) of coordinates for each concept (elements of the sets extent \(\times\) intent).

The extraction of the four regions of \(i\), the building of the FCA lattice and the generation of the FCA matrix for each region are done as follows:

**Algorithm II**

INPUT: \(i\) (Original image)

OUTPUT: positions \((LU,LD,RU,RD)\) // positions obtained from FCA , which are used for embedding

// To extract the four regions of the original image
leftUp, leftDown, rightUp, rightDown

// Find the FCA concepts for each region, where \(A\) is extent and \(B\) is intent
\(con_1=\text{concepts(leftUp)}\)
\(con_2=\text{concepts(leftDown)}\)
\(con_3=\text{concepts(rightUp)}\)
\(con_4=\text{concepts(rightDown)}\)

// Build position matrix from FCA concepts

for \(i=\{1,2,3,4\}\)

\(pos_i=\{}\)

for each \(e\) in \(con_i\)

\(pos_i \leftarrow pos_i \cup e(1) * e(2)\)

end

position = \((pos_1,pos_2,pos_3,pos_4)\)
function concepts
INPUT: Region// leftUp, leftDown, rightUp, rightDown
OUTPUT : SetOfConcepts
// Initialize the concept list to empty set.
SetOfConcepts={}
//Convert the region into binary matrix
BinMat = dec2bin(region,8)
for each row G in BinMat
    for each column M  in BinMat
        if BinMat(G, M)
            for each  column S in BinMat
                if BinMat(G, S)
                    add the column number to B
                end for each column S1 in B, and each row G1 in BinMat
                    if BinMat(G1,S1)
                        add the row number to A
                    end
    end
end
add (A,B) to SetOfConcepts
end
for each item in (Ai,Bi) replace the value with zero in BinMat
B={} and A={};
end
return SetOfConcepts.
end

5- We embedded the four watermarks in the four regions Left-Up, Left-Down, Right-Up, Right-Down of the original image, as illustrated in algorithm III, by using the following linear interpolation:

\[
iw \in \{iw_{LUp}, iw_{LDpos}, iw_{RUp}, iw_{RDpos}\} \quad (5.3)
\]

\[
iw_{LUp} = (1 - t)w_1 + ti_{LUp} \quad (5.4)
\]

\[
iw_{LDpos} = (1 - t)w_2 + ti_{LDpos} \quad (5.5)
\]

\[
iw_{RUp} = (1 - t)w_3 + ti_{RUp} \quad (5.6)
\]

\[
iw_{RDpos} = (1 - t)w_4 + ti_{RDpos} \quad (5.7)
\]

here \(t \in [0,1]\) such that \(iw\), \(w_1, w_2, w_3\) and \(w_4\) are the watermarked image and the four watermark images, \(iw_{LUp}, iw_{LDpos}, iw_{RUp}, iw_{RDpos}\), respectively, representing the Left-Up, Left-Down, Right-Up and Right-Down positions in the watermarked image. Here, \(t_{LUp}, t_{LDpos}, t_{RUp}, t_{RDpos}\)
Chapter 5: Watermarking Approaches

\(i_{RDpos}\) represent Left-Up, Left-Down, Right-Up and Right-Down positions in the original image. The position we use is that extracted based on FCA from the Boolean matrices.

The embedding steps can be summarized as the following algorithm (algorithm III):

**Algorithm III**

**INPUT:** \(i\) (original image), four watermark images \((w_1, w_2, w_3, w_4)\), positions
**OUTPUT:** \(iw\) (watermarked image)

```
for each item in \(w_1\) watermark
    \(iw(positions(LU)) = (1-t) * w_1 + t * i(positions(LU))\)

for each item in \(w_2\) watermark
    \(iw(positions(LD)) = (1-t) * w_2 + t * i(positions(LD))\)

for each item in \(w_3\) watermark
    \(iw(positions(RU)) = (1-t) * w_3 + t * i(positions(RU))\)

for each item in \(w_4\) watermark
    \(iw(positions(RD)) = (1-t) * w_4 + t * i(positions(RD))\)

Save \(iw\) Image
```

Figure 5.5 A illustrates the watermarked image after embedding the four watermark images \((w_1, w_2, w_3, w_4)\) by using the linear interpolations in four regions (Left-Up, Left-Down, Right-Up, Right-Down), based on FCA concepts, to determine the positions in the NROI of original image \(i\).

Figure 5.5 B represents our watermark image, which includes information extracted from the DICOM header IODs; each watermark is converted into an image.

Figure 5.5 B illustrates the watermarked image for two different values of factor \(t\). As we can see in this figure, when \(t\) is close to 1 the watermark is invisible and there is no degradation in the image quality (figure 5.6, (b)), but if
the $t$ is close to 0 the watermark is visible and there is a little degradation in the image quality, as we can see in figure 5.6, (c).

![Figure 5.6: Watermark embedding with different values of t](image)

(a) Original image, (b) and (c) watermarked images

### 5.2.3.2 Extraction phase

In the extraction phase (algorithm IV), the matrix positions that are extracted from a Boolean matrix based on FCA are required ($LU_{pos}$, $LD_{pos}$, $RU_{pos}$, $RD_{pos}$). Then the extraction done by using the linear interpolations is as follows:

\[ w_a = \{w_{a1}, w_{a2}, w_{a3}, w_{a4}\} \]

\[ w_{a1} = \frac{1}{t} w_1 - \frac{1-t}{t} iw_{ALU_{pos}} \quad (5.8) \]

\[ w_{a2} = \frac{1}{t} w_2 - \frac{1-t}{t} iw_{ALD_{pos}} \quad (5.9) \]

\[ w_{a3} = \frac{1}{t} w_3 - \frac{1-t}{t} iw_{ARU_{pos}} \quad (5.10) \]

\[ w_{a4} = \frac{1}{t} w_4 - \frac{1-t}{t} iw_{ARD_{pos}} \quad (5.11) \]

such that $w_{a1}$, $w_{a2}$, $w_{a3}$ and $w_{a4}$ are the extracted watermarks and $iw_{ALU_{pos}}$, $iw_{ALD_{pos}}$, $iw_{ARU_{pos}}$, $iw_{ARD_{pos}}$ are the attacked watermarked image in the FCA concept positions. Figure 5.7 illustrates the extraction scheme for our approach.

![Figure 5.7: Watermark extraction scheme](image)
The extraction steps can be summarized in the following algorithm (algorithm IV).

**Algorithm IV**

**INPUT:** twa (attacked watermarked image), (w₁, w₂, w₃, w₄) position (LU_FCA, LD_FCA, RU_FCA, RD_FCA)

**OUTPUT:** wₐ₁, wₐ₂, wₐ₃, wₐ₄ (attacked watermark images)

for each item in w₁ watermark

\[ wₐ₁ = \left(1/t\right) * w₁ * \left(1-t/t\right) * iwa(\text{position} (\text{LU}_\text{FCA})) \]

for each item in w₂ watermark

\[ wₐ₂ = \left(1/t\right) * w₂ * \left(1-t/t\right) * iwa(\text{position} (\text{LD}_\text{FCA})) \]

for each item in w₃ watermark

\[ wₐ₃ = \left(1/t\right) * w₃ * \left(1-t/t\right) * iwa(\text{position} (\text{RU}_\text{FCA})) \]

for each item in w₄ watermark

\[ wₐ₄ = \left(1/t\right) * w₄ * \left(1-t/t\right) * iwa(\text{position} (\text{RD}_\text{FCA})) \]

save wₐ₁, wₐ₂, wₐ₃, wₐ₄

end

5.2.4 Experimental results

We performed our tests on a database of 100 DICOM images and here we took as an example the stomach CT medical database images of size 512 × 512. The original images come from [DICOM] while the watermark contains the four watermark images built from the header of the medical image.

The watermarking process has as the secret key \( t \), which varies exclusively between 0 and 1 in order to achieve visible and invisible watermarking. Similarly, we tested our proposed watermarking algorithm against several kinds of attacks, introduced using Stirmark Benchmark [Petitcolas 12], such as median filtering, JPEG compression, rotation, etc... We added Gaussian, salt and pepper noise and other attacks as shown in figure 6.8 A, figure 6.8 B shows the retrieved attacked watermarks. Through the obtained results we concluded that the invisible watermarking (\( t \) close to 1) gives better results than the visible one (\( t = 0.02 \)).
Figure 5.8: Attacked watermarked and retrieved watermark images
A Attacked watermarked image with t = 0.98
B Retrieved the attacked watermark images with t = 0.98

5.2.4.1 Robustness
Table 5.4 shows the PSNR values for extracted watermarks from an attacked watermarked image after geometric and non-geometric attacks made with Stirmark, compared with the original watermark. We compared our results with the proposed methods in [Li 12], [Tsai 12] and [Miao 12]. Our proposed scheme outperforms the algorithms introduced in [Li 12], [Tsai 12] and [Miao 12].

In order to further verify the robustness under image processing operations, we added Gaussian, salt and pepper noise, JPEG compression with quality factors 60 and 90, and image filtering as 3 × 3 and 5 × 5, used in methods [Su 13], [Li 12], and [Miao 12]. Table 5.5 lists the results of adding noise, which means that our proposed algorithm has stronger robustness. The metric used to measure the quality is a Normalized Cross Correlation (NCC).
## Chapter 5: Watermarking Approaches

### Table 5.4: PSNR quality measurements for extracted watermark after attacks

<table>
<thead>
<tr>
<th>PSNR</th>
<th>AFFINE_5</th>
<th>CROP_50</th>
<th>JPEG_90</th>
<th>MEDIAN_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_{a1}$</td>
<td>48.4227</td>
<td>41.4469</td>
<td>45.6388</td>
<td>45.7755</td>
</tr>
<tr>
<td>$w_{a2}$</td>
<td>41.8699</td>
<td>43.8399</td>
<td>41.9063</td>
<td>43.6029</td>
</tr>
<tr>
<td>$w_{a3}$</td>
<td>39.4454</td>
<td>38.5097</td>
<td>41.4123</td>
<td>41.0731</td>
</tr>
<tr>
<td>$w_{a4}$</td>
<td>45.5536</td>
<td>39.0599</td>
<td>46.3968</td>
<td>47.1297</td>
</tr>
<tr>
<td>[Li 12]</td>
<td>29.65</td>
<td>27.65</td>
<td>29.27</td>
<td>30.31</td>
</tr>
<tr>
<td>[Tsai 12]</td>
<td>16.58</td>
<td>13.38</td>
<td>26.93</td>
<td>27.25</td>
</tr>
<tr>
<td>[Miao 12]</td>
<td>11.56</td>
<td>10.50</td>
<td>17.61</td>
<td>18.64</td>
</tr>
<tr>
<td>PSNR</td>
<td>NOISE_80</td>
<td>ROT_45</td>
<td>ROTCROP_2</td>
<td>ROTSCALE_2</td>
</tr>
<tr>
<td>$w_{a1}$</td>
<td>47.3029</td>
<td>52.2202</td>
<td>47.3536</td>
<td>43.7296</td>
</tr>
<tr>
<td>$w_{a2}$</td>
<td>43.3088</td>
<td>40.6519</td>
<td>42.5764</td>
<td>41.5464</td>
</tr>
<tr>
<td>$w_{a3}$</td>
<td>39.9710</td>
<td>36.9476</td>
<td>39.3824</td>
<td>37.8864</td>
</tr>
<tr>
<td>$w_{a4}$</td>
<td>42.0503</td>
<td>38.8461</td>
<td>42.1563</td>
<td>44.9723</td>
</tr>
<tr>
<td>[Tsai 12]</td>
<td>33.14</td>
<td>31.56</td>
<td>33.55</td>
<td>33.72</td>
</tr>
<tr>
<td>[Miao 12]</td>
<td>7.93</td>
<td>18.65</td>
<td>19.21</td>
<td>19.18</td>
</tr>
</tbody>
</table>

Table 5.4: PSNR quality measurements for extracted watermark after attacks
Chapter 5: Watermarking Approaches

Table 5.5: NCC results after common image processing attacks

<table>
<thead>
<tr>
<th>NCC</th>
<th>Gaussian</th>
<th>Salt &amp; pepper</th>
<th>JPEG 60</th>
<th>JPEG 90</th>
<th>Median Filter 3 x 3</th>
<th>Median Filter 5 x 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed approach</td>
<td>w1</td>
<td>0.9987</td>
<td>0.9980</td>
<td>0.9987</td>
<td>0.9988</td>
<td>0.9980</td>
</tr>
<tr>
<td></td>
<td>w2</td>
<td>0.9995</td>
<td>0.9989</td>
<td>0.9989</td>
<td>0.9988</td>
<td>0.9991</td>
</tr>
<tr>
<td></td>
<td>w3</td>
<td>0.9990</td>
<td>0.9988</td>
<td>0.9983</td>
<td>0.9983</td>
<td>.9988</td>
</tr>
<tr>
<td></td>
<td>w4</td>
<td>0.9993</td>
<td>9994</td>
<td>0.9996</td>
<td>0.9996</td>
<td>0.9993</td>
</tr>
<tr>
<td>[Su 13]</td>
<td></td>
<td>0.9633</td>
<td>0.9413</td>
<td>0.9681</td>
<td>0.9980</td>
<td>0.9965</td>
</tr>
<tr>
<td>[Li 12]</td>
<td></td>
<td>0.88</td>
<td>0.92</td>
<td>0.96</td>
<td>0.99</td>
<td>0.90</td>
</tr>
<tr>
<td>[Miao 12]</td>
<td></td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
<td>0.91</td>
</tr>
</tbody>
</table>

Table 5.5: NCC results after common image processing attacks

From the above results in tables 5.4 and 5.5, we can conclude that our proposed method has a stronger robustness against geometric, non-geometric and common image processing attacks.

5.2.4.2 Capacity

Our watermark consists of four watermark images. After applying various attacks as we see in figure 5.8, we can retrieve the watermark. Even though there are degradations in the watermark image quality, we still have the possibility to retrieve the watermark. Our approach provides a low capacity. This is because the watermark that is embedded is very small in terms of size compared with the original image size and in comparison with the works in [Su 13] [Li 12] [Miao 12], as we can see in table 5.6. Our original image size is 512 × 512.
5.2.4.3 Complexity

In terms of measuring the complexity with the proposed approach, we calculated the execution time for the embedding and extraction process using MATLAB 7.14 with a CPU of 2.4 GHz and 2 GB RAM. Our proposed approach has a lower complexity than [Su 13]. Table 5.7 shows the execution time for embedding and extraction processes for our proposed methods and those of [Su 13].

<table>
<thead>
<tr>
<th>Watermark size</th>
<th>Proposed Approach</th>
<th>(w_1)</th>
<th>200</th>
<th>Total = 880 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(w_2)</td>
<td>312</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(w_3)</td>
<td>152</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(w_4)</td>
<td>216</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Su 13]</td>
<td></td>
<td></td>
<td>4096</td>
<td></td>
</tr>
<tr>
<td>[Li 12]</td>
<td></td>
<td></td>
<td>1056</td>
<td></td>
</tr>
<tr>
<td>[Miao 12]</td>
<td></td>
<td></td>
<td>1024</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.6: The bits used for the watermark image

<table>
<thead>
<tr>
<th>Time</th>
<th>Proposed method</th>
<th>[Su 13]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watermark embedding time</td>
<td>0.4125</td>
<td>0.5244</td>
</tr>
<tr>
<td>Watermark extraction time</td>
<td>0.3392</td>
<td>0.3701</td>
</tr>
<tr>
<td>Total time</td>
<td>0.7517</td>
<td>0.8945</td>
</tr>
</tbody>
</table>

Table 5.7: Comparisons of the execution time between the proposed method and the method in [Su 13]

5.2.4.4 Tamper detection

Our approach makes it possible to detect if there have been removal attacks or the addition of any new watermarks. By subtracting the fourth watermark from the second watermark, our approach gives us the third watermark. By comparing the subtraction result with the third watermark, we can know if
any removal or addition has taken place. For instance, after the extraction phase, we obtained four watermarks $w_{a1}, w_{a2}, w_{a3}, w_{a4}$. By subtracting the $w_{a4}$ (File Modified Date) from $w_{a2}$ (Patient Date Of Birth), the result should be the patient age, this value is equal to $w_{a3}$.

5.2.5 FCA conclusion
We presented a reversible novel watermarking approach in the spatial domain. Our approach is innovative and based on using Formal Concept Analysis. Its main feature is that it generates the optimal position for embedding. The watermark is built from some header information of the DICOM image. It is embedded into the NROI of the medical image. Based on experimental results, our approach demonstrates a lower computational complexity, using low capacity for the watermark and has a high robustness. Moreover, the approach can detect the removal and/or addition and/or replacement during attacks, which would be useful for tamper detection issues. Although the proposed approach has been limited in this approach to medical image, it could be used with other kinds of images. Moreover, our FCA approach has the ability to detect the attacks by comparing the extracted concepts from the watermarked image after attacks with the original concepts from the original image. However, FCA provided a distribution embedding area, which makes the imperceptibility is high.
5.3 Generating Optimal Informed and Adaptive Watermark Image Based on Zero Suppressed Binary Decision Diagram

Watermarks generation manner is one of the most important aspects in watermarking schemes, and should aim to produce as small watermark as possible (low data quantity to be embedded in the multimedia) to decrease the complexity of computational processes. Although embedding a large amount of watermark data in almost all different media increases the chances of recovering it, this also increases the complexity, which can become impractical for real time applications. In this approach, we focus on the robustness of medical image watermarks and present the means to generate a small watermark. This idea is very innovative in the watermarking field. The proposed approach is based on Zero-Suppressed Binary Decision Diagrams (ZBDD) [Minato 01]. ZBDD has proven its effectiveness in many fields, such as data mining, big data processing, computer networks, etc. Application of ZBDD to medical image watermarking will help us to take into account not only the complexity and the capacity factors but also the watermark robustness.

An optimized watermarking algorithm should have a minimum of calculation with a high robustness requirements. Such algorithms are useful for real time applications. The importance of capacity lies in not increasing the size of the original image with the addition of the watermark. The overall size of the watermarked image should be limited by embedding watermark data that are small and efficiently robust. An invisible watermark plays an important role in increasing the robustness. So a robust watermark can be extracted perfectly after exposure to attacks.

It should be noted that until now, there has been no robust watermark algorithm which resists attacks when hiding data [Laouamer 13] [Tsougenis 14]. Generally, in order to have more chances to recover the watermark, we need to hide a greater quantity of data [Shahid 12]. Also, another important point is how a watermark is generated. The watermark generated in a single, fixed operation and does not necessarily suit a large variety of different situations. Such generation process is a non-dynamic generation process. The fixed watermark obliges enough capacity.

In this approach, we proposed a solution regarding the problem of watermark generation and quantity
of data to be dynamically embedded. The proposed approach, which we consider to be highly innovative and original in the field of watermarking, is based on Zero-Suppressed Binary Decision Diagrams (ZBDD). The ZBDD model is known to reduce the large-scale of data by removing the unimportant part. Moreover, the main idea of the proposed algorithm is to build an optimized watermark based on image features, which we call an informed watermark. The ZBDD procedure is used to obtain the highest value pixels, which give the watermark its characteristics. We have tested the robustness of our solution against many kinds of geometric and non-geometric attacks.

This part is organized as follows: Second section presents the binary decision diagram, ordinary binary decision diagram and zero suppressed binary decision diagram principles. Section three presents the proposed approach. Section four is dedicated to the experimental results. A comparative study is presented in section five. The chapter ends by the conclusion and discussions.

### 5.3.1 Binary decision diagram (BDD)

BDD is a way to represent Boolean functions. Representation by BDD was inspired by the Shannon representation [Shannon 38] for Boolean functions. This representation makes it possible, for a fixed $i$, to rewrite the function $f: \{0, 1\}^n \rightarrow \{0, 1\}$ as:

$$f(x_1, x_2, ..., x_n) = (x_i \land f[x_i = 1]) \lor (\neg x_i \land f[x_i = 0])$$

where $f[x_i = 1]$ is the value of the function when $x_i=1$, $f[x_i = 0]$ is the value of the function when $x_i=0$, and the symbols $\lor$ (union) and $\land$ (intersection) from classical set theory stand respectively for the symbols $\lor$ (meet) and $\land$ (join) from formal logic and lattice theory.

BDDs can represent large datasets in an efficient way for functions and are becoming the most popular choice for Boolean functions representation [Günther 02]. It is easier to understand binary decision diagrams with an example, as illustrated in table 5.8, and figures 5.9 and 5.10.
Table 5.8: Truth Table for the given Boolean function $F$

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

$f(x_1, x_2, x_3) = \neg x_1 \cap x_2 \cup x_3$

Figure 5.9 shows a binary graph representation of $F$

In this graph, the $x_3$ variable refers to $x_2$ by one of two values: one or zero. Then, every $x_2$ value refers, in the same way, to an $x_1$ value to reach the terminals of one or zero. The paths that reach a terminal node with the value 1 are the following:
Chapter 5: Watermarking Approaches

\[
\{(\neg x_1, \neg x_2, x_3), (\neg x_1, x_2, \neg x_3), (\neg x_1, x_2, x_3), (x_1, \neg x_2, x_3)\}
\]

In the binary tree graph, some of the paths or some of their sub-paths will be found to be inefficient. The BDD reduces the representation of the binary tree graph as illustrated in figure 5.10, by eliminating unnecessary sub-paths. The BDD representation has two terminals, a 0 terminal and a 1 terminal. The nodes have two edges, the 0 edges and the 1 edges.

\[
\neg x_1 \cap x_2 \cup x_3
\]

Figure 5.10: Example of a BDD representing the given function

5.3.1.1 The combination set notion
A combination set is a set of elements, where each element is represented by a \(n\) bit number \(x_n x_{n-1} \ldots x_1\), where \(x_i\) refers to a bit. The elements of the combination set describe the solution to a combination problem by manipulation of the combination set.

A combination set can represent Boolean functions called \textit{characteristic functions} with \(n\) input variables. It can be represented by applying BDD.

All the possible combinations in the set will be represented by paths called "1 paths" if the terminal node is one, or "0 paths" if the terminal node is zero, as shown in figure 5.11 [Tzoref-Brill 13].
Ordinary Binary Decision Diagram (OBDD)

Ordinary Binary Decision Diagram (OBDD) is a structure which transforms a BDD into a more compact graph representing the same Boolean function, thus reducing the size of the graph. Unlike standard BDD, OBDD representation is unique in the sense that it does not depend on the variable order. OBDD can significantly enhance the graph representation by keeping the data volume small and thus using only a small amount of memory. The principle of OBDD is to delete duplicate nodes of a binary decision diagram that have no high value for large-scale data. OBDD is based on two reduction rules, the first of which consists of deleting duplicate node that refers to the same following node.

For example, in Figure 5.12(a), the node $x$ refers to the same function of either of its potential values (one or zero), so we can reduce the representation by applying ordinary BDD to remove $x$ from the
Chapter 5: Watermarking Approaches

graph. The second rule is to combine equivalent sub-graphs, as shown in Figure 5.12(b). The \( x \) node on the left side points to \( f_1 \) if the value is one, and to \( f_0 \) if the value is zero. In both these cases of \( x \), we can reduce the representation by removing one \( x \) node [Kurai 07].

5.3.1.3 Zero-Suppressed binary decision diagrams (ZBDD)

Figure 5.13 shows a Zero-Suppressed BDD (ZBDD) [Shahid 12] and [Shannon 38] for a given Boolean function and illustrates how a binary decision diagram is reduced in order to obtain a ZBDD. The nodes from which both branches point directly at the terminal node 0 are removed. Figure 5.14 gives an example of node elimination whose full arc points to 0. Figure 5.13 (a) gives graph to be reduced and Figure 5.13 (b) gives the fully reduced graph. This representation is more convenient and concise than OBDD, particularly for some applications based on the combination set bits. So ZBDD are widely used for large-scale combination set data and deal with reduction rules that are explained in the ordinary BDD. In ZBDD, it is the combination between the inputs rather than their number that is important. We can apply logic operations for the combination set in the graph, such as union, difference, product, etc. [Minato 01].

![Graph to reduce and Fully reduced graph](image)

**Figure 5.13: Reducing ZBDD represented by a given function \( f = \neg x_1 \cap x_2 \)**

ZBDD uses algebraic operations to reduce the size of the combination set: these algebraic operations include:

<table>
<thead>
<tr>
<th></th>
<th>(Empty set, 0-terminal node)</th>
<th>( \setminus ) (Difference)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \cup )</td>
<td>(Union)</td>
<td>( \cap ) (Intersection)</td>
</tr>
<tr>
<td>( 1 )</td>
<td>(Unit set, 1-terminal node)</td>
<td>( \times ) (Product)</td>
</tr>
</tbody>
</table>
Some examples of reductions by algebraic functions:

\( \{ABC, AB\} \cup \{AB, C\} = \{ABC, AB, C\} \)

\( \{ABC, AB\} \cap \{AB, C\} = \{AB\} \)

\( \{ABC, AB\} - \{AB, C\} = \{ABC, C\} \)

\( \{ABC, AB\} \times \{AB, C\} = (ABC \times AB) + (ABC \times C) + (AB \times AB) + (AB \times C) = \{AB, ABC\} \)

The item set histogram describes the numbers of the combination sets and their frequency in the dataset. As an example, table 5.9 gives the combination sets and their frequencies in the data.

<table>
<thead>
<tr>
<th>Combination sets</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>16</td>
</tr>
<tr>
<td>CDE</td>
<td>12</td>
</tr>
<tr>
<td>ADH</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 5.9: Items set histogram

5.3.2 Proposed approach to hide data in a medical image

In this section, we present our approach to the watermarking process. Three stages will be discussed. The first step is the generation of the watermark based on the ZBDD in an informed and adaptive way. The second step is the embedding of the generated watermark in the host image and the last step consists in extracting and examining the watermark after attacks have been applied.

5.3.2.1 ZBDD-based informed and adaptive watermark generation

As mentioned above, the embedding process requires generation of the watermark. This step is based on ZBDD, which helps us to optimize the size of the generated watermark in an adaptive and informed manner. By informed watermarking, we mean the creation of a watermark based on the existing information of the original media (in our case: the patient name of the header’s medical image). By adapting, we mean generation of a watermark with the smallest size possible. This adaptability is an important quality of a practical watermarking method for real-time applications. The process of watermark generation can be summarized as the following steps:

1- Define the Boolean selection function \( f \), whose value is not always zero. In order to illustrate the process, let us consider \( f \) defined as follows:
Chapter 5: Watermarking Approaches

\[ f(A, B, C, D, E, F, G, H) = \neg B \cap C \cap \neg D \cap \neg F \]

2- Build a truth table for the Boolean function. If the Boolean function result equals one, out of the variable set find the set of combinations that produce one. Below, we illustrate the set of combinations for the Boolean function \( f(1) \) with the set of 1s in the variables:

\[ f = \{ CH, CG, CE, AC, CEH, CEG, CGH, ACH, ACG, ACE, CEGH, ACGH, ACEH, ACEG, ACEGH \} = 1 \]

3- In the original image, convert the pixel values into 8 categories, where each category has a range of 32 units of intensity. So, category A consists of pixel values (intensity) from 0 to 31, category B, contains values from 32 to 63, and so on.

4- In the converted image, find the frequency of each element of the set defined in step 2 (item set histogram) and convert this frequency to binary form in 8 bits.

<table>
<thead>
<tr>
<th>Combination</th>
<th>Frequency</th>
<th>M-Digits (Binary representation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CH</td>
<td>13</td>
<td>f_A f_B f_C f_D f_E f_F f_G f_H</td>
</tr>
<tr>
<td>CG</td>
<td>3</td>
<td>0 0 0 0 0 0 1 1</td>
</tr>
<tr>
<td>CE</td>
<td>79</td>
<td>0 1 0 0 1 1 1 1</td>
</tr>
<tr>
<td>AC</td>
<td>25</td>
<td>0 0 0 1 1 0 0 1</td>
</tr>
<tr>
<td>CGH</td>
<td>1</td>
<td>0 0 0 0 0 0 0 0 1</td>
</tr>
<tr>
<td>CEH</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>CEG</td>
<td>8</td>
<td>0 0 0 0 1 0 0 0 0</td>
</tr>
<tr>
<td>ACH</td>
<td>13</td>
<td>0 0 0 0 1 1 1 0 1</td>
</tr>
<tr>
<td>ACG</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>ACE</td>
<td>6</td>
<td>0 0 0 0 0 0 0 0 1 1 0</td>
</tr>
<tr>
<td>CEGH</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>ACGH</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>ACEH</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>ACEG</td>
<td>1</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 1</td>
</tr>
<tr>
<td>ACEGH</td>
<td>0</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>

*Table 5.10: Item set histogram and binary representation*
Table 5.10 describes the combination sets, their frequencies in the original image \( i \), and their binary representation. In Table 6.3, we have to remove those combinations for which the frequency is equal to zero, such as \( \{CEH, ACG, CEGH, ACGH, ACEH, ACEGH\} \). The symbol \( f_0 \) represents the least significant bit, \( f_1 \) represents the second least bit and so on until \( f_7 \), which represents the most significant bit.

5- Build the ZBDD Map for the result from the previous step for each combination set as illustrated in figure 5.14.

6- Find the ZBDD vector for the item set histogram as follows:

\[
\begin{align*}
  f_7 &= \{\} , f_6 = \{CE\}, f_5 = \{\} , f_4 = \{AC\} , f_3 = \{CH,CE,AC,CEG,ACH\} , f_2 = \{CH,CE,ACH,ACE\} , \\
  f_1 &= \{CG,CE,ACE\} , f_0 = \{CH,CG,CE,AC,CGH,ACH,ACEG\}
\end{align*}
\]
7- Apply ZBDD rules. Based on the ZBDD reduction and sharing rules, we can note some paths are included in other paths, such as the combination CH represented in $f_3$, which should be involved in path ACH. So, after applying ZBDD, we can obtain the paths illustrated as follows:

- Remove $f_7, f_5$ // because the combination sets have frequencies equal to zero
- In $f_3$, because CH is included in ACH, remove CH; because CE is included in CEG, remove CE; because AC is included in ACH, remove AC. // intersection and union rules
- In $f_2$, because CH is included in ACH, remove CH; because CE is included in ACE, remove CE
- In $f_1$, because CE is included in ACE, remove CE.
- In $f_0$, because CH is included in ACH, remove CH;

Finally:

\[
\begin{align*}
  f_7, f_5 &= \emptyset \\
  f_6 &= \{CE\} \\
  f_4 &= \{AC\} \\
  f_3 &= \{ACH, CEG\} \\
  f_2 &= \{ACH, ACE\} \\
  f_1 &= \{CG, ACE\} \\
  f_0 &= \{CGH, ACH, ACEG\}
\end{align*}
\]

<table>
<thead>
<tr>
<th>Item set histogram</th>
<th>Combinations</th>
<th>Offered spaces (pixels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_0$</td>
<td>{CGH, ACH, ACEG}</td>
<td>{1<em>3, 3</em>13, 4*1=46 }</td>
</tr>
<tr>
<td>$f_1$</td>
<td>{CG, ACE}</td>
<td>{2<em>3, 3</em>6=24 }</td>
</tr>
<tr>
<td>$f_2$</td>
<td>{ACH, ACE}</td>
<td>{3<em>13,3</em>6=57 }</td>
</tr>
<tr>
<td>$f_3$</td>
<td>{ACH, CEG}</td>
<td>{3<em>13,3</em>8=63 }</td>
</tr>
<tr>
<td>$f_4$</td>
<td>{AC}</td>
<td>{2*25=50 }</td>
</tr>
<tr>
<td>$f_5$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$f_6$</td>
<td>{CE}</td>
<td>{2*79=158 }</td>
</tr>
<tr>
<td>$f_7$</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 5.11: The available spaces for the item set histogram
Chapter 5: Watermarking Approaches

8- Based on the offered spaces, as illustrated in table 5.11, choose the item set histogram that provides enough watermarking space (capacity) and good payload. $f7$, $f5$ and even $f7$ are not appropriated (low capacity). $f2$ meets the requirements, so we chose $f2$ with combination \{ACH, ACE\}. ACH’s frequency is 13 and its combination length is three characters (13*3=39 positions). ACE’s frequency is 6 and its combination length is also three (6*3=18 positions). Therefore, the total available number of positions for watermark embedding is 57 (39+18=57).

9- Generate a suitable watermark based on the available size of the chosen combination set. The generating algorithm steps are described in the algorithm I.

The watermark-generating algorithm can be summarized in the algorithm I as follows:

```
Algorithm I
INPUT: i (original Image), worig (patient name from medical image header)
OUTPUT: w (watermark)
for each l(i,j)
    if l(i,j) between [0,31]
        l(i,j) = 'A';
    elseif l(i,j) between [32,63]
        l(i,j) = 'B';
    elseif ....
    else l(i,j) = 'H';
end
/* Define Truth table for 8 variables by a given Boolean function F */
/* Define the combinations CS set where F=1 */
for each CS
    if frequency(CS)=0/* Occurrence number for each CS */
        Remove CS;
    else
        Bfreq(CS)=binary(frequency(CS));
    end
    //Bfreq is a two dimension matrix with combination sets as rows numbers and values //from 0 to 7 as columns numbers
end
for each i from 0…7 // Initial
    fi={};
    for each CS
        if (Bfreq(CS,i)=1)
            fi=fi U {CS}
    end
end
for each i from 0 to 7
```
Chapter 5: Watermarking Approaches

\[
\begin{align*}
    f_i &= \text{ZBDD reduction and sharing (fi)} \\
    f &= \text{selection among suitable } fi \\
    \text{offered\_space} &= 0 \\
    \text{for each } CS \text{ in } f & \\
    & \quad \text{offered\_space} = \text{length}(CS)\ast\text{freq}(CS) \\
    & \quad /\ast\text{generate watermark } w \\
    w &= \text{worig(offeredspace)} \\
    \end{align*}
\]

5.3.2.2 Watermark embedding

The main region of interest in a medical image (ROI) is the visual part with the most important and relevant information of interest to physicians. Generally, medical images in gray scale are displayed with a black, uniform background. Although this background does not have an interest in itself, it makes it possible to see the ROI more clearly and understand the portions of the image required to make a diagnosis. Figure 5.15 shows the main region of interest for a given image while the ROI extracting is done based on algorithm II.

\begin{center}
\textbf{Algorithm II}
\end{center}

\begin{itemize}
    \item INPUT : Img \text{ Medical Image}
    \item OUTPUT : ROI \text{ Region of Interest (Img)}
    \item Read the medical image
    \item //Convert the image into double
    \item //Crop out a 10\% pixel border
    \item // Find the threshold between ROI and NROI
    \item //Find the optimal coordinates for top\_left and bottom\_right of the ROI
    \item //Determine width and height of the ROI
    \item //Return ROI(Img) = i
\end{itemize}

End

Figure 5.15: Determination of the image main ROI

The size of the watermark (the amount of text to be embedded) depends on the choice of combination and its number of occurrences (frequency). For example, choosing a watermark in the case of \( f_j \):
Chapter 5: Watermarking Approaches

\[ f_2(frequency \ of \ combination \ ACH, ACE) = \text{freq}_{ACH} \times \text{freq}_{ACE} \]

\[ \rightarrow \text{watermark size} = \text{combination length ACH} \times \text{freq}_{ACH} + \text{combination length ACE} \times \text{freq}_{ACE} \]

The watermark embedding algorithm can be presented as follows (Algorithm III):

**Algorithm III**

INPUT: ROI, w (ROI of original image and watermark respectively), Boolean function F
OUTPUT: i_w (watermarked image)

Choose t close to 1/invisible watermarking

\[ i_w = (1-t)w + t*ROI(CS) \]

Linear interpolation

end

5.3.2.3 Watermark extraction

The extraction process for watermark \( w_a \) (an attacked watermark), after applying an attack, consists in extracting \( w_a \) from the attacked image \( i_{wa} \). This requires the reverse operation to the embedding process applied to the entire set of combinations selected at the embedding step. We thus extracted watermark \( w_a \) for each type of attack we tested, which included JPEG, Median filtering, Adding noise and Rotation. We summarize the watermark extraction process in algorithm IV below.

**Algorithm IV**

INPUT: \( i_{wa} \), w (attacked watermarked image, watermark image respectively)
OUTPUT: \( w_a \) (attacked watermark image)

for the same used F in embedding process

for each CS in image \( i_{wa} \)

Choose same embedding value of t

\[ w_a = (1/t)*CS(i_{wa}) - (1-t/t)*w \]

save \( w_a \) as attacked extracted watermark image.

end

end

5.3.2.4 Attacks and extracted watermark

To test the robustness of the proposed algorithm, the watermarked image \( i_w \) was subjected to several types of attack. To do this, we used Stirmark Benchmark; one of the most commonly used benchmark software tools, by making attacks on a given image [Petitcolas 12]. We chose some examples of the most dangerous attacks, described in table 5.12, and tested our algorithm on several medical images,
Chapter 5: Watermarking Approaches

with different Boolean functions for each one. We present the generated watermarks and the extracted ones for each Boolean function.

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Attack Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crop_50</td>
<td>Cropping image (up to 50%)</td>
</tr>
<tr>
<td>JPEG_90</td>
<td>JPEG compression with a quality factor F=90</td>
</tr>
<tr>
<td>Median_9</td>
<td>Median filtering (3 × 3)</td>
</tr>
<tr>
<td>Noise_80</td>
<td>Gaussian Noise with density degree=80</td>
</tr>
<tr>
<td>Rot_45</td>
<td>Rotating image with 45 degree</td>
</tr>
<tr>
<td>RotScale_-2</td>
<td>Rotation + Rescale (Level -2)</td>
</tr>
</tbody>
</table>

Table 5.12: Description of the attack types used

Figures 5.16, 5.17, 5.18, 5.19, 5.20 and 5.21 below illustrate the watermarks extracted after applying different kinds of attacks:

Figure 5.16: Attacks on the watermarked hand image $i_{w_a}$ and the extracted watermarks $w_a$ in the case of the Boolean function $F = \neg B \cap C \cap \neg D \cap \neg F$

Figure 5.17: Attacks on the watermarked hand image $i_{w_a}$ and the extracted watermarks $w_a$ in the case of the Boolean function $F = \neg A \cap B \cap C \cap \neg F \cap \neg H$
Chapter 5: Watermarking Approaches

Figure 5.18: Attacks on the watermarked brain image $i_w$ and the extracted watermarks $w_a$ in the case of the Boolean function $F = \neg B \cap C \cap \neg D \cap \neg F$

Figure 5.19: Attacks on the watermarked brain image $i_w$ and the extracted watermarks $w_a$ in the case of the Boolean function $F = \neg A \cap \neg B \cap \neg D \cap F \cap \neg H$

Figure 5.20: Attacks on the watermarked brain image $i_w$ and the extracted watermarks $w_a$ in the case of the Boolean function $F = \neg B \cap C \cap \neg D \cap \neg F$

Figure 5.21: Attacks on the watermarked brain image $i_w$ and the extracted watermarks $w_a$ in the case of the Boolean function $F = \neg A \cap \neg B \cap \neg D \cap F \cap \neg H$
Chapter 5: Watermarking Approaches

We noted that for each image type and for each corresponding Boolean function, the original watermark \( w \) and the extracted watermark \( w_a \) are very similar to one another despite the different attacks, indicating that the proposed approach has a high robustness.

In the following section, we measure the degree of similarity between \( w \) and \( w_a \) through some well-known metrics such as PSNR (Peak Signal Noise Ratio) [Huynh-Thu 08] and correlation coefficient (CC) [Nakhmani 13] and [Imamura 11].

5.3.3 Watermarked image quality, watermark robustness and evaluation

To measure the robustness and the imperceptibility of an image watermarking algorithm, several metrics can provide answers. In this part, we are particularly interested in PSNR and CC.

The Boolean functions are used in our tests for all the illustrated images were:

\[
BF1 = \neg B \land C \land \neg D \land \neg F
\]
\[
BF2 = \neg A \land B \land C \land \neg F \land \neg H
\]
\[
BF3 = \neg A \land \neg B \land \neg D \land F \land \neg H
\]
\[
BF4 = \neg B \land \neg D \land E \land F \land \neg G
\]

5.3.3.1 Watermarked image quality

Imperceptibility is defined by the degradation in the watermarked image after embedding. So, a good quality watermarking approach has to preserve the watermarked image quality and it should be similar to the original image. In table 5.13, we show the quality of the watermarked image by calculating the PSNR values between the original image and the watermarked image.

<table>
<thead>
<tr>
<th>PSNR</th>
<th>Hand</th>
<th>Brain1</th>
<th>Brain2</th>
<th>Leg</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.F. 1</td>
<td>69.3270</td>
<td>66.8331</td>
<td>82.2948</td>
<td>69.9027</td>
</tr>
<tr>
<td>B.F.2</td>
<td>69.1272</td>
<td>60.9207</td>
<td>75.8523</td>
<td>71.8387</td>
</tr>
<tr>
<td>B.F.3</td>
<td>75.0513</td>
<td>70.5129</td>
<td>84.3446</td>
<td>75.1708</td>
</tr>
<tr>
<td>B.F.4</td>
<td>71.7414</td>
<td>70.5129</td>
<td>84.3446</td>
<td>75.1708</td>
</tr>
</tbody>
</table>

Table 5.13: PSNR values between \( i \) and \( iw \)
5.3.3.2 Watermark robustness

In this section, we test the robustness of our approach against different and dangerous attacks. It can be noted that the degrees of similarity between the original watermark $w$ and the extracted ones $w_a$ are very high, as can be seen in the results given in tables 5.14, 5.15, 5.16 and 5.17. We explain the results in the case of each metric. For PSNR, it should be noted that all its values for different attacks are beyond 34 dB, which means a strong similarity between $w$ and $w_a$. The CCs are very close to 1, which can be interpreted as a high similarity between $w$ and $w_a$.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>BF1</th>
<th>BF2</th>
<th>BF3</th>
<th>BF4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
</tr>
<tr>
<td>CROP_50</td>
<td>40.1018</td>
<td>0.9997</td>
<td>29.8648</td>
<td>0.9943</td>
</tr>
<tr>
<td>JPEG_90</td>
<td>37.8505</td>
<td>0.9989</td>
<td>29.7957</td>
<td>0.9941</td>
</tr>
<tr>
<td>MEDIAN_9</td>
<td>40.0017</td>
<td>0.9997</td>
<td>30.0467</td>
<td>0.9945</td>
</tr>
<tr>
<td>NOISE_80</td>
<td>37.9189</td>
<td>0.9988</td>
<td>29.9442</td>
<td>0.9942</td>
</tr>
<tr>
<td>ROT_45</td>
<td>37.6157</td>
<td>0.9997</td>
<td>29.9805</td>
<td>0.9943</td>
</tr>
<tr>
<td>ROTSCALE_-2</td>
<td>37.3323</td>
<td>0.9987</td>
<td>29.9660</td>
<td>0.9943</td>
</tr>
</tbody>
</table>

Table 5.14: Similarity metrics between $w$ and $w_a$ in the case of image “hand”

<table>
<thead>
<tr>
<th>Attacks</th>
<th>BF1</th>
<th>BF2</th>
<th>BF3</th>
<th>BF4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
</tr>
<tr>
<td>CROP_50</td>
<td>36.2317</td>
<td>0.9980</td>
<td>21.9538</td>
<td>0.9966</td>
</tr>
<tr>
<td>JPEG_90</td>
<td>36.9611</td>
<td>0.9980</td>
<td>44.5078</td>
<td>0.9999</td>
</tr>
<tr>
<td>MEDIAN_9</td>
<td>36.9611</td>
<td>0.9980</td>
<td>44.5078</td>
<td>0.9999</td>
</tr>
<tr>
<td>NOISE_80</td>
<td>35.6333</td>
<td>0.9972</td>
<td>40.4267</td>
<td>0.9991</td>
</tr>
<tr>
<td>ROT_45</td>
<td>36.2402</td>
<td>0.9979</td>
<td>47.2953</td>
<td>0.9999</td>
</tr>
<tr>
<td>ROTSCALE_-2</td>
<td>36.2317</td>
<td>0.9980</td>
<td>42.6714</td>
<td>0.9997</td>
</tr>
</tbody>
</table>

Table 5.15: Similarity metrics between $w$ and $w_a$ in the case of image “brain 1”

<table>
<thead>
<tr>
<th>Attacks</th>
<th>BF1</th>
<th>BF2</th>
<th>BF3</th>
<th>BF4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
</tr>
<tr>
<td>CROP_50</td>
<td>36.0896</td>
<td>0.9987</td>
<td>38.3022</td>
<td>0.9993</td>
</tr>
<tr>
<td>JPEG_90</td>
<td>36.1037</td>
<td>0.9987</td>
<td>37.3736</td>
<td>0.9990</td>
</tr>
<tr>
<td>MEDIAN_9</td>
<td>35.9711</td>
<td>0.9986</td>
<td>38.8671</td>
<td>0.9993</td>
</tr>
<tr>
<td>NOISE_80</td>
<td>34.3726</td>
<td>0.9981</td>
<td>36.1465</td>
<td>0.9989</td>
</tr>
<tr>
<td>ROT_45</td>
<td>35.6692</td>
<td>0.9987</td>
<td>36.6145</td>
<td>0.9992</td>
</tr>
<tr>
<td>ROTSCALE_-2</td>
<td>35.6677</td>
<td>0.9985</td>
<td>39.3871</td>
<td>0.9994</td>
</tr>
</tbody>
</table>

Table 5.16: Similarity metrics between $w$ and $w_a$ in the case of image “brain 2”
Chapter 5: Watermarking Approaches

Table 5.17: Similarity metrics between w and wa in the case of image “leg”

<table>
<thead>
<tr>
<th>Attacks</th>
<th>BF1</th>
<th>BF2</th>
<th>BF3</th>
<th>BF4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR</td>
<td>CC</td>
<td>PSNR</td>
<td>CC</td>
</tr>
<tr>
<td>CROP_50</td>
<td>38.0816</td>
<td>0.9991</td>
<td>41.2572</td>
<td>0.9996</td>
</tr>
<tr>
<td>JPEG_90</td>
<td>38.7965</td>
<td>0.9992</td>
<td>40.0483</td>
<td>0.9995</td>
</tr>
<tr>
<td>MEDIAN_9</td>
<td>38.7523</td>
<td>0.9992</td>
<td>42.0355</td>
<td>0.9996</td>
</tr>
<tr>
<td>NOISE_80</td>
<td>36.4988</td>
<td>0.9987</td>
<td>36.8882</td>
<td>0.9990</td>
</tr>
<tr>
<td>ROT_45</td>
<td>36.0470</td>
<td>0.9989</td>
<td>38.2284</td>
<td>0.9993</td>
</tr>
<tr>
<td>ROTSCALE_-2</td>
<td>38.5588</td>
<td>0.9992</td>
<td>41.9474</td>
<td>0.9996</td>
</tr>
</tbody>
</table>

Table 5.17: Similarity metrics between w and wa in the case of image “leg”

5.3.4 Comparative study

Our comparative study focuses on three aspects: imperceptibility, robustness and capacity.

5.3.4.1 Imperceptibility

Our comparative study focuses on three aspects: imperceptibility, robustness and capacity.

Imperceptibility was measured using PSNR and compared with the studies in [Tsougenis 14] and [Shahid 12]. Indeed, those works propose adaptive watermarking approaches whose watermark properties are similar to ours. Table 5.18 shows the average values of PSNR for our approach compared with these previous studies.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>PSNR</th>
<th>Hand</th>
<th>Brain1</th>
<th>Brain2</th>
<th>Leg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed</td>
<td>70</td>
<td>65</td>
<td>80</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>[Tsougenis 14]</td>
<td>39</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Shahid 12]</td>
<td>49</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.18: Comparative study of image quality

Table 5.18 shows there is a clear difference between our results and those from [Tsougenis 14] and [Shahid 12], as our image quality is much higher.

5.3.4.2 Robustness

In order to measure the robustness of our approach, we measured the PSNR and CC between the original watermark image and the attacked extracted watermark images. PSNR values were compared with the results in [Tsougenis 14] and average CC results were compared with those from [Shahid 12], as shown in tables 5.19 and 5.20.
Chapter 5: Watermarking Approaches

As we can note from tables 5.19 and 5.20, our approach obtained a better result than the previous studies in terms of robustness, with PSNR is around 37 dB and CC is around 0.9990.

### 5.3.4.3 Capacity
Capacity should be sufficient for the watermark payload, as is the case in our approach, but should also remain small enough to limit complexity. As shown in table 5.21, our approach provided a low capacity.

<table>
<thead>
<tr>
<th>Approach</th>
<th>JPEG</th>
<th>MEDIAN</th>
<th>NOISE</th>
<th>Cropping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed</td>
<td>37</td>
<td>38</td>
<td>36</td>
<td>39</td>
</tr>
<tr>
<td>[Tsougenis 14]</td>
<td>32</td>
<td>29</td>
<td>27</td>
<td>31</td>
</tr>
</tbody>
</table>

Table 5.19: PSNR robustness measurements and comparison with the work [Tsougenis 14].

<table>
<thead>
<tr>
<th>Approach</th>
<th>JPEG</th>
<th>MEDIAN</th>
<th>NOISE</th>
<th>Cropping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed</td>
<td>0.9990</td>
<td>0.9992</td>
<td>0.9995</td>
<td>0.9987</td>
</tr>
<tr>
<td>[Shahid 12]</td>
<td>0.9566</td>
<td>0.8075</td>
<td>0.9293</td>
<td>0.9233</td>
</tr>
</tbody>
</table>

Table 5.20: CC Robustness measurements and comparison with the work [Shahid 12].

As we can note from tables 5.19 and 5.20, our approach obtained a better result than the previous studies in terms of robustness, with PSNR is around 37 dB and CC is around 0.9990.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Hand</th>
<th>Brain1</th>
<th>Brain2</th>
<th>Leg</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.F.1</td>
<td>54</td>
<td>174</td>
<td>66</td>
<td>114</td>
</tr>
<tr>
<td>B.F.2</td>
<td>261</td>
<td>168</td>
<td>174</td>
<td>144</td>
</tr>
<tr>
<td>B.F.3</td>
<td>112</td>
<td>114</td>
<td>42</td>
<td>78</td>
</tr>
<tr>
<td>B.F.4</td>
<td>84</td>
<td>114</td>
<td>42</td>
<td>78</td>
</tr>
<tr>
<td>[Tsougenis 14]</td>
<td></td>
<td>1024</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Shahid 12]</td>
<td></td>
<td>1024</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.21: Adaptive watermark image size (bits) and compared with the works [Tsougenis 14] and [Shahid 12].
5.3.5 ZBDD conclusion and discussion
In this approach, we addressed the problem of generating watermarks as small as possible (small payload) to adapt the hidden data to real time applications by maintaining high robustness, high imperceptibility and low complexity within a medical image. We have proposed a novel and optimal approach that is completely innovative through its generation of an intelligent (adaptive) watermark based on ZBDD, a technique which has already proved its usefulness in many applications such as path reduction in wireless networks, production management, etc. An adaptive watermarking method based on Zero-Suppression in ZBDD can generate a watermark with a minimum size while preserving a strong robustness, thus fulfilling the needs mentioned above for low computational complexity and real time applications. We tested our algorithm under several attack scenarios and measured its robustness in the case of invisible watermarking based on linear interpolation. The results obtained show that our techniques represent a new-generation watermarking method offering low complexity, high robustness and imperceptible watermarks. This work compares favorably with the results from other methods in terms of imperceptibility, robustness and capacity.
5.4 A Novel Robust Informed Watermarking approach and Tamper Detection Based on Weber Law

In this section, we present our semi blind and informed watermarking approach based on the Weber differential descriptor to build a watermark from the original image in order to achieve high robustness and to detect the tampered zones. We divide the original image into n by m blocks and the centered pixel is chosen to be concerned for watermark embedding in the spatial domain. The tamper detection is proved into tampered watermarked image by comparing the extracted watermark after attacks with the original watermark image. We focused also through this approach on the watermarking robustness and tested it against different scenario of attacks. The experimental results show the perfect covering of tamper issue and also the watermark robustness.

The structure of this chapter is as follows: the second section presents the Weber law. The third section presents the proposed approach. Section four shows the obtained experimental results, while section five describes the proposed approach for tamper detection. In section six the comparative study and finally the conclusion are presented.

5.4.1 Weber law
Weber law in general describes the relation between quantity and intensity and also how to increase the ratio of the quantity regarding to the intensity. The ratio of the incremental threshold with the background intensity is constant, sometimes called Threshold Versus Intensity (TVI). When the increment threshold is measured on various intensity backgrounds, the threshold increases in the intensity proportion. This relationship is defined in Weber’s law [Chen 08], [Liu 13], [Chen 10]:

\[ \frac{\delta M}{M} = k \]  \hspace{1cm} (5.12)

where \( \delta M \) represents the incremental threshold, \( M \) the initial value of the intensity and \( k \) is a constant value of the fraction result. The previous fraction is known as Weber fractional as illustrated in figure 5.22.
Figure 5.22: Weber Law description

Weber Descriptors (WDs) are defined by two basic components: Differential Excitation $\chi$ and Orientation $\lambda$. Figure 5.23 shows how to compute the differential excitation of the pixel $M(x_i, y_j)$ with eight neighbors where $M1$ is the pixel $x_{i-1}$ and $y_{j-1}$, $M2$ is the pixel $x_i$ and $y_{j-1}$, $M3$ is the pixel $x_{i+1}$ and $y_{j-1}$, $M4$ is the pixel $x_{i+1}$ and $y_j$, $M5$ is the pixel $x_{i+1}$ and $y_{j+1}$, $M6$ is the pixel $x_i$ and $y_{j+1}$, $M7$ is the pixel $x_{i-1}$ and $y_{j+1}$ and $M8$ is the pixel $x_{i-1}$ and $y_j$.

$$\chi(i,j) = \arctan \left( \sum_{k=1}^{8} \frac{M_k - M_0}{M_0} \right)$$  \hspace{1cm} (5.13)

The Differential Excitation $\chi(i,j)$ is the intensity of current pixel $M_0$ and $k$ is the number of neighbors. The Differential Excitation range is between $[-\pi/2, \pi/2]$.

The second Weber descriptor, the Orientation, consists to compute the orientation of the current pixel based on the following interpolation:

$$\lambda(i) = \arctan \left( \frac{M_6 - M_2}{M_4 - M_0} \right)$$  \hspace{1cm} (5.14)

5.4.2 Robustness based proposed approach

Through this chapter, we will build our watermark based on the host image information using Weber Differential Excitation descriptor $\chi$. We divide the image into 3 by 3 overlapping blocks, then we compute the differential excitation for each block. The obtained matrix will be considered as the used watermark (Informed watermark). In the extraction phase, the extractor will extract the attacked
Chapter 5: Watermarking Approaches

watermark from the attacked watermarked image, then compare the original watermark with extracted one and finding the differences between both in order to precise the tampered blocks.

5.4.2.1 Embedding phase
The watermark embedding process is summarized by the following steps:

1- Divide $M \times N$ original image into an $F$ number of $3 \times 3$ blocks. $M$ and $N$ are the image size, while $F$ is the number of producing blocks.
2- Calculate the Weber differential excitation descriptor $\chi$ for each block using the equation described above.
3- The obtained values $(M/3 \times N/3)$ are considered as the informed watermark images $w_i$ as we can see in figure 5.25.
4- For each block in the original image, choose the center pixel and embed the intensity of the watermark pixel using the following linear interpolation:

$$i_{wn} = (1 - \alpha)w_n + \alpha i_n$$  \hspace{1cm} (5.15)

where $i_{wn}$ is the watermarked of the block $n$; $w_n$ is the watermark intensity of the block $n$ and $i_n$ is the center value of the original image of block $n$, such as $\alpha \in ]0, 1[ .$

5.4.2.2 Extraction phase
In the extraction process and after tampering the watermarked image, we extract the watermark image from tampered watermarked image and we find the tampered blocks as illustrated in the following steps:

1- Divide the $M \times N$ watermarked image into an $F$ number of $3 \times 3$ blocks; $M$ and $N$ are the image size; and $F$ the number of producing blocks.
2- Extract the watermark value for each block of the pixel of the center using the following linear interpolation:

$$w_{an} = \frac{1}{\alpha}w_n - \frac{1-\alpha}{\alpha} i_{wn}$$  \hspace{1cm} (5.16)

In the equation 5.16, $w_{an}$ is the extracted block $n$. 
3- Compare the extracted watermark with original one.

4- Detect the tampered blocks in the watermarked image.

![Brain](image1) ![Brain2](image2) ![Hand](image3) ![Leg](image4)

Figure 5.24: Original medical images $i_i$

![w (Brain)](image5) ![w (Brain2)](image6) ![w (Hand)](image7) ![w (Leg)](image8)

Figure 5.25: Informed watermark images $w_i$

5.4.3 Experimental results

The used gray scale medical images are of size $255 \times 255$ taken from [DICOM] as shown in figure 5.24 (we take into account that the image size divided by 3, the result is integer output without rest). Figure 5.25 presents the informed watermark image built from each original image, while figure 5.26 illustrates the watermarked image with different values of the factor $\alpha$

$$\begin{align*}
  & \text{if } \alpha \leftrightarrow 0, \quad i_w \mapsto i \\
  & \text{if } \alpha \leftrightarrow 1, \quad i_w \mapsto w
\end{align*}$$

Based on the value of $\alpha$, we can control the visibility/invisibility of the watermark. We can note from figure 5.26 that when $\alpha$ is close to zero, there is degradation in the watermarked image and the watermark become visible. When $\alpha$ equal to 0.5, the degradation will be less. Moreover, if $\alpha$ is close to one, there is no degradation in the watermarked image and the watermark became invisible, which is the suitable case of our embedding process.
Chapter 5: Watermarking Approaches

We illustrate in figure 5.27 the applied attacks on the watermarked images and we calculated the corresponding PSNR values between the original watermark and the extracted one after each attack.

<table>
<thead>
<tr>
<th>Attack</th>
<th>PSNR Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG</td>
<td>64.5181</td>
</tr>
<tr>
<td>NOISE</td>
<td>51.2365</td>
</tr>
<tr>
<td>AFFINE</td>
<td>64.7602</td>
</tr>
<tr>
<td>CROP</td>
<td>65.2270</td>
</tr>
<tr>
<td>MEDIAN</td>
<td>69.5591</td>
</tr>
<tr>
<td>ROTCROP</td>
<td>65.1963</td>
</tr>
<tr>
<td>ROTS</td>
<td>64.9007</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack</th>
<th>PSNR Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRAIN1</td>
<td>64.3387</td>
</tr>
<tr>
<td>BRAIN2</td>
<td>50.7160</td>
</tr>
<tr>
<td>BRAIN2</td>
<td>65.1963</td>
</tr>
<tr>
<td>BRAIN2</td>
<td>61.7086</td>
</tr>
<tr>
<td>BRAIN2</td>
<td>69.4764</td>
</tr>
<tr>
<td>BRAIN2</td>
<td>64.8440</td>
</tr>
<tr>
<td>BRAIN2</td>
<td>64.9294</td>
</tr>
<tr>
<td>HAND1</td>
<td>48.4442</td>
</tr>
<tr>
<td>HAND1</td>
<td>49.0834</td>
</tr>
<tr>
<td>HAND1</td>
<td>48.4995</td>
</tr>
<tr>
<td>HAND1</td>
<td>46.2958</td>
</tr>
<tr>
<td>HAND1</td>
<td>48.5336</td>
</tr>
<tr>
<td>HAND1</td>
<td>48.5356</td>
</tr>
<tr>
<td>HAND1</td>
<td>48.4877</td>
</tr>
<tr>
<td>LEG1</td>
<td>60.0634</td>
</tr>
<tr>
<td>LEG1</td>
<td>49.6290</td>
</tr>
<tr>
<td>LEG1</td>
<td>59.1150</td>
</tr>
<tr>
<td>LEG1</td>
<td>55.1386</td>
</tr>
<tr>
<td>LEG1</td>
<td>60.1391</td>
</tr>
<tr>
<td>LEG1</td>
<td>60.0075</td>
</tr>
<tr>
<td>LEG1</td>
<td>59.7995</td>
</tr>
</tbody>
</table>

Figure 5.27: The applied attacks and the corresponding PSNR values
Chapter 5: Watermarking Approaches

The watermarked image is attacked using Stirmark Benchmark software [Petitcolas 12]. We note that we achieved a high robustness through the PSNR values which exceeds the 34dB. So all the PSNR values are around 50-60 dB.

5.4.4 Tamper detection based proposed approach
We tried to tamper the watermarked image as shown in figure 5.28 where the circles illustrates the tampered zones. We extract the watermark from the tampered watermarked image, then we compare the extracted watermark with the original one in order to obtain the tampered blocks. We note also the differences between the original and extracted watermark for each medical image.

In the tamper detection appeared in figure 5.29, we can note that our proposed approach can determine perfectly the tampered blocks.

5.4.5 Comparative study
In order to prove the robustness and capacity of our method, we compared the payload and image quality with the work in [Walia 13], whose authors proposed a watermarking method based on Weber law (table 5.22).
Chapter 5: Watermarking Approaches

<table>
<thead>
<tr>
<th>Images</th>
<th>Payload</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brain</td>
<td>7225</td>
<td>71.39</td>
</tr>
<tr>
<td>Brain 2</td>
<td></td>
<td>68.35</td>
</tr>
<tr>
<td>Hand</td>
<td></td>
<td>69.28</td>
</tr>
<tr>
<td>Leg</td>
<td></td>
<td>70.79</td>
</tr>
<tr>
<td>[Walia 13]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Head</td>
<td>398</td>
<td>58.67</td>
</tr>
<tr>
<td>Brain</td>
<td>431</td>
<td>58.39</td>
</tr>
<tr>
<td>Angio</td>
<td>379</td>
<td>59.65</td>
</tr>
<tr>
<td>Abdomen</td>
<td>567</td>
<td>56.90</td>
</tr>
</tbody>
</table>

Table 5.22: Comparison of the payload and imperceptibility with work in [Walia 13]

Based on our results, we note our approach is perfectly detected the tempered zone. Moreover, our work carries more watermark bits with a higher quality and less degradation than [Walia 13].

5.4.6 Weber conclusion
In this approach, we presented a novel semi-blind watermarking technique in spatial domain. The proposed algorithms covered two security issues: the tamper detection and the watermarking robustness. The approach is based on the Weber differential excitation descriptor. We have tested our approach on different medical images with several scenarios of attacks and we have obtained a high efficiency of our algorithms both for robustness and tamper detection.
5.5 Novel CT Scan Images Watermarking Scheme in DWT Transform Coefficient

In this part, we present our watermarking framework in the frequency domain based on DWT technique, which makes it possible to ensure the image’s authenticity and, as a consequence, the reliability. Our approach also presents a high robustness and less complexity regarding the proposed algorithms in the literature.

In our approach, we apply one level DWT for both the used watermark and the original images. Then, we embed the watermark in the original image by using linear interpolation presented by our team in previous works such as [Laouamer 13], [Benhocine 13], [Benhocine 08] and [Benhocine 09]. Linear interpolation provides an imperceptible watermark without degradation in the quality of the watermarked image. However, the novelty and the contribution of this approach is in the extraction phase, which takes into account the watermarked image in the extraction process and not just the attacked watermarked image.

In the second section we present the wavelets decomposition principle. The third section is dedicated to the new watermarking approach we have proposed. In the fourth section, we present the test results of our algorithm. The chapter ends by a conclusion and perspectives in the fifth section.

5.5.1 Wavelet decomposition principle

Discrete Wavelet transform (DWT) is a mathematical model for decomposing a signal. It is valuable for handling of a non-fixed signals. The decomposition is based on small waves called wavelets. The one level wavelets decomposition principle for a given image is illustrated in figure 5.30. In fact, this decomposition can have several levels called n-levels, multi-resolution domain. The result of this decomposition gives four sub-bands: Low-Low (LL), Low-High (LH), High-Low (HL) and High-High (HH). The LL sub-band contains the estimated original image while the other sub-bands contain the missing details. The LL sub-band output from any stage can be decomposed further [Swami 13].

![Figure 5.30: 2D Medical image wavelet transform with one level decomposition.](image-url)
Chapter 5: Watermarking Approaches

The multi-resolution domain offers several advantages. The first advantage is that it defend for the used watermarking algorithms to be robust against JPEG 2000 compression. The second advantage is its power to choose the frequency set that is watermarked to control the most noticeable visual degradation in low and high frequencies. The embedding in the low frequency sub-band provides a high robustness, but the embedded watermark become visible which affects the image quality. This means a degradation in the watermarked image [Laouamer 13]. While the embedding in the high frequency sub-band supports more visibility and low degradation, but less robustness [Swami 13]. This property is due to the impairment of the visual human contrast sensitivity at high frequencies [Laouamer 15].

5.5.2 Proposed watermarking approach
In our work, we apply one level DWT for both the used watermark and the original images. Then, we embed the watermark in the original image by using linear interpolation presented by our team in the works [Laouamer 13], [Benhocine 13], [Benhocine 08] and [Benhocine 09]. Linear interpolation provides an imperceptible of the watermark without degradation in the quality of the watermarked image.

Our technique considers two phases: embedding and extraction processes. In the embedding phase, one level DWT is applied to the watermark and also to the original image. Then, we embed the watermark using linear interpolation. The inverse DWT (DWT\(^{-1}\)) is applied to the DWT coefficients of the watermarked image in order to obtain a "readable" watermarked image. In the extraction phase, one level DWT is applied to the watermarked and watermark images. We achieve the embedding process using linear interpolation to get a new watermarked image. Then, the attacked watermarked image and the new watermarked image are used to extract the attacked watermark using the linear interpolation. Finally, DWT\(^{-1}\) is applied to the extracted attacked DWT watermark image to obtain a readable attacked watermark image.
Chapter 5: Watermarking Approaches

5.5.2.1 Watermark embedding

Figure 5.31 illustrates the watermark embedding process which is based on the level-1 wavelet decomposition. The watermark is embedded through a linear interpolation

\[ i_w = (1 - t)w + ti \]  

where \( t \in ]0, 1[ \) and \( i, w \) and \( i_w \) are respectively the original image, the watermark and the watermarked image.

\( w_{DWT}, i_{DWT} \) and \( i_{wDWT} \) are respectively the watermark, the original image and the watermarked image in wavelet decomposition.

The main steps of the embedding process are as follows:

1. Divide the original image \( i \) and the watermark \( w \) into 8 × 8 blocks.
2. Apply the DWT (one level) to each block obtained in step one for the images \( i \) and \( w \). The matrices of the DWT coefficients give as results the \( i_{DWT} \) and \( w_{DWT} \) matrices.
3. Mark \( w_{DWT} \) in \( i_{DWT} \) by the following equation:

\[ i_{wDWT} = (1 - t)w_{DWT} + ti_{DWT} \]  

where \( i_{wDWT} \) are the watermarked matrices (visually this matrix is unreadable, so to make it readable we need to apply the step 4) and \( t \) is a given value \( \in ]0, 1[ \).

4. Apply the DWT inverse operation (DWT\(^{-1}\)) to all the blocks in order to obtain the readable image \( i_w \).

5.5.2.2 Watermark extraction

The novelty and the contribution of this is in the extraction phase, which takes into account the watermarked image in the extraction process and not just the attacked watermarked image. Figure
Chapter 5: Watermarking Approaches

5.32 shows the extraction scheme. We denote by “mark”, the embedded watermark by linear interpolation, while "extraction" refers to the watermark inverse embedding:

\[ w_a = \frac{1}{t} w_{DWT} - \frac{1-t}{t} i_{wa} \quad (5.19) \]

Where \( w_a \), \( i_{wa} \) and \( w_{DWT} \) are the extracted watermark, the attacked watermarked image and inverse DWT of watermark image, respectively. We summarized this process as follows:

1. Apply the DWT one level for each block of \( w \) and \( i_w \) to obtain \( w_{DWT} \) and \( i_{waDWT} \).

2. Mark \( w_{DWT} \) in \( i_{waDWT} \) by using equation (5.20) to obtain \( w_{aDWT} \).

\[ w_{IDWT} = (1-t)i_{wDWT} + tw_{DWT} \quad (5.20) \]

3. Apply the DWT one level to each block of the attacked watermarked image \( i_{wa} \) to obtain \( i_{waDWT} \) which is the DWT coefficient matrix of the attacked watermarked image.

4. Unmark \( i_{waDWT} \) with the same \( t \) value used in the embedding process using the equation (5.21) to obtain \( w_{aDWT} \).

\[ w_{aDWT} = \frac{1}{t} w_{IDWT} - \frac{1-t}{t} i_{waDWT} \quad (5.21) \]

5. Apply the DWT inverse to all the blocks of \( w_{aDWT} \) in order to obtain a readable and significant image \( w_a \).

![Watermark extraction process diagram](image-url)

**Figure 5.32: Watermark extraction process.**

### 5.5.3 Experimental results

We performed our tests on a gray CT scan medical image database that contains 250 images of size 256 × 256. The original images come from [Medical Samples]. The watermark image contains a full
Chapter 5: Watermarking Approaches

name. The watermarking process has a secret key, that varies exclusively between 0 and 1 in order to achieve a visible/invisible watermarking. We tested our proposed watermarking algorithm against several kinds of attacks of the Stirmark Benchmark [Laouamer 13] and [Benhocine 09]: median filtering, JPEG compression, rotation, noise and PSNR attacks. Through the obtained results we can conclude that the invisible watermarking (where \( t \) is close to 1) gives better results compared to the visible one (\( t = 0.2 \)) and the semi-invisible one (\( t = 0.5 \)) where the extracted watermarks are similar to the original one. As for the robustness of the proposed approach, we conducted tests in several cases (according to the values of \( t \)). Figure 5.33 illustrates the head original image, watermark image and head watermarked images obtained after applying our algorithm with several values of the secret key \( t \) (0.2, 0.5 and 0.98) for a visible, semi-visible and invisible watermarking.

![Figure 5.33: Embedding watermark by linear interpolation with different values of \( t \) (secret key).](image)

In figure 5.34, the first level (a) shows the attacked watermarked images, the second level (b) shows the extracted attacked watermark image and the third level (c) shows the differences between the original watermark image and the extracted attacked watermark in case of \( t=0.98 \).

![Figure 5.34: Watermark extraction results when \( t=0.98 \)](image)
Chapter 5: Watermarking Approaches

In figure 5.35, the first level (a) shows the attacked watermarked images, the second level (b) shows the extracted attacked watermark image and the third level (c) shows the differences between original watermark image and extracted attacked watermark in case of $t=0.5$.

![Figure 5.35: Watermark extraction results when $t=0.5$](image)

In figure 5.36, the first level (a) shows the attacked watermarked images, the second level (b) shows the extracted attacked watermark image and the third level (c) shows the differences between original watermark image and extracted attacked watermark in case of $t=0.2$.

![Figure 5.36: Watermark extraction results when $t=0.2$.](image)

We have also made the same tests on other images following the same steps in the cases of visible, semi-visible and invisible watermark by setting in each test the values of the key $t$. Figure 5.37 and figure 5.41 illustrate the results for used images sample such as: brain and hand image, while figure 5.38, figure 5.39 and figure 5.40 illustrate the results in case of attack when the original image and the watermark are those given in figure 5.37. Also, figure 5.41, figure 5.42 and figure 5.43 illustrate the results in case of attack for the hand image.
Figure 5.37: Embedding watermark by linear interpolation with different values of \( t \) (secret key).

Figure 5.38: Watermark extraction results when \( t = 0.98 \).

Figure 5.39: Watermark extraction results when \( t = 0.5 \).
Chapter 5: Watermarking Approaches

Figure 5.40: Embedding watermark by linear interpolation with different values of t (secret key).

Figure 5.41: Watermark extraction results when $t=0.98$.

Figure 5.42: Watermark extraction results when $t=0.5$. 
5.5.3.1 Robustness measurements

To assess the robustness of the proposed approach, we introduce the latest techniques used in the literature. It consists to calculate the Peak Signal to Noise Ratio (PSNR), Structural Similarity Index SSIM [Hore 10] and Universal Quality Index (UQI) [Wang 02] between the original watermark and the extracted watermark as we can see in table 5.23, figure 5.44 and figure 5.45.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>PSNR</th>
<th>SSIM</th>
<th>UQI</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG</td>
<td>69.1732</td>
<td>0.9997</td>
<td>0.9863</td>
</tr>
<tr>
<td>MEDIAN</td>
<td>51.1326</td>
<td>0.9986</td>
<td>0.9611</td>
</tr>
<tr>
<td>NOISE</td>
<td>41.1456</td>
<td>0.9794</td>
<td>0.9153</td>
</tr>
<tr>
<td>PSNR</td>
<td>65.8942</td>
<td>0.9999</td>
<td>0.9999</td>
</tr>
<tr>
<td>ROTATION</td>
<td>43.2264</td>
<td>0.9713</td>
<td>0.9237</td>
</tr>
</tbody>
</table>

Table 5.23: Robustness measurements after different attacks

Figure 5.44: Robustness measures in case of SSIM and UQI
5.5.3.2 Imperceptibility measurements

Our approach achieves a high imperceptibility regarding the watermark embedding. The degradation in the watermarked image after watermark embedding is very low. The optimal imperceptibility in our scheme is when $t$ is close to 1 ($t=0.98$). We have evaluated the imperceptibility for our approach by measuring the PSNR between the original image and the watermarked image. Table 5.24 shows the imperceptibility results of different values of $t$. While figure 5.46 shows the chart of these results.

<table>
<thead>
<tr>
<th>Image</th>
<th>$t=0.2$</th>
<th>$t=0.5$</th>
<th>$t=0.98$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>39.2345</td>
<td>41.4658</td>
<td>56.3476</td>
</tr>
<tr>
<td>Brain</td>
<td>39.4574</td>
<td>40.6244</td>
<td>54.3487</td>
</tr>
<tr>
<td>Hand</td>
<td>38.5657</td>
<td>41.7065</td>
<td>55.5504</td>
</tr>
</tbody>
</table>

Table 5.24: Imperceptibility measurement based on PSNR.

Based on the previous table and figure, our approach achieves a high imperceptibility when $t=0.98$. Moreover, the results indicate that the technique offers a high fidelity and imperceptibility, which means that our approach reserves the image quality after embedding, and there is no degradation effected to the watermarked image.
5.5.4 Comparative study

In this section, we compare the robustness of the proposed technique with the works in [Ahmad 14] and [Benrhouma 15]. We provided the values of PSNR and SSIM of the extracted watermark. Those works have used the DWT technique, where the watermark image size in those works has the same size with the watermark used in our work.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>[Ahmad 14]</th>
<th>[Benrhouma 15]</th>
<th>Proposed technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG Compression</td>
<td>28.287</td>
<td>38.71</td>
<td>69.1732</td>
</tr>
<tr>
<td>Noise</td>
<td>20.272</td>
<td>25.74</td>
<td>41.1456</td>
</tr>
<tr>
<td>Median</td>
<td>27.497</td>
<td>14.22</td>
<td>51.1326</td>
</tr>
<tr>
<td>Rotation</td>
<td>43.596</td>
<td>36.68</td>
<td>43.2264</td>
</tr>
</tbody>
</table>

Table 5.25: PSNR comparative results

![PSNR Comparative results](image)

Figure 5.47: PSNR Comparative results with the works in [Ahmad 14] and [Benrhouma 15]

<table>
<thead>
<tr>
<th>Attacks</th>
<th>[Ahmad 14]</th>
<th>[Benrhouma 15]</th>
<th>Proposed Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG Compression</td>
<td>0.9875</td>
<td>0.98</td>
<td>0.9997</td>
</tr>
<tr>
<td>Noise</td>
<td>0.9225</td>
<td>0.8</td>
<td>0.9794</td>
</tr>
<tr>
<td>Median</td>
<td>0.9852</td>
<td>0.6</td>
<td>0.9986</td>
</tr>
<tr>
<td>Rotation</td>
<td>0.9999</td>
<td>0.97</td>
<td>0.9713</td>
</tr>
</tbody>
</table>

Table 5.26: SSIM comparative results
Chapter 5: Watermarking Approaches

Figure 5.48: SSIM comparative results with the works in [Ahmad 14] and [Benrhouma 15]

It is obvious from the table 5.25 and 5.26, and figures 5.47 and 5.48, that our results are better than those results in term of robustness by measuring the PSNR.

5.5.5 DWT conclusion
We proposed in this part a new watermarking approach to ensure the CT scan medical image authentication and robustness, which is based on the wavelet transform. This approach is applicable to any kind of images, but more appropriate to the medical image because it maintains a high image quality and generates less degradation than existing methods. The embedding process is performed by a linear interpolation which makes it possible to have an inverse watermark after embedding. Our tests were performed on a sample of 250 images. The results obtained are very encouraging, especially when the watermark is invisible (the watermarking key close to 1). We have evaluated the robustness of our approach by comparing the original watermark and the extracted one after applying attacks. The comparison has been achieved by applying the best known similarity measures between the original and the extracted watermarks as the PSNR, SSIM, UQI. The experimental results and the comparative study show that the proposed technique present more robustness against different kinds of attacks than some relevant works presented in [Ahmad 14] and [Benrhouma 15].

5.6 Conclusion
In this chapter, we presented our contributions in watermarking field. They consist of three solutions in the spatial domain (FCA, ZBDD and Weber) and one solution in the frequency domain (DWT).
Chapter 5: Watermarking Approaches

Our FCA based watermarking approach is reversible and novel. Its main feature is that it generates the optimal position for embedding. The watermark is built from some header information of the DICOM image. It is embedded into the NROI of the medical image. Based on experimental results, our approach demonstrates a lower computational complexity, using low capacity for the watermark and has a high robustness. Moreover, the approach can detect the removal and/or addition and/or replacement during attacks, which would be useful for tamper detection issues. Although the proposed approach has been limited in this approach to medical image, it could be used with other kinds of images. Moreover, our FCA approach has the ability to detect the attacks by comparing the extracted concepts from the watermarked image after attacks with the original concepts from the original image. FCA also provided a distribution embedding area making the imperceptibility high.

In ZBDD approach, we addressed the problem of generating watermarks as small as possible (small payload) to adapt the hidden data to real time applications by maintaining high robustness, high imperceptibility and low complexity within a medical image. It is a novel and optimal approach that is completely innovative through its generation of an intelligent (adaptive) watermark based on ZBDD. ZBDD is a technique which has already proved its usefulness in many applications such as path reduction in wireless networks, production management, etc. An adaptive watermarking method based on Zero-Suppression in ZBDD can generate a watermark with a minimum size while preserving a strong robustness, thus fulfilling the needs mentioned above for low computational complexity and real time applications. We tested our algorithm under several attack scenarios and measured its robustness in the case of invisible watermarking based on linear interpolation. The results obtained show that our techniques represent a new-generation watermarking method offering low complexity, high robustness and imperceptible watermarks. This work compares favorably with the results from other methods in terms of imperceptibility, robustness and capacity.

In Weber approach, we presented a novel semi-blind watermarking technique in spatial domain. The proposed algorithms covered two security issues: the tamper detection and the watermarking robustness. The approach is based on the Weber differential excitation descriptor. We have tested our
approach on different medical images with several scenarios of attacks and we have obtained a high efficiency of our algorithms both for robustness and tamper detection.

Our DWT approach is a new watermarking method to ensure the CT scan medical image authentication and robustness. This approach is applicable to any kind of images, but more appropriate to the medical image because it maintains a high image quality and generates less degradation than existing methods. The embedding process is performed by a linear interpolation which makes it possible to have an inverse watermark after embedding. Our tests were performed on a sample of 250 images. The results obtained are very encouraging, especially when the watermark is invisible (the watermarking key $t$ close to 1). We have evaluated the robustness of our approach by comparing the original watermark and the extracted one after applying attacks. The comparison has been achieved by applying the best known similarity measures between the original and the extracted watermarks as the PSNR, SSIM, UQI. The experimental results and the comparative study show that the proposed technique present more robustness against different kinds of attacks than some relevant works presented in [Ahmad 14] and [Benrhouma 15].

The watermarking approaches provided the way to ensure the authenticity, integrity as well as the copyright issue but they did not ensure the confidentiality of the digital medical image. Cryptography aims to improve the confidentiality of the digital medical image. In the next chapter, we will present a novel and informed symmetric cryptography approach based on N-gram.
Chapter 6 Informed Symmetric Encryption Algorithm for DICOM Medical Image Based on N-grams

6.1 Introduction

There are two basic criteria for the choice of an image encryption/decryption method. The first one is computation complexity (cc), while the second is purely security. As for as cc is concerned, most of public key encryption systems are very slow and need more calculus. For example, the RSA algorithm is considered several hundred times slower than AES in software implementations and it is completely out of touch with hardware implementation. Similarly, it is very difficult and take more time to find the big number factorization in two prime numbers, so it becomes so inappropriate to use RSA comparatively to a symmetric system because the keys are so larger for the RSA and therefore encryption/decryption are getting longer. It is for this reason that they are not suitable for images [Puech 06]. For the security reason, problems related to the structure of public key encryption systems are posed. We note that the necessary keys size in public key cryptosystems to reach adequate security is greater than the key size in secret key cryptosystems. The notion of the importance of the key size to ensure security is not only legitimate in the case of the secret key.

In fact, these systems are based on the hypothesis that the only possible attacks are those we call exhaustive attacks that involve enumerating all possible keys. For example, in the case of a 128 bits key, the size of the enumerated space is $2^{128}$. But, in the case of the public key, the key size has legitimacy only when considering the same system. Indeed, the 512 bits RSA system for example, is less secure than 128 bits AES system. The only correct way to evaluate a public key cryptosystem is the complexity of the best known attack. What makes the difference; we are never free from theoretical breakthroughs. Very recently, work has successfully factored a 512 bit number [Ismail 10]. As a result, to have adequate security for the next years, it is generally advisable to use numbers $n$ of 1024 bits.

In this approach, we propose a new way to generate symmetric keys for image encryption / decryption in particularly the medical images by an informed process based on a technique that has been
demonstrated on textual analysis called N-grams. We denote by an informed cryptosystem, a system that generates keys based on the original image characteristics to be encrypted. Our obtained results are very significant. We detail them in this chapter.

The organization of this chapter is the following: in the second section the N-grams principle is presented. The third section is dedicated to the proposed algorithm, while, the fourth section presents the experimental results. The chapter ends with the conclusion.

6.2 N-Gram

The N-grams technique present many advantages. We cite its more important one [Brown 92] [Cavnar 94]:

- Compared to other techniques, the N-grams automatically capture the roots of the most common pixels.

- They operate independently of the nature and the quality of the image. In addition, with the N-grams, we do not need prior image segmentation.

- They are tolerant to small changes in the pixels intensities, for example, when an image is scanned; the optical recognition is often imperfect. So, it is possible that the pixel of value 220 is read as pixel value $\pm \varepsilon$ ($\varepsilon$ is known as a small value). A system based on pixels will be in difficulty to recognize that it is the pixel with value 220 because of misreading, while, a system based on N-grams is able to take into account the other N-grams in order to keep the recognition performance despite the deformation rate more or less acceptable.

For any given sequence, the N-grams series of this sequence (for $n = 2$: bigrams, $n = 3$: trigrams, $n = 4$: quadrigrams, etc. ...). are as follows:

\[
\text{Sequence } (n) = p_1, p_2, p_3, \ldots, p_i, \ldots, p_n
\]

\[
\text{Bigrams}(n-1) = p_1, p_2, p_3, \ldots, p_i, \ldots, p_n, i, p_{i+1}, \ldots, p_{n-1}, p_n
\]

\[
\text{Trigrams}(n-2) = p_1, p_2, p_3, \ldots, p_i, p_{i+1}, \ldots, p_{n-2}, p_{n-1}, p_n
\]
The N-grams principle was applied to the text. We exploit this theory to encrypt/decrypt images with another point of view differently compared to what exists in the literature. So, for a grayscale image of size $N \times M$, the bigrams and trigrams matrix ($n = 2$, $n = 3$) of size $N \times M - 1$ and $N \times M - 2$ respectively are defined as follows:

### Original Image $I$

$$
\begin{bmatrix}
 p_{11} & p_{12} & p_{13} & \cdots & p_{1j} & \cdots & p_{1M} \\
 p_{21} & p_{22} & p_{23} & \cdots & p_{2j} & \cdots & p_{2M} \\
 p_{31} & p_{32} & p_{33} & \cdots & p_{3j} & \cdots & p_{3M} \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
 p_{Ni} & p_{N2} & p_{N3} & \cdots & p_{Nj} & \cdots & p_{NM} \\
\end{bmatrix}
$$

### Bigrams Matrix of $I$

$$
\begin{bmatrix}
 p_{11}p_{12} & p_{12}p_{13} & \cdots & p_{1j-1}p_{1j} & \cdots & \cdots & p_{1M-1}p_{1M} \\
 p_{21}p_{22} & p_{22}p_{23} & \cdots & p_{2j-1}p_{2j} & \cdots & \cdots & p_{2M-1}p_{2M} \\
 p_{31}p_{32} & p_{32}p_{33} & \cdots & p_{3j-1}p_{3j} & \cdots & \cdots & p_{3M-1}p_{3M} \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
 p_{Ni}p_{Ni+1} & p_{ Ni+1}p_{Ni+2} & \cdots & p_{Nj-1}p_{Nj} & \cdots & \cdots & p_{NM-1}p_{NM} \\
\end{bmatrix}
$$

### Trigrams Matrix of $I$

$$
\begin{bmatrix}
 p_{11}p_{12}p_{13} & p_{12}p_{13}p_{14} & \cdots & p_{1j-2}p_{1j-1}p_{1j} & \cdots & \cdots & p_{1M-2}p_{1M-1}p_{1M} \\
 p_{21}p_{22}p_{23} & p_{22}p_{23}p_{24} & \cdots & p_{2j-2}p_{2j-1}p_{2j} & \cdots & \cdots & p_{2M-2}p_{2M-1}p_{2M} \\
 p_{31}p_{32}p_{33} & p_{32}p_{33}p_{34} & \cdots & p_{3j-2}p_{3j-1}p_{3j} & \cdots & \cdots & p_{3M-2}p_{3M-1}p_{3M} \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
 p_{Ni}p_{Ni+1}p_{Ni+2} & p_{Ni+1}p_{Ni+2}p_{Ni+3} & \cdots & p_{Ni-2}p_{Ni-1}p_{Ni} & \cdots & \cdots & p_{NM-2}p_{NM-1}p_{NM} \\
\end{bmatrix}
$$

Figure 6.1: The process of the proposed system for images securing exchange between the sender and the receiver.
Chapter 6: Informed Symmetric Encryption Algorithm for DICOM Medical Image Based on N-grams

6.3 Proposed algorithm based on N-grams

Our proposed approach is illustrated in the following scheme (figure 6.2).

Algorithm:
1. Reading DICOM Image // size 256×256 (grayscale)
2. Apply compression with JPEG Algorithm
3. Compute N-Grams of compressed image // n=2,…,end of the image rows// for our case we take n=2,3
4. Computing the pixel length matrix and consider it as the first key (key1)
5. Decrypting the encrypted image using the both keys, where key2 in represented by the value n of the N-grams.

The calculation of the pixel length matrix depends on the pixels size in the original image:

\[ \text{Pixel} \_\text{Length} \_\text{Matrix} = f(\text{Pixel} \_\text{Number} \_\text{Size}) \]

Consider the following example (figure 6.3) to illustrate how to compute the Pixel_Length_Matrix from a given matrix of size 5 × 5:

\[
\begin{array}{cccc}
23 & 6 & 25 & 88 \\
11 & 14 & 38 & 22 \\
13 & 141 & 6 & 74 \\
240 & 125 & 44 & 46 \\
216 & 148 & 9 & 147 \\
\end{array}
\]

\[
\begin{array}{cccc}
2 & 1 & 2 & 2 \\
2 & 2 & 2 & 2 \\
2 & 3 & 1 & 2 \\
3 & 3 & 2 & 3 \\
3 & 3 & 1 & 3 \\
\end{array}
\]

Figure 6.3: Example for computing the pixel length matrix
(a) Original input, (b) Corresponding pixel length matrix.
Chapter 6: Informed Symmetric Encryption Algorithm for DICOM Medical Image Based on N-gram

6.4 Experimental results
Our image database consists of 450 grayscale medical images of DICOM type with size 256×256 [Medical Samples]. The encryption / decryption results are as shown below for a set of nine medical images based on N-gram with $n = 2, 3$ (bigrams and trigrams) in Figures 6.4 and 6.5 respectively.

![Figure 6.4](image)

Figure 6.4: Results of the bigrams proposed encryption/decryption process

(a) Original Images I, (b) Encrypted Images EI, (c) Decrypted Images DI, (d) I-DI
We calculated the PSNR between the original image and the decrypted one for the sample images shown in Figure 6.4.
Chapter 6: Informed Symmetric Encryption Algorithm for DICOM Medical Image Based on N-grams

Figure 6.6: Histogram of some of tests images (Case of bigrams)

(a) Original Images ($I$), (b) Decrypted Images ($DI$), (c) Difference between $I$ and $DI$

Figure 6.7: Histogram of some of tests images (Case of trigrams)

(a) Original Images ($I$), (b) Decrypted Images ($DI$), (c) Difference between $I$ and $DI$
We found that the PSNR value is in the vicinity of 72 dB, which means that there is no significant degradation between each original image and the decrypted. The histograms of the original images and those decrypted in figure 6.4 are presented in figure 6.6 and 6.7 (for bigrams and trigrams respectively) show the same distributions of grayscale and the high resemblance between the original image and the decrypted one by measuring also the difference image which very close to the black image.

6.5 Conclusion
A limited number of cryptographic methods have been proposed until these days. These methods are mainly based on the key generation either in a symmetrical or asymmetrical way, where each has drawbacks both in terms of slowness (case of asymmetric systems) or secret key security (case of symmetric systems). The work presented in this chapter consisted to discover new perspectives in the field of cryptanalysis. This perspective is based on exploiting the characteristics of the image to generate symmetric keys for image encryption / decryption process which is purely informed. In this process, we have used the N-gram technique. This technique was used in the linguistic engineering and textual analysis. We have implemented this approach for securing medical images in particular. The used key is generated from the image itself (informed) using N-grams with n = 2 (bigram) and 3 (trigram). The PSNR between the original image and the decrypted image is around 72 dB, while the histograms of the original images and the decrypted images have the same distributions of grayscale and show a high resemblance between the original and the decrypted one. The obtained results are very significant and encouraging.

In the next chapter, we will present a hybrid watermarking and cryptography approach. The technique aims to take advantage of the benefit of both the cryptography and watermarking techniques.
Chapter 7 Technique Efficient and Robust Encryption and Watermarking Based on a New Chaotic Map Approach

7.1 Introduction
In this chapter, we propose a watermarking and encryption system based on a One Time Pad (OTP) encryption algorithm, which generates the key stream using an innovative approach. Indeed, A new chaotic map approach has been proposed and used for key generation.

The proposed hybrid scheme consists in applying a One Time Pad (OTP) encryption algorithm and a semi-blind watermarking approach to the host medical image. The encrypted watermark is embedded in the encrypted host image, directly in the spatial domain. The results obtained show perfect watermark extraction even after applying some attack scenarios.

The organization of this chapter is as follows: in the second section, we present the principles of One Time Pad (OTP) and chaotic maps. The third section deals with the proposed watermarking and cryptographic system. Section four is dedicated to attacking tests and their outcomes and section five for a comparison with other approaches. The chapter ends with a conclusion in section six.

7.2 One time pad principle and chaotic maps
One time pad refers to any encryption method in which each byte in the plaintext is encrypted by a corresponding key in the key stream. The one time pad key stream must be generated randomly and each value of the key will be between 0 and 255 in the case of RGB images. The inconvenience of OTP is that the key used cannot be reused more than once. This means that if the same plaintext is encrypted twice, the key will be generated differently. In the encryption process, the key stream should be of the same or a larger size than the plaintext [Rubin 96], [Leone 15].

Theoretically, the OTP cannot be broken because finding the key used for encryption will be a very difficult task, as its length depends on the length of the plaintext. As the plaintext lengthens, this will have an impact on the key length and it will become more difficult to discover the key [Cao 15]. The number of attempts needed to obtain the encryption key is defined by the following equation:

\[ \text{Possibility}(\mathcal{K}_i) = 2^l - 1 \]
where \( K_I \) is the key stream for index \( i \), and \( i \) is the length of the plaintext.

One Time Pad can be represented by the following equation:

\[
C_i = E(P_i, K_i) \quad \text{for} \quad i = 1, 2, 3, \ldots, n
\]

where \( C_i \) is the ciphered text; \( E \) the enciphering operation; \( P_i \) is the plaintext; \( K_i \) is the key stream that is used for encryption and \( i \) is the text position.

There are many ways to generate the key, one of which is called Auto Key. Auto Key generates the key in a simple and straightforward manner. The new value of the key has no correlation or fixed relation with the original key stream [Rubin 96]:

Let \( A \) and \( B \) be two independent simple substitutions. Let \( L \) be the new key stream for \( A \) and \( B \) substitutions, so:

\[
L_1 = A(K_1) + B(K_n)
\]

\[
L_i = A(K_i) + B(L_{i-1}) \quad \text{for} \quad i = 2, 3, \ldots, n
\]

where \( L_1 \) is the first key, which will be used for the first plaintext; \( A(K_1) \) is the first value in the substitution \( A \), and \( B(K_n) \) is the last value in the substitution \( B \). Auto key guarantees that the key will be the whole of key stream and that there is no similarity in the key’s values [Rubin 96].

Chaos theory explains the result of a technique that is highly sensitive to the initial conditions [Kocarev 01]. A Chaotic map is a method that generates the stream of values based on the first generated value by making some small changes in the next stream value. This method is applied in many fields like compression, encryption and modulation. The chaotic map is widely used in cryptosystems [Yap 15]. It is used in cryptography because of its predictable nature and its sensitivity to the initial value [Sneyers 97].

7.3 Proposed approach

Our present approach is based on two processes: encryption/watermarking and decryption/extraction.

In the encryption/watermarking process, we first generate the key using our chaotic approach, and
then encrypt the original and the watermark images by applying our OTP approach. Then, we embed the encrypted watermark into the encrypted original image in the spatial domain. Decryption/extraction consists in building the key using the same chaotic map equation. The attacked encrypted watermarked image is decrypted using the same OTP approach. Finally, we extract the attacked watermark image. This process can be summarized as follows.

### 7.3.1 The encryption and watermarking process

The encryption and watermarking process includes the key generation using our chaotic map. In this process, the encryption is based on the OTP technique. We then proceed to the embedding phase directly in the spatial domain. Here, we illustrate all the steps needed to carry out the encryption/watermarking phase.

#### 7.3.1.1 Chaotic map key generation

We generate the key with a size \( n \times m \) using the chaotic map, which is based on the first key (initial value). Any modification in the first key will automatically change the whole key stream. The principle of OTP encryption is to find a different key for each plaintext. We build the key stream defined by a matrix with the same size as the original image. Our chaotic equations are described by the following equations:

\[
x(1,1) = \infty
\]

\[
x(r, 1) = \text{abs}(\text{MaxIntensity} - 2x(r - 1,1)) \tag{7.2}
\]

\[
x(r, c) = \text{abs}(\text{MaxIntensity} - 2x(r, c - 1)) \tag{7.3}
\]

where \( x(1,1) \) is the first key element in the key stream; \( \alpha \) is a constant \( \in [0, 1] \). \( x(r, 1) \) is the \( r^{th} \) key in the first column \( r = \{2, 3, \ldots, n\} \). \( \text{MaxIntensity} \) is the highest value of the pixel intensity, which is equal to 255; and \( x(r, c) \) is the key of the row \( r \) and the column \( c \) such that \( r = \{1,2,3,\ldots,n\} \) and \( c = \{2,3,\ldots,m\} \).

The classical chaotic map provides keys with high sensitivity to the initial value, but without a domain space limit and a lower possibility that values will be similar. Our new formulation of the chaotic map provides us with a key matrix equal to the image size. For each image pixel there is a mismatch-specific key value. So, the similarity in the key values is still lower or may be zero. In order to keep
the image information without losing pixel values, we did not exceed the image pixel range. Indeed, the domain space based on our formula is between zero and 255, which is equal to the image pixel range. So, the encryption based on our formula produces an image as a result. Moreover, our formula uses \( \alpha \) as the initial value, while it is also the security key for the watermarking. This reduces the complexity of the overall encryption and watermarking process. By providing a high mismatch key based on our formula and the chaotic map condition concerning the sensitivity to the initial value, we can achieve the condition necessary for the OTP, whereby for each pixel we have to encrypt with a difference (one time) key.

7.3.1.2 Encryption based on OTP and the embedding process in the spatial domain

This step describes the OTP encryption and embedding process, which generates output consisting of an encrypted and watermarked image \( EN_{iw} \). Figure 7.1 illustrates this step.

\[
\begin{align*}
\alpha & \quad \text{Chaotic-Map} \\
& \quad \text{Key generation} \\
\text{OTP} & \quad \text{Encryption} \\
\text{MARK} & \quad \text{EN}_{iw}
\end{align*}
\]

where \( \alpha \in ]0,1[ \). \( i, w, EN_{i}, EN_{w} \) and \( EN_{iw} \) are the original image, original watermark image, encrypted original image, encrypted watermark image and encrypted watermarked image, respectively.

In this phase, we generate the key using our chaotic map. We encrypt the original and the watermark images based on OTP. Then, we embed the encrypted watermark into the encrypted original image by the following steps:

1- Generate the key matrix using equations 7.1, 7.2 and 7.3.

2- Read the original image \( i \).
3- Read the watermark image \( w \).

4- Encrypt the original and the watermark images using the following equations:

\[
EN_i(x, y) = (key(x, y) + i(x, y)) \mod 256 \quad (7.4)
\]

\[
EN_w(x, y) = (key(x, y) + w(x, y)) \mod 256 \quad (7.5)
\]

where \( m \) and \( n \) are the image size; \( x = 1, \ldots, m \); \( y = 1, \ldots, n \). \( EN_i \) and \( EN_w \) are the encrypted original image and encrypted original watermark, respectively.

5- The obtained encrypted image is embedded by a linear interpolation as defined in the following equation:

\[
EN_iw(x, y) = (1 - \alpha) \cdot EN_w(x, y) + \alpha \cdot EN_i(x, y) \quad (7.6)
\]

7.3.2 The decryption and extraction process

To increase the security of our approach, so as to avoid potential hacking, we do not send the key to the receiver side. So, we regenerate the key using equations 7.1, 7.2 and 7.3, illustrated in the encryption phase, and then decrypt the attacked encrypted watermarked image \( EN_{iwa} \). Finally, we extract the attacked watermark image \( w_a \). The decryption and extraction processes are conducted as follows:

1. Generate the key matrix using equations 7.1, 7.2 and 7.3.

2. Read the attacked encrypted watermarked image \( EN_{iwa} \).

3. Decrypt the \( EN_{iwa} \) using the following equation:

\[
DE_iw_a(x, y) = (EN_{iwa}(x, y) + \text{mod}_{base} - key(x, y)) \mod 256 \quad (7.7)
\]

where \( x = 1, \ldots, m \); \( y = 1, \ldots, n \). \( DE_iw_a \) is the attacked decrypted watermarked image; and \( \text{mod}_{base} \) is the base used in the modulus operation, which in our case is equal to 256.

4. Extract the attacked watermark image \( (w_a) \) From \( DE_iw_a \) using the following linear interpolation:

\[
w_a(x, y) = \frac{1}{\alpha}(w(x, y)) - \frac{1-\alpha}{\alpha}DE_{iwa}(x, y) \quad (7.8)
\]
Chapter 7: Efficient and Robust Encryption and Watermarking Technique Based on New Chaotic Map

Figure 7.2 illustrates the decryption and the watermark extraction process.

\[
\begin{align*}
\alpha & \quad \text{Chaotic-Map} \quad \text{Key generation} \\
EN_{i_{wa}} & \quad \text{OTP Decryption} \quad D\!E_{i_{wa}} \quad \text{UNMARK} \quad w_a
\end{align*}
\]

**Figure 7.2: Decryption and extraction process**

### 7.4 Tests and outcomes

We performed our tests on a medical image of 256 × 256 pixels in size, on a database sample of 100 different medical image types including X-ray, Ultrasound, CT-scan and others. The DICOM images are from [DICOM]. The watermark used represents the logo of the LAB-STICC of size 256 × 256 pixels. The encrypted watermarked image is attacked by applying Stirmark Benchmark software [Petitcolas 12]. Figure 7.3 illustrates the results of the encryption/watermarking process described earlier.

![Figure 7.3: Encryption and watermarking results](image)

(a) original image, (b) watermark image, (c) encrypted original image, (d) encrypted watermark, (e) encrypted watermarked image with \( \alpha = 0.99 \), (g) encrypted watermarked image with \( \alpha = 0.5 \), (f) encrypted watermarked image with \( \alpha = 0.01 \).

The value of \( \alpha \) controls the initial value of the OTP key, as well as the imperceptibility of the watermark image in the watermarked image. When \( \alpha \) is close to one, the watermark is invisible in the
watermarked image in figure 7.3 (e). Also, it is semi-visible in the watermarked image when the $\alpha$ value is 0.5, see figure 7.3 (f). However, the watermark is visible when $\alpha = 0.01$, figure 7.3 (g). As we can see in these results, the best case for an invisible watermark is one for which the value of $\alpha$ is close to one.

7.4.1 Performance under watermark attacks
In this section, we present the applied attacks to watermarked image. Figure 7.4 illustrates different kinds of attacks where the attacks descriptions are illustrated in table 7.1.
We applied the geometric and non-geometric attacks of table 7.1 to the watermarked image.

**Figure 7.4: Test results for decryption and extraction**
Table 7.1: The applied attacks descriptions

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Attack Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cropping</td>
<td>Cropping watermarked image (up to 50%)</td>
</tr>
<tr>
<td>JPEG</td>
<td>JPEG compression of watermarked image with a quality factor QF=80</td>
</tr>
<tr>
<td>Noise</td>
<td>Add 1% salt and pepper noise into the watermarked images.</td>
</tr>
<tr>
<td>Rotation</td>
<td>Rotating image with 45 degree</td>
</tr>
<tr>
<td>Scale</td>
<td>Reduce the watermarked image (up to 30%)</td>
</tr>
</tbody>
</table>

Also, we calculated the Peak Signal to Noise Ratio (PSNR) values, the Normalized Cross Correlation (NCC), the Structural Similarity Index (SSIM) and Bit Error Rate (BER) between the original watermark $w$ and the extracted watermark $w_a$ after applying the different geometric and the non-geometric attacks. The obtained results are given in table 7.2. We note that all the PSNR exceed 34 dB and that NCC and SSIM values are very close to 1. Moreover, BER is close to zero. This means that there is an almost perfect similarity between $w$ and $w_a$.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>No Attacks</th>
<th>CROP</th>
<th>JPEG</th>
<th>NOISE</th>
<th>ROT</th>
<th>SCALE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>59.1131</td>
<td>51.5059</td>
<td>57.2738</td>
<td>58.7928</td>
<td>51.1538</td>
<td>51.5962</td>
</tr>
<tr>
<td>NCC</td>
<td>0.9974</td>
<td>0.9972</td>
<td>0.9985</td>
<td>0.9975</td>
<td>0.9969</td>
<td>0.9975</td>
</tr>
<tr>
<td>SSIM</td>
<td>0.9992</td>
<td>0.9966</td>
<td>0.9990</td>
<td>0.9991</td>
<td>0.9961</td>
<td>0.9966</td>
</tr>
<tr>
<td>BER</td>
<td>0.0262</td>
<td>0.0641</td>
<td>0.0373</td>
<td>0.0267</td>
<td>0.0620</td>
<td>0.0623</td>
</tr>
</tbody>
</table>

Table 7.2: Similarity measures between $w$ and $w_a$ based on PSNR, NCC and SSIM measures

7.4.2 Encryption attacks
For the encryption attack tests, we considered the xor encryption attack as an example in order to evaluate the robustness of our approach, not only against geometric and non-geometric attacks but also for the encryption attacks. In our case, we applied the xor attack with:

$$key = 17_{10} (10001_2)$$

Figure 10.5 illustrates the extracted watermark obtained after the xor attack. To assess the robustness of our approach against this kind of attack, we also measured and compared the PSNR, NCC and SSIM values between the original watermark and the extracted one, giving values of 53.6899 for PSNR, 0.9998 for NCC and 0.9977 for SSIM.

Here also, we note that the PSNR, NCC and SSIM values are very encouraging, which allows us to conclude that our approach is robust even against cryptographic attacks.
Chapter 7: Efficient and Robust Encryption and Watermarking Technique Based on New Chaotic Map

7.5 Comparative study
We evaluated the robustness of our encryption and watermarking approach by comparing it with some other known methods proposed in the literature. The results show that our approach is more robust than the others against different kinds of attacks. Table 7.3 gives the results compared with those obtained with the approaches described in [Guo 15] and [Zheng 13].

<table>
<thead>
<tr>
<th>Attacks</th>
<th>CROP</th>
<th>JPEG</th>
<th>NOISE</th>
<th>ROT</th>
<th>SCALE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR</td>
<td>BER</td>
<td>PSNR</td>
<td>BER</td>
<td>PSNR</td>
</tr>
<tr>
<td>Our Approach</td>
<td>51.50</td>
<td>0.06</td>
<td>57.27</td>
<td>0.03</td>
<td>58.79</td>
</tr>
<tr>
<td>[Guo 15]</td>
<td>39</td>
<td>0.05</td>
<td>39.3</td>
<td>0.05</td>
<td>39.8</td>
</tr>
<tr>
<td>[Zheng 13]</td>
<td>37.9</td>
<td>0.07</td>
<td>37.5</td>
<td>0.05</td>
<td>37.8</td>
</tr>
</tbody>
</table>

Table 7.3: Comparison of the robustness of our method with some other related works [Guo 15] and [Zheng 13]

It is obvious that the proposed approach gives a better robustness than the methods presented in [Guo 15] and [Zheng 13].

7.6 Conclusion
In this approach, we proposed an innovative hybrid encryption watermarking scheme to improve the security and ensure the integrity of medical image content. The new formula of the chaotic map provided us with a key matrix equal to the image size, where for each image pixel there is a mismatch-specific key value. The generated key stream used for the OTP cryptosystem is based on a new way of applying the chaotic map approach. Here, the initial value of the key stream in the chaotic map is the same as the key used for watermarking, where the embedding and extraction are based on linear interpolation. Medical image encryption and watermarking were done by generating the key stream. A linear-interpolation based watermarking approach was also proposed to reinforce the robustness.
Chapter 7: Efficient and Robust Encryption and Watermarking Technique Based on New Chaotic Map

The properties of our chaotic map and OTP approach provided us with a reversible and predictable watermarking system. If a change is made to the first value of the key, the extractor can know that there has been tampering based on the linked values of the keys, and can recover the lost data.

Our contribution focuses on a new form of chaotic map to generate keys with specific properties, as well as achieving better efficiency, high robustness and low complexity in the encryption and watermarking approach.

The obtained results are very encouraging with regard to both security and robustness compared with existing techniques. The known similarity measurement metrics PSNR, NCC, SSIM and BER were used to assess the efficiency of the proposed approach.

The experimental results of the watermark extraction prove the efficiency of encryption based on our chaotic map improvement and OTP approach, as the extracted watermark image quality is higher than that produced by the existing encryption and watermarking approaches with which it was compared. The real advantage is that it offers an improvement of the security of medical images and a protection of the integrity of medical image content compared with other methods.
Conclusion and Future Works

Conclusion
Telemedicine requires high-security. The medical image has to be protected during the transmission. Confidentiality, authenticity and integrity are the main requirements in the medical field. The watermarking technique can demonstrate and ensure the integrity and the authenticity of the medical image after the transmission, while the cryptography can verify the confidentiality of the medical image.

Nowadays, there are a lot of approaches for securing the digital medical material during the transmission either based on watermarking or cryptography. The exciting security solutions based on the watermarking technique have a gap in the watermarking requirements. The compromise towards an adequate management between robustness and visibility is still unanswered. Moreover, real time application like telemedicine requires less computational complexity, where the time is a very important factor in the telemedicine scenario requirements. The existing approach did not provide a good security solution to dealing with the all telemedicine watermarking requirements. Based on that, we need a watermarking approach to provide a high robustness, low degradation in the watermarked image and less complexity of the embedding and extraction process.

The other way to secure the digital material is based on cryptography technique. The cryptography technique proves the security issue by assuming the intended sender and intended receiver has some security aspects called keys. The existing symmetric cryptography approaches in the medical image have a gap in the security issue of sharing the key while the gap in the existing asymmetric cryptography approaches in the medical image is that it takes a long execution time. On the other hand, the symmetric techniques allow achieving less computational complexity compared to asymmetric techniques while the latter provides a more secure key. So, we need a cryptographic approach to providing the digital medical image with a securing system with less complexity and high-security sharing key.
Conclusion and Future Works

In this chapter, we briefly concludes the thesis and highlights the major contributions. We aim to ensure and prove the security characteristics of the medical image during the transition, which can not only authenticate medical image, but would also be able to prove its integrity and its originality (owner). The authorized user in the telemedicine system would be able to extract the secret information, also the user would be able to detect any modifications in the received medical image. Finally, this research focuses on supporting the health care production in order to implement a secure, robust and privacy system for the intact sharing and usage of the medical image.

In this thesis, we have proposed robust and innovative watermarking approaches for authenticity and integrity of the digital medical image. Some of them are in the spatial domain, as the approaches are based on the FCA and ZBDD principles. In FCA approach, we investigated a novel and robust watermarking approach in the spatial domain. Our approach is innovative and based on using Formal Concept Analysis to generate the optimal position for embedding. The watermark is built from some header information of the DICOM image. It is embedded into the region of non-interest (NROI) of the medical image. Our approach demonstrates a lower computational complexity, using low capacity for the watermark and has a high robustness. Moreover, the approach can detect the removal and/or addition and/or replacement during attacks, which would be useful for tamper detection issues. In ZBDD approach, we addressed the problem of generating watermarks as small as possible (small payload) based on ZBDD to adapt the hidden data to the real time applications by maintaining high robustness, high imperceptibility and low complexity within the medical image. The results obtained show that our techniques represent a new-generation watermarking method offering low complexity, high robustness and imperceptible watermarks.

Furthermore, we presented a novel semi-blind watermarking techniques in the spatial domain in order to cover two security issues: the tamper detection and the watermarking robustness. The approach is based on the Weber differential excitation descriptor. The obtained approach has a high efficiency. Our algorithms seems to be very good both for robustness and tamper detection issues.
Conclusion and Future Works

Regarding our contribution for watermarking in the frequency domain, we have also proposed a new watermarking approach in the frequency domain to protect and to ensure the CT scan medical image authentication and robustness, which is based on the wavelet transform. It uses a linear interpolation with a coefficient t, the results obtained are very encouraging, especially when the watermark is invisible (interpolation coefficient t close to 1).

Our watermarking approaches either in spatial and frequency domain are semi-blind in order to achieve two goals. One of them is the robustness. The authentic receiver can extract the watermark from the watermarked image in order to ensure the copyright and the owner of the material. The second goal is the authenticity and integrity. The decoder can compare the extracted watermark with the original watermark in order to ensure the authenticity of the digital medical image which can be subject to malicious or unmalicious attacks.

The confidentiality of the medical image is considered in this work by proposing cryptographic approaches which solve some of the problems identified in this domain (complexity, robustness, imperceptibility). In this perspective, we have proposed an approach exploiting the characteristics of the image to generate the key of encryption / decryption. It is purely informed encryption and decryption approach based on N-gram technique. We have implemented this approach for securing the confidentiality of the medical images. The PSNR between the original image and the decrypted image is around 72 dB, while the histograms of the original images and the decrypted images have the same distributions of grayscale and therefore a show high resemblance between the original and the decrypted.

Finally, we proposed an innovative hybrid encryption and watermarking scheme in order to ensure the reliability (integrity and authenticity) and confidentiality of the digital medical image based on OTP and a new chaotic map approach. The new formula of the chaotic map provided us with a key matrix equal to the image size, where for each image pixel there is a mismatch-specific key value. The generated key stream used for the OTP cryptosystem is based on a new way of applying the chaotic map approach. The properties of our chaotic map and OTP approach provided us with a reversible and
predictable watermarking system. The experimental results of the watermark extraction prove the efficiency of encryption based on our chaotic map and OTP approach. The real advantage, compared with other methods is that it contributes to the improving of the security of medical images and of the integrity protection of medical image content.

In this thesis, the two main parameters representing the features of the medical image watermarking, namely the robustness and the execution time were considered.

Our approaches, by comparing with the existing approaches, have high robustness regarding to the geometric and non-geometric attacks. Also, we achieved less degradation in the watermarked image after the watermark embedding, as well as, less execution time for embedding and extraction process. Furthermore, we have proposed efficient and innovative way to generate an adaptive watermark is proposed. In addition, a novel cryptography approach has been proposed. Its advantages compared with the existing cryptography approaches are that the complexity is low while the key is secure.

**Future works**
As far as future works are concerned, we plan to continue our research in the following directions:

- **Blind image watermarking**
The introduced watermarking approach in our thesis is based on a semi-blind watermarking technique. The original watermark is required during the extraction phase. Our approaches provided a good compromising between robustness, imperceptibility, complexity and capacity in the digital medical image field. However, blind watermarking technique increases the security factor in this domain. There are several blind image watermarking approaches that have been presented in the watermarking field. But, their robustness is not high enough in comparison to the semi-blind techniques.

- **New measurement tools based on FCA**
Formal Concept Analysis is a mathematical method. It is presented in chapter 5 section 2. We proposed a robust and low degradation watermarking system, where the FCA principle worked to find the optimal insertion position in the medical image (5.2). We aim to use the FCA principle to measure the image quality by exploiting the image features. The FCA measurement tool will be designed to
measure the degradation either between the original image and the watermarked image to measure degradation due to the watermarking, or between the original watermark and the extracted watermark to measure the robustness of the watermarking technique.

- **Relational concept analysis (RCA)**
  In 5.2, we have presented the FCA principle to find the optimal embedding area in the medical image. RCA is the extension of the FCA, which provides a conceptual hierarchy. RCA is more general and allows a deeper analysis than FCA. RCA considers several contexts with the relation between them, it takes into account the object categories and links between objects and it provides a set of interconnected lattices. In other words, the relation between objects and attributes can be extended to a relation between concepts (concept relation). By investigating RCA in the watermarking field, we suppose the obtained results will help improve the robustness of the watermarking.

- **Orientation Weber law descriptor for tamper recovering**
  In 5.4, we proposed a novel watermarking technique for two goals. One of them is the robustness and the other is the tamper detection. The approach is based on the first Weber law descriptor (differential excitation $\chi$) in order to detect the tampered zones in the watermarked image. However, the approach is discovering the tampered zones but does not recover the original watermark. By using the second Weber law descriptor (Orientation $\lambda$), we believe that the original image can be reconstructed from the watermark image. The orientation Weber law will provide a blind recovery watermarking system for the original image.

- **Chaotic map cryptography**
  In chapter 7, we presented a new way to generate the encryption and decryption key based on chaotic map. The initial value is the security key that is used in the watermarking system and the other key is linked to the initial value (initial condition). Our chaotic map has provided us with an efficient and effective generating encryption key way, where the key size was the same as the image size. Moreover, the key is generated one time at the sender and one time at the receiver. However, the link between the secret key and the control factors must be generated accurately to verify that the chaotic map is developing in a chaotic method. We believe that deep study of this approach is still required to improve the security in the algorithm.
Conclusion and Future Works
References


References


References


References

[Medical Samples] http://www.barre.nom.fr/medical/samples


References


References


SUMMARY IN FRENCH

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

Muath AlShaikh

Cette thèse aborde la problématique de l’image médicale en tant qu’élément important de la télémédecine sous l’angle de la sécurité de l’information transmise. Nous appliquons les méthodes de cryptographie, de tatouage de l’image (watermarking) et des méthodes hybrides, cryptographie-watermarking à la sécurité de l’image médicale.

La thèse est structurée en une introduction, une première partie dédiée à l’état de l’art et comportant 4 chapitres, une deuxième partie présentant les contributions de la thèse et comportant 3 chapitres, une conclusion et un regard sur les futures possibilités de développement. Les intitulés des 7 chapitres de la thèse sont les suivants :

Chapitre 1 : Le tatouage de l’image numérique ;
Chapitre 2 : La cryptographie de l’image numérique ;
Chapitre 3 : Techniques hybrides de tatouage de l’image et cryptographie ;
Chapitre 4 : L’image numérique médicale et la sécurité de la télémédecine ;
Chapitre 5 : Les approches de tatouage proposées ;
Chapitre 6 : Un algorithme de cryptage symétrique informé pour les images DICOM basé sur les N-grams ;
Chapitre 7 : Une technique efficace et robuste de tatouage et de cryptage de l’image basée sur une nouvelle approche de carte chaotique (chaotic map).

Introduction

Dans l’introduction, il est présenté l’importance de la sécurité et de la sureté de l’information dans le contexte de l’Internet et des nouvelles technologies.
Par ailleurs, dans le contexte de l’importance croissante dans le monde de la qualité du système médical, la télémédecine occupe un rôle très important. Dans le cadre de cette dernière l’image médicale occupe une place importante.

La protection de l’image médicale comprend au moins deux aspects principaux : la sécurité et l’authentification. La transmission de l’image médicale doit avoir trois caractéristiques : la confidentialité, l’authenticité et la fiabilité. La confidentialité représente le fait que l’accès à l’image médicale ne doit être permis qu’à des utilisateurs autorisés. L’authenticité est la propriété qui assure que l’image à la sortie du canal de transmission soit « identique » à celle qui est entrée dans le canal de transmission. La fiabilité représente la propriété suivant laquelle l’intégrité de l’image par rapport aux attaques possibles doit être assurée.

Les approches cryptographiques, les approches de tatouage et les approches hybrides (combinant cryptographie et tatouage) protègent les données médicales pendant la transmission et permettent de satisfaire convenablement les propriétés ci-dessus.

Le but de ce travail est d’améliorer les méthodes existantes de cryptographie et de tatouage, en proposant de nouvelles approches de protection de l’image médicale. Les méthodes proposées assurent une bonne confidentialité, intégrité et fiabilité pour la transmission de l’image médicale.

**Chapitre 1: Le tatouage de l’image numérique**

Le tatouage de l’image numérique est l’art de cacher de l’information secrète dans les données d’origine. Les données d’origine sont visibles par tous, alors que les données cachées ne sont visibles et modifiables que par des utilisateurs autorisés. Le tatouage de l’image peut être utilisé pour vérifier l’authenticité et l’intégrité du signal hôte ou pour vérifier l’authenticité du propriétaire.

Un autre domaine de recherche développé pour la sécurité de l’information est la stéganographie. Les deux domaines, le tatouage et la stéganographie ont comme objectif principal la sécurité de l’information. La différence entre les deux est que dans le cas du tatouage les deux informations, celle qui est cachée et celle qui cache sont en relation l’une avec l’autre, tandis que dans le cas de la stéganographie ces deux informations ne sont pas en
relation [Shih 07]. En stéganographie, le message caché doit être invisible, tandis qu’en tatouage, il peut être visible ou invisible. En stéganographie, Le message caché doit être caché de telle manière qu’il ne puisse pas être détecté par des utilisateurs non-autorisés, tandis qu’en tatouage le message caché doit être caché tel qu’il ne soit pas enlevé ou remplacé par des personnes non-autorisées.

La structure de ce chapitre est la suivante : dans le premier sous-chapitre, nous présentons la définition du tatouage de l’image. Le deuxième sous-chapitre contient les propriétés des techniques de tatouage, le troisième sous-chapitre présente les objectifs et les applications du tatouage. Le quatrième sous-chapitre analyse la classification des méthodes de cryptage et de décryptage, le cinquième sous-chapitre présente les approches de tatouage visible. La robustesse en tant que propriété du tatouage et les attaques sont présentés dans le sixième sous-chapitre. Le septième sous-chapitre analyse la notion d’évaluation de la qualité d’une image.

Chapitre 2: La cryptographie de l’image numérique

Ce chapitre contient en début la définition de la cryptographie : l’art de l’encryptage (chiffrement) et du décryptage des données pour les protéger pendant la transmission et le stockage de l’information. La cryptanalyse est l’étude et l’analyse des approches cryptographiques [Mel 01]. L’objectif principal de l’encryptage est d’assurer la sécurité du message transmis via un canal non-sécurisé. Le décryptage est la phase de reconstruction du message original à partir du message encrypté.


Dans le sous-chapitre 2.4, il est présenté l’état de l’art dans le domaine des techniques cryptographiques et, notamment, un aperçu sur les algorithmes d’encryptage symétrique, sur l’encryptage standard des données (Data Encryption Standard (DES)), sur l’encryptage
standard avancé (Advanced Encryption Standard (AES)) et sur les algorithmes d’encryptage asymétrique.


Entre les approches symétrique et asymétrique, en termes de caractéristiques de la cryptographie comme technique de sécurisation de l’information, il y a la différence principale suivante: les techniques symétriques sont moins sûres, mais elles nécessitent un temps d’exécution moins long que les techniques asymétriques, tandis que les techniques asymétriques sont plus sûres, mais requièrent un temps d’exécution plus long que les techniques asymétriques.

Chapitres 3: Techniques hybrides de tatouage et cryptographie

Les techniques cryptographiques assurent une protection à priori. Pour pouvoir vérifier l’intégrité, l’authenticité et l’originalité des données après le décryptage on peut utiliser des techniques de tatouage [Bouslimi 12]. Les techniques hybrides de cryptographie et tatouage sont obtenues par la combinaison entre cryptographie et tatouage. Les quatre modes de combinaison entre cryptographie et tatouage sont : tatouage suivi par encryptage (Watermarking Followed by Encryption (WFE)), encryptage suivi par tatouage (Encryption Followed by Watermarking (EFW)), tatouage /décryptage combiné (Joint Watermarking / Decryption (JWD)) et tatouage /encryptage combiné (Joint Watermarking / Encryption (JWE)). Ces méthodes sont présentées dans les sections 3.2, 3.3, 3.4 et 3.5.

Chapitre 4: L’image médicale numérique et la sécurité en télémédecine

Dans ce chapitre, nous présentons les définitions de la télémédecine et de l’image médicale, de l’image médicale numérique, le statut et la position de l’image médicale dans le domaine de la télémédecine, les systèmes existants de stockage et de transfert des images médicales (HIS et PACS) et les caractéristiques de sécurité propres à l’image médicale. Nous présentons aussi des applications visant la sécurité des images médicales.

La sous-section 4.1.1 contient la définition de l’image numérique, la sous-section 4.1.2 la définition de l’image numérique médicale [Huang 11 (a)]. La section 4.2 contient la
description du système d’archivage et communication des images PACS (Picture Archiving and Communication System).

La section 4.3 est dédiée à la définition et l’analyse du domaine de la télémédecine. La section 4.4 présente le format standard des images médicales (Digital Imaging and Communications in Medicine (DICOM) développé dans le but d’une unification en ce qui concerne, le traitement, la transmission, le stockage des images médicales. Une image médicale est composée de l’entête de l’image et du corps de l’image. L’entête contient des informations sur l’identité du patient, le corps de l’image est composé de deux régions : la région d’intérêt (region of interest ROI) et la région de non-intérêt (region of non-interest NROI). La première contient les informations d’intérêt strictement médical sur le patient (l’image sur les éléments de sa maladie), la deuxième représente la frontière de tout l’ensemble. Les figures 4.2 et 4.3 présentent les parties de l’image médicale selon DICOM.

Le standard DICOM est composé de 15 parties. Dans la partie n° 15, se trouvent les éléments de sécurité de l’image regroupés en 4 profils : profil de sécurité de l’utilisation, profil de sécurité de transport, profil de signature numérique et profil de sécurité de stockage. Leur description est donnée dans la sous-section 4.5.3. La section 4.6 comporte une discussion sur les besoins de sécurité de l’image médicale : confidentialité, intégrité, authentification, instanciés dans le cas de ce type d’image. Le sous-chapitre 4.7 présente quelques applications de sécurité développées pour l’image médicale regroupées en : applications basées tatouage et applications hybrides tatouage-cryptographie.

La deuxième partie de cette thèse contient l’apport original de l’auteur dans les chapitres 5, 6 et 7. Les approches décrites dans les sections 5.2, 5.3 et 5.4 du chapitre 5 sont des approches de tatouage dans le domaine spatial. La section 5.5 présente une approche de tatouage dans le domaine fréquentiel. Le chapitre 6 aborde une approche de cryptographie et le chapitre 7 une approche hybride (combinaison de tatouage et de cryptographie). Toutes ces contributions ont été publiées ou soumises à la publication dans des conférences ou des revues internationales.

Les résultats obtenus montrent que dans le cas de la télémédecine où les applications développées sont des applications en temps réel, le domaine spatial est meilleur grâce à la complexité réduite qu’il assure. Le domaine fréquentiel est meilleur dans le cas des applications requérant une robustesse élevée.
Chapitre 5 (section 5.2): L’analyse de concepts formels (Formal Concept Analysis - FCA) pour l’amélioration de la robustesse du tatouage de l’image médicale dans le domaine spatial

Dans ce chapitre nous présentons une nouvelle approche pour le tatouage de l’image médicale dans le domaine spatial basée sur l’analyse de concepts formels (Formal Concept Analysis (FCA) [Ganter 12]. La FCA nous permet de trouver la position optimale d’insertion de la marque dans la région de non-intérêt (NROI) de l’image médicale. Les informations contenues dans la marque sont extraites de l’entête de l’image. Elles sont : Nom du patient, Date de naissance, Age du patient, Date de modification du fichier. Les relations qui existent entre ces informations nous permettent de détecter si une éventuelle attaque est arrivée (Tamper Detection).

Nos résultats expérimentaux montrent que l’image marquée intégrée possède une très bonne qualité après l’extraction dans le cas sans attaque, une qualité satisfaisante même après des scénarios d’attaques et qu’on peut avoir une complexité computationnelle réduite.

Ce chapitre est organisé de la façon suivante : dans les deux premières sections, nous présentons le modèle formel de la FCA, les définitions et quelques domaines d’application. Dans la troisième section nous présentons notre approche (la procédure d’insertion de la marque et d’extraction de la marque). Dans la quatrième section, nous présentons les résultats expérimentaux (la robustesse, la capacité, la complexité et la résistance aux attaques). Les conclusions sont présentées dans la cinquième section.

La caractéristique principale de cette approche est le fait qu’elle détecte d’abord la position optimale de l’insertion de la marque en se basant sur la FCA. L’idée est de construire les concepts formels au sens de la FCA pour les zones Gauche-Haut, Gauche-Bas, Droite-Haut et Droite-Bas vues comme des matrices booléennes. Toutes les transformations portant sur l’extraction des quatre zones ci-dessus et sur la construction des treillis de concepts au sens de FCA pour ces zones sont données par l’algorithme II. Nous choisissons comme objets les numéros de ligne et comme attributs les numéros de colonnes de ces matrices. L’algorithme III présente l’étape de l’insertion de la marque. L’insertion se fait par l’interpolation linéaire. La figure 5.5 A présente l’image tatouée après l’insertion par l’interpolation linéaire des quatre images marque. La figure 5.5 B présente les images
marque contenant des informations DICOM. La procédure d’extraction est également basée sur l’interpolation linéaire.

Les résultats expérimentaux (section 5.4) montrent une complexité computationnelle réduite, une capacité réduite pour la marque et une robustesse assez élevée. L’insertion est aussi caractérisée par une grande imperceptibilité. En plus, par cette méthode, on peut détecter l’enlèvement ou l’addition d’informations liées à une attaque. Cette méthode basée sur le modèle FCA peut détecter les attaques en comparant les concepts FCA de l’image extraite avec les concepts obtenus de l’image d’origine. Et cela, grâce à la construction du treillis FCA qui représente la structure de treillis FCA associé à une image.

Chapitre 5 (section 5.3): Un tatouage de l’image adaptif et informé d’une manière optimale pour l’image médicale basé sur le diagramme de décision binaire par suppression des zéros (Zero-Suppressed Binary Decision Diagram – ZBDD)

La façon de générer la marque a une très grande importance dans les schémas de tatouage. On a besoin des marques les plus petites possibles qui peuvent être insérées et extraites avec une complexité computationnelle réduite et, en même temps, que la robustesse et la résistance aux attaques soient assurées. Dans cette approche, nous nous focalisons sur la robustesse de l’image médicale et sur la possibilité de générer des marques les plus petites possibles pour ce type d’image.

Par cette approche, nous proposons une solution au problème de la génération des marques qui contient une grande quantité de données qui seront insérées d’une manière dynamique. Le diagramme de décision binaire par suppression des zéros (Zero-Suppressed Binary Decision Diagram – ZBDD) est connu par sa capacité de réduction des parties moins importantes appartenant à des données de grande taille.

L’idée de base de l’algorithme proposé dans ce chapitre est de construire une marque (marque de tatouage) optimisée basée sur les caractéristiques de l’image initiale marque informée. La procédure ZBDD est utilisée pour obtenir les valeurs les plus élevées des pixels qui vont donner les caractéristiques de la marque. Nous avons testé la robustesse de notre solution contre certaines attaques géométriques et non-géométriques.

Chapitre 5 (section 5.4): Une nouvelle approche de tatouage informé de l’image et de détection de modifications malveillantes basée sur le descripteur d’excitation différentielle de Weber

Dans ce chapitre, nous présentons une approche de tatouage semi-aveugle et informé basée sur le descripteur d’excitation différentielle de Weber. La méthode proposée a comme principal objectif la construction d’une marque à partir de l’image initiale de manière à obtenir une robustesse élevée et détecter les éventuelles zones attaquées. L’analyse des résultats est orientée vers la robustesse du tatouage et vers la sensibilité aux différentes attaques. Le chapitre présente d’abord la loi de Weber, ensuite la méthode proposée, les résultats expérimentaux obtenus et la détection des fausses informations (attaques). Finalement, une étude comparative est réalisée.

La loi de Weber décrit la relation entre la quantité et l’intensité de l’information. Le descripteur de Weber a deux composantes : l’excitation différentielle et l’orientation. La marque du tatouage est construite à partir de l’image hôte en utilisant la loi de Weber. L’image hôte est divisée en 3 blocs superposés pour lesquels on calcule l’excitation différentielle. La nouvelle matrice ainsi obtenue est utilisée comme la marque de tatouage (marque informée). Dans la phase d’extraction, si l’image tatouée a été attaquée, l’extracteur compare l’image d’origine marquée avec l’image extraite. Les différences entre les deux montrent les zones attaquées. La phase d’insertion est présentée dans la sous-section 5.4.1, la phase d’extraction dans la sous-section 5.4.2. La section 5.4 contient les résultats expérimentaux. La détection des zones attaquées est présentée en section 5.4.5 (figures 5.28 et 5.29).
L’étude comparative réalisée dans la section 7.5 entre cette méthode et celle de [Walia 13] montre que notre méthode donne de meilleurs résultats pour la capacité et la dégradation. Elle permet une plus grande capacité de la marque avec moins de dégradation que celle de [Walia 13].

**Chapitre 5 (section 5.5): Une nouvelle architecture de tatouage de l’image dans le domaine fréquentiel (les coefficients de la transformée en ondelettes discrètes – DWT Transform Coefficient)**

Dans ce chapitre, nous présentons notre méthode de tatouage dans le domaine fréquentiel basée sur les techniques de la transformée en ondelettes discrètes (DWT Transform Coefficient). Cette méthode peut assurer l’authenticité et, par conséquence, la fiabilité du processus entier de transmission de l’image médicale. Notre méthode s’avère posséder une grande robustesse et être d’une complexité computationnelle réduite par rapport aux autres méthodes de même type. Dans notre approche, nous utilisons un seul niveau DWT autant pour la marque utilisée que pour les images initiales. L’insertion de la marque dans l’image initiale est faite par l’interpolation linéaire ([Laouamer 13], [Benhocine 13], [Benhocine 08] and [Benhocine 09]). Cette méthode d’insertion assure l’imperceptibilité de la marque sans dégradation de la qualité de l’image tatouée. L’élément nouveau de cette approche est la phase d’extraction qui prend en compte l’image tatouée et non seulement l’image tatouée attaquée.

Dans la section 5.5.2 nous présentons le principe de décomposition du signal en ondelettes. Ensuite, dans la section 5.5.3, nous présentons notre approche et, dans la section 5.5.4, les résultats obtenus.

Cette méthode est appropriée pour assurer l’authentification et la robustesse des images médicales. Bien que l’approche soit applicable à tout type d’image, elle est très intéressante dans le cas de la télémédecine, parce qu’elle assure une qualité élevée de l’image transmise avec moins de dégradation par comparaison aux autres méthodes du même type.

Les résultats obtenus sont très encourageants, surtout dans le cas où la marque est invisible. La comparaison avec d’autres méthodes a été réalisée en utilisant les mesures de similarité bien connues comme PSNR, SSIM, UQI. Les résultats expérimentaux montrent que la technique proposée assure plus de robustesse contre différents types d’attaques que les méthodes présentées dans [Ahmad 14] et dans [Benrhouma 15].
Chapitre 6: Un algorithme de cryptage symétrique informé pour les images DICOM basé sur les N-grams

Dans le choix d’une méthode d’encryptage / décryptage, il y a deux critères de base : la complexité computationnelle et la sécurité en soi. Beaucoup de systèmes d’encryptage basés sur des clés publiques sont très lents et demandent beaucoup de calculs. Par exemple, l’algorithme RSA est considéré cent fois plus lent que l’algorithme AES dans les implémentations logicielles et il est complètement hors de portée avec des implémentations matérielles. De même, il est très difficile et cela prend beaucoup de temps de trouver un grand nombre de factorisations de deux nombres premiers, donc il devient inapproprié d’utiliser RSA par comparaison à un système symétrique. C’est parce que la clé est très grande pour l’algorithme RSA et l’encryptage / décryptage est long. Le système RSA n’est pas approprié pour les images [Puech 06]. Par conséquent, pour des raisons de sécurité, des problèmes liés à la structure des systèmes d’encryptage à clé publique sont posés. On peut remarquer que la taille des clés des crypto-systèmes publiques est plus grande que la taille des clés des systèmes avec clé secrète pour le même degré de sécurité. D’où l’importance de la taille de la clé, importance qui est légitime aussi pour les systèmes à clé publique.

En fait, ces systèmes sont basés sur l’hypothèse que les seules attaques possibles sont les attaques appelées attaques exhaustives. Les attaques exhaustives sont les attaques qui présupposent toutes les clés possibles. Par exemple, dans le cas d’une clé sur 128 bits, la taille des espaces possibles est de $2^{128}$. Mais dans le cas d’une clé publique la taille de la clé est légitime seulement si on considère le même système. En effet, le système RSA sur 512 bits est moins sécurisé que le système AES sur 128 bits. Le seul moyen d’évaluer correctement un système à clé publique est selon la complexité de la meilleure attaque connue.

Très récemment, on a factorisé avec succès des nombres sur 512 bits [Ismail 10]. Il est envisageable pour une meilleure sécurité d’aller à 1024 bits pour le futur.

La méthode des N-grams présente plusieurs avantages :

- Elle capte automatiquement les racines de plusieurs pixels communs.

- Les N-grams sont indépendants de la nature et de la qualité de l’image. Par les N-grams nous n’avons pas besoin de faire une segmentation à priori de l’image.

- Ils tolèrent un petit changement de l’intensité des pixels.

L’organisation de ce chapitre est la suivante : dans la section 6.2, nous présentons la théorie des N-grams (bi-grams, tri-grams, ….). La section 6.3 présente notre algorithme et la section 6.4 présente les résultats obtenus.

Notre base de données est composée de 450 images DICOM en différentes échelles de gris, de taille 256 x 256. L’encryptage / décryptage a été réalisé pour 9 images par bi-grams et tri-grams (figures 6.4 et 0.5). Nous avons obtenu un PSNR proche de 72 dB, ce qui prouve qu’il n’y a pas une dégradation significative entre l’image initiale et celle décryptée. Les histogrammes des images initiales et des images décryptées de la figure 6.4 sont présentés dans les figures 6.6 et 6.7 pour les bi-grams et tri-grams, respectivement.

**Chapitre 7 : Une technique efficace et robuste de tatouage et de cryptage de l’image basée sur une nouvelle approche de carte chaotique (chaotic map).**

Dans ce chapitre, nous proposons un système de tatouage et de cryptage basé sur un algorithme d’encryptage de type one-time pad (OTP) qui génère une suite chainée de clés. Pour la génération des clés, nous proposons une approche de type carte chaotique (chaotic map).

Il s’agit d’un schéma hybride composé d’un algorithme d’encryptage de type OTP et d’un tatouage semi-aveugle de l’image médicale hôte. La marque déjà encryptée est insérée dans l’image hôte encryptée dans le domaine spatial. Les résultats obtenus prouvent une parfaite extraction, même après certaines attaques.

Le chapitre est organisé comme suit : nous présentons d’abord le principe de l’OTP et la notation d’application de type chaotique (chaotic map). Ensuite, le système hybride de
tatouage et cryptographie est présenté. La section 7.4 présente les tests basés sur différentes attaques et la section 7.5 une comparaison avec d’autres approches.

Les tests ont été réalisés sur des images médicales DICOM de 256 x 256 pixels provenant de radiographies à base de rayons X, d’ultrason ou de CT-scan (scanner assisté par ordinateur). La marque utilisée est le logo LAB-STICC de dimension 256 × 256 pixels. L’image encryptée est attaquée en utilisant la plateforme logicielle Stirmark [Petitcolas 12].

L’étude comparative est présentée dans le tableau 7.3.

La méthode proposée s’avère assurer une meilleure intégrité et une meilleure sécurité du contenu des images médicales par rapport aux autres méthodes.

**Conclusion**

Les méthodes de tatouage proposées dans cette thèse ont une grande robustesse par rapport aux attaques géométriques et non-géométriques. Elles se caractérisent en général par une faible dégradation de l’image après le décryptage et un temps d’exécution assez court pour l’encryptage et le décryptage. L’approche cryptographique proposée est nouvelle en cryptographie. Elle se caractérise par une complexité computationnelle réduite et une clé sûre.

**Travaux futurs**

Les recherches entreprises seront continuées dans les directions suivantes :

- Tatouage aveugle
- Nouvelles mesures de qualité du tatouage basées sur la FCA
- Application de l’analyse des concepts relationnels (Relational Concept Analysis (RCA)) au tatouage de l’image
- Approches de tatouage basées sur le deuxième descripteur de la loi de Weber
- Cryptographie basée sur les approches chaotiques
Protection des contenus des images médicales par camouflage d’informations secrètes pour l’aide à la télémédecine

Résumé

La protection de l’image médicale numérique comporte au moins deux aspects principaux: la sécurité et l’authenticité. Afin d’assurer la sécurité, l’information doit être protégée vis-à-vis des utilisateurs non autorisés. L’authenticité permet quant à elle de s’assurer que la donnée reçue n’est pas modifiée, n’est pas altérée, et qu’elle est bien envoyée par l’expéditeur supposé. La « technique » cryptographique garantit la sécurité en faisant l’hypothèse que l’expéditeur et le destinataire ont des clés permettant respectivement de crypter et de décrypter le message. De cette manière, seule la personne possédant la bonne clé peut décrypter le message et accéder au contenu de la donnée médicale.

Dans cette thèse, nous avons apporté plusieurs contributions. La principale contribution est la proposition de solutions de tatouage d’images médicales robustes et réversibles dans le domaine spatial basées respectivement sur l’analyse de concepts formels (FCA) et le diagramme de décision binaire par suppression des zéros (ZBDD). La seconde est une approche de tatouage d’image médicale semi-aveugle pour la détection de modifications malveillantes. Une autre contribution est la proposition d’un système de chiffrement symétrique sécurisé basé sur les N-grams. La dernière contribution est un système hybride de tatouage et de cryptographie d’image médicale qui s’appuie sur une nouvelle forme de carte chaotique (chaotic map) pour générer des clés ayant des propriétés spécifiques, et qui permet d’obtenir une meilleure efficacité, une grande robustesse et une faible complexité par rapport aux approches existantes.


Medical Image Content Protection by Secret Information Hiding to Support Telemedicine

Abstract

The protection of digital medical image comprises at least two main aspects: security and authentication. In order to ensure the security, the information has to be protected from the unauthorized users while the authentication confirms that the received data is not affected or modified and is sent by the intended sender (watermarking). The cryptography technique proves the security issues by assuming the intended sender and intended receiver have some security aspects called keys. So, after encryption of the digital material from the sender side, the person who has the key (receiver) can decrypt and access the content of the digital material.

In this thesis, we have brought several contributions. The main one is the provision of robust and reversible medical image watermarking solutions in the spatial domain based respectively on FCA and ZBDD. The second one is a semi-blind medical image watermarking approach for the tamper detection. Another contribution is the proposal of a secure symmetric encryption system based on N-gram. The last contribution is a hybrid watermarking and cryptography medical image system which focuses on a new form of chaotic map to generate keys with specific properties, and achieves better efficiency, high robustness and low complexity than the existing approaches.

Keywords: Watermarking, Cryptography, DICOM, Medical Image, Attacks, Robustness, Imperceptibility, ZBDD, FCA, Weber, Chaotic Map, OTP, N-gram.