DIGITAL IMAGE WATERMARKING USING REDUNDANT WAVELET TRANSFORM FOR COPYRIGHT PROTECTION

by

LIM SAY YARN

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

February 2007

ACKNOWLEDGEMENTS

Special acknowledgement is given to my supervisor, Dr. Khoo Bee Ee for her invaluable guidance, support, patient, constructive criticisms and comments as well as fruitful discussions, without it I would not have succeeded in carrying out this research. In addition, I am proud to be associated with her in the research.

I am grateful to my loving family, who has given me their unfailing support, encouragement, love and understanding throughout the years. I must also thank to my colleagues in School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Mr. William Koay Fong Thai, Mr. Ng Theam Foo, Mrs. Kho Hiaw San and Ms. Wang Shir Li, who provided the wisdom, encouragement, help and motivation in the research. Special thanks to Mr. Foon Dah Way, and Mr. Lee Seng Soon from School of Computer Sciences, Universiti Sains Malaysia for their time and guidance, which inspire me in working my dissertation.

Last but not least, I would like to express sincere thanks to the School of Electrical and Electronic Engineering, Universiti Sains Malaysia for providing the necessary facilities for this research. In addition, the provision of financial assistance (Skim Biasiswa Khas) from Institute of Post-Graduate Studies, Universiti Sains Malaysia, was crucial in getting the thesis done.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PUBLICATIONS & SEMINARS

1 Multi-Layer Multiple-Key Digital Image Watermarking Scheme

Lim Say Yarn, Khoo Bee Ee
School of Electrical and Electronic Engineering
Universiti Sains Malaysia, Engineering Campus
Pulau Pinang, Malaysia.

Proceeding of 2nd National Conference on Computer Graphics and Multimedia. Selangor, 2004, pp. 251 - 255.

2 A Logo-Based Watermarking Scheme Based On Stationary Wavelet Transform

Lim Say Yarn, Khoo Bee Ee
School of Electrical and Electronic Engineering
Universiti Sains Malaysia, Engineering Campus
Pulau Pinang, Malaysia.

Proceeding of the International Conference on Robotics, Vision, Information and Signal Processing ROVISP 2005
pp. 613 – 617.

TEKNIK TERA AIR BERASASKAN JELMAAN WAVELET BERLEBIHAN UNTUK PERLINDUNGAN HAK CIPTA GAMBAR DIGITAL

ABSTRAK

Pada masa kini, pengurusan hak cipta gambar digital menarik perhatian para penyelidik dari seluruh dunia. Salah satu kaedah untuk melindungi hak cipta gambar digital ialah dengan menggunakan teknik tera air. Teknik tera air membenam maklumat hak cipta digital ke dalam gambar digital supaya maklumat ini tidak boleh dilihat oleh manusia. Maklumat hak cipta yang terbenam ini boleh dikeluarkan semula untuk pemeriksaan dan menyelesaikan masalah hak cipta sesuatu gambar digital. Satu teknik tera air baru yang berasaskan jelmaan wavelet berlebihan (Redundant Wavelet Transform) telah diperkenalkan. Jelmaan wavelet berlebihan ini digunakan dalam proses membenam tera air kerana ciri-cirinya yang boleh mengekalkan bilangan pekali yang sama dengan saiz gambar digital asal dalam proses jelmaan. Ini menambahkan muatan tera air yang boleh dibenam ke dalam satu gambar. Selain itu, seperti yang diketahui umum, maklumat tera air yang terbenam dalam domain frekuensi adalah lebih tegap ke atas serangan. Tera air yang merupakan logo digunakan dalam skim tera air baru ini memudahkan proses pengenalpastian. Tera air yang terbenam adalah berdasarkan pengubahsuaian satu blok pekali jelmaan wavelet berlebihan. Skim tera air yang berasaskan jelmaan wavelet berlebihan ini boleh digunakan pada gambar-gambar berwarna kelabu dan juga gambar-gambar berwarna. Ciri-ciri teknik tera air seperti kualiti persepsi gambar dan ketegapan pada gambar yang mengandungi tera air telah dikaji. Selain itu, satu alat tanda aras, StirMark, juga digunakan untuk mengkaji keberkesanan skim tera air baru ini. Keputusan ujikaji menunjukkan bahawa skim tera air ini dapat menghasilkan gambar-gambar yang mengandungi tera air yang berkualiti percepsi baik dan gambar-gambar ini tegap ke atas serangan proses-proses gambar umum.

DIGITAL IMAGE WATERMARKING USING REDUNDANT WAVELET TRANSFORM FOR COPYRIGHT PROTECTION

ABSTRACT

The concern of the digital image copyright management raised the research interest all over the world recently. One of the methods to protect our copyright of digital image is using the watermarking technique. Watermarking technique hides digital copyright information into the digital images imperceptibly. This digital copyright information can be extracted for the verification purpose when a copyright issue was in question. A new redundant wavelet transform based digital image watermarking scheme was introduced. Redundant wavelet transform is used in the watermark embedding process because of its property that the size of coefficients remains the same as the original image after decomposition process. This increases the capacity of the watermarks that can be embedded into one image. Besides that, as commonly known, watermark information which is embedded in frequency domain is more robust to attacks. Logo-based watermark is used in the watermarking scheme so that it can easily be identified during the verification process. The watermarks are embedded by adaptively modifying a block of redundant wavelet transform coefficients. This redundant wavelet transform watermarking scheme can be used on gray scale images and color images. The properties of the watermarking scheme such as the perceptual quality of the watermarked images and robustness were tested. Besides that, a benchmark tool, StirMark, is applied to watermarked images to evaluate the performance of the watermarking scheme. The experimental result showed that the watermarking scheme produced a good perceptual quality of the watermarked image and possessed its robustness to some common image processing attacks.

CHAPTER ONE
INTRODUCTION

1.0 Background

Nowadays, most of the images are saved in digital format. Digital images can be captured easily with scanners, digital cameras, or camcorders. The advantages of saving images in the digital format include ease in creation, modification, and distribution. The rapid usage of the digital images through the Internet introduces a new set of challenging problems regarding security and illegal distribution. Digital images, which are uploaded to the Internet, are easily copied, modified, and distributed again without the permission of the owner. These illegal actions become more serious by the proliferation of high-capacity digital recording devices (Cox et al, 2002). In other words, the issue of copyright protection becomes more significant. The possibility of unlimited copying of digital images without any loss of quality may cause the image producers and content providers a considerable financial loss (Hartung and Kutter, 1999). Therefore, a technique that can protect the rights of the digital images owner is urgently needed.

One possible solution is to embed some invisible information into the digital images before the images are distributed. This embedded information can be extracted out for different purposes. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work (Cox et al, 2002). Some of the watermarks are visible while most watermarks of interest are invisible. Digital watermarking technique can be used in a wide variety of applications, such as digital media copyright protection, copy control, content authentication and broadcast monitoring (Nikolaidis and Pitas, 1996), (Bloom et al, 1999), (Yu et al, 2004), (Wang and Pearmain, 2006).

Digital images are commonly shared through the Internet, as the Internet is the most important source of information, and offers world-wide channels to deliver and to exchange the information. One of the common image formats is JPEG because it offers high compression while retaining high image quality. Associated with the widespread circulation of digital images are issues of copyright infringement and privacy. Identifies the owner of the digital images, even the digital image is distorted, is a challenging problem for researchers. The development of digital watermarking for copyright protection provides a possible solution to this problem.

1.1 Motivation

Digital image watermarking for copyright protection is a process of insertion of invisible copyright owner information (watermark) into digital images before the images are distributed. The watermark is hidden imperceptibly in the original digital images while the quality of the watermarked images is maintained. This watermark can be extracted for verification when a copyright issue is in question.

For copyright protection, a watermarking scheme should produce a good visual quality watermarked image, in which the embedded watermark should introduce small distortions on the original image. A robust watermarked image that can resist common signal processing attacks due to digital images transmission or distribution process is also required.

Besides visual quality of image after watermark insertion and watermarked image robustness issue, the traditional watermarking scheme, also known as the symmetric watermarking scheme (Cox et al, 2002), requires a complete disclosure of the watermarking key in the watermark verification process. The disclosure of the watermarking key enables the attacker to completely remove the watermark once the

key is known. Thus, the embedded watermark no longer protects the copyright of the owner of the image (Craver and Katzenbeisser, 2001).

One alternative to solve this traditional watermarking problem is to embed more watermarks into the image and generate different watermarking keys for watermark verification (Kim et al, 2004). Although one of the watermarking keys will remove the embedded watermark by the attacker, other embedded watermarks are able to protect the image's copyright if their watermarking keys remain secret.

Embedding more watermarks into one image requires a high capacity embedding mechanism. The advantages of Redundant Discrete Wavelet Transform (RDWT) make this high capacity watermark embedding scheme possible. Besides, a study by Meerwald and Uhl (Meerwald and Uhl, 2001) shows that the frequency domain watermarking scheme maintains the visual quality and robustness of the watermarked image (Corvi and Nicchiotti, 1997), (Inoue et al, 1998), (Xia et al, 1998), (Lumini and Maio, 2000), (Vehel and Manoury, 2000),.

1.2 Objectives

This dissertation is concerned with the implementation of digital watermarking techniques to overcome the digital images copyright protection issue. The main aim of this research is to develop a robust and high capacity digital watermarking technique for copyright protection using Redundant Discrete Wavelet Transform. To achieve this aim, several objectives are identified, as follows:

1. to devise a robust and high capacity watermarking scheme using Redundant Discrete Wavelet Transform.
2. to conduct a comprehensive analysis on the feasibility, robustness, and performance of the watermarking scheme.

3. to perform simulations of the watermarking scheme on grayscale images as well as different kinds of color model images.
4. to evaluate the integrity of the watermarking scheme by using standard benchmark test.

1.3 Scope and Approach

This dissertation mainly focuses on developing the copyright protection digital watermarking scheme. Although digital watermarking can be applied to many digital media, such as text, audio, video and 3D graphic, the proposed digital watermarking scheme is used only for digital images.

The development of the digital image watermarking is focused on the frequency domain watermarking scheme. Properties such as perceptibility and robustness are the main concern in which they are the main requirements of a copyright protection watermarking scheme (Cox et al, 2002). Common digital image processing operations that can lead to failure of watermark extraction are identified, tested, and evaluated.

In order to achieve the objectives of the dissertation, several tasks have been identified and carried out. To develop a high robustness watermarking scheme, wavelet transform is used during the watermark embedding and extracting process. To achieve a high capacity of the embedded watermark, Redundant Discrete Wavelet Transform is chosen to transform the original images into wavelet coefficients, where more watermarks can be embedded. To test the robustness of the proposed watermarking scheme, several signal/image processing operations are applied to the watermarked images, and the effectiveness of the scheme depends on the verification of extracted watermarks. To examine the applicability of the proposed watermarking

scheme, different types of grayscale images as well as color images are tested. To verify the overall performance of the proposed scheme, a benchmarking test, StirMark, is carried out.

1.4 Dissertation Organization

This dissertation is organized in such a way that it systematically leads to realization of the research objectives, as follows.

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

Chapter 2 presents a literature review on the field of digital watermarking that are related to this research. This covers the current and past researches that have been carried out worldwide.

Chapter 3 describes the development of the proposed algorithm, which is an imperceptible, robust, and high capacity copyright protection watermarking scheme. The watermarking scheme covers the pre-processing of watermark, the watermark embedding process, and the watermark extraction process. Tools for the performance evaluation are also identified as well as the benchmarking tool, StirMark.

Chapter 4 presents the simulations of the proposed watermarking scheme on grayscale images. Performance of the scheme is evaluated according to the requirement of watermarking properties. A comparison between the proposed watermarking scheme and two other watermarking schemes is presented. The benchmark test of the proposed watermarking scheme is also carried out.

Chapter 5 discusses the implementation of the proposed watermarking scheme in real applications using color images. Several color models are introduced, and the performance of the watermarking scheme is tested and examined.

Chapter 6 concludes this project, and presents the contributions of this research. Some suggestions for future research are also suggested.

CHAPTER TWO
LITERATURE REVIEW

2.0 Introduction

Information exchange through the Internet happens anytime and anywhere. Thus, copyright enforcement and data authentication become a very difficult task. Various techniques have been developed to protect the Intellectual Property Rights (IPR) in open network environments. Normally network security issues are handled through cryptography. Cryptography is a technique based on a secret key to encipher or to conceal the information. Only someone who has access to the key is capable of deciphering the encrypted information (Van Der Lubbe, 1998). However, cryptography technique does not protect against unauthorized copying after the information has been successfully transmitted (Piva et al, 2002).

Besides cryptography, steganography and watermarking are used to protect the digital media content. Both techniques often share similar principles and basic ideas but distinguish mainly in terms of robustness against attacks (Hartung and Kutter, 1999). A definition for cryptography, steganography and watermarking are given in Cox et al. (2002), as follows:

- Cryptography – The study and practices of securing messages.
- Steganography – The art of concealed communication by hiding messages in apparent innocuous objects, such as images. The existence of a steganographic message is secret.
- Watermarking – The practice of altering a Work by embedding a message about that Work. Work refers to a song, video, picture or media content which can have watermarks embedded in it.

In general, watermarking techniques can be applied to broadcast monitoring, owner identification, proof of ownership, authentication, transactional watermarks, copy control and covert communication (Cox et al, 2000). Major applications of digital watermarking are copyright protection and authentication. The definition of the watermarking property may vary from application to application. For instance, watermark in the copyright protection is the copyright statement whereas it is the proof of the originality for the authentication.

Digital watermarking schemes are introduced in the early 1990's (Katzenbeisser, 2003). However, watermarking attracts the interest of researchers during the last few years owing to the awareness of the digital media copyright management and the wide usage of digital watermarking techniques. Thus, many kinds of watermarking schemes are proposed. Watermarking technique is initially used to counteract copyright infringements but now it is used in various applications such as copy protection and labeling of digital goods.

2.1 History of Digital Watermarking

Secret communication has begun since ancient time, and it is as old as communication itself. There are several ways to communicate secretly in the past. Paper watermarks were one of the methods. The art of papermaking was invented in China over a thousand years ago. In a study by Cox et al (2002), paper watermarks did not appear in Italy until about 1282. These paper watermarks were used to differentiate the paper makers. The marks were made by adding thin wire patterns to the paper molds. The oldest watermarked paper is found in archive dates back to year 1292 and has its origin in Fabriano, Italy, which is the birthplace of watermarks (Hartung and Kutter, 1999).

The first 'copyright' law, 'Statute of Anne' was introduced by the English Parliament in 1710. However, nearly hundred years before this 'copyright' law, Claude Lorrain already introduced a method for protecting his intellectual property (Hartung and Kutter, 1999). Besides, there is a case in 1887 in France called "Des Decorations" clearly illustrating the legal power of watermarks (Hartung and Kutter, 1999).

However, it is hard to determine the exact period of watermark in digital format is first discussed. In Cox's survey (Cox et al, 2002), several cases related to watermarking were identified, such as in 1979, W. Szepanski described a machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes and in 1988, L. Holt, B. G. Maufe and A. Wiener described a method for embedding an identification code into an audio signal. From the survey, the term 'digital watermark' was appearing to have first used by N. Komatsu and H. Tominaga in 1988 (Cox et al, 2002).

The idea of digital watermarking arose independently in 1990s. The first international workshop which included digital watermarking as one of its primary topics, Information Hiding Workshop was held in 1996 (IHW, 2005). Currently most of the local or international conferences on Signal Processing field include digital watermarking as their topic.

2.2 Fundamental of Digital Watermarking

In general, digital watermarking is a technique to hide information by embedding it into the work (Cox et al, 2002). The hidden or conveyed information can be extracted at anytime by users. The work may be a multimedia object from audio, video, image and 3D graphic. A simplest watermark would be the bar code placed on an image to label the image. However, the watermark, depending on applications and

requirements, might contain additional information including the copyright and the identification of the purchaser of that particular copy of material.

Watermark is unique for every owner and different watermarks can be embedded into different objects. The embedding algorithm incorporates the watermark into the work whereas the watermark extraction algorithm is used to extract the watermark and authenticate or verify the work in order to determine both the owner and the integrity of the work.

The basic of digital image watermarking scheme involves three processes. The first process is to generate the watermark which carried the copyright information. Second process is to embed the watermark into the original host image. The last part is the extraction and verification process when a correct security key is used. Figure 2.1 and Figure 2.2 show the generic digital image watermarking embedding and extraction scheme respectively.

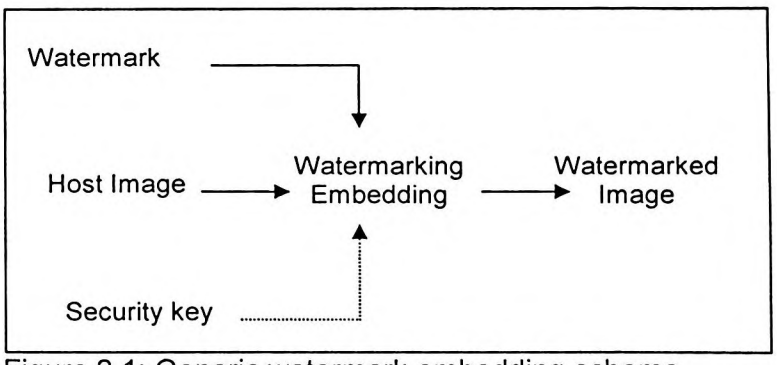

Figure 2.1: Generic watermark embedding scheme.

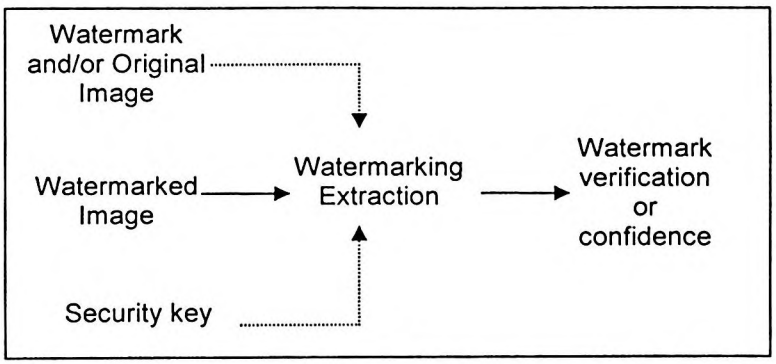

Figure 2.2: Generic watermark extraction scheme.

2.2.1 Watermark Generation

This process designs the watermark signal W to be added to the host image. Typically, the watermark signal depends on a key K and watermark information I (Hartung and Kutter, 1999), (Cox et al, 2002), (Barni et al, 2003).

$$W = f_0(I,K) \tag{2.1}$$

It may also depend on the host image X which it is embedded into.

$$W = f_0(I,K,X) \tag{2.2}$$

2.2.2 Watermark Embedding

An embedding method is designed to hide the watermark signal W into the host image X yielding watermarked image Y (Hartung and Kutter, 1999). The generic scheme is shown in Figure 2.1.

$$Y = f_1(X,W) \tag{2.3}$$

2.2.3 Watermark Extraction

In this process, the corresponding extraction method is designed to recover the watermark information I from the watermarked image by using the correct key together with the original host image

$$I' = g(X,Y,K) \tag{2.4}$$

or without the original host image (Hartung and Kutter, 1999). The generic scheme is shown in Figure 2.2.

$$I' = g(Y,K) \tag{2.5}$$

2.3 Classification of Digital Watermarking

There are many classifications of watermarking techniques in terms of their application areas, working domain, and perceptions. In the content of security issue, some watermarking researchers classified watermarking scheme into symmetric watermarking scheme and asymmetric watermarking scheme (Eggers et al, 2000).

Symmetric watermarking scheme is a scheme that the watermarking keys for watermark embedding and extraction must be identical (Eggers et al, 2000). Most of the proposed watermarking scheme, such as Cox's secure spread spectrum watermarking scheme (Cox et al, 1997) is a symmetric watermarking scheme. Asymmetric watermarking scheme adopts the concept of public-key cryptography (Arto Salomaa, 1996) with the intention to overcome the weakness of symmetric watermarking scheme. In asymmetric watermarking scheme, a key is used to embed the watermark (called a private key) but a different key (called a public key) is used to extract and verify the watermark. This public key consists of information to successfully prove the presence of a watermark only but the key cannot be used to make any attacks possible (Craver and Katzenbeisser, 2001).

Besides classifying the watermarking technique into symmetric or asymmetric, Saraju P. Mohanty has also divided the watermark and watermarking technique into various categories in various ways (Mohanty, 1999), as shown in Figure 2.3.

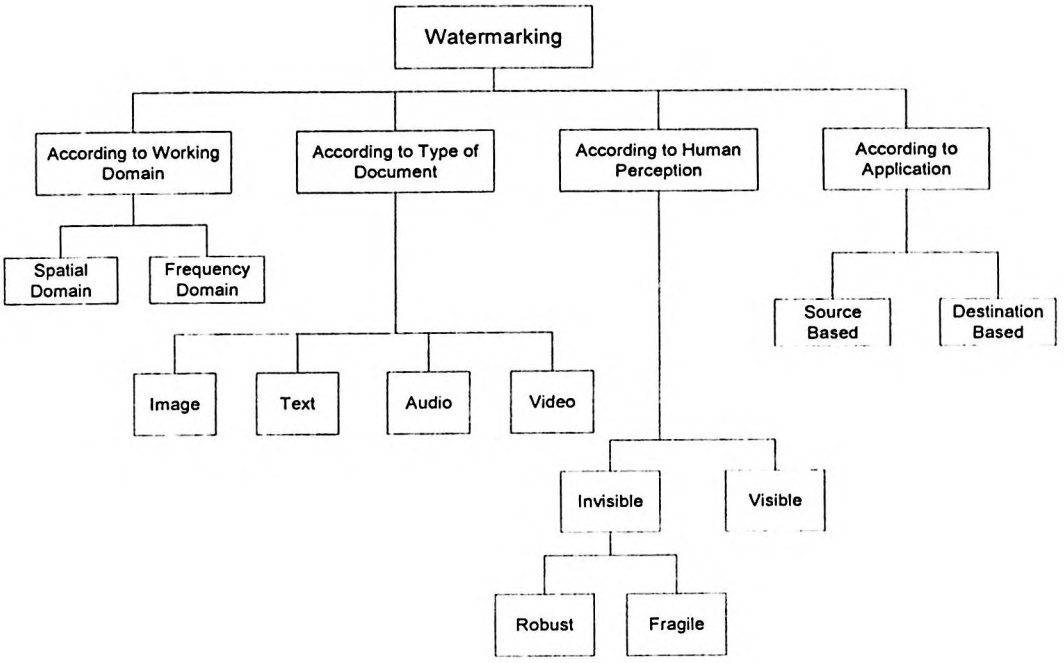

Figure 2.3: Classification of digital watermarking (Mohanty, 1999).

Watermarking scheme can be divided into four sub-categories by the type of work/document that watermark is embedded into.

- Text watermarking – The way to hide a watermark into a text content is to insert the watermark in the font shape and the space between characters and the line spaces (Kim et al, 2003), (Micic, et al., 2005).
- Image watermarking – There has been many researchers for image watermarking so far. The intensity value of an image is used to hide the watermark. Watermark embedding and extraction widely utilizes the characteristics of human visual system (HVS) (Kutter and Petitcolas, 1999).
- Video watermarking – Watermark hidden in the video can be used as an invisible label for copyright protection, or as auxiliary information for video segmentation, retrieval, annotation, indexing and error concealment. This watermarking technique is similar to image

watermarking but requires real time extraction and robustness for compression (Wang and Pearmain, 2006), (Lin and Delp, 2004).

- Audio watermarking – This technique hides pre-specified data and carries some information into the audio stream such that it is not audible to the human ear. The application of this technique becomes an important issue because of the Internet music. However the robustness and inaudibility are the major concerns (Lemma et al, 2003), (Tefas et al, 2005).

According to human perception, digital watermarking can be classified into visible and invisible watermarking. Visible watermarking directly confirms the existence of watermark. The watermark is visible to casual viewers. However, visible watermarking will degrade the quality of original content and the watermark is exposed to attacks. In contrast to visible watermarking, invisible watermarking hides a perceptually invisible watermark in the work. Invisible-robust watermark can resist any kind of alterations and the watermark can only be recovered with appropriate mechanism. Invisible-fragile watermark refers to a watermark that is easily destroyed after any manipulation process on watermarked data. This watermarking method mainly used in authentication and covert communication (Kirovski and Malvar, 2001).

Watermark can also be classified according to its applications as follows (Mohanty, 1999):

- Source based – Watermark is used as a proof of ownership or originality. The watermark is unique to identify the owner and to determine whether the watermarked data has been tampered with.
- Destination based – Every distributed watermarked data has a unique watermark and it identifies the particular holder.

On the other hand, digital watermarking can be classified by working domain into two sub-categories: spatial domain and frequency domain. In spatial domain, the original work is directly used for watermark embedding without performing any transformation process. Lee and Jung (Lee and Jung, 2001) had proposed to use least significant bit (LSB) and patchwork methods in this spatial domain. In frequency domain, the original work is first transformed into frequency coefficients using Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT) or wavelet transform. The watermark is then distributed to the transformation coefficients. The inverse-transformation of watermarked coefficients forms the watermarked data. Mohanty (Mohanty, 1999) had pointed out that the frequency domain watermarking scheme is more robust than spatial domain watermarking scheme.

2.3.1 Spatial Domain Digital Image Watermarking

Early work on digital watermarking for still images is focused on hidden information in spatial domain. For example, modification of Least Significant Bit (LSB) of image intensity value is the popular technique to hide the watermark information (Van Schyndel et al, 1994). Chang-Hsing Lee and Yeuan-Kuen Lee (Lee and Lee, 1999) proposed an adaptive digital image watermarking technique by adaptively modified the image intensity value according to watermark information. Besides that, watermark also can be embedded by using patchwork method where a pair of image intensity value is chosen randomly and their brightness is increased or decreased depending on watermark information (Lee and Jung, 2001). However, the embedded watermark in spatial domain can be removed easily by simple attacks. On the other hand, the watermark is failed to be detected after the additional of the noise (Wolfgang et al, 1999), (Cox et al, 1997).

2.3.2 Frequency Domain Digital Image Watermarking

In order to solve the weakness of the spatial domain watermarking scheme and increase its robustness, the frequency domain watermarking scheme is proposed. A well-known frequency domain watermarking technique is proposed by Cox et al (1997). They prepared a set of sequences which is independent and identically distributed. These sequences are embedded into perceptually significant spectral component of the Discrete Cosine Transform (DCT) coefficients of an image. The watermark embedding method is derived from spread spectrum in communication application. Another DCT based watermarking scheme is proposed by Piva et al (1997). Their watermarking scheme transforms the original image into frequency coefficients using blocked DCT transform and the watermark is then inserted in the middle band. Both DCT based watermarking schemes shows better robustness against common image processing attacks as compared to spatial domain watermarking method.

As a result of better efficiency of compression and good quality of output images for JPEG 2000 compression, Discrete Wavelet Transform (DWT) based watermarking scheme draws a lot of researchers' interest (Fotopoulos and Skodras, 2002), (Suhail and Obaidat, 2001).

2.3.2.1 Wavelet Transform Based Watermarking Scheme

Wavelet is a 'small wave' which has its energy concentrated in time (Stephane Mallat, 1999). It is a useful tool for the analysis of transient, nonstationary or time-varying phenomena. Wavelet has the oscillating wave-like characteristic and also has the ability to allow simultaneous time and frequency analysis with a flexible mathematical foundation (Burrus et al, 1998), (Stollnitz et al, 1996). Nowadays, wavelet transform is commonly used for feature extraction in image processing (Ji and Quan, 2005), (Xing Wang, 2006), (Zhang et al, 2005) and as well as watermarking field

(Meerwald and Uhl, 2001). During the wavelet transform, the vector truncation of wavelet coefficient is nearly optimal for data compression. Thus, JPEG 2000 compression, which used wavelet transform as its basis function, is introduced for image compression and the compressed image has a little distortion as compared to normal JPEG compression (Gonzalez et al, 2004). Taking the advantages of this JPEG compression, the watermarked image should resist to this compression technique too.

A lot of wavelet transform watermarking schemes are proposed and some of the wavelet transform watermarking schemes are claimed to be compatible with the image compression JPEG 2000 (Meerwald and Uhl, 2001). Xia et al (1997) use Discrete Wavelet Transform (DWT) to decompose the original image and embedded the modeled Gaussian noise watermark into the middle and high frequency bands of DWT coefficients. In the watermark detection process, the cross correlation between the DWT coefficients of the original image and watermarked image are calculated. In the watermarking scheme proposed by Kundur and Hatzinakos (Kundur and Hatzinakos, 1997), the watermark is also embedded into the wavelet transform domain. The strength of the embedded watermark is based on the contrast sensitivity value of the original image. The result is robust against additive noise, rescanning and JPEG compression. Hsieh et al (2001) has embedded a logo based watermark into multiresolution wavelet transform coefficients. Their watermark is embedded into selected coefficients with local information in the sub-bands of wavelet coefficients. This approach is based on the qualified significant wavelet tree (QSWT). The extracted watermark is a visually recognizable image. Their experimental result show that the proposed wavelet transform watermarking scheme is robust to JPEG compression, image processing operation and even compound attacks.

2.3.2.2 Redundant Wavelet Transform Watermarking Scheme

Standard DWT technique will down sample the coefficients to half when the level of resolution increased. This critically sampled dyadic of DWT technique limits the capacity of watermark data to number of wavelet coefficients. Thus, some researchers proposed watermarking scheme using Redundant Discrete Wavelet Transform (RDWT). Figure 2.4 delineates a general two level decomposition process of standard Discrete Wavelet Transform (DWT) and Redundant Discrete Wavelet Transform (RDWT). RDWT (also called as Stationary Wavelet Transform (SWT) (Michel Misiti et al, 2000)), or the *a trous* algorithm (Adhemar Bultheel, 1999), (Stephane Mallat, 1999) which is an alternative wavelet transform paradigm functioning to a certain extent as an approximation to the continuous wavelet transform. RDWT based signal processing is claimed to be more robust than DWT based technique (Hien et al, 2004). Therefore, watermarking techniques using RDWT will produce an over complete, over sampled expansion system at the watermark embedding stage (Hien et al, 2004).

Cao et al (2001) proposed a RDWT based image-adaptive watermarking scheme. In their scheme, the strength of the watermark is controlled by the significance of coefficient. Besides that, Hien et al (2004) introduced another RDWT based logo watermark embedding scheme. A logo image of watermark is adaptively embedded into the RDWT coefficients and for the watermark detection process they proposed a new intelligent Independent Component Analysis base detector to extract the watermark. However, both Cao et al (2001) and Hien et al (2004) watermarking schemes is a symmetric watermarking scheme, where only one watermark is embedded into the host image.

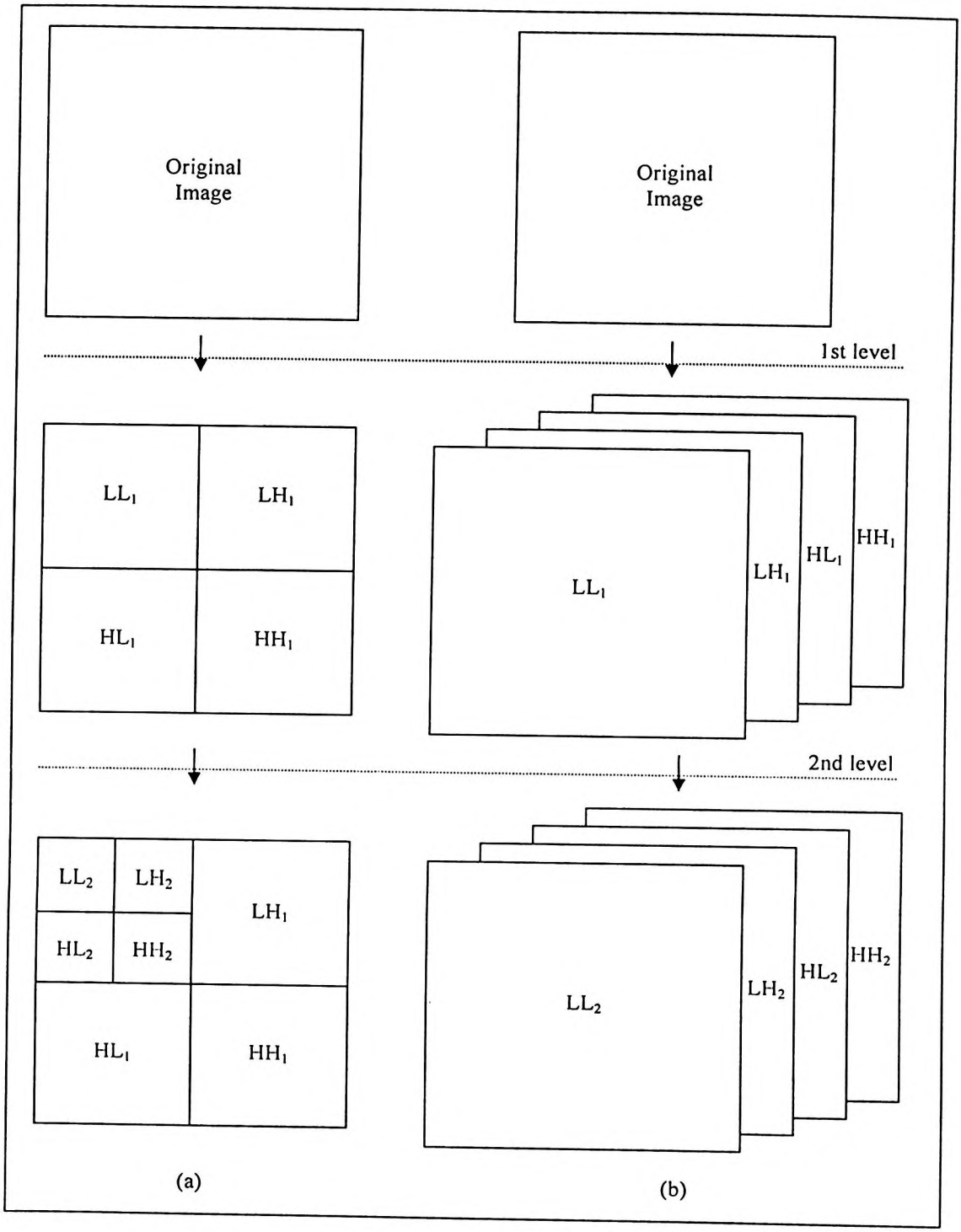

Figure 2.4: Two level decomposition of (a) DWT and (b) RDWT. L and H indicate the low-pass and high-pass filter respectively.

2.4 Properties of Digital Image Watermarking

The performance of watermarking schemes can be evaluated using a set of defining properties (Cox et al, 2002). There are a number of papers that have discussed the properties of digital watermarking (Wolfgang et al, 1999), (Petitcolas et al, 1999), (Hartung and Kutter, 1999). The major properties are robustness, tamper resistance, fidelity, computational cost, false positive rate, data payload and security issue. However, these properties vary very much depending on the applications and it is difficult to evaluate watermarking scheme without first indicating the context in which it is to be applied. While this dissertation applies the digital watermarking scheme on copyright protection of digital images, four important properties which meet the requirement of digital image watermarking in this application will be discussed.

- Fidelity or Perceptibility – A watermark is said to have high fidelity if the degradation of the Work has caused the embedded watermark difficult for a viewer to perceive (Cox et al, 1997). Embedding an imperceptible watermark into a digital image offers more robustness on watermarked image for copyright protection (Nikolaidis and Pitas, 1996).
- Robustness – It means that the embedded watermark still can be detected after the image has undergone common signal processing operation, such as lossy compression, halftoning, spatial filtering, printing and scanning and geometric distortion.
- Data payload or Capacity – It refers to the number of bits of a watermark or number of watermarks encoded within an image. It is highly dependent on the host image that supports or conveys the watermarks and the quality of watermarked image it aimed for (Alexandre Paquet, 2001).
- Security – The security of watermarking scheme lies on Kerckhoff's assumption, i.e. the method used to encrypt the data, is known to the

unauthorized party (Alexandre Paquet, 2001). Therefore the security of a watermark refers to its ability to resist hostile attacks. Unauthorized removal, unauthorized embedding and unauthorized detection are the hostile attacks that intent to thwart the watermarking purpose.

2.5 General Attacks on Digital Image Watermarking

Normally watermarking attacks occurred during the transmission from image owner to end user, or during the watermark detection process. Some common signal processing operations will make the watermark undetectable during the transmission of the watermarked image to the end user. These common signal processing operations include additional of noise, data compression, digital to analogue (D/A) or analogue to digital (A/D) conversion and geometric distortions (rotation, translation, scaling, and cropping) (Voloshynovskiy et al, 2001). These processes may be introduced unintentionally or inadvertently.

In contrast to the first type of attacks, the second type of attacks which happen during the watermark detection process may be applied with the explicit goal of hindering watermark reception. Figure 2.5 shows a summary of the different attacks on digital watermarking systems (Kutter et al, 2000).

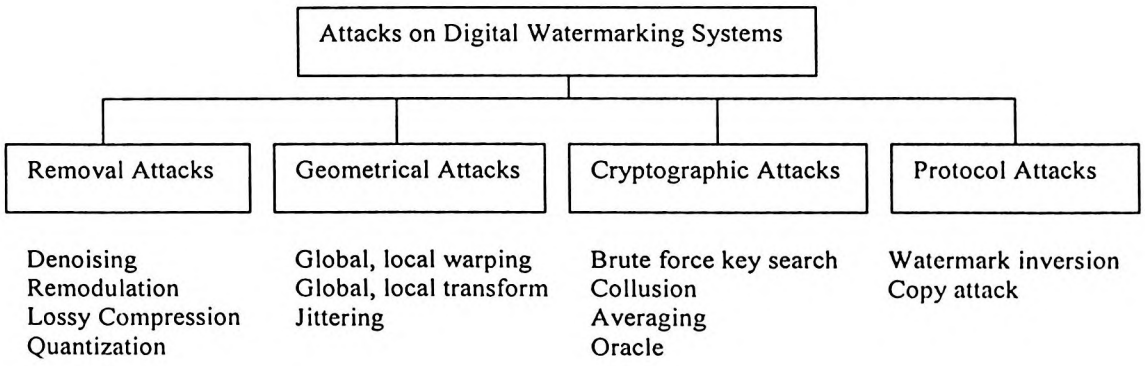

Figure 2.5: Types of attacks on digital watermarking systems (Kutter et al, 2000).

Removal attacks include attacks that aim at removing the watermark without degrading the quality of the watermarked image (Nikolaidis et al, 2001). This kind of attacks include unintentional attacks occur during common signal processing operation, malicious attacks includes attacks like additional of noise. Collusion attack such as remodulation tries to combine different watermarked version of the same image to generate an average image that is very close to the original.

Instead of removing watermark, geometrical attacks aim to distort the watermark detector synchronization with the embedded information (Voloshynovskiy et al, 2001). For image watermarking, geometrical attack introduces a global or local warping, transform or jittering on pixel intensity values in such a way that the watermark detector can not find the watermark. The most known benchmarking tools for image watermarking, StirMark (Kutter and Petitcolas, 1999), integrates a variety of geometric attacks.

Cryptographic attacks are very similar to attacks used in cryptography application. The attack will crack the security methods in watermarking schemes and cause the watermark detector unable to detect the embedded watermark. Then it finds a way to remove the embedded watermark information or to embed misleading watermarks. Through and exhaustive search, brute force attacks can find the secret of embedded information. Oracle attack (Cox and Linnartz, 1998) is a tool to create a non-watermarked signal when a watermark detector is available. In practical, application of cryptographic attacks is restricted due to their high computational complexity (Voloshynovskiy et al, 2001).

The intentions of the protocol attacker are not aimed at destroying the embedded information or disable the watermark detector through local or global data manipulation. Their goal is to render the watermarking scheme unreliable by subtracts

or estimates a watermark from the watermarked data and then claims to be the owner of the watermarked data. Significant example of protocol attacks are concept of invertible watermarks and copy attacks (Kutter et al, 2000).

2.6 Summary

In this chapter, a brief introduction on history of watermarking technique is presented. The fundamental of digital watermarking schemes that involve three processes are described. There are watermark generation, watermark embedding and watermark extraction process.

Many classifications of digital watermarking technique are presented. Watermarking techniques are classified according to their application areas, working domain, perceptions and security issue. For digital image watermarking, some spatial domain watermarking techniques are identified and described. In contrast to spatial domain, frequency domain digital image watermarking techniques draw more research interest because of the high robustness of watermarked image. In frequency domain, wavelet transform based watermarking scheme is more popular where it is compatible with the new image compression standard. In addition, redundant wavelet transform that offer more wavelet coefficients for watermark embedding is also highlighted. Some redundant wavelet transform watermarking schemes are presented.

The performance of watermarking schemes is evaluated by defined properties. Properties such as perceptibility, robustness, capacity and security are dependant on the application of the watermarking scheme. Besides that, attacks on digital watermarking scheme are also introduced. These attacks determine the robustness of the watermarking scheme.

CHAPTER THREE
DEVELOPMENT OF THE PROPOSED WATERMARKING SCHEME

3.0 Introduction

Watermarking is an application driven solution. The properties of watermarking technique such as robustness, capacity and perceptibility issues are highly dependent on the application that watermarking served. Besides these properties, security issues also play an important aspect for watermarking technique. For copyright protection application, the watermark served as a proof of the original owner for the watermarked work.

In many proposed digital image watermarking schemes, the extraction of watermark depends on the watermark key or security key which is generated during the watermark embedding process. This key specifies necessary information for watermark embedding and extraction process. Thus, it is wise to keep it secret. Unfortunately, this security key will be exposed to public after the watermark verification process. Once the key is known to public, an attacker is able to remove the watermark completely from the watermarked image (Craver and Katzenbeisser, 2001). As a consequence, the watermarking system is secured provided that there is no need to verify the embedded watermark. Once the embedded watermark is used to prove the ownership of copyright, the watermark can be removed. However, if several digital images are embedded with the same watermark and security key, these watermarked images are insecured as well.

This drawback of symmetric watermarking system can be solved by embedding more than one watermark into the host image (Craver and Katzenbeisser, 2001). One of the watermark key is used for the verification process while the remaining keys are kept private and secret (Kim et al, 2004). This type of watermarking scheme is called

asymmetric watermarking scheme because the system is analogous to public-key cryptography (Craver and Katzenbeisser, 2001), (Furon and Duhamel, 2003).

Embedding multiple watermarks into the host image generates multiple security keys for the watermark extraction process. An attacker may remove one or two of the embedded watermarks if he knows the specific watermark key. However, the attacker may not be able to remove all the embedded watermarks if he does not have all the watermark keys. Closet point or brute force attack may remove all the watermarks (Barni et al, 2003). Unfortunately, it is hard to remove them without degrading the perceptual quality of the image.

For the watermark extraction process, the correct security key is required to extract a particular watermark. In real application process, client receives only one watermark key for the verification process with the intention that the disclosure of this watermark key cannot remove all the embedded watermarks. Thus, the copyright of the image is still under protection.

Copyright protection of digital images requires a robustness and perceptual imperceptible watermarking scheme. Frequency domain watermarking scheme offer a high robustness result on watermarked image and the embedded watermark in high-pass frequency coefficients will not impact the image visual fidelity (Cox et al, 1997). Thus, wavelet transform-based watermarking technique will be adopted in the proposed watermarking scheme. In additional, wavelet transform-based watermarking scheme is also compatible with the new image compression standards, JPEG 2000.

Considering the capacity issue, embedding multiple watermarks into an image require a number of wavelet coefficients. One of the advantages of Redundant Discrete Wavelet Transform is that the size of the decomposed coefficients is equivalent to the