THE USAGE OF WATERMARKING TO STORE PATIENT INFORMATION AND DIAGNOSIS IN MEDICAL IMAGES

RAZLINDA BINTI ABD RAZAK

THESIS SUBMITTED IN FULFILMENT OF THE DEGREE OF COMPUTER SCIENCE

FACULTY OF COMPUTER SYSTEM AND SOFTWARE ENGINEERING

2011

ABSTRACT

This thesis focuses on the implementation of medical image watermarking in DICOM. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. Watermarking methods applied to medical images embedding, an area known as a region of non interest (RONI) needs to be defined on the image to retain the original information. The watermarked image produced should have visual quality similar to its original version. Watermarked image algorithm will be embedding using least significant bit (LSB). LSB is used because of its simple technique. Watermark image consist of RONI where the LSB will embed and store the patient's information and diagnosis. The pixels that will use for embed patient information is 2x2 pixels each of 8 value bits. To embed patient's information and diagnosis, the text will convert into binary using ASCII code.

ABSTRAK

Tesis ini memberi tumpuan kepada pelaksanaan watermarking imej perubatan di DICOM. Digital watermarking adalah proses menerapkan maklumat menjadi isyarat digital dengan cara yang sukar untuk menghapuskan. Kaedah watermarking digunakan untuk menerapkan imej perubatan, kawasan yang dikenali sebagai kawasan bukan faedah (RONI) perlu ditakrifkan pada imej untuk mengekalkan maklumat yang asal. Imej tera air yang dihasilkan harus mempunyai kualiti visual yang sama dengan versi asal. Algoritma imej tera air akan diterapkan menggunakan bit penting kurangnya (LSB). LSB digunakan kerana teknik yang mudah. Imej watermark terdiri daripada RONI mana LSB akan membenamkan dan menyimpan maklumat pesakit dan diagnosis. Piksel yang akan digunakan untuk maklumat pesakit embed adalah piksel 2x2 setiap 8 bit nilai. Untuk menanamkan maklumat pesakit dan diagnosis, teks yang akan ditukar kepada binari menggunakan kod ASCII.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 DIGITAL WATERMARKING

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures, text or video, for example. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time.

Watermark can be divided into visible and invisible types. The information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden). The watermark may be intended for widespread use and is thus made easy to retrieve or it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or otherdescriptive information to the signal in a way that is difficult to remove. It is also possible to use hidden embedded information as a means of covert communication between individuals.

Watermark can be further categorized into fragile and semi-fragile types (Caldelli et al., 2010) which are suitable for the usage of content authentication. A fragile watermark can easily be destroyed and become undetectable after the watermarked image has been modified in anyway. If a fragile watermark is detected correctly, it can be assumed that the image had not been modified or tampered. A semi fragile watermark is destroyed by illegitimate modification but unaffected by legitimate distortion such as compression. It is normally used for selective authentication. Both fragile and semi-fragile watermark types may have localization capability.

Digital watermarking is the technology that embeds directly additional information by modifying imperceptible either the original data or some transformed version of them. It is divided into two basic categories: Spatial domain watermarking. Interchanges the lower order bits of the pixel values with the watermark or adds some fixed intensity value representing a visual watermark to the pixel values of an image. Frequency domain watermarking; Inserts the watermark into the coefficients of a transformed image, for example using the DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) that is difficult to detect .

1.2 MEDICAL IMAGE WATERMARKING AND MOTIVATION

The purpose of medical image security is to maintain privacy of the patient information in the image and to assure data integrity that prevents the image from tampering (Cao et al., 2003). Watermarking can be used in medical images to prevent unauthorized modification by authenticating the content of the image.

The medical image has been digitized by the development of computer science and digitization of the medical devices. There are needs for database service o f the medical image and long term storage because of the construction of PACS (Picture Archiving and Communication System) following DICOM (Digita1 Imaging Communications in Medicine) standards, telemedicine, and et al. Furthermore, authentication and copyright protection are required to protect the illegal distortion and reproduction of the medical information data.

Digital watermarking technique for medical image that prevents illegal forgery that can be caused after transmitting medical image data remotely. A wrong diagnosis may

be occurred if the watermark is embedded into the whole area of image. Therefore, the watermark embed into some area of medical image, except the decision area that makes a diagnosis so called region of interest (ROI) area, to increase invisibility. The watermark is the value of bit-plane in wavelet transform of the decision area for certification method of integrity verification. (Hyung et al., 2005)

1.3 DIGITAL IMAGING AND COMMUNICATION IN MEDICINE (DICOM)

Medical images can be stored in a DICOM (Digital Imaging and Communications in Medicine) compliant format. DICOM standard was developed in 1982 by American College of Radiology and National Electrical Manufacturers Association (NEMA) to aid the distribution and viewing of medical images, such as CT scan, MRI and ultrasound. Part 10 of the standard describes a file format for the distribution of images. This format is an extension of the older NEMA standard. Most people refer to image files which are compliant with Part 10 of the DICOM standard as DICOM format files. The objective of DICOM is to allow diagnostically accurate representation and processing of medical imaging data to a digital format. It is not simply an image format but a data transfer, storage and display protocol to cover all functional aspects of digital medical imaging.

A single DICOM file contains both a header which stores information about the patient's name, the type of scan, image dimensions, as well as all of the image data which can contain information in three dimensions. The standard of DICOM is a medical image format and communication interface. All the equipments that accord with DICOM format can connect with PACS and transport and exchange information with other equipments directly. The data of DICOM files acquired from standard digital medical image equipments have to be converted into general images or media images. (Rodriguez et al, 2001).

1.4 PROBLEM STATEMENTS

Digital watermarking is a technique of hiding specific identification data for copyright authentication. Most of the medical images are compressed by joint photographic experts group (JPEG) standard for storage. The watermarking is adapted here for interleaving patient information with medical images during JPEG

compression, to reduce storage and transmission overheads. The text data is encrypted before interleaving with images in the frequency domain to ensure greater security.

We can give the medical images to the patient directly or send to the patient and also can maintain as a soft and hard copy in the hospital for diagnosing and later in the future purpose. While sending or giving the data to the patient it has to check that whether the data belongs to particular patient or not and also provide the record of the patient. In this method some duplication will be performed and information will wrongly deliver in false acceptance of result. By using watermarking technique the memory needed to store the patient information is minimized.

In addition, it also can retrieve patient's information and diagnosis from the image if the file containing the info is missing from the patient's database. In addition, exposure to the database. Damage occurs and the patient information and diagnosis can be taken from the images.

References to the doctor. The doctor can make a referral to the patient. Patient information and diagnosis were used as evidence to the patient through a given image. Such information is a strong evidence to the patient, if relevant, the sickness or not.

1.5 RESEARCH AIM

The aim of this research is to store patient information and diagnosis watermarking for medical image.

1.6 RESEARCH OBJECTIVE

There are two research objectives:

i. To develop a watermarking algorithm to store patient's data and diagnosis on medical images.
ii. To test watermark scheme using selected modality.

1.7 THESIS ORGANIZATION

The thesis is divided into the following chapters:

Chapter 1: This chapter presents watermarking as an alternative method for store patient's information in medical images. DICOM format will be focus of the research.

Chapter 2: The previous works on watermarking is reviewed in this chapter. It covers on watermarking scheme and DICOM to store the medical images.

Chapter 3: This chapter proposes a watermarking to store patient information and diagnosis scheme for medical images.

Chapter 4: This chapter shows the experimental result and discussion

CHAPTER 2
LITERATURE REVIEW

2.1 INTRODUCTION

This chapter introduces watermarking in details as well as its previous works. It consists of section 2.2 describes the classification of watermarking by domain. Section 2.3 presents the requirements in image watermarking. Section 2.4 describes the applications watermarking. Section 2.5 explains the concept of region of interest. Section 2.6 introduces the concept of medical image watermarking. Section 2.7 describes the classification of watermark attacks. Lastly, Section 2.8 explains the DICOM standard and the storage information.

2.2 WATERMARKING TECHNIQUE

A wide range of modifications in different domains can be used as watermarking techniques include the spatial domains which embed the watermark by directly modifying the pixel values of the original image. The second class includes the transform domain methods, which embed the data by modulating the transform domain signal coefficients. The transform domain techniques have been found to have the greater robustness, when the watermarked signals are tested after having been subjected to common signal processing.(Zain, J.M. and Clarke, M., 2007)

2.2.1 Spatial Domain

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression (A. Khan and A.M. Mirza., 2007)

2.2.1.1 LSB (Least Significant Bit)

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component (Syed.,2007)

2.2.2 Transform Domain

The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform (DCT). The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image.

Most DCT based methods transform 8x8 sized block image into the transform coefficients with the same size. Most energy is concentrated on some coefficients including DCT coefficient. Discrete Wavelet Transform (DWT) based methods decompose an image into each sub band. Each band also keeps some information of spatial property. Therefore, the processing time of these methods can be fast by using the multi resolution characteristic, and a watermark can be inserted into certain sub bands. Discrete Fourier Transform (DFT) has the property of analyzing a signal into various sine waves.(Vidyasagar et al., 2005)

Techniques used needs a certain amount of computation but it can overcome possible compression and more robust against geometric transformation such as rotation, scaling, translation and cropping (Song et al., 2010)

2.3 REQUIREMENT OF IMAGE WATERMARKING

The major requirements of digital watermarking are:

2.3.1 Transparency

The digital watermark should not affect the quality of the original image after it is watermarked. (Cox et al., 2002) Define transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work". Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

2.3.2 Robustness

This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. (Cox et al., 2002) Defines robustness as the "ability to detect the watermark after common signal processing operations". Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks.

2.3.3 Capacity or Data Load

This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the watermarking during extraction. Watermark should be able to carry enough information to represent the uniqueness of the image. Different application has different payload requirements (Cox et al., 2002)

2.3.4 Computational Complexity

The watermarking scheme should not be computationally complex especially for applications where real-time embedding is desired. In a hospital environment for instance, where thousands of medical image are produced daily, watermarking process needs to be less time consuming so that the operation of the hospital is not affected. Reducing the number of computations also means lower cost for computer hardware. (SC Liew., 2011)

2.4 WATERMARKING APPLICATION

There are main applications of digital watermarking. They are copyright protection, broadcast monitoring, content archiving, tamper detection, metadata insertion and digital fingerprinting.

2.4.1 Copyright Protection

This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

2.4.2 Broadcast Monitoring

As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not. (Vidyasagar et al., 2005)

2.4.3 Content Archiving

Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a very fragile technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems. (Vidyasagar et al., 2005).

2.4.4 Tamper Detection

Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

2.4.5 Digital Fingerprinting

This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner. (Syed., 2006)

2.4.6 Metadata Insertion

Metadata refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records. (Vidyasagar et al., 2005)

2.5 CONCEPT OF REGION OF INTEREST (ROI)

Region of interest is an area of the image which is considered as important to the user. In medical images for instance, the ROI is the area which is used for diagnosis purposes. In the medical image watermarking, a ROI can be defined and often the watermark is being embedded in the region of non-interest (RONI) to maintain the originality of the ROI. In a situation where the ROI is used for watermark embedding, the process can be reversed by extracting the watermark and the original ROI information is restored.

2.6 MEDICAL IMAGE WATERMARKING

Medical image watermarking requires extreme care when embedding additional data the medical images because the additional information must not affect the image quality. Medical images are stored for different purposes such as diagnosis, long time storage and research. In the medical field the importance of the medical data security has been emphasized, especially with respect to the information referring to the patients (personal data, studies and diagnosis). On the one hand the amount of digital medical images transmitted over the internet has increased rapidly, on the other hand the necessity of fast and secure diagnosis is important in the medical field, i.e. telemedicine, making watermarking the answer to more secure image transmissions. For applications that work with images, the watermarking aim is to embed a visible or invisibly message in an image.

A well-known solution to protecting the copyright of images is digital watermarking. The traditional digital watermarking technique works by embedding an invisible digital watermark into another digital image. This watermarked can retrieve in order to prove that the ownership of this image is ours. After embedding, this watermark should be perceptually invisible. The watermark should be able to be retrieved after some image processing or compression. The algorithm of this technique should be able to be published to everyone and still hold the security. (C. I. Podilchuk and E. J. Delp., 2001)

The embedding procedure here is carried out by modifying the least significant bits (LSB) directly. The information of the watermark is embedded in the LSB of selected pixels. Embedding information into the frequency domain is more robust than into the spatial domain; however, the spatial domain can carry more embedded information than

the frequency domain. Unfortunately, most watermark embedding schemes, spatial and frequency domains alike, have the same drawbacks.

First, the watermark image is a binary image, which excludes it from the general situation. The watermark image must be meaningful and representative. Thus, the less restriction of the watermark image is, the better the scheme will be. Second, the watermark scheme reduces the image quality. If someone pirates this copyright image someday, watermark can be retrieve by the secret data from this suspect image. The major difference between this method and the traditional watermark techniques is that the quality of the cover image will not be reduced after processing. Therefore, no one can detect any abnormality because have never modified the cover image. (Chang et al., 2002)

2.7 CLASSIFICATION OF WATERMARK ATTACKS

Digital watermarking is not as secure as data encryption. Therefore, digital watermarking is not immune to hacker attacks. Voloshynovskiy et al. (2001) had classified watermark attacks into four categories as below.

2.7.1 Removal Attacks

The aim of removal attacks is to remove the watermark signal from the watermarked image without breaking the security of the watermarking algorithm. It does not attempt to find out the encryption techniques applied or how the watermark is being embedded. This category includes compression, noising, sharpening and histogram equalization. (SC Liew., 2011)

2.7.2 Geometry Attack

In geometry attack the watermark is distorted using spatial or temporal alteration of stego data. Included in this category are skewing, image rotation and translation.

2.7.3 Cryptographic Attack

The aim of this kind of attack is to break the security measures applied in the watermarking schemes. Once the security measure is broken, the embedded watermark is removed or a misleading watermark is embedded. Brute-force search is one of the techniques in this category. This technique attempts to break the security of the watermark by using a large number of known possible measures to find meaningful secret information.

2.7.4 Protocol Attack

The last category is the protocol attack. It is aim at attacking the entire concept of watermarking application such as in copyright protection. The attacker adds its own watermark into an image and causes the true ownership of the image in question.

2.8 DICOM

The American College of Radiology and the National Electrical Manufactures Association created a committee to develop a set of standards to serve as the common ground for various medical imaging equipment vendors. The set of standards will allow newly developed equipments to communicate and participate in sharing medical image information within the PACS environment. The standard is called DICOM or the current version known as DICOM 3.0, consist of 16 parts. Each DICOM document is identified by a title and standard number, which takes the form "PS 3.X-YYYY," where "X" is commonly called the part number and "YYYY" is the year of publication. For example, DICOM Part 1 has a title of "Introduction and Overview" and document number PS 3.1-1996. Watermarking is not currently in the standard. It only provides guidelines for the implementation of digital signature to ensure the integrity of medical images. (DICOM 1993)

A DICOM file contains a header and image data. The header stores information about the name of the patient, patient id, gender, study description date of birth, diagnosis, the name of the doctor and one or more images compressed or in raw format. Its aims are to support the distribution and viewing of medical images from CT, MRI, US and other medical modalities. The DICOM format is an extension of the older NEMA standard. These files cannot be viewed on a computer. In order to do that, the DICOM files must be processed the information must be extracted and eventually stored

in a database. So, the information can be viewed anytime, subjected to some processing or queries. This processing mainly refer to operations that may lead to the improvement of the image quality and clarity, rotations that allow viewing from several angles, providing help for the medical personnel. (Stanescu et al., 2005)

2.9 LITERATURE REVIEW

Hyung-Kyo et al [2] we use internet now days and all system are digital with technology. The medical image has been digitized by the development of computer science and digitization of the medical devices. There are needs for database service of the medical image and long term storage because of the construction of PACS (Picture Archiving and Communication System) following DICOM (Digita1 Imaging Communications in Medicine) standards, telemedicine, and et al. We also need, authentication and copyright protection are required to protect the illegal distortion and reproduction of the medical information data. In this paper, we use digital watermarking technique for medical image that prevents illegal forgery that can be caused after transmitting medical image data remotely with internet. A wrong diagnosis may be occurred if the watermark is embedded into the whole area of image. Therefore, we embed the watermark into some area of medical image, except the decision area that makes a diagnosis so called area of interest (AOI) area in our paper, to increase invisibility. The watermark is the value of bit-plane in wavelet transform of the decision area for certification method of integrity verification. The experimental results show that the watermark fused by the proposed algorithm can survive successfully in image processing operations such as JPEG lossy compression.

Tirkel et al were one of the first used techniques for image watermarking. Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modifications. The algorithm proposed by Kurah and McHughes to embed in the LSB and it was known as image downgrading.

Osamah and Khoo (2011) proposed a scheme that consists of two types of watermarks. For the first type of the watermark is embedded to the spatial domain. In additional, the second watermark is embedded in the transform domain. The image is first divided into 16 x 16 pixels blocks. The first watermark consists of patient's data

and the hash value of the ROI, is embedded into ROI itself by usage a modified difference expansion technique. The second watermark is compressed and embedded into the region of non-interest (RONI) by using DWT technique.

CHAPTER 3

METHODOLOGY

3.1 INTRODUCTION

This chapter is starts with section 3.2 where it describes the research methodology used in this chapter. Proposes the usage of store patient information and diagnosis watermarking scheme. The watermark consists of patient information and diagnosis is extracted from the DICOM image. Section 3.3 discusses about embedding patient information. Section 3.4 discusses about extraction the watermarked images and 3.5 discusses about the hardware and software that used.

3.2 RESEARCH METHODOLOGY

This research is about to store patient information and diagnosis into medical images using watermarking algorithm. Medical images that will be used in this research are ultrasound, X-ray, MRI and dental images.

The most direct technique is by embedding a watermark within the spatial domain had been used by Jasni and Abdul (2006) and Yang and Shen (2010). There is no mathematical calculation needed and this reduces the computation. The watermark is embedded directly into the LSBs of the image pixels. One bit of information can be embedded into the LSB of a pixel. For example if the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. The watermark is

usually embedded in the RONI where most pixel values are zero. The embedded watermark can be retrieved and the LSB of the RONI is reset to zero. The second advantage of this method is the embedding capacity where it has a theoretical 1 bits per pixel as compare to only 0.5 bits per pixel in the difference expansion by Tian (2003) method.

Based on LSB technique, I propose a watermarking algorithm. So, no one will expect that the hidden watermark text is there. Figure 3.1 and 3.2 shows the process of the proposed method. First, I select the image which is a grayscale image and select text file containing patient id, date, gender and diagnosis in notepad then, I embed the watermark in the image embedding algorithm. Before embed the patient information, I need to convert to binary value using ASCII code. Then, I will get the watermarked image. Then, the receiver will retrieve the watermark back. The watermark will be extracted from the watermarked image**.**