A STUDY AND ANALYSIS OF WATERMARKING ALGORITHMS FOR MEDICAL IMAGES

By

OSAMAH MOHAMMED ABDO AL-QERSHI

Thesis submitted in fulfillment of the
requirements for the degree of
Master of Science

December 2010

ACKNOWLEDGMENT

I would like to express my deep and sincere gratitude to my supervisor, Dr. Khoo Bee Ee. Her wide knowledge and her logical way of thinking have been of great value for me. Her understanding, encouraging and personal guidance have provided a good basis for the present thesis.

I also would like to thank my co-supervisor, Dr Mohammed Ezane Aziz, for his valuable notes and comments, and for supplying the medical images used for testing and evaluation during my study.

I owe my loving thanks to my wife Amal, and to my family. Without their encouragement and understanding it would have been impossible for me to finish this work. My special gratitude is due to my brothers, my sisters and their families for their loving support.

Also, I would like to express my sincere thanks to the School of Electrical and Electronic Engineering, Universiti Sains Malaysia for providing the necessary facilities for this research.

Lastly, I offer my regards and blessings to all those who supported me in any aspect during the completion of this thesis.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

CHAPTER TWO: LITERATURE REVIEW

CHAPTER THREE: REVERSIBLE WATERMARKING FOR DATA HIDING APPLICATIONS

CHAPTER FOUR: REVERSIBLE WATERMARKING FOR DATA HIDING AND AUTHENTICATION

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

ACR	American College of Radiology
bpp	bit per pixel
CD	Compact Disk
CR	Computed Radiography
CT	Computerized Tomography
DCT	Discrete Cosine Transform
DE	Difference Expansion
DFT	Digital Fourier Transform
DICOM	Digital Imaging and Communications in Medicine
DWT	Discrete Wavelet Transform
ECG	Electrocardiogram Graph
HVS	Human Visual System
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MD5	Message-Digest algorithm 5
MR	Magnetic Resonance
NEMA	National Electrical Manufacturer Association
PER	Patient Electronic Record
PSNR	Peak Signal to Noise Ratio
QoS	Quality of Service
ROI	Region of Interest
RONI	Region of Non-Interest
ROE	Region of Embedding
RS Code	Read-Solomon error correction code
SNR	Signal to Noise Ratio
SSIM	Structural Similarity Index
US	Ultra Sound
VW2D	Variable-Watermark Two-Dimensional

KAJIAN DAN ANALISIS ALGORITMA PEMBENAMAN TERA AIR UNTUK IMEJ PERUBATAN

ABSTRAK

Teknik-teknik pembenaman tera air menyembunyikan data digit ke dalam imej-imej digit untuk pelbagai keperluan dan aplikasi seperti perlindungan hak cipta, pengesahan, dan penyembunyian data. Salah satu tujuan sistem pengurusan kesihatan ialah pengarkiban rekod pesakit dengan selamat. Namun, rekod-rekod tersebut mungkin memerlukan kapasiti media yang sangat besar untuk disimpan, masa yang lama untuk dihantar apabila diperlukan, dan mengakibatkan kos yang tinggi. Teknologi penyulitan klasik adalah alat penting yang boleh digunakan untuk melindungi data yang dihantar melalui rangkaian komputer tetapi ia tidak menyelesaikan semua masalah perlindungan data digit. Algoritma pembenaman tera air adalah teknologi baru untuk pengesahan gambar digit. Ia dicadangkan untuk mengatasi masalah pengesahan, keupayaan dan kos kerana algoritma pembenaman tera air boleh digunakan untuk menyimpan nota perubatan yang berbeza seperti grafik, teks, dan lain-lain. Hal ini mengelakkan keperluan menyimpan fail data berasingan dengan gambar-gambar perubatan. Empat algoritma pembenaman tera air dicadangkan di dalam tesis ini bagi tujuan yang berbeza untuk sistem pengurusan kesihatan Dua algoritma terawal merupakan algoritma pembenaman tera air bolehbalikan dan boleh digunakan untuk aplikasi penyembunyian data. Kedua-dua algoritma yang dicadangkan menunjukkan kapasiti pembenaman yang tinggi dengan kualiti visual yang sangat baik. Algoritma ketiga yang dicadangkan merupakan algoritma bolehbalikan dengan kebolehan pengesahan, pengesanan gangguan dan kemudahan pemulihan imej yang telah didapati diubahsuaikan. Algoritma tersebut menunjukkan prestasi yang baik dalam kapasiti penyembunyian dan kualiti visual. Ciri pengesahan, pengesanan gangguan dan kemudahan pemulihan untuk algoritma tersebut telah dibuktikan dalam eksperimen. Algoritma keempat adalah algoritma yang ditambahbaikan dari algoritma ketiga. Algoritma tersebut merupakan algoritma hibrid yang mempunyai kebolehan pengesahan, pengesanan gangguan dan kemudahan pemulihan. Keputusan kajian algoritma tersebut menunjukkan prestasi yang baik dalam kemampuan untuk menyimpan data pesakit dan juga dalam aspek kualiti visual. Kebolehan pengesahan, pengesanan gangguan dan pemulihan bagi algoritma tersebut telah dibuktikan dalam eksperimen. Selain itu, algoritma tersebut menunjukkan beberapa ketahanan terhadap jenis gangguan hingar seperti jenis hingar garam dan lada dan pemotongan. Umumnya, prestasi keempat-empat algoritma bergantung pada jenis imej yang mengalami teknik pembenaman tera air.

A STUDY AND ANALYSIS OF WATERMARKING ALGORITHMS FOR MEDICAL IMAGES

ABSTRACT

Digital watermarking techniques hide digital data into digital images imperceptibly for different purposes and applications such as copyright protection, authentication, and data hiding. One of the objectives of health care management systems is to securely archive patients' records. Moreover, these records may require very large media capacity to store, long time to transmit, and consequently incur higher cost. Classical encryption technology is an important tool that can be used to protect data transmitted over computer networks but it does not solve all digital data protection problems. Digital watermarking is an emerging technology for digital image authentication. It is proposed to overcome the problems of authentication, capacity and cost as the watermarking schemes can be used to store different medical records such as graphs, text, etc. This eliminates storing separate data files along with the medical images. In this thesis, four digital watermarking algorithms were proposed for medical images. The first two algorithms are reversible and can be used for data hiding application. The proposed two algorithms showed high embedding capacity with very good visual quality. The third algorithm is a reversible algorithm with authentication, tamper detection, and recovery facilities. The algorithm showed good performance in terms of hiding capacity and visual quality. Also the proposed algorithm could authenticate the watermarked images. In case of tampering, the proposed algorithm could detect the tampered areas and even recover those areas in some cases. The fourth algorithm is a hybrid algorithm with authentication, tamper detection, and recovery facilities. The results showed good performance in terms of the ability to store patient's data and visual quality. Also the authentication and tamper detection facilities were tested same as in the third proposed algorithm. In addition, the algorithm showed some robustness against certain types of noise such as salt and pepper and cropping. The general performances of the four proposed algorithms depend on the modality of the image undergone watermarking.

CHAPTER ONE
INTRODUCTION

1.0 Background

During the last few years, medical data management systems have been changed in the consequence of the fast and significant advancements in information and communication technologies. One of the main activities that medical data management system involves is the exchange of databases between hospitals and health centers over efficient transmission channels. The process of data exchange involves transmission of different types of data format: medical images, texts, and graphs. The transmission of such a large amount of data when done separately using ordinary commercial information transmitting channels like Internet, results in extreme memory utilization, an increase in cost and time of transmission. Using the Internet for transmitting medical images may render them accessible to unauthorized people (Anand and Niranjan, 1998).

Medical Images are produced by wide variety of imaging equipments, such as computed tomography (CT), magnetic resonance imaging (MR), ultrasound (US), etc. Now, these medical images generally are stored in digital forms on different types of storage media. However, the digital images are very easy to be modified by any image processing computer software. Hospitals, insurance companies, as well as patients might want to modify the image for various reasons. One of those reasons is the possibility of using the modified images, i.e. tampered images, for illegal purposes (Wu *et al.*, 2008).

One possible solution is digital watermarking, which is a commonly used technique to hide data into images and authenticate images as well. Medical image watermarking is a particular subset of image watermarking whereby medical images are embedded with invisible information that may be used to declare ownership, improve the security, and verify the integrity of medical images (Planitz and Maeder, 2005).

The development of digital watermarking for digital medical images provides a possible solution for the problems related to digital medical images' applications; storage, speed of transmission, protection, and authentication. Digital watermarking techniques are divided into two basic categories: spatial domain watermarking and frequency domain watermarking. Spatial domain watermarking constitutes interleaving the watermark bits directly into image pixels. The images are generally manipulated by altering one or more of the bits of the bytes that make up the pixels of the image (Schyndel *et al.*, 1994, Wolfgang and Delp, 1996, Wong, 1999). Frequency domain watermarking involves applying transformation techniques like Digital Fourier Transform (DFT), Digital Cosine Transform (DCT), or Digital Wavelet Transform (DWT), and then the watermark is embedded into some selected frequency components to obtain watermarked images (Nayak *et al.*, 2004a).

The spatial domain techniques are weak against attacks, so the watermarking achieved using such technique is called fragile. On the other hand frequency domain watermarking techniques are quite strong against attacks, so they are called robust. Frequency domain techniques are much elaborated techniques have the advantage of offering a good trade-off between robustness and visual quality of the watermarked image. However, their main drawback is their complexity, computational cost, and the lack of reversibility (Darmstaedter *et al.*, 1998).

1.1 Motivation

Exchanging medical records among heath care systems may introduce risks for inappropriate use of medical information circulated in open networks. This gives the ease with which digital medical contents can be manipulated. It is well known that the integrity and confidentiality of medical records is a critical issue for ethical as well for legal reasons. One of the suggested solutions, which can be used to protect data transmitted over computer networks, is encryption technology. Encryption technology is an important tool that but it doesn't solve all digital data protection problems (Boucherkha and Benmohamed, 2005). At the receiver's side, decrypted content may be subject to unauthorised use or manipulation. Digital watermarking is an emerging technology for digital medical image authentication. Image authentication is usually achieved by fragile schemes, which can detect any manipulation made to a digital image to guarantee the content integrity. Besides authentication, watermarking schemes can be used to store different medical records such as graphs, text, etc. This eliminates storing separate data files along with the medical images (Osborne, 2005).

For medical images, a watermarking method is usually designed depending on an application framework fulfilling different requirements (Coatrieux and Lecornu, 2006):

1. Capacity: the amount of information that can be embedded.
2. Robustness: a fragile watermark will not survive any image processing.

3. Security: based on secret knowledge for watermark content access (usually a secret key). It includes authenticity and integrity control.
4. Imperceptibility.

Depending on the nature of the requirements of the application, the appropriate watermarking type is selected. Thus, copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes (Lin and Delp, 1999b). A fragile watermarking scheme detects any manipulation made to a digital image to guarantee the content integrity while a robust scheme prevents the watermark removing unless the quality of the image is greatly reduced (Boucherkha and Benmohamed, 2004).

Another classification of medical image watermarking is based on Region of Inertest (ROI). ROI is an area of the image which contains important information and must be stored without any distortion (Wakatani, 2002). ROI-based digital watermarking techniques for medical images must avoid altering the data in ROI by embedding the watermark in other area than the ROI (Giakoumaki *et al.*, 2006a, Lee *et al.*, 2005, Zain and Clarke, 2007). The advantage of such techniques is keeping the most important area for diagnosis, which is the ROI, intact in order to eliminate the possibility of misdiagnoses.

Many watermarking schemes of different modalities were proposed for medical images (Anand and Niranjan, 1998, Nayak *et al.*, 2004a, Woo *et al.*, 2005, Zain and Fauzi, 2007, Giakoumaki *et al.*, 2006a, Guo and Zhuang, 2007, Wu *et al.*, 2008, Wakatani, 2002, Chiang *et al.*, 2008). However, these algorithms do not meet all medical image watermarking requirements because of the lack of reversibility, the lack of ability to authenticate at least the ROI, or the limitation of the hiding capacity. This makes the medical image watermarking an open area for research (Planitz and Maeder, 2005).

In order to overcome the limitations of the previous schemes, this research adopts the idea of gathering the advantages of two single schemes in one scheme. By combining the characteristics of fragile watermarking and robust watermarking, a reversible ROI-based technique can be generated. This algorithm can be used for data hiding, authentication, and recovery, while showing some robustness against certain types of attacks. Data hiding capability is used to embed patient’s data for the purpose of identification and annotation; i.e. patient’s data and report. Image authentication verifies the originality of an image by detecting malicious tampering to figure out how the image was modified or which portion of it has been tampered with. Image recovery is the ability of recovering tampered or modified regions of the image after detecting tampering.

1.2 Objectives

This research is concerned with developing a digital watermarking algorithm to help in solving the problems of patient’s data size and authentication of patient's medical records for health applications. The main goal of this research is to investigate and develop suitable watermarking algorithms for medical image authentication and data hiding applications.

In order to achieve this goal, several objectives are identified, as follows:

1- To devise a reversible high-capacity watermarking scheme for medical images.

2- To devise a reversible high-capacity ROI-based watermarking scheme for medical images which can be used for data hiding, tamper detection and localization, and recovery.

3- To add robustness to the ROI-based scheme using a robust technique in frequency domain in order to obtain a hybrid scheme.

4- To conduct a comprehensive analysis on the feasibility, robustness, capacity, and performance of the algorithms developed.

5- To perform the watermarking algorithms on different medical image modalities; Magnetic Resonance (MR), Computerised Tomography (CT), Ultrasound (US), and Computed Radiography (CR).

1.3 Scope and Approach

This thesis mainly focuses on developing a proper medical image watermarking algorithm for data hiding, authentication, tamper detection, and recovery. The targeted algorithm must satisfy medical image watermarking requirements (Coatrieux *et al.*, 2000, Coatrieux and Lecornu, 2006). It should have the following properties and capabilities:

1- High embedding capacity: In order to facilitate hiding patient’s data and other side information necessary for authentication and tamper detecting and recovery.

2- Reversibility: In order to avoid misdiagnoses.

3- Tamper detecting and localisation: To detect and localise modified or tampered areas.

4- Recovery: In order to recover the original areas which have been modified by a malicious attack.

5- Robustness: In order to survive certain levels of some attacks.

6- ROI-based: In order to focus on the most important area in the image.

1.4 Methodology

In order to achieve the objectives of the thesis, several reversible watermarking schemes are investigated and combined leading to improved watermarking schemes. By using 16 different grayscale medical images of different modalities, the performances of the proposed schemes are evaluated in terms of the verification of the extracted watermark, hiding capacity, visual quality using peak signal to noise ratio (PSNR) and structural similarity index (SSIM).

The first step in this research is to investigate and review the available watermarking schemes for medical imaged which can be found in the literature. This intensive investigation will reveal the advantages and disadvantages of the existing watermarking techniques.

In order to achieve the first objective, the existing reversible watermarking techniques will be studied and reviewed in order to propose a suitable algorithm for data hiding applications in medical images.

The second objective of this research is concerned with adding authentication facility, besides data hiding ability, to the watermarking scheme. Hence, the watermarking algorithm, which is proposed to fulfill the first objective, will be modified in order to enhance its functionality by adding the tamper detection and recovery for the most important region in the image, i.e. the ROI.

To achieve the third objective, the ROI-based algorithm, which is proposed to fulfill the second objective, is modified by adding some level of robustness against certain types of attacks. This should be done without losing the reversibility of ROI.

For the fourth and fifth objectives, all of the proposed schemes will be tested on 16 DICOM images of different modalities; MR, CT, US, and CR. The performances of the proposed algorithms are evaluated for hiding capacity and visual quality. The hiding capacity measures the number of bits of the watermark compared to the number of pixels in the image, (bpp) bit per pixel. The visual quality is evaluated using (PSNR) peak signal to noise ratio, and (SSIM) structural Similarity Index. PSNR, which is commonly used to measure the visual quality of embedded images, and the SSIM index is a method for measuring the similarity between two images. SSIM is designed to improve on traditional methods like PSNR which have proved to be inconsistent with human eye perception (Wang *et al.*, 2004).

For the ROI-based watermarking algorithm, the same visual quality evaluation will be conducted on the same 16 test images with different ROI sizes. The size of ROI is defined as a percentage of the size of the image. The performance of the proposed algorithm is evaluated for hiding capacity, visual quality, and authentication capability.

The overall performance of the final proposed algorithm will be evaluated for hiding capacity, visual quality, authentication capability, and robustness. The robustness is tested against salt and pepper noise and cropping. To simulate transmission errors, salt and pepper noise of different densities was added to the watermarked images. Then, the signal to noise ratio (SNR) is computed for the noisy image. For each noisy image, the percentage of extracted data is calculated.

In order to test robustness of the algorithm towards cropping attack, both ROI and RONI of the watermarked images undergo cropping attack separately. The center of ROI is cropped, assuming that the region of the interest should be in the center, while random areas in RONI are cropped. The cropped areas are different in size and for each size; the percentages of the retrieved data form RONI and ROI are calculated.

1.5 Thesis Organisation

This thesis is organized in order to reflect the importance of digital medical image watermarking leading to realisation of the research objectives, as follows.

Chapter 1 presents a general introduction to research work, and the background and the motivation of this research are discussed. Also, the objectives, scope and approach are identified in this chapter.

Chapter 2 presents a literature review on the field of digital medical image watermarking, which are related to this thesis. This chapter covers the current and past researches that have been carried out and found in the literature.

Chapter 3 describes the development of the first and second proposed algorithms, which are completely reversible and based on difference expansion (DE) technique. For each algorithm, the processes of embedding and extracting are presented along with testing and evaluating results in terms of hiding capacity and visual quality for 16 DICOM images. Also, the results obtained for each algorithm are discussed.

Chapter 4 describes the third proposed algorithm which is a ROI-based reversible watermarking algorithm. The ROI concept is introduced with authentication and tamper detection and recovery capabilities. The embedding and extracting processes are presented along with testing and evaluating results in terms of hiding capacity, and visual quality for 16 DICOM images. Also, the results obtained are discussed in this chapter.

Chapter 5 describes the development of the fourth proposed algorithm which is a hybrid algorithm as it has a reversible part and a nonreversible part. The processes of embedding and extracting are presented along with simulation results in terms of hiding capacity, visual quality, and robustness for 16 DICOM images. Also, the results obtained are discussed in this chapter.

Chapter 6 concludes this research, and presents the contribution of this research. Some ideas for future work are also suggested.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

Most hospitals and health care systems involve a large amount of data storage and transmission such as administrative documents, patient information, medical images, and graphs. Among these data, the patient information and medical images need to be organized in an appropriate manner in order to facilitate using and retrieving such data and to avoid mishandling and loss of data (Nayak *et al.*, 2008).

On the other hand, the transmission of such a large amount of data when done separately using ordinary commercial information transmitting channels like the Internet, it results in excessive memory utilisation, an increase in transmission time and cost and also make that data accessible to unauthorised access (Anand and Niranjan, 1998).

In order to overcome the capacity problem and to reduce storage and transmission cost, data hiding techniques are used for concealing patient information with medical images. Those data hiding techniques can be also used for authentication and tamper detection to judge the images integrity and fidelity.

2.1 Data Hiding: Steganography and Watermarking

An important subdiscipline of data hiding is steganography, which can be defined as the process of encoding secret information by concealing every existence of the information (Lin and Delp, 1999a). Steganography is different from cryptography which is about protecting the contents of the message. Throughout the history, people have used many steganographic techniques like wax technique, shaved head, transparent ink, and microdots technique.

Another type of data hiding technique is *watermarking*. Digital watermarking can be defined as the process of embedding data into a multimedia object in such a manner that the embedded data can be detected or extracted later. The embedded data is usually called the watermark, while the multimedia object, in which the watermark is embedded, is usually called the host or the cover.

There are three fundamental differences between watermarking and steganography:

1. Watermarking, in comparison to steganography, has to be robust against possible attacks, and does not always need to be hidden as some systems use visible digital watermarks (Braudaway *et al.*, 1996).
2. The data embedded by the watermarking system is always associated to the digital multimedia object to be protected or its owner while in steganographic systems there is no relation between the data hidden and the host.
3. Steganographic communications are usually between one sender and one receiver while watermarking techniques are usually one-to-many (Petitcolas, 2000).

2.2 Watermarking: History and Terminology

Paper watermarks, which are a part of handmade papermaking, appeared nearly 700 years ago. The oldest watermarked paper found in archives dates back to 1292 and has its origin in the town which has played a major role in the evolution of the papermaking industry, Fabriano in Italy. At the end of the 13th century about 40 mills were sharing the paper market in Fabriano and producing paper with different format, quality, and price. After that invention, watermarks quickly spread in Italy and then over Europe and although initially used to indicate the paper brand or paper mill, they later served to indicate the paper quality, strength, and format (Kutter and Hartung, 2000).

Plain watermarking is strongly related to the invention of papermaking in China. It was intensively used in the 18th century in America and Europe as a trademark and a method against counterfeiting books and money (Cox *et al.*, 2001). The concept of watermarking has been expanded because of the fast progression in digitization of our world to include more applications such as authenticating ownership claims and protecting property interests. However, in principle digital watermarks are like their paper forefathers (Mohanty, 1999). The similarity between paper watermarks and digital watermarking is obvious: paper watermarks in bank notes or stamps inspired the first use of the term "water mark" in the context of digital data (Tirkel *et al.*, 1993).

Watermarking is relatively young research field, and over the past few years, watermarking has emerged as the leading candidate to solve problems for still images. In spite of the very active research and heavy industrial demand (Dugelay and Roche, 1999).

2.3 Fundamental of Digital Image Watermarking

Digital Image watermarking is the process of embedding small amount of data, called a watermark, into a digital image, using a secret key, in such a manner that the watermark can be detected or extracted later in order to make assertion about the image (identification, authentication, …, etc). From the previous definition, it is obvious that every watermarking technique consists at least of two different processes: watermark embedding process, and watermark detection and extraction process (Pérez-González and Hernández, 1999).

The process of embedding watermark can be illustrated by Figure 2.1. The original image is denoted by **I**, the watermark by **W**, the secret key by **K**. The embedding function, which is denoted by **E**, takes the image **I,** the watermark **W,** and a secret key **K** as inputs, and produces a new watermarked image $\mathbf{I_w}$. The process of embedding the watermark can by represented by the following equation:

$$\mathbf{I_w = E\ (I,W,K)} \qquad (2.1)$$

Depending on the watermarking technique, the original image can be either transformed into frequency domain or the embedding process can be done in spatial domain. If the frequency domain is used, the inverse transform must be applied in order to extract the watermark and obtain the watermarked image.

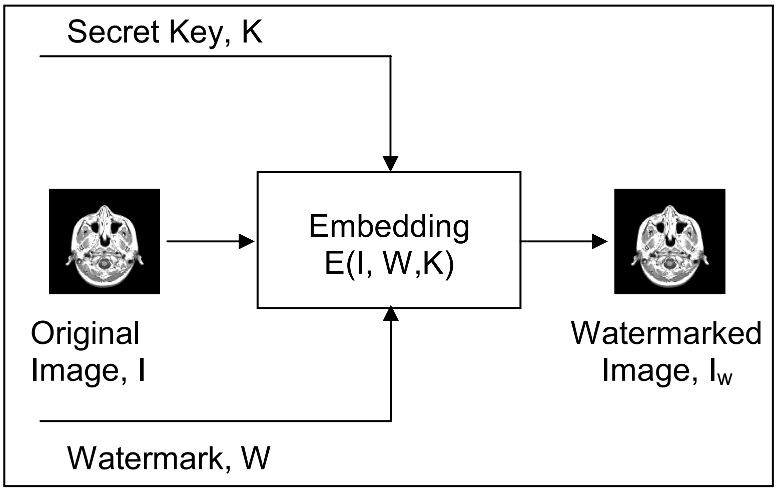

Figure 2.1: Watermark embedding process (Kutter and Petitcolasb, 1999)

The process of extracting or detecting is illustrated by Figure 2.2. The Detecting function, denoted by **D**, takes on its input the image $\mathbf{I_w}$ whose ownership is to be determined. In this procedure the same key **K** is used and the original Image **I** can also be included, depending on the watermarking algorithm. The process of extracting the watermark can by represented as follows:

$$\mathbf{W = D\ (I_w, I, K,)} \qquad (2.2)$$

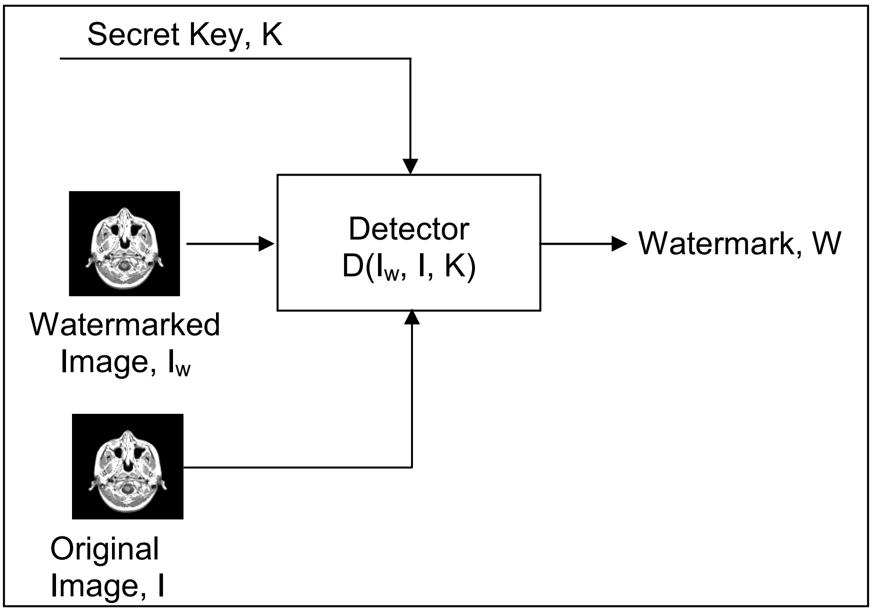

Figure 2.2: Watermark detecting process (Kutter and Petitcolasb, 1999)

2.4 Types of Digital Image Watermarking

Digital watermarking techniques can be classified into several categories depending on different parameters and criteria. The focus of this thesis is on digital images so, digital watermarking techniques can be classified as in Figure 2.3, which is a simplified classification of many classifications represented in previous literature (Kutter and Hartung, 2000, Jean-Luc Dugelay and Roche, 2000, Arnold *et al.*, 2004, Shi, 2005, Dai and Yeh, 2007).

2.4.1 According to Working Domain

As it can be noted, one of the criteria is working domain in which the watermarking is implemented. In *Spatial Domain* methods, the watermark information is embedded directly into images pixels. The images are generally manipulated by altering one or more of the bits of the byte that make up the pixels of the image (Schyndel *et al.*, 1994). In this technique, the least significant bit (LSB) is used to achieve embedding process.

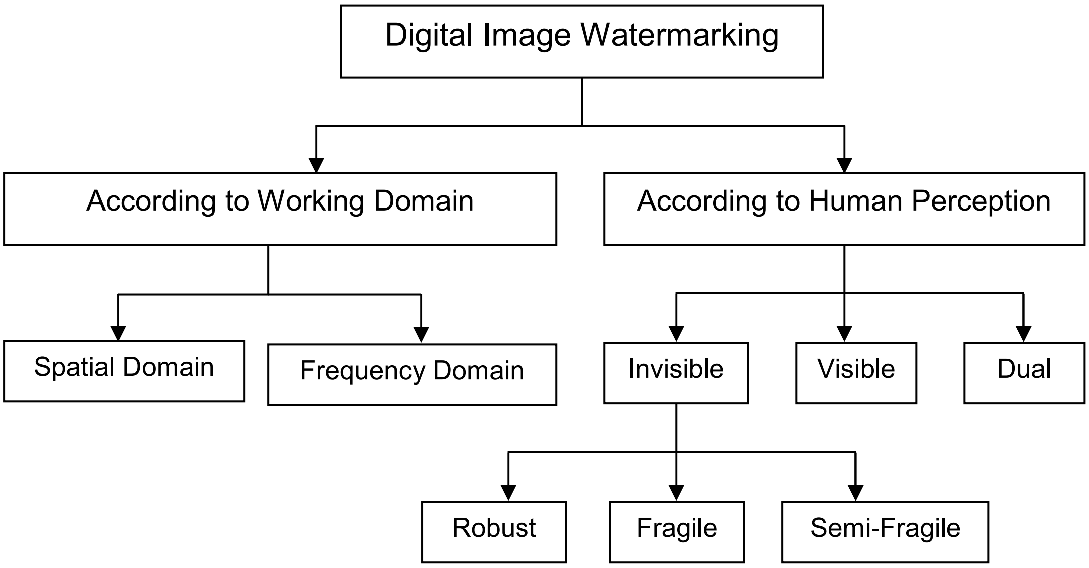
Digital Image Watermarking
According to Working Domain
According to Human Perception
Spatial Domain
Frequency Domain
Invisible
Visible
Dual
Robust
Fragile
Semi-Fragile

Figure 2.3: Types of digital image watermarking

In their Variable-Watermark Two-Dimensional (VW2D) technique, Wolfgang and Delp (1999) modified Schyndel's algorithm to enhance robustness. A bipolar *M*-sequence is added to the image as a watermark, where a correlation detector is used for watermark detection.

A different spatial domain watermarking technique which is based on statistical image processing is the patchwork. This technique is based on changing statistical distribution of luminance values in the set of pseudo-randomly selected pairs of image pixels to imperceptibly embed a single bit of information in a cover image (Bender *et al.*, 1996, Lee and Jung, 2001).

Another spatial domain watermarking proposed was proposed by Wong, which utilizes a hash function that is used to generate a digest. During embedding process, the cover image, image dimensions, and the watermarking key are hashed, and then used to modify the LSB of the cover image (Wong, 1999).

The advantages of using spatial domain for watermarking can be summarized as follows:

- Fragile
- Less image degradation
- Easy and fast in embedding and extracting

However, the embedded watermark in spatial domain can be easily removed or destroyed by simple attacks. Moreover, it cannot be extracted after simple communication noises (Kutter and Hartung, 2000).

In ***Frequency Domain*** methods, the watermark information is embedded in the transform domain. The general approach used in these methods is to map the image, or blocks of the image, into the transform domain using either Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT), or the Wavelet Transform. Then the watermark is embedded into the transformed image using some particular technique followed by an inverse transform to obtain the watermarked image (Boucherkha and Benmohamed, 2004).

The properties of a transform can be used to characterise how an image has been damaged or alerted. Also, applications may require a watermark to possess some robustness to certain types of modification such as brightness change (Lin and Delp, 1999a).

Many frequency domain methods have been proposed for digital image watermarking, and it is well known that transform domain watermarking schemes have better performance in comparison to spatial ones, since they reflect the properties of the human visual system (HVS) in order to achieve an optimal trade-off between robustness and visual quality (Unser and Aldroubi, 1996). Among the other frequency domain transforms, wavelet-based schemes particularly have gained great attention in recent years, because those schemes take advantage of the frequency information and spatial information of the transformed image in multiple resolutions which cannot be achieved by DCT or DFT (Kundur and Hatzinakos, 1999).

Using DWT, the embedding may be achieved by additive watermarking of a spread spectrum signal (Lu *et al.*, 2000, Kaewkamnerd and Rao, 2000), image fusion (Ganic and Eskicioglu, 2004), or quantization (Kundur and Hatzinakos, 1999, Lin and Delp, 1999a, Zhao *et al.*, 2004). In additive watermarking algorithms, the watermark data is a sequence of numbers (usually pseudorandom Gaussian sequence) w of length L, which is embedded, in the selected subset of the signal coefficients f. The general embedding formula has the following form:

$$f' = f + a \cdot f \cdot w(k), \quad k = 1,....,L \qquad (2.3)$$

where a is the embedding strength and f' is the modified coefficients of the host data. The watermark detection procedure is usually based on correlation. In watermarking algorithms based on image fusion, the logo image is used as a watermark instead of a pseudorandom sequence. On the other hand, quantization schemes perform nonlinear modifications and detect the embedded message by quantizing the received samples to map them to the nearest reconstruction points. In other words, the coefficients are modified according to the bit of watermark.

2.4.2 According to Human Perception

According to human perception, digital image watermarks can be classified into three different categories, as follows:

1. **Visible** watermarks are ones which are embedded in an image in such a way that they are visible when the image is viewed.
2. **Invisible** watermarks are imperceptible and they cannot be detected by just viewing the digital image.
3. **Dual** watermark is a combination of the visible and the invisible watermarks. In this type of watermarks, an invisible watermark is used as a back up for the visible watermark (Mohanty *et al.*, 1999).

According to robustness of the digital watermark, invisible watermarks can also be classified into three different categories, as follows:

1. **Robust** watermarking is a technique in which watermark should withstand the standard modifications and signaling operations that usually known as attacks, and it can be recovered with suitable decoding operation only.
2. **Fragile** watermarking is a technique in which watermark gets destroyed when watermarked image is modified or tampered with.

3. **Semi-Fragile** watermarking is not robust as much as robust watermarking technique but has the same property of tamper and modification detection that fragile watermarks have.

2.5 Properties of Digital Image Watermarking

The characteristics of watermarking have been discussed repeatedly through the literature (Mintzer *et al.*, 1997, Yang and Huang, 2004, Lin and Delp, 1999a, Kutter and Petitcolasb, 1999). The main properties reviewed are: robustness, visual quality (perceptual transparency), payload (hiding capacity), security, and complexity.

2.5.1 Robustness

Robustness refers to the ability of embedded data to remain intact if the watermarked image undergoes processing, such as sharpening or blurring, filtering, addition of random noise, scaling and rotations, lossy compression, cropping, and conversion from digital to analog form and then re-conversion back to digital form. The watermark must be difficult to remove. The attempt to destroy the watermark should result in the degradation of the perceptual quality of the host image so as to render it unusable.

2.5.2 Visual Quality (Perceptual Transparency)

A digital watermark should not be noticeable to the viewer. However, the act of embedding the watermark in the host image introduces some noise or distortion to the host image. It is important that the embedding process has no significant degradation to the visual quality of the host image.

2.5.3 Payload (Embedding Capacity)

Payload refers to the size of the information, the watermark, which can be concealed in the cover image. For copyright protection applications, the payload is usually low, while in data hiding application the payload is usually high.

2.5.4 Security

It refers to the capability of resisting intentional removing of the watermark by deletion, modification or buying of the watermark in another illicit one. Typically a secret key (embedded key) is used for embedding the watermark data in cover image. At the receiver side usually the same key is used for extracting or detecting the watermark. Another key maybe used for encrypting the watermark. That means that the watermark can be firstly encrypted using one encryption key then embedded using a different key.

2.5.5 Complexity

Computational complexity is defined as the number of operations (additions, divisions, multiplications, etc.) needed to embed and extract the watermark. Those operations depend on the type of the algorithms used and the domain of watermarking (frequency domain or spatial domain).

2.6 Applications of Digital Image Watermarking

According to the classifications and the properties of digital image watermarking, one can discover that digital watermarking techniques are developed based on the applications (Zheng *et al.*, 2007). Among others, the following applications of watermarking are more common:

2.6.1 Copyright Protection

It is one of the main applications of digital image watermarking. It is achieved by embedding information about the owner into the image to be protected in order to prevent parties from claiming to be the rightful owners of the image. Thus, it is required that the watermarks used for that purpose are supposed to be very robust against various attacks intended to remove the watermark.

2.6.2 Image Authentication

Authentication of an image can be achieved by detecting any change to or tampering with the image. Fragile and semi-fragile watermarks are used, which has low robustness to the modifications of the host image, are used for this purpose. Fragile watermarks are used to figure out how digital image was modified or which portion of it has been tampered with. This can be done by dividing an image into a number of blocks and creating and embedding a fragile watermark into each and every block (Muharemagic and Furht, 2004). Semi-fragile watermarking can also be used for quality measurement as the extracted watermark can give more information about the degradation of the host image, such as PSNR of the degraded host image. When the original reference is not available at the receiver side, it will be very useful to use watermarking in order to evaluate the quality of service (QoS) of the transmission or the overcrowding for broadcasting or network transmission (Zheng *et al.*, 2007).

2.6.3 Content Description and Data Hiding

The watermark may contain some descriptive information of the host image such as labeling and captioning or some data related to the image like reports in case of medical images. For this kind of application, the embedding capacity of the watermarking technique should be relatively large and there is usually no strict requirement for the robustness.

2.7 Medical Images

Among the wide spectrum of technologies in modern medicine, medical imaging is the most rapidly expanding technology. The ability to take pictures of the human body has many useful clinical applications. Different modalities of medical imaging have revealed over the years, each with their own advantages and disadvantages. For any patient who needs his or her body visualized, doctors select the most appropriate imaging technique (Lee, 2008). The first medical images started with X-rays, The next modality, ultrasonography, took sixty years to appear, and currently, 3D imaging of anatomical structures is possible with CT and MRI scans (Broyles, 2008).

An X-ray image is obtained by passing X-rays through the body and the image appears on photographic film. X-rays show dense body parts like bones as very white and less dense tissues as dark. Common uses of X-ray include determining whether or not a patient has broken bones (Murphy, 2005).

CT scans use the same technology as an X-ray but in a 3D way. Instead of the flat pictures in a standard X-ray, a CT scan offers several images. Those images give the radiologists the chance to view not just a frontal view of an organ but an inner, outer, and view within (Murphy, 2005).

In MRI or magnetic resonance imaging, a magnet is used to line hydrogen atoms in the human body in order to allow them to receive radio waves. The body sends back radio signals to the MRI machine which are converted into detailed a series of images of the body part (Murphy, 2005).

The Digital Imaging and Communications in Medicine (DICOM) is the most common standard in digital medical systems. The standard was created to be a vendor-independent standard in order to enable communication of diagnostic and therapeutic information, images and associated data of any kind. Connectivity, compatibility, and work-flow optimization are the main intentions (Mildenberger *et al.*, 2002). The DICOM standard has become the superior standard for the communication of medical images because it is widely available from different vendors and is rapidly expanding to include nonradiologic imaging (Horii, 1997).

The development of the DICOM standard is based on the cooperation of the American College of Radiology (ACR) with the National Electrical manufacturer Association (NEMA). In 1985, the joint committee of ACR-NEMA issued the version 1.0 of the standard. Further development was achieved resulting in version 2.0 and 3.0 in 1988 and 1993 respectively (Mildenberger *et al.*, 2002). A single DICOM file consists of two parts:

1. A header (which contains information about the patient's name, the type of scan, image dimensions, etc),
2. The image data (which can contain information in three dimensions).

This is different from the popular Analyze format, which stores the image data in one file with the extension (.img) and the header data in another file with extension (.hdr). Another difference between DICOM and Analyze is that the DICOM image data can be compressed (encapsulated) by means of lossy or lossless compression techniques to reduce the image size (Rorden, 2009).

2.8 Medical Image Watermarking

Medical images are stored for different purposes such as diagnostic, long time storage, and research (Raúl *et al.*, 2007). When a medical image is diagnosed by a doctor at distant site, it cannot be exposed to public by using unsecured channel to transmit it (Frommer, 2000). Moreover, any authorized person can access the images within a medical database and can modify those images maliciously. So, medical information database must be protected and secure.

Ethics and legislative rules control security of medical information, which gives rights to patient and duties to the health professionals (Coatrieux *et al.*, 2000). The assurance of image identity and integrity is the common data security concern in medical information systems. Image identity means that information represented by the image is for the correct patient and is from the correct source. These facts may be detailed elsewhere in the medical records associated with (but stored separately from) the image, but a possibility exists that wrong details may have been recorded. Image integrity means that information confirming no changes have been made to the original image as acquired by the medical imaging device, by a variety of manipulations which can occur during transfer or processing (Maeder and Planitz, 2005). To overcome those security issues, digital image watermarking techniques are proposed.

2.8.1 Requirements for Medical Image Watermarking

Medical images like any other type of images have some requirements such as perceptual transparency, payload (expressed in bit per pixel), security, and