Université d'Ottawa • University of Ottawa

PERMISSION DE REPRODUIRE ET DE DISTRIBUER LA THÈSE

PERMISSION TO REPRODUCE AND DISTRIBUTE THE THESIS

NOM DE L'AUTEUR / NAME OF AUTHOR:	Huiping Guo
ADRESSE POSTALE / MAILING ADDRESS:	104-45 Mann Avenue Ottawa, Ontario K1N 6Y7
GRADE / DEGREE:	**ANNÉE D'OBTENTION / YEAR GRANTED**
Ph.D - Computer Science	2003
TITRE DE LA THÈSE / TITLE OF THESIS:	
Digital Image Watermarking for Ownership Verification	

L'auteur permet, par la présente, la consultation et le prêt de cette thèse en conformité avec les règlements établis par le bibliothécaire en chef de l'Université d'Ottawa. L'auteur autorise aussi l'Université d'Ottawa, ses successeurs et cessionnaires, à reproduire cet exemplaire par photograhie ou photocopie pour fins de prêt ou de vente au prix coûtant aux bibliothèques ou aux chercheurs qui en feront la demande.

Les droits de publication par tout autre moyen et pour vente au public demeureront la propriété de l'auteur de la thèse sous réserve des règlements de l'Université d'Ottawa en matière de publication de thèses.

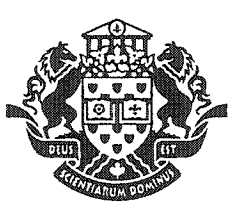
The author hereby permits the consultation and the lending of this thesis pursuant to the regulations established by the Chief Librarian of the University of Ottawa. The author also authorizes the University of Ottawa, its successors and assignees, to make reproductions of this copy by photographic means or by photocopying and to lend or sell such reproductions at cost to libraries and to scholars requesting them.

The right to publish the thesis by other means and to sell it to the public is reserved to the author, subject to the regulations of the University of Ottawa governing the publication of theses.

N.B. LE MASCULIN COMPREND ÉGALEMENT LE FÉMININ

Sept. 08, 2003
DATE

Huiping Guo
(AUTEUR) SIGNATURE (AUTHOR)



Université d'Ottawa · University of Ottawa

Université d'Ottawa · University of Ottawa

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

GUO, Huiping

AUTEUR DE LA THÈSE - AUTHOR OF THESIS

Ph. D. (Computer Science)

GRADE - DEGREE

School of Information Technology and Engineering

FACULTÉ, ÉCOLE, DÉPARTEMENT - FACULTY, SCHOOL, DEPARTMENT

TITRE DE LA THÈSE - TITLE OF THE THESIS

Digital Image Watermarking for Ownership Verification

N. Georganas

DIRECTEUR DE LA THÈSE - THESIS SUPERVISOR

EXAMINATEURS DE LA THÈSE - THESIS EXAMINERS

A. El Saddik

D. Hatzinakos

E. Kranakis

J. Zhao

J.-M. De Koninck, Ph.D.

LE DOYEN DE LA FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

SIGNATURE

DEAN OF THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

Digital image watermarking for ownership verification

by

Huiping Guo

A thesis submitted to the University of Ottawa in partial fulfillment
of the requirements for the degree of Doctor of Philosophy

Ottawa-Carleton Institute of Computer Science
School of Information Technology and Engineering
University of Ottawa

Ottawa, Ontario, Canada

September 2003

Abstract

The development of the Internet has greatly contributed to the expanded use of digital media, for example, images, audio, video, VRML objects. These media can be duplicated unlimitedly without any quality loss and can also be easily distributed and tempered. This presents problems of digital media security, such as copyright protection and authentication, which creates a pressing need for digital media protection schemes. A new emerging technology, digital watermarking, protects digital media by embedding a robust signal directly into the media, thus providing a promising way to protect the digital media from illicit copying and manipulation.

In this thesis, we mainly consider digital image watermarking for ownership verification. Though lots of such schemes have been proposed in literature, there are still some problems that have not been addressed or have not been adequately addressed such as how to detect a watermark progressively while at the same time be robust to geometrical transformations, how to embed a watermark in the fractal domain and how to embed a watermark into an object in an image instead of into the whole image. Several new watermarking algorithms are proposed here to address these problems respectively and experiments show satisfactory results.

The next problem that has been ignored by the watermarking community is the joint ownership verification. If an image is created collaboratively by multiple owners, all current watermarking schemes will fail to protect the image from potential dishonest owners, since they are only designed to protect an image from dishonest users. To address this problem, a novel framework of the watermarking system that makes use of a secret sharing scheme is proposed. Based on this framework, several new watermarking algorithms are proposed where the secret watermark embedding key is split into shares and each owner holds one share. Multiple watermarks contributed by each owner are embedded into spectrum domain of the image and multiple thresholds are set so that the watermark can verify joint ownership as well as partial ownership. To the best knowledge of the author, the problem of joint ownership has not been addressed so far and the watermarking schemes proposed are the first ones to address them.

Acknowledgements

I would like to express my sincere gratitude to my advisor, Dr. Nicolas D. Georganas, for his guidance, encouragement and support in every stage of my graduate study. His knowledge, kindness, patience, openmindedness and vision have provided me with lifetime benefits.

I wish to also acknowledge the members of my Ph.D advisory committees, Dr.Zhao and Dr.Kranakis for their valuable comments and suggestions on the thesis proposal. In particular, I wish to express thanks to Dr.Zhao for the enlighting discussions and helps in my study.

I would like to thank all members of the DISCOVER family, for the great and relaxed work environment and precious discussions. Special thanks to Dr. Abed EI Saddik for the valuable discussions and help and Francois Malric for the technical support throughout this work.

I am also grateful to my parents and parents-in-law for the years of care, support and encouragement received from them.

Finally, I would like to thank Junjie Lu, my husband, for his love, encouragement and endless support while I completed this work.

Contents

List of Tables

List of Figures

List of Acronyms

AWGN — Additive White Gaussian Noise

CDMA — Code Division Multiple Access

DCT — Discrete Cosine Transform

DFMT — Discrete Fourier-Mellin Transform

DFT — Discrete Fourier Transform

DWT — Discrete Wavelet Transform

DVD — Digital Video Disc or Digital Versatile Disc

HVS — Human Vision System

IFS — Iterated Function System

JND — Just Noticeable Difference

JPEG — Joint Photographic Experts Group

LIFS — Local Iterated Function System

LSB — Least Significant Bit

MPEG — Motion picture Experts Group

QIM — Quantization Index Modulation

ROI — Region of Interest

SA-DCT — Shape Adaptive Discrete Cosine Transform

VSS — Visual Sharing Scheme

Chapter 1

Introduction

1.1 Watermarks: history

Since the beginnings of the human being, we have tried to capture what we see and what we hear and recorded them. Since this information helps us communicate and understand well, it has been realized that there is a large commercial potential for trading such information. Fraudulent people, however, have put an enormous effort in stealing and copying these pieces of information. Countermeasures were needed and one solution called paper watermarks was proposed.

Paper watermarks first appeared in the art of handmade papermaking about 700 years ago. The oldest watermarked paper found in archives dates back to 1292 and has its origin in the town of Fabriano in Italy which has played a major role in the evolution of the papermaking industry. At the end of the 13th century about 40 paper mills were sharing the paper market in Fabriano and producing paper with

different format, quality, and price. At that time paper mills produced raw paper with very coarse surfaces not yet suitable for writing. This raw paper material was given to other artisans who smoothed the paper surface with the help of a hard stone, called calendar, to make it suitable for writing. The post-treated paper was then counted, folded and finally sold to merchants who stored it in huge warehouses for resale with large profits. Competition not only between the 40 paper mills but also between artisans and merchants was very high and it was difficult for any party to keep track of paper provenance and thus format and quality identification [87]. The introduction of watermarks was the perfect method to eliminate any possibility of confusion. After their 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 as indication for paper format, quality and strength, and were also used as the basis for dating and authentication of paper [78].

Today, paper watermarks still play an important role in the papermaking industry. They provide a level of security, which prevented people for the past 700 years from easily duplicating and tampering documents. Thus, watermarks have served as a very simple, but still effective, way of copy protection and authentication.

Nowadays the world is going digital. With the increasing availability and distribution of media in digital form, the protection of intellectual property and the recognition of manipulations faces new challenges. Popular file formats (like JPEG,MPEG and MP3) facilitate the exchange of digital images, videos or sound clips. Books are published electronically and films are distributed on DVDs. The possibility of easily

and cheaply reproducing digital content without permission raised the concern of the music, film and entertainment industries.

Although classical analogue storage media such as VHS video and audio cassettes can also be copied, they suffer from the inevitable quality loss, which limits the illegal distribution of copyrighted content. In the digital form, however, media can be duplicated unlimitedly without any quality loss and can also be easily distributed and tempered. This presents problems of digital media security, such as copyright protection and authentication, which creates a pressing need for digital media protection techniques.

The concept of paper watermarks and their history largely motivated the development of digital watermarking as a possible approach to solve the above mentioned problems. The analogy between paper watermarks and digital watermarking is obvious: paper watermarks in bank notes or stamps inspired the first use of the term "watermark" in the context of digital data [78]. The first publications that focused on watermarking of digital images were published by Tanada et al. [165] in 1990 and Tirkel et al. [168] in 1993. Since 1995, digital watermarking has gained lots of attention and has evolved very fast.

1.2 Why digital watermarking

A number of technologies have been developed to provide media protection. Two of them are cryptography and steganography. However, due to their limitations, they

cannot fully protect the digital media. Digital watermarking complements cryptography and steganography by embedding a robust signal directly into the data, thus providing a promising way to protect the digital media from illicit copying and manipulation.

1.2.1 Watermarking and steganography

Classical steganography concerns itself with ways of embedding a secret message (which might be a copyright mark, or a serial number) in an original message [1]. The embedding is usually parameterized by a key; without knowledge of this key, it is very difficult for the third party to detect or remove the embedding material.

There is a significant difference between watermarking and steganography. In the latter, a successful attack consists of the third party's knowledge that a given object is present. While in the former, all the participants in the scheme may be aware that marks are in use, so a successful attack does not mean detecting a mark, but rendering it useless. This could be done by removing it or by other attacks.

Another difference is based on the intent of use. Both employ mechanisms for hiding information. In steganography, the goal is to try to hide a message within some other content. This message may have nothing to do with the carrier. Watermarks, on the other hand can be some information related to the carriers. For example, they may convey some information about the carrier, author, or owner. The existence of an embedded watermark may be known or unknown. The goal of watermarking

is to protect the hidden information from being tampered with, without necessarily worrying about whether the presence of the watermark is known or not [40].

Finally, steganography is usually not robust against modification of the data, or has only limited robustness and protects the embedded information against technical modifications that may occur during transmission and storage, like format conversion, compression or digital-to-analog conversion. Watermarking, on the other hand, is designed specially for resilience against unintentional or intentional attacks which may destroy or remove the hidden information .

1.2.2 Watermarking and cryptography

While steganography is about concealing the existence of messages, cryptography is about concealing the content of the messages, where we transform the messages so as to make it meaningless to the interceptor [1].

Many of the problems that watermarking addresses are similar to problems solved by cryptography for secure communications. For example, we may want to assure the integrity of digital media when they are distributed, so that we can know whether they have been tampered. Cryptography has addressed similar problems of message integrity using digital signatures. Also, we may want to keep an association between the digital media and the creator, distributor, or buyer of that media. Cryptography has also solved this problem, named non-repudiation, in secure communications.

However, traditional cryptosystems suffer from one important drawback: they do not associate cryptographic information with media permanently. Cryptography can

hide a message from plain view by encrypting it with a secure key prior to transmission, and can also provide auxiliary information to effectively authenticate the message and guarantee non-repudiation. When the receiver gets the message and decrypts it, it is clear. Thus, cryptography can not make any guarantees about the redistribution, duplication or alteration of the message after it has passed through the cryptosystem. On the contrary, in digital watermarking, the watermarks are embedded directly into the content. After that, the watermarks and the content are inseparable. At any time, the watermarks in the content can be used to authenticate the content or to prove the ownership of the content. Thus watermarking provides extended guarantees about digital content and it significant advantages over cryptography [1, 40].

1.3 Contributions of this thesis

In this thesis, we mainly consider digital image watermarking schemes. An important application of digital image watermarking is copyright protection. We have developed several digital watermarking algorithms to solve some special problems of single and joint ownership verification for digital images. The following is a list of our contributions:

Digital image watermarking for single ownership:

1. **A multi-resolution image watermarking scheme in the spectrum domain**

Many spectrum domain watermarking schemes have been proposed in recent years, but they seldom deal with the problem of progressively detecting the embedded watermark, which is desirable in some situations. A new watermarking algorithm is proposed to address this problem by embedding the watermark in the DCT domain of an image in a multi-resolution way. The DCT coefficients are treated as wavelet transform coefficients, and each watermark bit is embedded into a block of coefficients repeatedly layer by layer using a wavelet watermarking scheme, so that the embedded watermark can be detected progressively. Furthermore, for the scheme to be robust against geometric transformations, a second spread spectrum circular watermark is embedded in the DFT domain. Experimental results show that this scheme is robust against JPEG compression, additive noise, as well as rotation and translation.

2. **A spread spectrum image watermarking scheme in the fractal domain**

   Fractal image compression is an important image compression technology. In some cases, it may be desirable to embed a watermark in the fractal domain, but few work has been on this area. We present a digital watermarking scheme which adds a spread spectrum watermark in the fractal domain of an image during the process of fractal image coding. The watermark is embedded into an image by modifying scale factors of its fractal code. Experimental results show that this scheme is robust against JPEG compression, print, cropping, photocopying and scanning.

3. **Digital image watermarking for arbitrarily shaped objects**

   Many image watermarking schemes have been proposed in recent years, but they usually involve embedding a watermark to the entire image without considering a particular object in the image only which the image owner may be interested in. We propose a watermarking scheme that can embed a watermark to an arbitrarily shaped object in an image. Before embedding, the image owner specifies an object of arbitrary shape that is of a concern to him. Then the object is transformed into the spectrum domain using shape adaptive DCT and a watermark is embedded by modifying the spectrum coefficients in an additive way. Experimental results show that this scheme is robust against JPEG compression, median filtering and additive noise.

Digital image watermarking for joint ownership:

1. **A novel framework of digital watermarking systems**

   The current watermarking schemes are only designed to protect an image from dishonest users and cannot protect the image from potential dishonest owners, if the image is created jointly by multiple owners. This is indeed the problem of joint ownership verification, which has never been noticed and addressed. To solve this problem, a novel framework of digital watermarking system which is based on a secret sharing scheme in cryptography is proposed and some related issues are discussed.

2. **Digital image watermarking for joint ownership**

   Based on the proposed framework, two digital watermarking algorithms are proposed. The first one applies Shamir's threshold scheme (2.2) to a watermarking algorithm. A watermark, which is a gaussian distributed random vector determined by two keys, is embedded to selected coefficients in all middle bands in the wavelet domain of an image, so that only when the two keys are put together can the ownership be verified. The second algorithm is a modification of the first one. Three random watermarks are embedded to middle bands in the wavelet domain of an image. For the watermark detection, two thresholds are set, so the watermark detector can verify partial ownership as well as full ownership. Experimental results show that the first algorithm is robust to JPEG compression, additive noise, median filtering, cropping, histogram equalization, intensity adjustment. The second algorithm is robust to JPEG compression and additive noise.

3. **Flexibly verifying joint ownership using digital image watermarking**

   In the digital image watermarking community, the problem of joint ownership has not been adequately addressed. We propose a novel watermarking algorithm that makes use of a generalized secret sharing scheme in cryptography to address this problem. Given that multiple owners create an image jointly, only an authorized group of owners are given distinct shares and can create watermarks jointly. Then, each authorized owner's contribution to the watermarks is put in the different sub-bands in the wavelet domain of an image so that

the watermark detector can verify joint ownership as well as partial ownership. Experimental results show that the proposed algorithm is robust against JPEG compression, additive noise, median filtering, cropping, histogram equalization, intensity adjustment, additive salt & pepper noise, multiplicative speckle noise, scaling and rotation.

Publications resulting from this research:

1. H.Guo and N.D.Georganas, " A Novel Approach to Digital Image Watermarking Based on a Generalized Secret Sharing Scheme ", ACM Multimedia Systems Journal, special issues on Multimedia Security, (to appear)

2. H.Guo and N.D.Georganas, " Jointly Verifying Ownership of an Image Using Digital Watermarking ", Inter. Journal of Multimedia Tools and Applications, (revised and under 3^{rd} review)

3. H.Guo and N.D.Georganas, "Multiresolution Image Watermarking Scheme in the Spectrum Domain", Proc. Can. Conf. on Elec. And Comp. Eng., Winnipeg, May 2002

4. H.Guo and N.D.Georganas, "A Spread Spectrum Domain Watermarking Scheme in Fractal Domain", Proc. 21st Biennial Symp. on Communications, Kingston, June 2002

5. H.Guo and N.D.Georganas, "Digital Image Watermarking for Arbitrarily Shaped Objects", Proc. 21st Biennial Symp. on Communications, Kingston, June 2002

6. H.Guo and N.D.Georganas, "Digital Image Watermarking for Joint Ownership", Proc. ACM Multimedia 2002, Juan Les Pins, France, December 2002 (15% acceptance rate)

7. H.Guo and N.D.Georganas, " Joint ownership verification for an image using digital watermarking ", Inter. Conf. on Information Technology: Coding and Computing, Los Vegas, April 2003

8. H.Guo and N.D.Georganas, " Blind joint ownership verification for digital images ", Can. Conf. on Elec. And Comp. Eng., Montreal, May 2003

9. H.Guo and N.D.Georganas, " Digital image watermarking for joint ownership verification without a trusted dealer involved in the system", Inter. Conf. on Multimedia and Expo(ICME), Baltimore, July 2003

1.4 Organization of this thesis

This thesis is organized as follows:

In chapter 1 the concept of watermarking technology is introduced. Chapter 2 gives a detailed overview of the current watermarking technologies for images.

The following three chapters mainly target single ownership verification for digital images. In chapter 3, a composite watermarking scheme is proposed, which embeds two watermarks to different spectrum domains to address different problems. Chapter 4 gives a new watermarking scheme that embeds a spread spectrum watermark in the fractal domain of an image during the process of fractal image coding. In

chapter 5, another new watermarking algorithm is proposed where a watermark is embedded into any arbitrarily shaped objects instead of the whole image.

The next three chapters focus on joint ownership verification for digital images which has never been addressed so far. Chapter 6 gives a novel framework of a watermarking system that can solve this problem. Based on this framework, the following two chapters present some example watermarking schemes. In chapter 7 a novel watermarking scheme that makes use of Shamir's secret sharing scheme is proposed to address the problem of joint ownership as well as partial ownership verification for digital images. In chapter 8, a more robust watermarking scheme is proposed where the problem of flexible joint ownership verification for digital images is addressed.

Finally, conclusions are given in chapter 9.

Chapter 2

The Watermarking Technology

In this chapter, the concept of watermarking technology is introduced. The general framework of watermark embedding, extraction and detection is given, followed by the watermarking classifications, properties and applications. This chapter also presents various attacks that a watermarking system should be immune to. Several benchmarks tools that evaluate different watermarking systems are introduced at the end. Finally, an overview of the current watermarking technologies for digital images is given.

2.1 General framework

Generally, the watermarking system can be seen as a communication system. The digital image (or its frequency domain transform) is viewed as a communication channel and, correspondingly, the watermark is viewed as a signal that is transmitted through

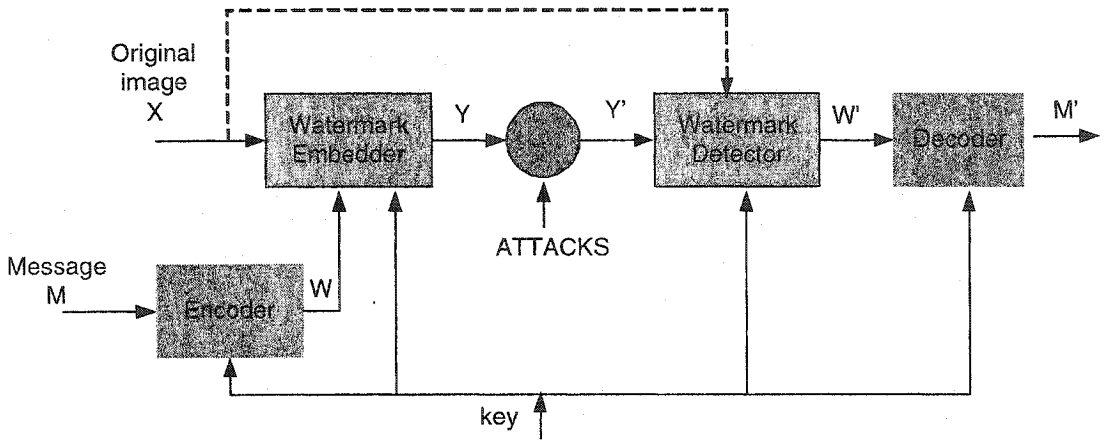


Figure 2.1: The framework of a watermarking system

it. Attacks and unintentional signal distortions are treated as noise that the watermark must be immune to. Figure 2.1 shows the block diagram of a watermarking system. As shown in this figure, the watermarking system consists of two main parts, i.e. watermark embedding and watermark detection.

2.1.1 Watermark embedding

Before embedding, the host image is usually transformed to a domain that facilitates data embedding. A message M is to be embedded in the host image which contains information about the owner. This can be some binary data, a small logo image or a seed value to a pseudo-random number generator to produce a sequence of numbers with a certain distribution (e.g. Gaussian or uniform).To convert the message M into an efficient form for communication, it is usually encoded using either error correction codes (ECC) or modulated using some form of modulation. In the general case, the type of ECC and the set of basis functions for modulation can be key-dependent. The

above conversion is performed in the encoder and produces the watermark W. The host image and the generated watermark are then fed into the watermark embedder. The watermark embedder performs the insertion of the watermark into the host image using a key and then yields the watermarked image:

$$Y = T^{-1}(h(T(X)), W)) \tag{2.1}$$

where T is any orthogonal transform like block DCT, full-frame FFT, DCT or wavelet, and where h denotes the embedding function. The most practically used class of embedding functions is the linear additive model:

$$Y = h(X, W) = X + W \tag{2.2}$$

The watermarked image is then distributed, for example put on a web server or transmitted to a customer. Usually, before distribution, the watermarked image is compressed which can introduce some distortion to it. Also, during the process of transmission and distribution, transmission errors and some other processing tasks may further add distortions to the watermarked image. Especially, geometric image transformations such as rotation, scaling and translation have been proved to be very harmful to the embedded watermark [112]. In addition to these, more serious hostile attacks described in section 2.3 that attempt to remove or disable the embedded watermark, may apply to the watermarked image.

2.1.2 Watermark detection

Eventually, after the watermarked image has undergone the above mentioned distortions, one would like to detect the embedded watermark from the watermarked image. First, the watermark extractor performs an estimate W' of the watermark based on the attacked version Y' of the watermarked image:

$$W' = Extr(T(Y'), [X], Key) \tag{2.3}$$

In general, the extraction should be key-dependent. The original image X may or may not be used by the extractor. If X is used, the scheme is called private watermarking; if X is not used, the scheme is called public watermarking.

Then, the extracted watermark W' is decoded by the decoder to generate the reconstructed message M'. In some watermarking systems, the watermark detector can not recover the embedded messasge, but only output some confidence measure indicating how likely it is for a given watermark to be present in the original image [78]. A widely used confidence measure is the normalized correlation:

$$\delta = \frac{M' \cdot M}{|M'| \cdot |M|} \tag{2.4}$$

The dot function gives the scalar product of the two vectors of the same length. To make a final decision about whether the given message is embedded or not, the

watermark detector compares δ with a predefined threshold T. If δ is above T, the given message is decided to be present; otherwise, it is not.

2.2 Requirements and applications

2.2.1 Requirement

To be effective, there are a number of desirable properties that a watermark should exhibit. These properties are discussed in more detail next.

Inperceptibility

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. That is, the watermark should be invisible [22]. Artifacts introduced through a watermarking process are not only annoying and undesirable, but may also reduce or destroy the commercial value of the watermarked data. It is therefore important to design watermarking systems which exploit properties of human vision or auditory system in order to maximize the energy of the watermark under the constraint of not exceeding the perceptible threshold [78].

Modification and multiple watermarks

In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital video discs, a disc may be watermarked to allow only a single copy. Once this copy has been made, it is then necessary to alter the

watermark on the original disc to prohibit further copies. Changing a watermark can be accomplished by either (1) removing the first watermark and then adding a new one or (2) inserting a second watermark such that both are readable, but one overrides the other. The first alternative does not allow a watermark to be tamper resistant since it implies that a watermark is easily removable. Allowing multiple watermarks to co-exist is preferable and also facilitates the tracking of content from manufacturing to distribution to eventual sales, since each point in the distribution chain can insert its own unique watermark [22, 117].

High detection reliability

The watermark should be detected with a high degree of reliability [119]. More important, the probability of false-positives and false negatives detection has to be extremely small. In this context, "false-positives" means detection of a watermark even when there is no watermark; "false-negatives" means missed detection of a watermark when there is a watermark.

Robustness

The watermark must be difficult (hopefully impossible) to remove. Any attempts to remove or destroy a watermark should result in severe degradation in quality before the watermark is lost. In particular, the watermark should be robust to attacks described in section 2.3.

Capacity

Capacity refers to how many watermarks can be embedded without degrading the quality of the host media and can also be extracted correctly. It is an important factor that affects robustness, detectability and uniqueness of a watermark.

2.2.2 Applications

Broadcast monitoring

We can use watermarks for broadcast monitoring by putting a unique watermark in each video or sound clip prior to broadcast [24]. Automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where each clip appears. In this way, copyright owners can ensure that their property is not illegally rebroadcast by pirate stations.

Owner identification

A digital watermark can be used to identify the owner by providing complementary copyright marking functionality. Since the watermark becomes an integral part of the image and the watermark and the image are inseparable, we do not need to worry about that the copyright notice might be lost [24].

Proof of ownership

Watermarks can be used not just to identify copyright ownership, but to actually prove ownership [24, 115]. For example, to establish ownership over an image, Alice

can generate a watermark based on a private key and embed it to the image. Then, she makes the watermarked image available to the public. Later, when Bob makes a copy of the watermarked image and claims that he owns the image, Alice can demonstrate her watermark in Bob's image with or without the help of her unmarked original image. Since Alice's original image is not available to Bob, he can not do the same. For such a scheme to work, the watermark has to resist common image processing operations as well as all kinds of intentional attacks.

Authentication and integrity verification

When a digital image is used for legal purposes such as medical applications, news reporting, or commercial transactions, the originator of the image has to be verified while ensuring the image has not been changed, manipulated, or falsified. Although authentication of a digital image can be done through conventional cryptographic techniques, the advantage of using a watermark is that the authenticator is inseparably bound to the image. When the watermarked image is checked, the watermark is extracted using a unique key associated with the source, and the integrity of the image is verified through the integrity of the extracted watermark [24, 115].

Fingerprinting

Monitoring and owner identification applications place the same watermark in all copies of the same content. On the contrary, to avoid unauthorized duplication and distribution of a publicly available digital image, an author can embed a distinct

watermark (or fingerprinting) into each copy of the image. If unauthorized copies are found later, the origin of the copy can be determined by retrieving the fingerprint. In this application, the watermark needs to be invisible and invulnerable to deliberate attempts by forgery, removal or invalidation [24, 115].

Copy control

Fingerprinting watermarks as well as watermarks for monitoring, identification, and proof of ownership do not prevent illegal copying. Rather, they serve as powerful deterrents and investigative tools. However, it is also possible for recording and playback devices to react to embedded signals. In this way, a recording device might inhibit recording of a signal if it detects a watermark that indicates recording is prohibited. Such systems are currently being developed for DVD video [24].

Content labelling

A watermark embedded into an image can comprise an annotation, giving further information about the image. For example, an image could be annotated to describe the time and place the photograph was taken, a procedure that could be done automatically by the processor in the camera [115].

2.3 Watermarking attacks

2.3.1 Classified attacks

One important property of watermarking is robustness. Ideally, robust watermarking should be resistant not only to simple signal manipulation such as JPEG compression but also to malicious attacks such as collusion attacks. The following are classified attacks that watermarking commonly undergoes.

Simple attacks

Simple attacks are attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked image, without attempting to identify and isolate the watermark. Examples include linear and general non-linear filtering, waveform based compression (JPEG,MPEG), addition of noise, addition of an offset, cropping, quantization in the pixel domain, conversion to analog, and γ correction.

Removal attacks

Remove attacks attempt to analyze the watermarked image, estimate the watermark or the original image, separate the watermark from the watermarked image and discard only the watermark [40, 63, 119]. "Collusion attacks" is a such example. Several conspirators have copies of the same image, each embedded a unique watermark. It is then possible for them to average the copies of the image pixel by pixel into a new

image that closely resembles the original image and does not contain any detectable watermark.

Inversion attacks

If an attacker knows how the watermark was embedded into the image, he can simply detect the embedded watermark and reverse the embedding process to remove the watermark [40, 119]. To foil this kind of attack, many watermarking schemes use a secret key to determine where the watermark is embedded. Without the key, it is very difficult to locate the watermark.

Synchronization attacks

Unlike the above intentional attacks, a synchronization attack does not attempt to remove the watermark, but instead changes the watermarked image so that the embedded watermark is not detectable [29, 40, 63]. An example is a "Mosaic attack" where an image is chopped into small distinct sub-images. Though by viewing the sub-images side-by-side in an appropriate way, the entire set of chopped images is just as useful as the original image, the watermark in each sub-image is too short to be detectable. Other examples include geometric distortions like zooming, rotation, shifting, pixel permutations, sub-sampling etc. Under these attacks, the proper synchronization of the watermarked data and the watermark is lost, which renders the embedded watermark undetectable.

Interpretation attacks

An interpretation attack (other possible names include ambiguity attacks, deadlock attacks, confusion attacks etc.) seeks to forge invalid or multiple interpretations from watermark evidence [29, 28]. For example, an attacker can attempt to make another watermark appear in the same watermarked image with strength equal to that of the owner's watermark, thereby creating an ownership deadlock. This particular attack exploits the invertibility of the watermarking method, allowing the attacker to remove as well as add watermarks. To foil this kind of attack, two methods can be used. One is to use a one way hashing function of the original image, making it impossible for an attacker to remove a watermark. The other way is to use time stamping services.

2.3.2 Benchmarking of watermarking systems

It is very difficult to test the robustness of various watermarking algorithms, because the criteria and the standard test images used to demonstrate the claims vary from one algorithm to the other. To give a fair comparison of robustness between different watermarking algorithms, benchmarking tools specify a variety of attacks against which the watermark should be robust. The resistance of the algorithms to these attacks is then averaged to allow comparison.

Stirmark

StirMark is the first benchmarking tool for simple robustness testing of image watermarking algorithms [137, 136]. In its simplest version, Stirmark simulates a resam-

pling process, i.e. it introduces the same kind of errors into an image as printing it on a high quality printer and then scanning it again with a high quality scanner. It applies a minor geometric distortion: the image is slightly stretched, sheared, shifted and/or rotated by an unnoticeable random amount and then resampled using either bi-linear or Nyquist interpolation. In addition, a transfer function that introduces a small and smoothly distributed error into all sample values is applied. This emulates the small non-linear analog/digital converter imperfection typically found in scanners and display devices. StirMark introduces a practically unnoticeable quality loss in the image if it is applied only once. However, after a few iterated applications, the image degradation becomes noticeable.

Checkmark

In [134, 172],the authors propose a second generation benchmark for image watermarking. They claim that StirMark tests are limited since they do not properly model the watermarking process and then are limited in their potential to removing the best watermarks. In the Checkmark, some additional attacks are proposed including denoising attack, watermark copy attack, active desynchronization and denoising followed by perceptual remodulation. These attacks are intended to complement those in the StirMark. Further, the test results are presented as a function of application, since it is unlikely that one technology will be suitable for all applications.

2.4 Image watermarking: state of the art

Generally, watermarking schemes can be classified into two categories: spatial domain watermarking and spectrum domain watermarking. This section first introduces some spatial domain watermarking methods shortly and then focuses on spectrum domain watermarking schemes, such as spread spectrum watermarking, adaptive watermarking and geometric transforms resistant watermarking. Also in the latter category, some latest watermarking technologies are described such as quantization watermarking.

2.4.1 Spatial domain watermarking

Early watermarking methods usually belong to the spatial domain watermarking category in which the watermark is embedded by directly modifying the pixel value of an image. A well known spatial domain watermarking scheme called "patchwork" is proposed by Bender et al. [78, 7]. In this algorithm, the owner selects n-pixel pairs pseudorandomly according to a secret key K_s. He then modifies the luminance values (a_i, b_i) of the n pairs of pixels adding 1 to all values a_i and subtracting 1 from every b_i. In the extraction process, the n-pixel pairs which were used in the encoding step to host the watermark are retrieved, again using the secret key K_s. Then, the sum of difference between a_i and b_i is computed. If the image actually contained a watermark, we can expect the sum to be $2n$, otherwise it should be approximately zero.

Digimarc Corporation describes a method that adds or subtracts small quantities from each pixel [21]. Addition or subtraction is determined by comparing a binary mask of L bits with the LSB of each pixel. If the LSB is equal to the corresponding marks bit, then the random quantity is added, otherwise it is subtracted. The watermark is subtracted by first computing the difference between the original and watermarked images and then by examining the sign of the difference, pixel by pixel, to determine if it corresponds to the original sequence of additions and subtractions. Other schemes include the ones in [128].

A common drawback of spatial domain watermarking schemes is that they are not very robust to common signal processing. So recent research generally focuses on spectrum domain watermarking schemes. We shall mainly discuss this kind of schemes in the following.

2.4.2 Watermarking as a communication problem

As mentioned above, the watermarking system draws a close analog to the communication system, so some communication technologies can be applied to the watermarking system for performance improvement, such as spread spectrum communications, error control coding and communications with side information.

Spread spectrum watermarking

Spread spectrum is a transmission technique in which a pseudo-noise code, independent of the information data, is employed as a modulation waveform to "spread"

the signal energy over a bandwidth much greater than the signal information bandwidth. At the receiver, the signal is "despread" using a synchronized replica of the pseudo-noise code [49]. Spread spectrum is the key technology of the Code Division Multiple Access (CDMA) system in which multiple users are allowed to transmit their own band-limited signal in the same bandwidth simultaneously. Every user is assigned a key dependent pseudo-noise code which spreads the energy of the signal. The pseudo-noise codes have low cross-correlation values and are unique to every user, so a receiver which has knowledge about the code of the intended transmitter, is capable of collecting (despreading) the desired signal [49].

Spread spectrum techniques for watermarking purposes have aroused a lot of interest. Many watermarking methods for images and video are based on ideas from spread spectrum radio communications, namely additive embedding of a (signal adaptive or non-adaptive) pseudo-noise watermark pattern, and watermark recovery by correlation [63].

Cox et al. first applied spread spectrum technology to watermarking [21]. He states that for a watermarking scheme to be robust, the watermark must be embedded into perceptually significant regions of an image's frequency domain, that is, low frequency components of the image, since perceptually insignificant components are likely to be affected by the distortions introduced by common signal processes. In order to insert a watermark into the most perceptually significant regions of spectrum without such alterations becoming noticeable, they originally conceive their approach by analogy to spread spectrum communications in which a narrowband signal is

transmitted over a much larger bandwidth such that the signal energy present in any single frequency is imperceptible. Similarly, the watermark is spread over many frequency bins so that the watermark energy in any single frequency is too small to be noticeable. Nevertheless, because the watermark detector knows the location and content of the watermark, it is possible to concentrate these weak signals into a single signal with high signal-to-noise ratio. However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins.

In this scheme, a watermark consists of a sequence of real numbers $X = x_1, x_2, \ldots, x_n$. Each value x_i is chosen independently according to $N(0,1)$, where $N(\mu, \sigma^2)$ denotes a normal distribution with mean μ and variance σ^2. The image is first globally DCT transformed. Then the n largest coefficients are selected and are grouped into a vector V. The watermark X is embedded into V according to:

$$V' = V(1 + \alpha X) \tag{2.5}$$

where α is a scale factor that adjusts the strength of the watermark. The larger the factor, the stronger the watermark. Accordingly, the watermark is more likely to be visible.

V' is then inserted back in place of V. The watermarked image is obtained by inverse DCT transforming the modified coefficients.

The watermark detector needs the original image to detect whether a given watermark is embedded or not. First, the possible watermark X' is extracted according

to the inverse formula of (2.5). Then the correlation value between X' and X is measured in the same way as described in section 2.1. If the value is above a predefined threshold, the given watermark is determined to be present; otherwise, it is not.

Error control coding for watermarking

In a communication system, error control coding is widely used for channel coding. Before sending a message through a channel, the message is error control coded, that is, some redundant information is added to the message, so that the receiver can correctly identify the message, even if it is partly corrupted by the channel noise and the bit error rate is greatly reduced. While in a watermarking system, an image can be viewed as a communication channel a watermark is going to transmit through and the different attacks can be treated as a noise signal the watermark may undergo. Before embedding, if the watermark is error control coded, there will be more chances for the watermark detector to recover the embedded watermark. Based on this idea, numerous authors applied error control codes to watermarking systems in order to improve the robustness of the watermark.

There are many error control codes available. One of the simplest and earliest, is the Hamming code, which ensures that any two coded messages always differ in at least three bits, and allows correction of single-bit errors. More sophisticated codes, such as BCH and trellis codes, allow a greater number of errors to be corrected. Some of the best-performing codes fall into the class of turbo codes, which a few researchers have begun using to encode a watermark message [135]. These codes are

often described in terms of methods of correcting symbol errors. Different codes are suitable for different types of errors. For example, random errors are well handled by Hamming codes, whereas burst errors (errors in groups) are better handled by BCH codes [25].

Watermarking with side information

Since Shannon introduced communications with side information at the transmitter, it has been discovered that in some types of channels it often does not matter whether the side information is available to the transmitter, the receiver, or both; its interference can be eliminated. Recently, a few researchers have begun to apply the lessons learned from communications with side information to watermarking schemes [25]. It is claimed that although all watermark embedders receive the unwatermarked image as input, many ignore this information when deciding on the watermark to be embedded. These blind embedders work by embedding a weak signal to the original image. Other embedders make partial use of the unwatermarked image to locally adjust the watermark strength. However, these embedders still ignore the effect of the original image on watermark detection [116]. In [26], it is observed a watermark embedder can be made more effective, if it is designed to exploit the information it has about the original image, together with knowledge of the watermark detector to be used [116]. This information serves as side information at the transmitter(watermarking embedder). The watermarking embedders in these systems are referred to as *informed embedders.*

In [116], the authors implement a general informed embedding algorithm, which follows the steps:

1. Extract a signal,v, from the unwatermarked image, I. The extraction process is denoted by $X(I)$. The extracted signal v is the side information and is assumed to be zero-mean independent and Gaussian [149].

2. The watermark is mixed with the side information and the original image through a *mixing function*,$f(v, w, I)$, to produce a new vector, v', that is perceptually similar to v, but is inside the watermark detection region around w.

3. Modify I to obtain I' using an *inverse extraction function*, $X^{-1}(v', I)$. The inverse extraction function produces the watermarked image that yields v' when the signal extraction process is applied to it, and which is perceptually close to I.

According to the mixing function $f(v, w, I)$, different embedding strategies can be explored to solve specific optimization problems such as:

1. Find the added mark that maximizes robustness, while keeping within a prescribed limit on perceptual distortion.

2. Find the added mark that minimizes perceptual distortion, while maintaining a prescribed level of robustness.

More complicated expressions of the problem, where they try to balance the trade-off between fidelity and robustness, are also possible.

2.4.3 Perceptual adaptive watermarking

Two important properties of watermarks are invisibility and robustness. To some extent, the two properties are contradictory, both determined by the strength of watermarks. If watermarks are stronger, they are more robust, but also they are more likely to be visible. Thus, a good compromise should be made between the two properties. One effective way to do this is to develop adaptive watermarking schemes that make use of the three properties of the human visual system: frequency sensitivity, luminance sensitivity and contrast masking. Such schemes should embed as strong watermarks as possible while at the same time make them invisible. Since invisibility is closely related to HVS, watermarking methods based on HVS is an important research area and draws lots of attention from watermarking researchers. In [25], the authors give a simple perceptually adaptive watermarking scheme. Given a fixed perceptual distance, a global embedding strength is adjusted automatically. A more sophisticated use of perceptual modeling is to locally scale the watermark, attenuating some areas and amplifying others [140]. In this scheme, a JND(Just Noticeable Difference) is computed for each DCT coefficient according to Watson's perceptual model [176]. The JND measures the amount by which a coefficient may be changed before leading to one JND, $\delta C(x, y)$. The watermark is then shaped according to the JNDs and embedded into the original image as follows:

$$C'(x, y) = C(x, y) + w(x, y) \tag{2.6}$$

where $|w(x,y)| < \delta C(x,y)$. Thus, the embedded watermark is as strong as possible while the distortions introduced by the watermark are invisible.

More complex algorithms do not only consider the sensitivity of the eye to the signal feature introduced by the watermark coefficients. They also consider the embedding context, i.e., the content of the signal in the surroundings of the watermarked coefficient [170]. In these algorithms, more elaborated masking models are used. Please refer to [169, 181] for details.

2.4.4 Geometric transforms resistant watermarking

There has been much emphasis on the robustness of watermarks to common signal processing operations such as compression and signal filtering. However, it has recently become clear that even very small geometric distortions can prevent the detection of a watermark [101]. This problem is most pronounced when the original un-watermarked image is unavailable to the detector. Several authors propose different methods to address this problem.

Kutter presents a scheme by giving the watermark a recognizable structure [86]. The watermark is encoded with a small, rectangular pattern, and embedded several times in the image in a tiled grid. Then, regardless of the watermark pattern, the grid structure can be recognized by looking at the auto-correlation function of the image, which will contain corresponding peaks. These peaks can be analyzed to identify any affine distortions.

Ruanaidh etc. present a watermarking method that embeds a watermark to the Discrete Fourier-Mellin Transform(DFMT) domain [147]. Since the DFMT has properties of rotation, scale and translation invariance, the proposed method is robust to rotation, scale, translation transformations and any combinations of them.

Based on this method, Perie etc. propose a scheme which use a template to recover the embedded information [132]. In this scheme, the watermark is composed of two parts, a template and a spread spectrum message containing the payload. The template contains no information in itself, but is used to detect transformations undergone by the image. Once detected, these transformations are inverted and then the spread spectrum signal is decoded. Unlike the algorithms which use log-polar and log-log-maps to find the transformation [133], they propose searching the space of all possible transformations. Since an exhaustive search leads to an intractable problem, they further prune the search space, which leads to robust detection of transformations reasonably quickly. Correspondingly, the watermark extraction process is divided into two phases: a template detection phase followed by a watermark decoding process. The extraction process does not require the presence of the original image. The problem with these methods is that they require the insertion and detection of two watermarks, one for detecting distortions and one to carry the data payload. Thus it is more likely that they reduce the image fidelity. Another problem is that, if all images are watermarked with the same template, they may be fragile to collusion attacks. An alternative method is proposed by Lin etc. [101], which is based on

developing a watermark that is invariant to geometric distortions, so that there is no need to identify and invert them. Other similar techniques include [110, 146].

2.4.5 Quantization watermarking

In spread spectrum watermarking schemes, it is desirable that the detector can detect the watermark without the knowledge of the original image. In this case, the original image has to be seen as noise, since it can not be subtracted from the suspect image. The performance of these blind watermarking schemes suffers from host-signal interference when correlating the watermark with the suspect image [113]. It is shown that if a watermark is embedded in a non-linear way, e.g. via quantization, the interference from the host signal can be eliminated [112]. In quantization watermarking schemes, a watermark is usually embedded by forcing a kind of relationship between some selected coefficients, so the detector can detect the watermark blindly without any interference from the host signal.

An early quantization watermarking method is proposed by [80] in which a watermark of a binary sequence is embedded. First, 8×8 DCT coefficients blocks are pseudo-randomly selected. Within each block b_i, two coefficients from the mid-frequency range are again pseudo-randomly selected. Then each block is quantized using the JPEG quantization matrix and a quality factor Q and the two selected coefficients are modified such that the relationship between their distance value and a prespecified strength factor denotes one watermark bit. This scheme is later extended by Benham [8] and Zhao [191] by enforcing a relationship between three instead of

two coefficients. This improvement allows to encode the watermark bit in a more robust way and provides a technique to skip blocks that are not suitable for watermark embedding.

Ohnishi etc. [129, 130] propose another watermarking scheme. In this scheme, a two-level multi-resolution representation is obtained using a Haar wavelet transform. All coefficients of the approximation image (LL subband) are selected and spread with a pseudo-random noise sequence. Then, the spread transform coefficients are segmented into blocks of size $B \times B$ and the Fourier transform is applied individually on each block to compute its frequency representation. To embed a single watermark bit, the DC coefficient of a block is uniformly quantized with a step size δ.

A different approach is taken in another algorithm proposed by Xie [188, 189]. Like the one in [130], the original image is wavelet decomposed to obtain a low-frequency approximation representation and the watermark is embedded solely in the approximation image. Each time, the coefficient trip of a non-overlapping 3×1 sliding window is selected and the three coefficients of the window are sorted in ascending order according to their magnitude. Then the range between the minimal and the maximal value is split into intervals of length:

$$\delta = \alpha \cdot \frac{2}{max - min} \tag{2.7}$$

Next, the median of the coefficient triple is quantized to become a multiple of δ in order to represent one bit of watermark information. Though the scheme is proposed

for image authentication applications, its robustness makes it also suitable for other purposes such as copyright protection. It is claimed in [112] that the robustness is mainly determined by the number of decomposition steps. Very good robustness can be achieved by employing a five-level wavelet decomposition using Daubechies-7/9 bi-orthogonal filters.

In [82, 84, 85], Kundur proposes a wavelet based quantizaton watermarking scheme. The Daubechies family of orthogonal wavelet filters is used to derive a multi-resolution representation of the image data. The decomposition level is 3 or 4. The algorithm pseudo-randomly selects locations in the detail subbands. Each time, a coefficient triple is selected from three distinct detail subbands of one decomposition level. The selected coefficient triple is sorted in ascending coefficients magnitude order. Then the median coefficient is quantized to represent the information of a single watermark bit. The quantization step size controls the robustness of the watermark. Coarser quantization will lead to more robust watermark embedding, however, this will also introduce more distortions.

Inspired by Costa's work [20] and other quantization watermark schemes, Chen introduces a class of quantization based watermarking methods called quantization index modulation(QIM) [12, 13, 14]. This class of techniques defines a number of quantization vectors which are indexed by the watermarking bit; a different quantization vector is used to embed a different watermark value and the watermark is embedded by mapping the pixel value to the nearest reconstruction point of the se-

lected quantization vector. The minimum distance between the sets of reconstruction points of different quantizers determines the robustness of the embedding.

In [12], a special case of QIM called dithered quantization for self-noise suppression is presented. Dithered quantizers are quantizer ensembles where the quantization cells and reconstruction points of every quantizer in the ensemble are shifted version of some base quantizer Q. The shift is given by a dither vector d. Dithered quantization is an operation in which a dither vector d of length L is added to the input x prior to quantization. The output of the subtractive quantization operation is denoted by:

$$s(x; m) = Q(x + d(m)) - d(m) \tag{2.8}$$

where x is the original signal and $s(x; m)$ is embedding function which can also be viewed as a collection of functions of x, indexed by the watermark m.

Since the subtractive dither quantization error does not depend on the quantizer input, if the dither signal d has a uniform distribution within the range of one quantization bin ($d(m) \in [-\delta/2, \delta/2]$), an expected squared error $e^2 = \delta^2/12$ can be derived [112].

The authors claim that QIM systems in general, and dither modulation in particular, offer significant performance advantages over previously proposed spread spectrum and low-bits modulation systems in terms of the achievable trade-offs among information-embedding rate, distortion and robustness. When the original signal is unknown, the QIM watermarking systems are more robust than spread spectrum wa-

termarking systems for a given rate and embedding introduced distortion, since the minimum distance of QIM systems is nonzero while that of spread spectrum systems is zero.

2.4.6 Relationship between watermarking and compression

From the above mentioned algorithms, we can see that digital image watermarking technology is closely related to image coding technology. For a watermark to be robust, it is usually embedded in the spectrum (transform) domain of an image, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Transform coding is now the de-facto standard in image and video coding, while the DCT (JPEG, MPEG-1, 2, H.261, H.263) and the DWT (JPEG2000) are mostly used. Accordingly, watermarking in the spectrum domain usually concerns with DCT, DWT and DFT. The domain choice depends on:

1. Watermarking system requirements. Different transform domains have their own particular properties, which we can make use of to design a watermarking system to meet special requirements. For example, for watermarking to be robust against geometric transforms, we can embed a watermark to the DFT domain; if you want to progressively detect a watermark, you can embed it to the DWT domain due to the hierarchical nature of the DWT.

2. The nature of the original image. Sometimes, the original image is compressed. Thus, it is desirable to embed a watermark to the compressed image without

decompressing it. Nowadays, different compression standards are in use, which are based on different transforms. For example, JPEG is based on DCT and JPEG 2000 is based on DWT. So, if the original image is a JPEG image, we had better apply a DCT domain watermarking scheme to it and if the original image is a JPEG2000 image, a DWT watermarking scheme is preferable. Thus, we do not need to decompress the original image from a domain and then transform it to another domain before embedding a watermark.

On the other hand, watermarking and compression are competing techniques. The first aims at adding invisible information in an image, while the second one attempts to remove redundant information. Although very robust watermarks that are resistant to current compression technologies have been developed, these algorithms may not survive forthcoming compression techniques, e.g. content-based ones. Thus, how to make a watermarking scheme robust against all current and future compression techniques is a promising research area.

2.5 Summary

This chapter describes the watermarking technology, including the general framework, watermarking requirements and applications, watermarking attacks. Finally, an overview of the current image watermarking algorithms is given.

Chapter 3

A Multi-resolution Image Watermarking Scheme

3.1 Introduction

Many spectrum domain watermarking schemes have been proposed in recent years, but they seldom deal with the problem of progressively detecting the embedded watermark. Although some wavelet domain watermarking schemes can progressively detect the embedded watermark, it may be desirable to do so in the DCT domain, since the DCT-based JPEG standard is widely used in today's image compression community. In some cases, due to limited network bandwidth, it is desirable to transmit the image progressively and thus detect the watermark progressively. This chapter addresses this problem by embedding the watermark in the DCT domain of an image in a multi-resolution way. The DCT coefficients are treated as wavelet

transform coefficients, and each watermark bit is embedded into a block of coefficients repeatedly layer by layer using a wavelet watermarking scheme, so that the embedded watermark can be detected progressively. Furthermore, for the scheme to be robust against geometric transformations, a second spread spectrum circular watermark is embedded in the DFT domain. Experimental results show that this scheme is robust against common signal processing procedures such as compression and additive noise, as well as geometric transformations such as rotation and translation.

3.2 Watermark embedding

The embedding procedure consists of two steps: DCT domain embedding and DFT domain embedding.

3.2.1 DCT domain embedding

Suppose the original image is of size $N \times N$.

1. The original image is split into blocks of size 8×8, and each block is DCT transformed;

2. A number of blocks are pseudo-randomly selected according to a key. In this way, the location of a watermark is secured, which increased the security level of the system. To embed the watermark sequence according to a key, the number of selected blocks matches the number of the watermark bits;

3. The coefficients of each selected block are reordered like three-level wavelet transformed coefficients. As shown in Figure 3.1, the 64 coefficients are organized into a sequence of one coarse image and 9 detail sub-band images. The coarse image contains only one coefficient, which is the DC coefficient of the image block. At each level, there are three sub-band images, corresponding respectively to the horizontal, vertical and diagonal sub-images.

0	1	4	5	16	17	18	19
2	3	6	7	20	21	22	23
8	9	12	13	24	25	26	27
10	11	14	15	28	29	30	31
32	33	34	35	48	49	50	51
36	37	38	39	52	53	54	55
40	41	42	43	56	57	58	59
44	45	46	47	60	61	62	63

Figure 3.1: 64 DCT coefficients as three level WT coefficients

4. A watermark bit is embedded into all possible coefficient triplets from the same locations of three distinct detail sub-bands of the same decomposition level (the coefficients of the same number in Figure 3.3). For each coefficient triple, it is embedded using a method similar to the one described in [81]:

1. The selected coefficient triple is sorted in ascending order: $f_1(m,n)$'$f_2(m,n)$'$f_3(m,n)$

2. The range of values between $f_1(m,n)$ and $f_2(m,n)$ are divided into bins of width:

$$\delta = \frac{f_3(m,n) - f_1(m,n)}{2Q-1} \tag{3.1}$$

where Q is a key-specified quantization variable.

3. $f_2(m,n)$ is quantized to the nearest value of vertical line segment shown in bold (to embed a 1) or dashed (to embed a 0) specified in Fig. 3.2;

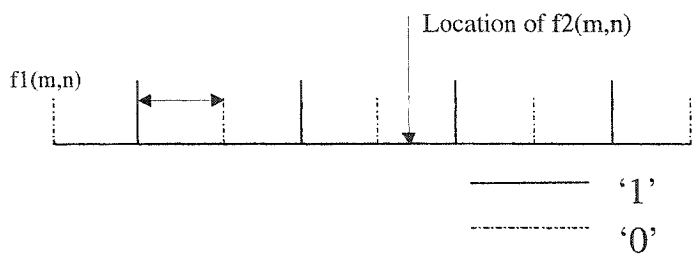


Figure 3.2: Embed a watermark bit

The same watermark bit is embedded repeatedly layer by layer, so that it can be detected progressively.

0	1	2	3	6	7	8	9
1	1	4	5	10	11	12	13
2	3	2	3	14	15	16	17
4	5	4	5	18	19	20	21
6	7	8	9	6	7	8	9
10	11	12	13	10	11	12	13
14	15	16	17	14	15	16	17
18	19	20	21	18	19	20	21

Figure 3.3: Coefficient triplets selected to embed a watermark bit

3.2.2 DFT domain embedding

1. The watermarked image after step 1 is discrete Fourier transformed according to:

$$F(u,v) = \frac{1}{N \cdot N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} I(x,y) e^{-j\frac{2\pi}{N}(ux+vy)} \tag{3.2}$$

$$M = |F(u,v)| \tag{3.3}$$

$$\phi = \angle F(u,v) \tag{3.4}$$

2. Given another key, generate multiple circular spread spectrum watermarks, each watermark obtained in a similar way as in [11].

$$W_i(u,v) = \begin{cases} w_{ik} & k = 0, \ldots, L_i, \qquad if\ u^2 + v^2 = R_i^2 \\ 0 & otherwise \end{cases}$$

where W_i is the i^{th} watermark , w_{ik} is the k^{th} element of W_i and R_i is the radius of the i^{th} insertion circle (Figure 3.4). The watermark on the smallest circle is the basic watermark and other watermarks are the repeated versions of the basic watermark.

3. Embed the watermarks into the magnitude of the Fourier spectrum.

$$M'(u,v) = M(u,v) + \alpha \times W_i(u,v) \tag{3.5}$$

Additionally, since the DFT magnitudes are symmetric, the DFT domain embedding process should keep this property. That is:

$$M'(u,v) = M'(N-u, N-v) \tag{3.6}$$

4. The watermarked image I' is obtained by applying the inverse Fourier transform of M' and ϕ.

$$I'(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} F'(u,v)e^{j\frac{2\pi}{N}(ux+vy)} \tag{3.7}$$

$$M' = |F'(u,v)| \tag{3.8}$$

$$\phi = \angle F'(u,v) = \angle F(u,v) \tag{3.9}$$

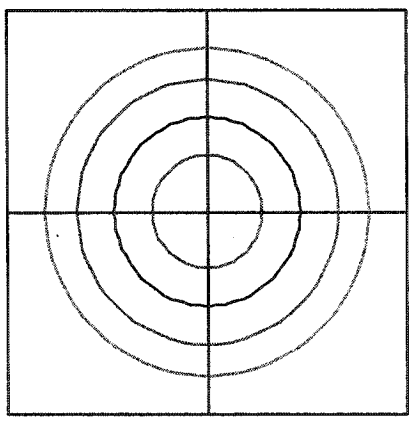


Figure 3.4: Multiple circular watermarks

The DFT domain embedding algorithm has been inspired by the scheme proposed by V.Licks [98], but it differs from [98] in that only one circle is used in [98], while this method introduces multiple circles, so it is more robust.

3.3 Watermark detection

The watermark extraction is just the reverse process of the watermark embedding process. It also consists of two steps: DCT domain detection and DFT domain detection. A final decision of whether watermarks exist or not is based on the result of the two detectors.

3.3.1 DCT domain detection

Since the watermark is embedded by forcing some relationships between coefficients, the watermark can be extracted directly from this relationship.

1. The suspect image is divided into 8×8 blocks and each block is DCT transformed;

2. A number of blocks that may contain the watermark is selected, according to the same embedding key;

3. The coefficients of each selected block are reordered like three-level wavelet transformed coefficients;

4. A watermark bit is extracted from a selected block. The numbers of 1s and 0s extracted from the coefficient triplet are counted; if the number of 1s is greater than that of 0s, then the watermark bit embedded in this block is 1, otherwise, it is zero.

5. Step 4) is repeated until all the watermark bits are extracted. After the watermark extraction, the normalized cross-correlation is used to measure the similarity of the extracted watermark W_1' and the original watermark W_1.

$$\delta_1 = \frac{\sum_{k=1}^{N} W_{1k}' \cdot W_{1k}}{\sqrt{\sum_{k=1}^{N} W_{1k}'^2 \cdot \sum_{k=1}^{N} W_{1k}^2}} \tag{3.10}$$

If δ_1 is greater than a pre-specified threshold, then the watermark is determined to be present in the image. Otherwise, it is not. So, for a watermarking scheme to be effective, it is very important to set the appropriate threshold that minimizes the number of false negative and false positive alarms. In order to set an appropriate one, we correlate the extracted watermark with 499 random watermarks and the embedded watermark. The threshold should be greater than the maximum correlation value between the extracted watermark and the random watermarks and be much less than that between the extracted watermark and the embedded watermark. Experimental results suggest a value of 0.3 should be used for the test image.

3.3.2 DFT domain detection

Like DCT domain detection, the correlation value is calculated between the extracted watermark and the embedding watermark. If it is above a given threshold, a watermark is embedded, otherwise, it is not. Before detection, the suspect image is transformed to the DFT domain.

1. Extract the watermark. According to the different embedding radius R_i, extract the watermarks that are put on the circles. Note that there may exist several

identical watermarks on one circle. Let us denote the k^{th} watermark on the i^{th} circle as W_{ik}

2. Use the same key to generate the embedding watermark W_2. The length of W_2 is L.

3. Correlate the extracted watermark with W_2.

One property of DFT is that rotation in the space domain results in rotation of the same angle in the DFT domain. Since the embedded watermark is circular, the rotation over the watermark causes some shifts of the watermark vector. So, we need to compute the cross-correlation between the embedding watermark and the extracted watermark for all possible shifts.

$$\delta_2 = \max_{i,k} \left[\frac{\sum_{m=0}^{L-1} W_{ik}(m) \cdot W_2(m)}{\sqrt{\sum_{m=0}^{L-1} W_{ik}^2(m) \cdot \sum_{m=0}^{L-1} W_2^2(m)}} \right] \tag{3.11}$$

3.4 Experimental results

In this section, some experimental results are demonstrated to show the effectiveness of the proposed watermarking scheme. Figure 3.5 shows the test image used in the experiments. The size of the image is 256×256 . For the DCT watermarking embedding, since the image is divided into a sequence of 8×8 blocks and one block is used to embed one watermark bit, the number of watermark bits should be less than 1024. In the experiments, the length of watermark is 400. For the DFT watermarking embedding, four watermarking radii (20,40,80,160) are used. Figure 3.6 is the

Figure 3.5: The original image

Figure 3.6: The watermarked image (PSNR = 36.23)

watermarked image. We can see that the watermark is invisible and the watermarked image looks almost the same as the original image.

3.4.1 Progressively detecting the watermark

To test that the watermark can be detected progressively, the watermarked image is manipulated as three watermarked images. The first image only keeps the DC and the first level detail sub-band coefficients; the second image keeps the DC and the first two level sub-band coefficients and the third keeps the DC and all the detail sub-band coefficients. In this case, the correlation values of the three extracted watermarks are close to 1, while the maximum correlation value of random watermarks is less than 0.2. This means an embedded watermark can be detected reliably even from a coarse watermarked image, which is desirable in a limited bandwidth network environment.

3.4.2 Robustness to common signal processing

First, white Gaussian noise of different strengths is added to the watermarked image to test the robustness of the method. Figure 3.7 shows the result. We can see that even for stronger noise, the embedded watermark has a high correlation value. Next, the watermarked image is compressed using JPEG. Figure 3.8 shows the plot of the correlation values vs. different quality factors for JPEG compression. When the quality factor is larger than 10, the corresponding correlation value is high enough to detect the watermark. This demonstrates that the scheme is very robust to JPEG compression

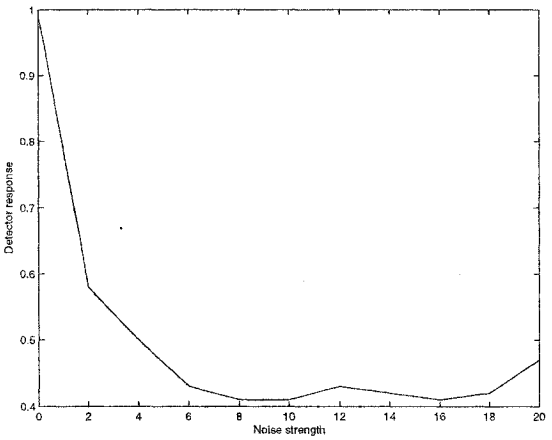


Figure 3.7: Results for additive white noise

3.4.3 Robustness to geometric transformations

Geometric transformations are very effective attacks to most watermarking algorithms. After applying geometric transformations to the watermarked image, most watermarking detectors are unable to detect the embedded watermark because the

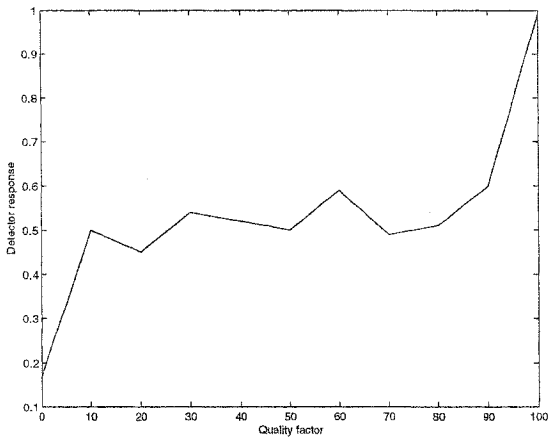


Figure 3.8: Result for JPEG compression

synchronization between the extracted watermark and the embedding watermark is lost. The proposed scheme adds a spread spectrum watermark to the DFT domain of an image to address this problem particularly.

Rotation is an important kind of geometric transformation. The watermarked image is now under 4° rotation attack. From Figure 3.10, we can see that the detection value of the embedded watermark (500th) is still above the maximum detection value of other random watermarks. So the embedded watermark can be easily detected.

Figure 3.9: The shifted watermarked image

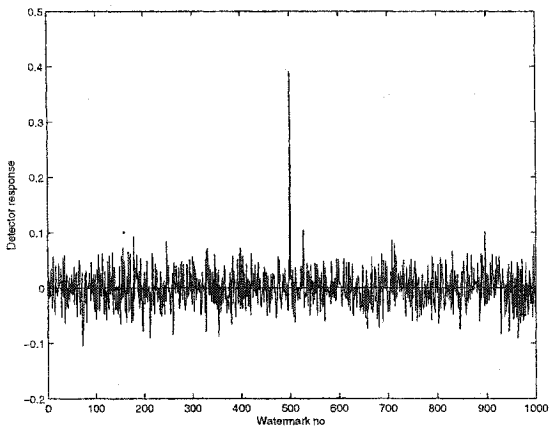


Figure 3.10: Results for rotation

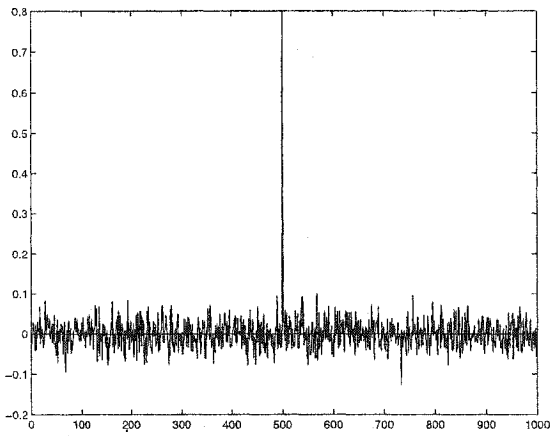


Figure 3.11: Results for translation

Translation is another kind of geometric transformation. Figure 3.9 is a watermarked image shifted down and right by 100 pixels respectively. Since the watermark is only embedded into the magnitude of the DFT domain and one property of DFT is that shifting in the space domain of an image only causes a shift in phase of the Fourier spectrum but does not change the magnitude, the watermark is not affected by this operation. This can be seen clearly from Figure 3.9, which shows the detection response of the embedded watermark.

3.5 Summary

In this chapter, a composite watermarking scheme that embeds two watermarks to different spectrum domains to address different problems is presented. The first watermark is added to the DCT domain of the image in a multi-resolution way so that it can be detected progressively. For the scheme to be robust against geometric transformations, another circular watermark is placed on multiple circles of the DFT spectrum. Experimental results demonstrate that this method can detect the embedded watermark progressively. Furthermore, this scheme is robust to common signal processing operations such as JPEG compression, additive noise and geometric transformations.

Chapter 4

A Novel Fractal Domain Watermarking Scheme

This chapter presents a digital watermarking scheme which adds a spread spectrum watermark in the fractal domain of an image during the process of fractal image coding. The watermark is embedded into an image by modifying scale factors of its fractal code. Experimental results show that this scheme is robust against JPEG compression, print, photocopying and scanning.

4.1 Introduction

Compared to the prolific watermarking schemes in the previously discussed spectrum domain, there are only a few watermarking schemes in the fractal domain. One is proposed by Puate [141], in which a digital signature is added to an image during

fractal image compression. For each range block, the search space for best matched domain block is limited to certain ranges according to different embedding bits. To retrieve the embedded signature, a fractal image coder is applied on the watermarked image again. In [96], Li took another approach. All isometric transforms are classified into two classes and the signature is signed by searching for best matched block using isometric transforms in different classes. There are some problems with the above two schemes. First, both apply some constrains during fractal coding, so the matched block is indeed not the best matched block. Second, the security of these schemes relies on the positions of range blocks that contain the watermark. If we change the fractal code of every range block, the watermark will be removed.

To address these problems, this chapter presents a novel scheme which employs spread spectrum watermarking in the fractal domain. Experimental results show that the proposed scheme is superior to Li's scheme.

4.2 Fractal image coding

Fractals were first introduced by B.Mandelbrot [111] who found that many objects have the property of self-similarity. Up to now, they have been widely used in physics, chemistry, biology, graphics, image processing, etc. In [6], Barsley applied fractals to image compression based on the self-similar property of images. He assumed that images can be closely approximated by a set of transformations of the same image. The set of transformations is called IFS (Iterated Function System), which is

determined by a number of parameters. Suppose we are given an arbitrary image. If we find a relatively small number of parameters, these parameters can represent the image. Then we only need to store these parameters instead of the whole image. This is the basic idea of fractal image compression. The following are some basic theorems related to fractal image compression [41].

4.2.1 The contractive mapping fixed point theorem

Let X be a complete metric space and $f : X \rightarrow X$ be a contractive mapping. Then there exists a unique point $x_f \in X$ such that for any point $x \in X$:

$$x_f = f(x_f) = \lim_{n \rightarrow \infty} f^n(x) \tag{4.1}$$

Such a point is called a fixed point or attractor of the mapping f . The mapping f is indeed the IFS of an image which consists of a number of transformations:

$$f = \bigcup_{i=1}^{n} f_i \tag{4.2}$$

If f_i for every i is contractive, their union, is also contractive. This theorem guarantees that if the IFS of an image is contractive, then applying the IFS on any initial image iteratively, we can get one and only one reconstructed image, that is, the fixed point of the IFS.

4.2.2 Collage theorem

With the hypothesis of the Contractive Mapping Fixed Point Theorem,

$$d(x, x_f) \leq \frac{1}{1-s} d(x, f(x)) \tag{4.3}$$

where s is the contractive factor less than 1 and d is the distance between the two points. The Collage theorem tells us that if we can find a f that makes x and $f(x)$ close enough, we guarantee that x and the attractor of the f, x_f, are close enough. Thus, the main problem of fractal image coding is to find a number of contractive transformations. After applying these transformations on the original image, the produced collage should be sufficiently close to the original image. Then, we can view the set of transformations as the IFS or fractal code of the original image. At the decoding end, the collage theorem guarantees that we can get the reconstructed image from the IFS.

Initially, the IFS was found manually, which cost lots of effort and time. Jacquin first developed an algorithm that can find a set of contractive transformations automatically [75]. In his work, the IFS was improved to LIFS (Local Iterated Function System), which takes advantage of the fact that a part of an image is similar to another bigger part of the image. The whole image is split into non-overlapped blocks and each block is approximated by applying one of the transformations on another bigger block. The fractal coding algorithm used in this paper is based on that work. The following section will describe the scheme in detail.

4.3 Watermark embedding and detection

The watermark is a sequence of random real numbers generated according to a key. These numbers are distributed according to a normalized Gaussian distribution. It is then embedded into an image during the process of fractal image coding. Before encoding, the image is first regularly segmented into non-overlapping $B \times B$ blocks, called Range blocks (R). At the same time, the image is split into overlapping blocks called domain blocks (D). All domain blocks are grouped into a domain pool. The goal of the encoding scheme is to find the best matched domain block for each range block so that the distance between the range block and the transformed best matched domain block is minimum. Usually, domain blocks are bigger than range blocks because we want the transformations contractive. For simplicity, the size of domain blocks is chosen as $2B \times 2B$.

To make parameters of the transformation as few as possible, the transformation, denoted as ϕ, is split into 3 transformations: contraction transformation c , isometric transformation t and gray transformation g.

$$\phi = c \circ t \circ g \tag{4.4}$$

Since the domain blocks are larger than range blocks, the contraction transformation makes the size of domain blocks the same as the size of range blocks.

The purpose of the isometric transformation is to change the orientation of the domain block so it matches the orientation of the range block. It is made up of

8 transformations including 4 reflections and 4 rotations. The gray transformation makes the pixel value of a domain block as close to that of the range block as possible. It has two parameters: luminance scaling and luminance shifting o.

$$R = s \cdot D' + o \tag{4.5}$$

where D' is a domain block that has been contracted and isometrically transformed. The two parameters are obtained by minimizing the distance between the transformed domain block and the range block.

$$s = \frac{n\sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i}{n\sum_{i=1}^{n} a_i^2 - (\sum_{i=1}^{n})^2} \tag{4.6}$$

$$. o = \frac{1}{n}(\sum_{i=1}^{n} b_i - s\sum_{i=1}^{n} a_I) \tag{4.7}$$

where n is the number of pixels in a range block, a_i and b_i are the pixel values of the domain block and range block respectively. Now, the watermark is embedded by modifying the s parameter as:

$$s' = s + \alpha \cdot w \tag{4.8}$$

and the o parameter is modified accordingly:

In Eq.(4.8), w is the embedding watermark and α is the factor that controls the strength of the watermark. So the modified gray transformation is:

$$R' = s' \cdot D' + o' \tag{4.9}$$

For each range block, the best matched domain block is found by searching all the domain blocks in the domain pool and by trying all eight isometric transformations.

In Li's algorithm [96], the authors simply classify eight isometric transforms into two classes for embedding digital watermark. Two reflections and two rotations belong to the first class and the other four isometric transforms belong to the second class. Based on the watermark bit, one of the class is chosen for searching the best matched domain block. Because of this constraints, the matched block found may not match the range block well.

The information we need to store is: the location of the best matched domain block, one of the 8 isometric transformations, and the parameters of the gray transformations: s' and o'. After the image is fractal encoded, given any initial image of the same size, applying the fractal code on the initial image iteratively, we can get the decoded image which contains the watermark. To detect whether an image contains a watermark or not, the same embedding key is needed to generate the given watermark. Then, the suspect image is fractal encoded to get a set of fractal codes. A correlation value between the embedding watermark and a series of scale factors is computed:

$$\delta = \frac{\sum_{i=1}^{n} s_i \cdot w_i}{\sqrt{\sum_{i=1}^{n} s_i^2 \cdot \sum_{i=1}^{n} w_i^2}} \tag{4.10}$$

If δ is greater than a pre-specified threshold, then the watermark is determined to be present in the image. Otherwise, it is not. So, for a watermarking scheme to be effective, it is very important to set the appropriate threshold that minimizes the number

of false negative and false positive alarms. In order to set an appropriate one, we correlate the extracted watermark with 1000 random watermarks and the embedded watermark. The threshold should be greater than the maximum correlation value between the extracted watermark and the random watermarks and be much less than that between the extracted watermark and the embedded watermark. Experimental results suggest a value of 0.15 should be used for the test image.

4.4 Experimental results

In this section, some experimental results are demonstrated to show the effectiveness of the proposed watermarking scheme. Figure 4.1 shows the test image used in the experiments. The size of the image is 256×256. The range block is of size 4×4, so the length of watermark is 4096. Figure 4.2 is the watermarked image. We can see that the watermark is invisible and the watermarked image looks almost the same as the original image.

In the following, some common signal processing techniques are applied to the watermarked image and the results are compared with the results of the algorithm in [139]. First, the watermarked image is JPEG compressed with different quality factors. Table 4.1 shows the detection value of the two algorithms versus the quality factor. From the table, we can see that both algorithms are well robust to JPEG compression, while our algorithm produces a higher detection value than Li's.

Figure 4.1: The original image

Figure 4.2: The watermarked image (PSNR = 37.45)

Table 4.1: Detection value vs. quality factor

Quality factor	10	20	30	40	50	60	70	80	90	100
Detection value (Li's)	0.08	0.13	0.15	0.3	0.38	0.46	0.52	0.73	0.85	0.98
Detection value (Our)	0.1	0.15	0.26	0.36	0.45	0.54	0.58	0.76	0.87	0.98

Figure 4.3 shows a cropped version of the watermarked image, in which only the central quarter of the image remains. Figures 4.5 and Figure 4.6 show the two watermark detectors' response to 1000 random watermarks. The 500th watermark is the embedded watermark.

Although the detection value is not as high as that in previous experiments, it is still higher than the maximum detection value of random watermarks. Ours is a little bit higher than Li's.

Figure 4.4 shows the watermarked image after printing, photocopying, then scanning and finally rescaling to a size of 256×256. Clearly the image suffers from several levels of distortion after each of the four processes. Figure 4.7 and Figure 4.8 show

Figure 4.3: The cropped image

Figure 4.4: The watermarked image after printing photocopying and scanning

the results. We can see that Li's scheme fails while the watermark in our scheme is still detectable.

4.5 Summary

In this chapter, a watermarking scheme that embeds a spread spectrum watermark in the fractal domain during the process of fractal image compression is proposed. The watermark is embedded by modifying the scale factors of IFS. Experimental results demonstrate that this method is robust to common signal processing operations such as JPEG compression and cropping, as also superior to Li's watermarking scheme under different image distortions.

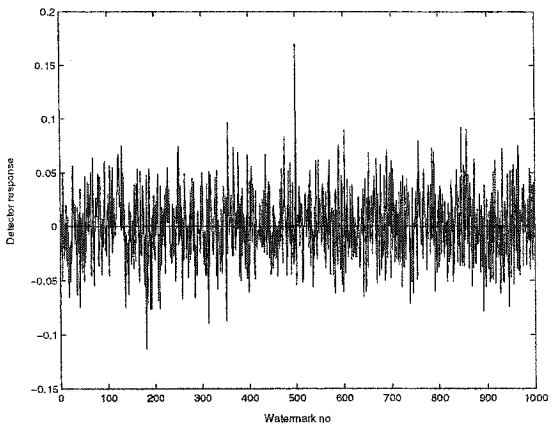


Figure 4.5: Results for cropping(Our scheme)

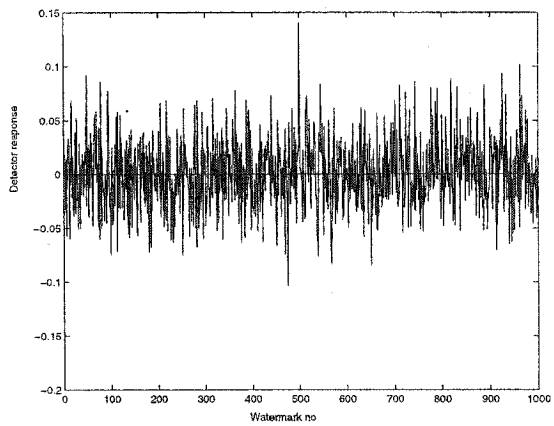


Figure 4.6: Results for cropping(Li'scheme)

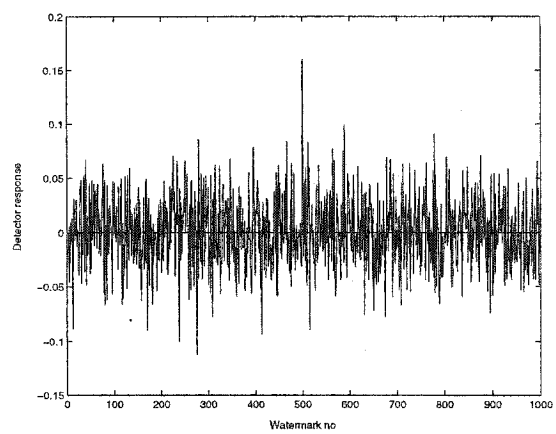


Figure 4.7: Detector's response (Our scheme)

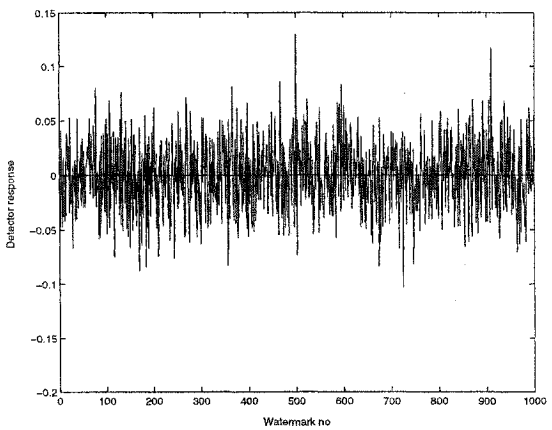


Figure 4.8: Detector's response (Li'scheme)

Chapter 5

Digital Image Watermarking for Arbitrarily Shaped Objects

5.1 Introduction

Many image watermarking schemes have been proposed in recent years, but they usually involve embedding a watermark to the entire image without considering a particular object in the image only which the image owner may be interested in. In some situations, the image owner may be more interested in an object of an image than the whole image, so it's desirable to embed a watermark in the object to protect it better. To address this problem, we propose a watermarking scheme that can embed a watermark in an arbitrarily shaped object of an image based on shape adaptive DCT. Before embedding, the image owner specifies an object of arbitrary shape that is of a concern to him. Then the object is transformed into the spectrum domain

using shape adaptive DCT and a watermark is embedded by modifying the spectrum coefficients in an additive way. Experimental results show that this scheme is robust to common signal processing procedures such as compression, median filtering and additive noise.

5.2 Shape adaptive DCT

Shape adaptive DCT, an extended version of the current block-based DCT, is usually used to encode an arbitrarily shaped object in an image block of size $M \times M$ [42]. The shape information of the object is assumed to be encoded separately and transmitted to the receiver for decoding the image. The basic concept of the proposed method is outlined in Figure 5.1 for coding an arbitrarily shaped image foreground segment contained within a 8×8 reference block. Figure 5.1-a shows an example of an image block segmented into two regions, foreground (gray) and background (light). To perform the vertical transform of the foreground, the length (vector size $N, 0 < N < 9$) of each column $j (0 < j < 9)$ of the foreground segment is calculated, and the columns are shifted and aligned to the upper border of the 8×8 reference block (Figure 5.1-b).

Depending on the vector size N of each particular column of the segment, a one dimensional DCT transform matrix DCT-N, where

$$DCT_N(p,k) = c_0 \cdot cos\Big[p \cdot (k + 0.5) \cdot \frac{\pi}{N}\Big] \qquad p,k = 0,1,...,N-1 \qquad (5.1)$$

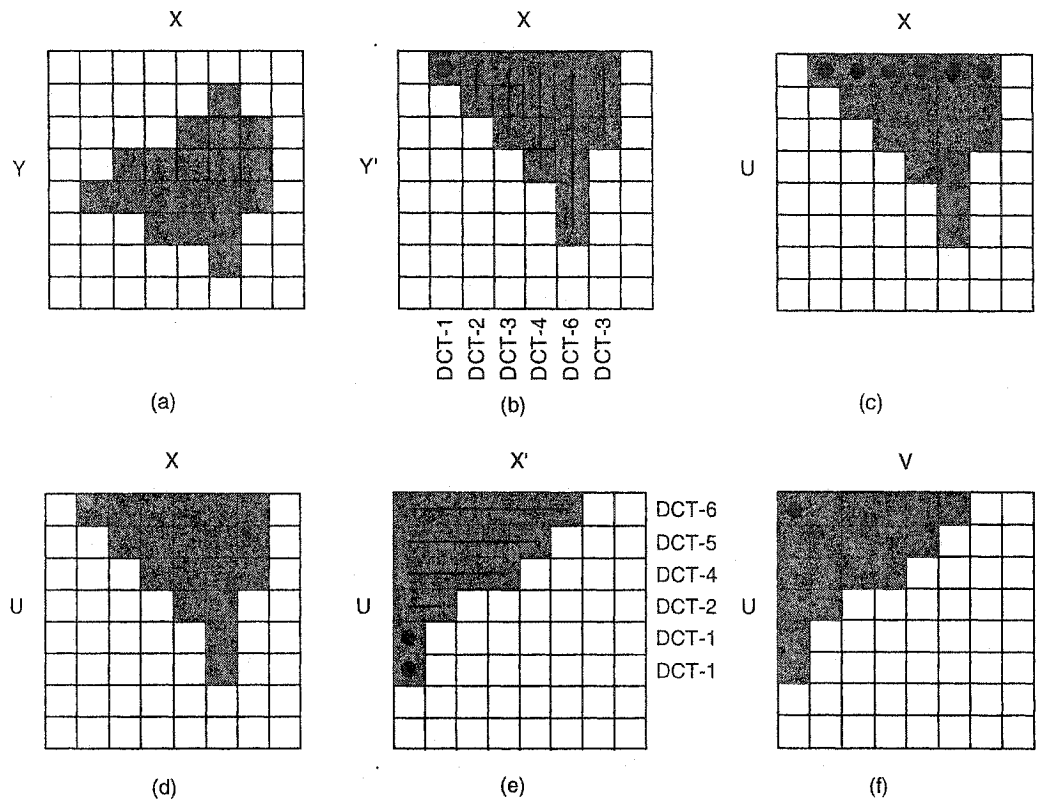


Figure 5.1: SA-DCT

containing a set of N DCT-N basis vectors is selected for each particular column and applied to the first N pels of the column and $c_0 = \sqrt{\frac{1}{2}}$ if $p = 0$; $c_0 = 1$ otherwise. The N vertical DCT-coefficients c_j for each column x_j are calculated according to the equation:

$$c_j = \sqrt{\frac{2}{N}} \cdot DCT_N \cdot x_j \tag{5.2}$$

For example, in Figure 5.1-b the right most column is transformed using DCT-3 basis vectors. After SA-DCT in the vertical direction, the lowest DCT coefficients

(DC values •) for the segment columns are found along the upper border of the 8×8 reference block (Figure 5.1-c).

Then, the horizontal DCT transformation is performed along the vertical SA-DCT coefficients with the same index (i.e., all vertical DC coefficients are grouped together and are SA-DCT transformed in the horizontal dimension). The length of each row is calculated, and the rows are shifted to the left border of the 8×8 reference block, and a horizontal SA-DCT adapted to the size of each row is calculated using the above two equations. This results in the final number of DCT-coefficients that is identical to the number of pixels contained in the foreground. Also, the coefficients are located in the upper left border of the reference block, and depending on the actual shape of the foreground, the remaining coefficients are concentrated around the DC coefficients. Figure 5.1-f shows the final location of the resulting DCT coefficients within the 8×8 image block.

At the receiving end, based on the same reference block, the decoder performs the Inverse SA-DCT in both the horizontal and vertical directions to get the original pixel values.

5.3 Watermark embedding and detecting

The proposed method consists of two parts: watermark embedding and watermark detecting. At first, the image owner needs to specify the object that he is interested in and a reference image is generated accordingly. The entire image is thus

segmented into foreground that contains the object and background. A watermark is then generated according to an embedding key. It consists of a sequence of random real numbers which are distributed according to a normalized Gaussian distribution. Based on the reference image, the selected object is transformed into frequency domain using the above SA-DCT algorithm. Let us denote the frequency coefficients as c and the watermark as w. The watermark is embedded according to:

$$c_w = c + \alpha \cdot w \tag{5.3}$$

where α is the factor that controls the strength of the watermark. For a watermarking scheme to be robust, it is desirable that α is a variable which is adjusted according to the properties of the human vision system or some other information. Recently, Cox proposed [26] a watermarking model: watermarking as communication with side information at the transmitter. He states that since both the original unwatermarked image and the watermark detector are available to the watermarking embedder, if the watermark embedder exploits this information when embedding a watermark, the embedding algorithm will be more effective. So α is set according to both the unwatermarked image and the watermarking detector. Suppose that the watermarking detector makes use of linear correlation to detect a watermark, that is:

$$\delta = \frac{1}{N} c_w \cdot w \tag{5.4}$$

If δ is above a pre-defined threshold, the image contains the watermark, otherwise, it does not. Now δ is set to a fixed value k that is much higher than the threshold.

$$k = \frac{1}{N} c_w \cdot w = \frac{1}{N}(c + \alpha \cdot w) \cdot w \tag{5.5}$$

From the above equation, we can get the value of α:

$$\alpha = \frac{N \cdot k - c \cdot w}{w \cdot w} \tag{5.6}$$

so the embedding equation becomes:

$$c_w = c + w \cdot \frac{N \cdot k - c \cdot w}{w \cdot w} \tag{5.7}$$

The watermarked image is obtained by applying the inverse SA-DCT to the watermarked DCT coefficients. Please note that the watermark is only in the selected object, other parts of the image don't contain the watermark. To detect whether an image contains a watermark or not, the same embedding key is needed to generate the given watermark w. Then, the object in the suspect image is separated according to the accompany reference image. After that, shape adaptive DCT is applied on the object. The coefficients that contain the embedded watermark are extracted and grouped to a coefficient vector c'_w. Suppose that the watermarked image is distorted

by random noise n, that is $c'_w = c_w + n$. A correlation value between c'_w and w is computed.

$$\begin{aligned}
\delta &= \frac{1}{N} c'_w \cdot w = \frac{1}{N}(c_w + n) \cdot w \\
&= \frac{1}{N}(c + w \cdot \frac{N \cdot k - c \cdot w}{w \cdot w} + n) \cdot w \\
&= \frac{1}{N}(c \cdot w + w \cdot w \cdot \frac{N \cdot k - c \cdot w}{w \cdot w} + n \cdot w) \\
&= \frac{1}{N}(c \cdot w + N \cdot k - c \cdot w + n \cdot w) \\
&= \frac{1}{N}(N \cdot k + n \cdot w) \\
&= k + \frac{1}{N} \cdot n \cdot w
\end{aligned} \tag{5.8}$$

Where k is a fixed value determined by the embedder. Since n is random, the correlation value between n and w is very small and δ is nearly equal to k.

5.4 Experimental results

In this section, some experimental results are demonstrated to show the effectiveness of the proposed watermarking scheme. Figure 5.2 shows the test image used in the experiments. The size of the image is 256×256. The selected object is shown in Figure 5.3. Figure 5.4 shows the watermarked image. Here, the fixed value k is set to 40. The difference image between Figure 5.2 and Figure 5.4 is shown in Figure 5.5. We can see that the watermark is only contained in the selected object.

Figure 5.2: The original image

Figure 5.3: The specified object

Figure 5.4: The watermarked image (PSNR = 53.51)

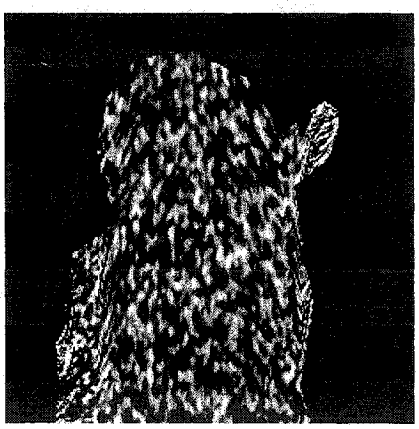


Figure 5.5: The difference image

In the following, some common signal processing techniques are applied to the watermarked image. First, the watermarked image is JPEG compressed with different quality factors. Figure 5.6 shows the plot of detection value versus the quality factor. Obviously, even if the quality factor is very small, the corresponding correlation value is not far from the fixed value 40 and it is high enough to detect the watermark. This demonstrates that the scheme is very robust to JPEG compression Then, white Gaussian noise of different strengths is added to the watermarked image to test the

robustness of the method. Figure 5.7 shows the result. We can see that even for stronger noise, the embedded watermark has a high correlation value.

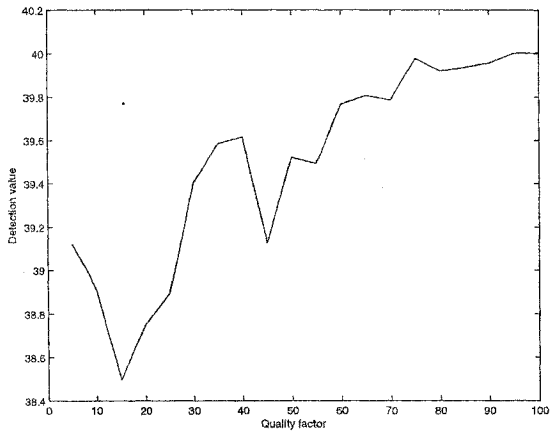


Figure 5.6: JPEG attacks

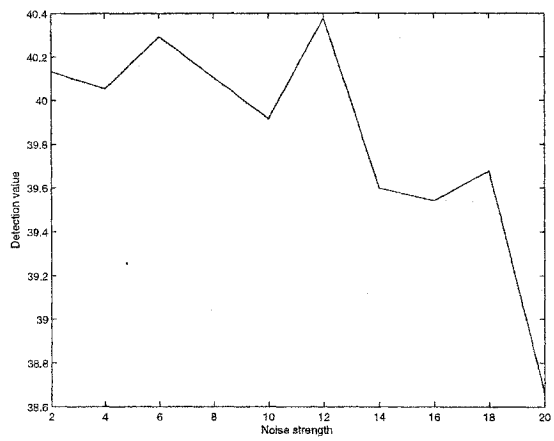


Figure 5.7: Noise attacks

Next, a $S \times S$ median filter is applied on the watermarked image. Table 5.1 shows the detection value versus different window sizes. We can see that the watermark is still detectable even after it is 5×5 filtered.

Table 5.1: Detection value vs. window size

Window size	1	2	3	4	5
Detection value	40.0	37.1	38.6	35.6	36.7

5.5 Summary

This chapter proposes a watermarking scheme that can embed a watermark to an arbitrarily shaped object in an image. Before embedding, the image owner specifies an object of arbitrary shape that is of a concern to him. Then the object is transformed into the spectrum domain using shape adaptive DCT and a watermark is embedded by modifying the spectrum coefficients in an additive way. Experimental results show that this scheme is robust to common signal processing procedures such as compression, median filtering and additive noise.

Chapter 6

A New Framework of Digital Watermarking Schemes

In this chapter, a new framework of digital watermarking schemes is proposed to address the problem of joint ownership verification for digital images, which has never been addressed so far. The secret sharing scheme, which is used in the proposed framework, is introduced. Finally, some related issues are discussed.

6.1 Limitations of previous work

In chapter 2, several digital image watermarking schemes are introduced, but they have one common problem: all of them only intend to protect the digital image from illicit users and none of them can protect the digital image from potential dishonest owners, if the digital image is created collaboratively by several owners.

In the real world, there are applications where there are more than one owner of an image. For example, several people from different companies collaboratively create and own a digital image. A photographer and an actor share the ownership of the actor's image taken by the photographer. A picture of several people is shared by these people, etc. In these cases, multiple owners need to share the ownership of an image. Besides, the owners will not trust each other. Another application will be in access control for an image created by multiple owners.

In the current watermarking algorithms, only one key is involved. The same key is used for both watermark embedding and detection. Anyone who holds the key and can pass the watermark verification is supposed to be the owner. But what happens if two or more people create an image collaboratively? With the current watermarking schemes, each of them is assigned the same key. Suppose one of them, call him A, sells the image secretly without the consent of others. When this is discovered, the other owners have no recourse, because the key A holds is enough to prove that he is the owner. Others who have the same key can not present enough evidence to prove that that the image was created by them jointly not by A alone. This is indeed a problem of joint ownership, which the current watermarking schemes fail to notice and address. Though in some watermarking schemes, there are multiple secret embedding keys involved [19, 121, 122, 123, 124], for example, one key for generating a watermark and other keys for encoding the watermark and for randomizing the embedding locations, the same keys are to be held by all joint owners, so the problem of joint ownership can not be solved. Some researches [139, 140] propose public key

watermarking methods which involve two different keys, a private key for watermark embedding and a public key for watermark detection. These methods only intend to solve the problem of key reuse. They do not solve the above mentioned problem either. In [175], the authors propose a watermarking scheme that protects the digital data from illegal copying, but this scheme mainly targets at identifying dishonest users who get the data legally and copy it illegally. It has no ways of dealing with possible dishonest owners, however.

6.2 Secret sharing schemes

In the real world, there exists an interesting situation: For a very important facility or location, such as a vault in a bank, it is desirable that any combination of several parties can gain access to it but not any individual party can do so [154]. The solution to this problem is called a secret sharing scheme. In this scheme, a secret is broken into several pieces called shares, so that certain subsets of those shares can reconstruct the secret. The secret is held by a trusted third party called a dealer. An entity given a share is called a participant.

There are many kinds of secret sharing schemes such as Shamir's threshold scheme, geometric threshold scheme, multilevel schemes, etc. Shamir's scheme [152, 192] is the basic secret sharing scheme. It is fast and is easy to be implemented by both software and hardware. We mainly use it in this thesis.

Shamir's secret sharing scheme is a (t, n) threshold scheme in which n shares are distributed to n participants so that:

1. The secret can be recovered from the knowledge of any t or more shares.

2. The secret can not be recovered from the knowledge of fewer than t shares.

Here, t is often regarded as the threshold of the scheme. Assume the dealer has a secret $K \in Z_p$, where p is a prime number that is larger than $n+1$ and Z_p is a set that contains all integers from 0 to $p-1$. The secret is distributed to the n participants $P_1, P_2, \cdots, P_n$ as follows:

1. The dealer chooses n distinct, non-zero elements in Z_p , denoted $x_i, 1 \leq i \leq n$. The values are public and are given to P_i.

2. The dealer secretly chooses independently at random $t-1$ elements of Z_p , $a_1, a_2, \cdots, a_{t-1}$.

3. For $1 \leq i \leq n$, the dealer constructs the following polynomial and computes $y_i = f(x_i)$.

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \tag{6.1}$$

4. For $1 \leq i \leq n$, the dealer gives the share y_i to P_i.

Since it is a fact that a polynomial $y = f(x)$ of degree $t-1$ is uniquely defined by t points (x_i, y_i) with distinct x_i , any t participants should be able to compute the value of K as a function of shares they collectively hold. Suppose that participants

$P_{i_1}, \cdots, P_{i_t}$ want to determine the Key. They pool their shares $y_{i_j} = f(x_{i_j})$ where $1 \leq j \leq t$ and $f(x)$ is the secret polynomial chosen by the dealer. Since $f(x)$ has degree at most $t-1$, $f(x)$ can be written as:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \tag{6.2}$$

where the coefficients $a_0, \ldots, a_{t-1}$ are unknown elements of Z_p and $a_0 = K$ is the Key. Since $y_{i_j} = f(x_{i_j})$, we can obtain t linear equations in the following matrix form:

$$\begin{pmatrix} 1 & x_{i_1} & x_{i_1}^2 & \ldots & x_{i_1}^t \\ 1 & x_{i_2} & x_{i_2}^2 & \ldots & x_{i_2}^t \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_t} & x_{i_t}^2 & \ldots & x_{i_t}^t \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_t} \end{pmatrix} \tag{6.3}$$

The determinant of the coefficient matrix A is:

$$detA = \prod_{1 \leq j \leq k \leq t} (x_{i_k} - x_{i_j}) \bmod p \tag{6.4}$$

Since all x_i are distinct, no item $x_{i_j} - x_{i_k}$ in this product is equal to zero. We have that $detA \neq 0$. Thus, the system has a unique solution over Z_p , which is determined by the formula:

$$f(x) = \sum_{j=1}^{t} y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \left(\frac{x - x_{i_k}}{x_{i_j} - x_{i_k}}\right) \tag{6.5}$$

and the key :

$$K = f(0) = \sum_{j=1}^{t} y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \tag{6.6}$$

Suppose we define

$$b_j = \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \tag{6.7}$$

Then

$$K = \sum_{j=1}^{t} b_j y_{i_j} \tag{6.8}$$

Now, what happens if only $t-1$ participants attempt to compute K. They will have a system of $t-1$ equations in t unknowns. Despite that they only need to figure out one of the unknowns, they will never solve the equations. Thus, $t-1$ participants can not get the key.

6.3 Proposed framework

Figure 6.1 shows the new proposed framework, which consists of four components: share distribution, watermarking embedder, share reconstruction and watermark detector.

6.3.1 Share distribution

In the framework, the secret to share is the watermark embedding key. Suppose an image is owned by n owners and they agree on that no less than k owners can jointly verify the ownership. According to a secret sharing scheme, the key is split into n

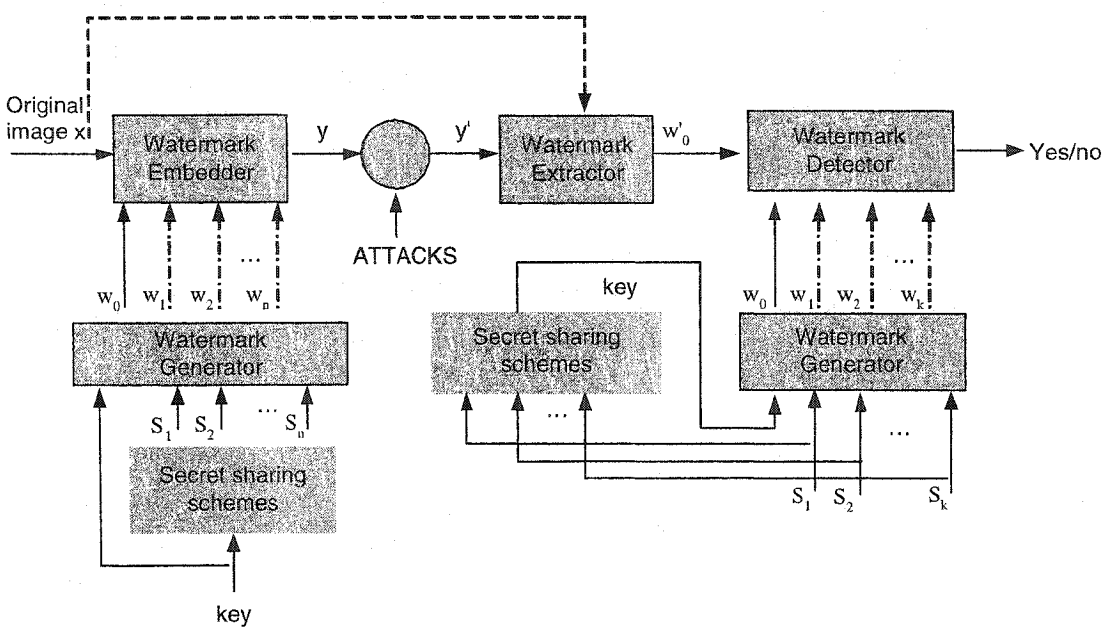


Figure 6.1: The proposed framework of a watermarking system

shares and every participant is assigned to a share. A dealer who is trusted by all participants may or may not be involved in the process and the watermark embedding key is known only to the dealer.

6.3.2 Watermark embedding

The secret key and the generated shares are fed into a watermark generator which generates one or multiple watermarks. Every owner makes his own contribution to the watermarks. The generated watermarks are embedded in a similar way as described in section 2.1.1.

6.3.3 Share reconstruction

To detect the watermarks, the secret key has to be recovered first. Only no less than k owners can put their shares together to recover the key. The recovered key and the shares are fed into the same watermark generator to generate the original watermarks.

6.3.4 Watermark detection

The watermarks are detected in a similar way as described in section 2.1.2. The difference is that multiple threshold may be set to differentiate the full ownership and partial ownership.

6.4 Discussions

6.4.1 Visual cryptography

Visual cryptography was first introduced by Naor and Shamir [127]. Based on a secret sharing scheme, it conceals an image in n noise like share images so that only when no less than k share image are superimposed, can the original image be recovered. For example, Figure 6.2 is an image to hide, which is split into two share images as shown in Figure 6.3 and Figure 6.4. The recovered image from the two share images is shown in Figure 6.5. Any share image alone can not reveal any information about the original image.

The image watermarking scheme based on the proposed framework is different from visual cryptography schemes. First, in the image watermarking scheme, the

secret to share is a key which determines the watermark to be embedded. After embedding, the watermarked image looks almost the same as the original image. While in visual cryptography schemes, the image itself is the secret to share and the share images look like noise images which can not reveal any information about the original image from appearance. Second, in visual cryptography schemes, the shared image can be recovered without any cryptographic computation and the recovered image contains some distortions. On the contrary, in watermarking schemes, we need to use a secret sharing scheme again to get the secret key and the key can be reconstructed perfectly. Third, the aim of visual cryptography is only to hide an image from plain view which the design objective of a digital watermarking scheme is to render the embedded watermark robust against all kinds of attacks.

In short, though both visual cryptography and image watermarking schemes are for image security by making use of a secret sharing scheme, they are different in terms of design objective and computing methods.

6.4.2 Secret sharing and watermarking schemes

First, not all secret sharing schemes can be applied to watermarking schemes. For those that can be used in a watermarking system, they can not be used in all current watermarking systems. We have to devise new watermarking schemes that can make use of a secret sharing scheme to solve the problem of joint ownership for digital images. In these new watermarking schemes, watermark embedder and detector have

to be carefully designed so that jointly created watermarks can be embedded in a special way and can be detected jointly for joint ownership verification.

Second, in the proposed framework, the secret sharing scheme has nothing to do with the robustness of the watermarking algorithms. In all watermarking schemes, there are keys involved to either determine the embedding watermarks or determine the location of the watermarks. So the security of the whole watermarking system is divided into two parts: the security of the keys and the robustness of the watermarking algorithm itself. As to the security of keys, we mean that the keys are secure enough so that it is very hard or impossible for an attacker to guess the keys. As to the robustness of watermarking algorithms, we mean that whether the watermark embedder and detector are well designed so that the embedded watermark is still detectable even after the watermarked image undergoes possible attacks. Of course, both parts are very important to a watermarking system. But in the watermarking community, the emphasis is put on the second security part: the robustness of a watermarking algorithm, under an assumption that the first security part of a watermarking system, that is, the security of keys, is ensured. Thus, watermarking researchers have tried their best to create effective watermarking algorithms where the watermarks as strong as possible are embedded and are still detectable after attacks. In our proposed watermarking schemes, the same assumption is made, that is, we assume that the security of keys and their shares are ensured. In a good secret sharing scheme, if the share holders do not have enough shares, they may never collude to get the missing share for reconstructing the shared secret. Thus, the secret sharing scheme

can increase the security level of the first part of the system, but it does not affect the security of the second part of a watermarking system. After watermarks are created jointly using a secret sharing scheme, this has nothing to do with the watermarking embedding and detection. So a secret sharing scheme is not related to the robustness of the watermarking scheme. Only the watermarking embedder and detector decide the robustness of a watermarking algorithm.

Third, in the proposed framework, we do not just simply apply a secret sharing scheme to one watermarking algorithm. In all secret sharing schemes, there are only two outcomes. When all required shares are present, the secret can be recovered; otherwise, it is not. As to digital image watermarking for joint ownership, when the embedding key can not be recovered, we may wish to decide whether the share holders partially own the image or have nothing to do with the image at all. Thus, we devised new watermarking algorithms where each owner makes his contribution to the watermarks and the watermark detector can detect each owner's contribution. In this way, the watermark detector will produce three outcomes: when enough shares are present, the detector will give a positive response and the share holders fully own the image; when no shares are present, the detector will give a negative response and the share holders do not own the image; when only part of the required shares are present, the detector will give a response in the middle and the share holders partially own the image. In a secret sharing scheme, the last two cases are combined into one case and we do not need to differentiate them. But it is desirable that, in a

watermarking scheme, we can differentiate the last two cases so that full ownership as well as partial ownership can be verified.

In short, to develop a digital watermarking scheme for joint ownership, we have to create smart watermarking embedders and detectors to embed and detect jointly created watermarks, under the assumption that keys and shares are secret. Furthermore, more complicated embedders and detectors are needed to be able to verify partial ownership.

6.4.3 Perfectness of a secret sharing scheme and the detection value

A secret sharing scheme is called perfect, if only authorized participants can recover the shared secret [74]. If the secret sharing scheme in the proposed framework is perfect, then in a watermarking scheme under the framework, only if all required shares are correct, can the secret key be recovered and thus also all the related watermarks. The watermark detector will give a high correlation value indicating full ownership assertion. If some of the shares are required, the secret key can not be recovered. The corresponding watermark and the incorrect share related watermark are not correlated with the corresponding right watermark. Thus, the watermark detector will give a response between positive and negative indicating partial ownership assertion. Finally, if no share is correct, no watermark is correlated to the right watermark and the watermark detector will give a negative response.

However, the above discussions are not always true, because the watermarked image may be distorted due to some image processing operations. In some case, even if all the required shares are correct and the secret key can be recovered, the watermark detector may still produce a low correlation value duo to the serious distortion of the watermarked image. Conversely, it hardly happens that given incorrect shares the watermark detector can produce a high correlation value. Thus, we should try to improve the robustness of our watermarking scheme.

6.4.4 Why a secret share scheme

The proposed watermarking scheme makes use of a secret sharing scheme to generate shares for each participant. Watermarks corresponding to each share and the shared secret are embedded so that both full ownership and partial ownership can be verified. The advantages of this kind of approach are:

1. The access structure is more flexible by applying a secret sharing scheme. If a secret sharing scheme is not used and each owner embeds his watermark spatially multiplexed into the image, we have no ways to control the authorized set in which participants can jointly verify the ownership. In the proposed scheme, for simplicity, we suppose there are only two owners. But in reality, there may be more participants. For example, suppose there are four participants (A,B,C,D). The access structure is (A,B) and (C,D). By applying a secret sharing scheme, we can easily generate shares for (A,B) and (C,D), so that only (A,B) and (C,D) can verify the ownership. If no secret sharing schemes are used

and each participant embeds his or her own watermark, even if the watermark detector can be designed to accept two watermarks, we have no way to make it only accept watermarks from (A,B) and (C,D). In this case, unauthorized sets such as (B,C) and (A,D) can verify the joint ownership as well, which is not desirable.

2. In the proposed framework, the secure secret based watermark is embedded to establish a secure connection between owners. If two owners pick their own watermarks and embed them without using a secret sharing scheme, each owner can choose randomly another watermark and embed it into locations where the other owner's watermark is. Later on, he can claim full ownership with his two keys. In the proposed scheme, this can not happen, because any owner alone can not figure out the secret shared based watermark, which makes significant contribution to the correlation value.

6.4.5 Private image watermarking for joint ownership

In private image watermarking schemes, the watermark detector needs the original image to detect the embedded watermark. If a secret sharing scheme where a dealer is involved is applied to private image watermarking schemes, there is a problem regarding who should keep the original image. There are three choices:

1. Both the dealer and the joint owners keep it.

2. Only the joint owners keep it.

3. Only the dealer keeps it and the joint owners are not allowed to keep it.

Here, we are considering multiple owners of an image who are not trusted by each other. Thus, it is not a good choice that the un-trusted owners keep the original image. If so, the potential dishonest owner can illegally distribute the original image instead of the watermarked one. To prevent this, only the dealer should keep the original image and the joint owners should not keep it.

6.4.6 The capacity issue of watermarking systems in the framework

In the new proposed framework, we give a general description of the watermarking system for joint ownership verification. If only the secret key based watermark is embedded, the related watermarking scheme is scalable, since the number of owners does not affect the number of watermarks. The problem with this kind of watermark schemes is that it cannot verify partial ownership as described in the following two chapters. If both the key related watermark and the share related watermarks are embedded, the watermarking scheme can verify partial ownership, but it is not scalable. How to make this kind of watermarking scheme scalable is still under study. In our following proposed algorithms, we assume that there are 2 or 3 owners, so the maximum number of watermarks is 3. There is enough capacity for three watermarks.

6.5 Summary

In this chapter, a novel framework of digital watermarking system which is based on a secret sharing scheme in cryptography is proposed. The framework mainly solves the problem of joint ownership verification for digital images. Related issues are discussed. In the following two chapters, some example watermarking algorithms based on this framework will be introduced to show the effectiveness of the framework.

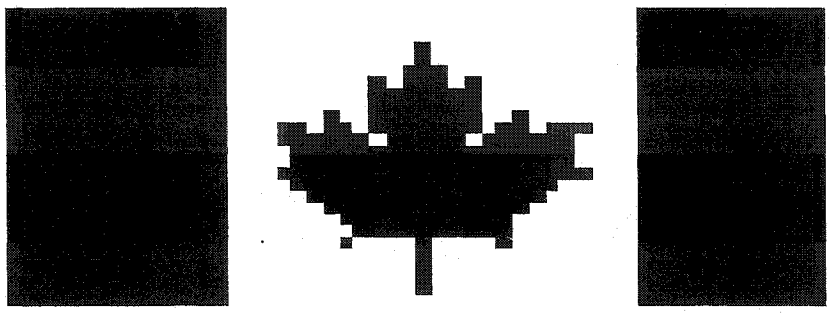


Figure 6.2: Original image to hide

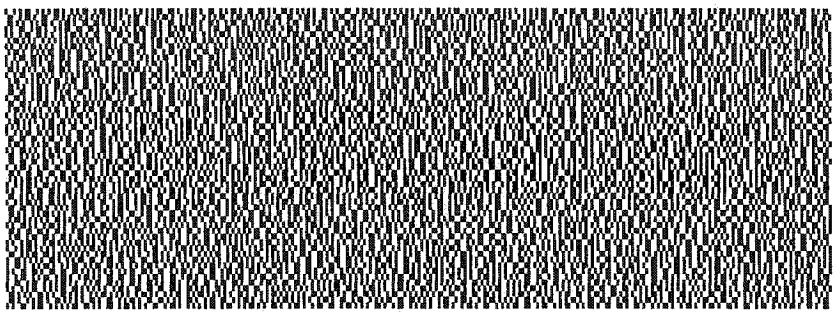


Figure 6.3: Secret share image no.1

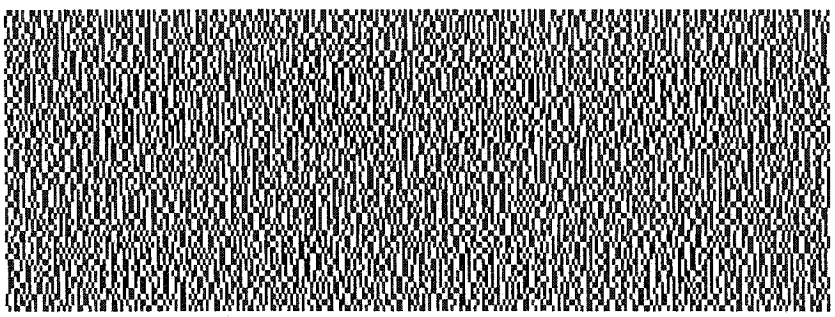


Figure 6.4: Secret share image no.2

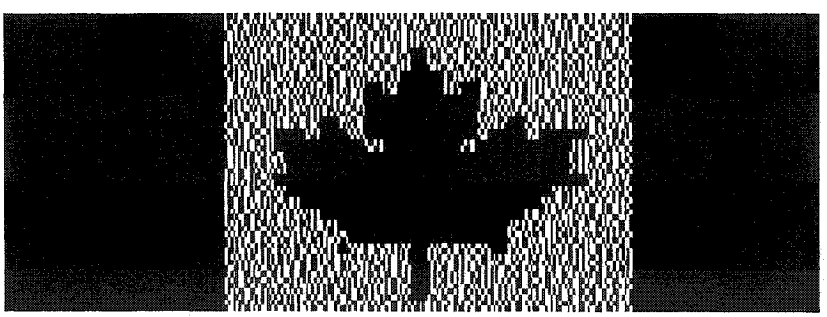


Figure 6.5: Recovered image

Chapter 7

Digital Image Watermarking for Joint Ownership

7.1 Introduction

To address the problem of joint ownership, this chapter introduces a secret sharing scheme to the watermarking system. Two algorithms are proposed based on the framework proposed in chapter 6. Both of them apply Shamir's threshold (2,2) scheme [154, 152] to wavelet domain watermarking algorithms for images. Suppose two people create an image jointly. Each of them is given a different key. The first algorithm embeds a watermark determined by the two keys to some middle band coefficients in the wavelet domain of the image, so that only when the two keys are put together can the ownership be verified. Any one of the keys alone can not be used to verify the ownership. The second algorithm is a modification of the first one. Three

watermarks are embedded to different locations in the wavelet domain of an image. For the watermark detection, two thresholds are set, so the watermark detector can verify partial ownership (any one of the two keys present) as well as full ownership (both keys present). Although in [174], a watermarking scheme based on visual secret sharing(VSS) is proposed, the scheme only intends to repeat the watermark throughout the image for avoiding the image cropping. The specified problem is not solved yet.

To our best knowledge, the problem of joint ownership has not been noticed and solved so far and the proposed schemes are the first ones to address it.

7.2 Watermark embedding and detection

Here, the secret to share is the key that determines the embedding watermark. The secret is shared between n participants who create an image collaboratively so that the watermark detector can give a positive response only when any $t(t \leq n)$ shares are present. In the following, two new algorithms are introduced to address the problem of joint ownership which the current watermarking schemes ignore. The first one applies Shamir's threshold (2,2) scheme to watermarking systems so that only when the two keys are put together can the ownership be verified. The second algorithm embeds three random watermarks to the wavelet domain of an image to verify partial ownership as well as full ownership.

7.2.1 Algorithm 1

Embedding

Before embedding, the parameters n and t have to be decided first. For simplicity, both of them are set to 2. Then, the dealer chooses a prime number p. For security reasons, p should be a large number. Since any secret numbers are from Z_p and all computations are done in Z_p, if p is not large enough, the secrets can be easily found by attackers through a simple brute force attack. After that, the dealer chooses a secret key k known only to him, a secret coefficient a that is used to construct the secret polynomial and two non-zero public elements (x_1, x_2). The two secret shares are computed according to the polynomial:

$$y_i = k + ax_i \bmod p \qquad 1 \leq i \leq 2 \tag{7.1}$$

The shares y_1 and y_2 are given to the two participants P_1 and P_2 respectively. Now, each participant P_i holds a pair (x_i, y_i), in which $x_i s$ are public and $y_i s$ are private. Later, when there is a need to verify the ownership, both y_1 and y_2 must be present to get the secret k.

The image to be watermarked is discrete wavelet transformed to the spectrum domain using haar wavelets. The wavelet separates an image into several sub-images corresponding to horizontal, vertical and diagonal details at each resolution level and a coarsest resolution level. An important issue in a watermarking system is where to put the watermark. Tradeoffs must be made between perceptual invisibility and

robustness. Obviously, a watermark that is put in the lowest pass band is more robust, since the coefficients in this band are less likely to be affected by distortions introduced by common signal processing operations. But it is likely to be visible because human eyes are more sensitive to the change of low frequency coefficients. On the contrary, human eyes are not sensitive to high frequency but the high frequency coefficients are more likely to be changed during transmission or by other signal processing operations. So watermarks in the high frequency band are invisible but not robust. Also, longer watermarks tend to be more robust. Considering this, the watermark is placed on a number of coefficients of high magnitude in all middle frequency bands between the lowest and the highest frequency band. Assume the image is L level wavelet transformed, resulting in $(3L + 1)$sub-images. Then, according to the secret k, a watermark W which is an i.i.d gaussian random vector, is generated:

$$W = \{w_1, w_2, \ldots, w_n\} \tag{7.2}$$

where n is the length of W. Then, the n highest magnitude wavelet coefficients in all the middle bands $(3L-3)$ are extracted and grouped into a vector X. The watermark is embedded into X in a similar way as in[21]:

$$X' = X(1 + \alpha W) \tag{7.3}$$

where α is a factor that controls the strength of the watermark. The insertion procedure is nonlinear so that the energy of the added watermark is proportional to the

coefficient's magnitude. When a coefficient is small, the energy of the watermark is also small, so the watermark is invisible; when a coefficient is large, the energy of the watermark is increased accordingly, so the watermark is more robust. The choice of the watermark length n is also very important. The longer the watermark, the more robust the system is. But longer watermarks may lead to visible distortions. So tradeoffs must be made between robustness and invisibility.

The watermarked image is then obtained by applying inverse DWT to the modified wavelet coefficients.

Detection

To detect the watermark, both participants have to pool their keys y_1 and y_2 to get the secret k. Then the watermark W determined by the k is generated. Next, both the suspect image and the original image are wavelet transformed. The possible embedded watermark W' is extracted according to the inverse embedding formula and correlation value between W' and W is computed:

$$\delta = \frac{\sum_i W'(i) * W(i)}{\sqrt{\sum_i W'(i)^2}} \tag{7.4}$$

If δ is above a predefined threshold T, the given watermark is decided to be present, otherwise, it is not. Thus, for a watermarking scheme to be effective, it is very important to set the appropriate threshold that minimizes the number of false negative and

false positive alarms. Since the detection value follows a standard normal distribution and the W and W' are not correlated, the probability of false alarms is:

$$p = \frac{1}{2\pi} \int_T^{\infty} e^{(-\frac{1}{2}t^2)} \tag{7.5}$$

In practice, an error probability of 10^{-10} is enough for many applications[193], so T is set to 6 ($p = \frac{1}{2\pi} \int_6^{\infty} e^{(-\frac{1}{2}t^2)} = 9.87 \times 10^{-10}$). Now, consider the following situations:

1. Both y_1 and y_2 are available.

2. Either y_1 or y_2 is available .

3. Neither of them is available

In the first case, the secret k can be constructed and the watermark detector will give a positive response. The two people holding the shares are supposed to be the joint owners. In the third case, suppose two people present two random numbers. For sure, the number that is computed from the two random numbers is not equal to k . Thus, the watermark detector will give a negative response and the two people are not the owners. In the second case, though one of the keys is present, k can not be found from it alone either and the watermark detector will produce the same result as in the third case.

7.2.2 Algorithm 2

Embedding

In some situations, we may wish to differentiate the above last two cases so that we can know whether a key holder is one of the owners or is not related to the suspect image at all. To achieve this goal, the second algorithm is developed. The second algorithm is similar to the first one except that three watermarks are involved. The first watermark W_0 is generated according to the secret k which is computed from y_1 and y_2.

$$W_0 = \{w_1, w_2, \ldots, w_n, w_{n+1}, \ldots, w_{2n}\} \tag{7.6}$$

The other two watermarks are generated according to the keys of the two participants respectively.

$$W_i = \{w_{i_1}, w_{i_2}, \ldots, w_{i_n}\} \qquad i = 1, 2 \tag{7.7}$$

where each element in W_0 and W_i is drawn independently according to a normalized gaussian distribution with zero mean and unit variance. Obviously the length of W_0 is twice the length of W_i. The image to be watermarked is wavelet transformed into the spectrum domain and the $4n$ largest coefficients in all middle bands are selected and grouped in the following form:

$$X = \{X_0, X_1, X_2\} \tag{7.8}$$

The length of X_0 is twice the length of the other two vectors. The three watermarks are embedded into the three vectors respectively, resulting X'.

$$X'_{0|1|2} = X'_{0|1|2}(1 + \alpha W_{0|1|2}) \tag{7.9}$$

$$X' = \{X'_0, X'_1, X'_2\} \tag{7.10}$$

Similarly, the watermarked image is then obtained by applying inverse DWT to the modified wavelet coefficients. .

Detection

The watermark detector is a little bit more complicated than the first one, because we have to consider all possible situations. Both the suspect image and the original image are wavelet transformed. The possible embedded watermarks W' are extracted according to the inverse embedding formula and are grouped together to form a vector:

$$W' = \{W'_0, W'_1, W'_2\} \tag{7.11}$$

The length of W'_0 is $2n$ while the length of the other two vectors is n. Furthermore, W'_0 is divided into two sub-vectors of equal length $W'_0 = \{W'_{01}, W'_{02}\}$. Two people pool their shares k_1, k_2 to compute the secret k. Then three watermarks W_0, W_1 and W_2 according to k, k_1, k_2 are generated respectively. The length of W_0 is twice the length of the other two watermarks. To make their length the same, a random watermark W_r of length n is generated. The random watermark is put at the end of W_1 and W_2

to form two new watermarks:

$W_1^s = \{W_1, W_r\}$ and $W_2^s = \{W_2, W_r\}$. W_0 is divided into two sub-vectors of the same length: $W_0 = \{W_{01}, W_{02}\}$. Now, all sub-vectors in the above three watermarks have the same length n. The correlation values between the three watermarks and vectors in W' are computed respectively:

$$\begin{aligned} \delta_0 &= \frac{W_0' \cdot W_0}{|W_0'|} = \frac{(W_0 + N) \cdot W_0}{|W_0'|} \\ &= \frac{W_{01} \cdot W_{01} + W_{02} \cdot W_{02} + N \cdot W_0}{|W_0'|} \\ &\simeq \frac{W_{01} \cdot W_{01} + W_{02} \cdot W_{02}}{|W_0'|} \end{aligned} \tag{7.12}$$

where N is the distortion the watermarked image suffers during the process of transmission. For simplicity, N is viewed as random noise. Since W_0 is i.i.d gaussian distributed, the correlation value between N and W_0 is close to zero. Similarly, we can get the other two values:

$$\begin{aligned} \delta_1 &= \frac{\{W_1', W_2'\} \cdot W_1^s}{|\{W_1', W_2'\}|} = \frac{\{W_1 + N, W_2 + N\} \cdot \{W_1, W_r\}}{|\{W_1', W_2'\}|} \\ &= \frac{W_1 \cdot W_1 + W_2 \cdot W_r + W_1 \cdot N + W_r \cdot N}{|\{W_1', W_2'\}|} \\ &\simeq \frac{W_1 \cdot W_1}{|\{W_1', W_2'\}|} \end{aligned} \tag{7.13}$$

and

$$\delta_2 = \frac{\{W_2', W_1'\} \cdot W_2^s}{|\{W_2', W_1'\}|}$$

$$
\begin{aligned}
&= \frac{\{W_2 + N, W_1 + N\} \cdot \{W_2, W_r\}}{|\{W_2', W_1'\}|} \\
&\simeq \frac{W_2 \cdot W_2}{|\{W_2', W_1'\}|}
\end{aligned} \tag{7.14}
$$

The detection value is the maximum of the above three values:

$$\delta = \max \delta_i \qquad i = 0, 1, 2$$

Now, let us discuss the above mentioned cases.

1. Both y_1 and y_2 are available

   In this case, the secret k can be correctly reconstructed and the three embedded watermarks can be generated perfectly. All the three correlation values should be high, while δ_0 is higher than δ_1 and δ_2 , since in Eq.(7.12) the whole watermarks contribute to the correlation value, while in Eq.(7.13) and Eq.(7.14) only one half of the watermark contribute to the correlation value. Thus, $\delta = \delta_0$.

2. Either y_1 or y_2 are available

   In this case, the secret k can not be correctly reconstructed and the according watermark is not the embedded watermark, so δ_0 is small. Only the watermark generated according to y_1 or y_2 is the right one, so either δ_1 or δ_2 should be high. Thus, $\delta = \delta_1$ or $\delta = \delta_2$.

3. Neither y_1 nor y_2 are available

   In this case, all the three embedded watermarks can not be found. The three

generated watermarks are random, so the corresponding three correlation values are all small. The detection value δ which takes one of the three values is also small.

From the above discussion, it is easily seen that the three cases are differentiated. Accordingly, two thresholds T_1 and T_2 ($T_1 < T_2$) are set. The watermarking detector takes the following decision rules:

1. If $\delta < T_1$, the two people who present their keys are not the owners at all.

2. If $T_1 < \delta < T_2$, the person who gives the key that contributes to the high detection value is one of the owners and s/he only partly owns the image.

3. If $\delta > T_2$, the two people are the owners and they fully own the image.

So, the watermark detector in the second algorithm can verify full ownership as well as partial ownership. In this paper, T_1 and T_2 are set to 17 and 6 respectively.

As we see, in the second algorithm, more watermarks are embedded to give more information about the owners, so it is more complex that than the first one. For full ownership assertion, the robustness of the two algorithms is almost the same. But for partial ownership assertion, we can not expect the same robustness, due to the contribution of shorter watermarks to the correlation value.

Figure 7.1: Original image

7.3 Experimental results

In this section, some experimental results are demonstrated to show the effectiveness of the proposed watermarking schemes. Figure 7.1 shows the test image used in the experiments. The size of the image is 256×256. Figure 7.2 and Figure 7.3 are the watermarked image (denoted as WM1 and WM2)using the two proposed algorithms. The watermark strength α is set to 0.1, the decomposition level is 4 and the watermark length n is 1000 and 500 in the two algorithms respectively. Clearly, the two watermarked images look almost the same as the original one, which shows that the embedded watermarks are invisible. As to the robustness test, since the framework of the proposed scheme is different from that of other watermarking schemes, the well known benchmark tools such as Stirmark are not applicable and are not used in the test.

Figure 7.2: Watermarked image(algorithm 1, PSNR = 39.33)

Figure 7.3: Watermarked image(algorithm 2, PSNR = 36.67)

7.3.1 Joint ownership verification

To demonstrate that the proposed schemes can verify the joint ownership, Figure 7.4 and Figure 7.5 show the detector's response under different conditions. In Figure 7.4, the 100th watermark is the watermark determined by the two shares and the detection value is high enough for a positive response. The 250th and the 400th watermarks are the watermarks from only one of the two shares alone. Clearly, the responses to the two watermarks are both negative, which means that any one of the two keys alone can not be used to verify the ownership.

In Figure 7.5, though the three watermarks are the same in the second algorithm as in the first one, the detector's responses are different. The detection value of the first watermark is the same, which means that the holders of the two keys are the joint owners. But the other two watermarks, which are from only one embedding key, behave differently from random watermarks. The detection values are lower than that of the first one but much higher than that of other random watermarks. This

means that the right key holder is only one of the owners and he does not fully own the image.

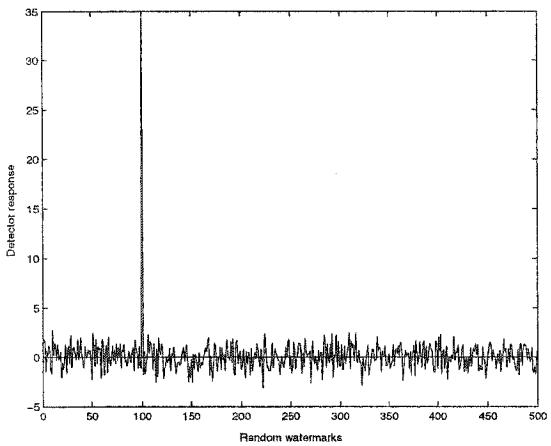


Figure 7.4: Detector's response to watermarked image(algorithm 1)

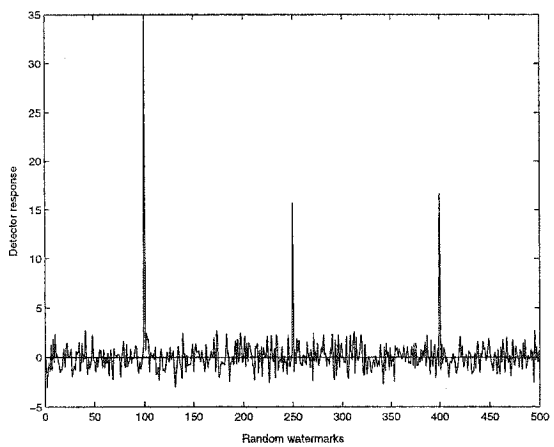


Figure 7.5: Detector's response to watermarked image(algorithm 2)

7.3.2 JPEG compression

The two watermarked images are JPEG compressed with different quality factors. Figure 7.6 and Figure 7.7 show the plot of detection value versus the quality factors

for WM1 and WM2 respectively. Obviously, for WM1, even if the quality factor is equal to 5 when WM1 is seriously distorted, the corresponding correlation value is still above the threshold . But for WM2, since there are two thresholds and we have to differentiate detection values to two kinds of watermarks, we can not expect the same robustness as for WM1. From Figure 7.7, we can see that when the quality factor is greater that 15, the two kinds of watermarks can be well separated.

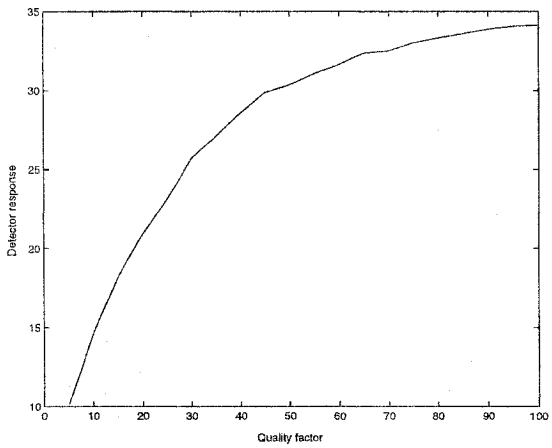


Figure 7.6: Detector's response to watermarked image after JPEG compression(algorithm 1)

7.3.3 Additive white noise

White Gaussian noise of different strengths is added to the watermarked images to test the robustness of the methods. Figure 7.8 shows the results for WM1. We can see that even for stronger noise, the embedded watermark has a high correlation value.

Figure 7.9 and Figure 7.11 show WM2 under noise attacks and the corresponding detection value. The strength of the noise is 30 and the watermarked image is very

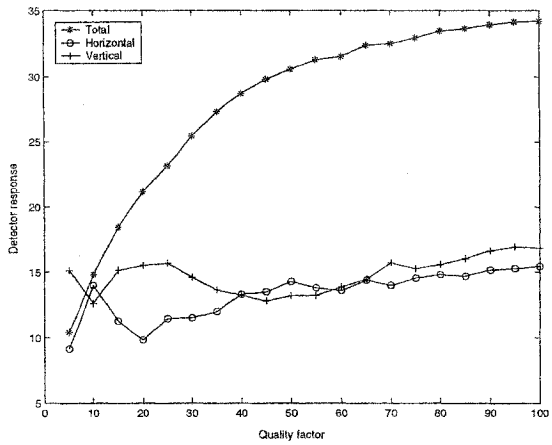


Figure 7.7: Detector's response to watermarked image after JPEG compression(algorithm 2)

noisy. In this case, the detection values to three watermarks are 17, 8 and 7, which are still above the corresponding thresholds and can be separated.

7.3.4 Median filtering

Figure 7.12 shows the test results for WM1. We can see that the watermark is still detectable even after it is 5×5 median filtered(Figure 7.10).

7.3.5 Cropping

Figure 7.13 shows a cropped version of the watermarked image WM1, in which only the central quarter of the image remains. Figure 7.15 shows the corresponding detector's response and we can see the watermarks can be detected.

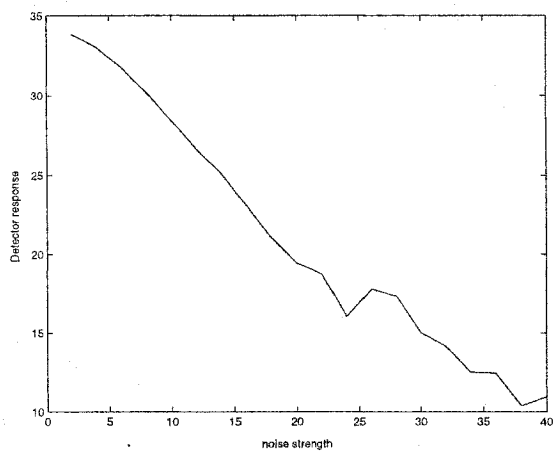


Figure 7.8: Detector's response vs. white noise strength(algorithm 1)

7.3.6 Histogram equalization

Histogram equalization is usually used for image enhancement. It is a kind of histogram modeling techniques that modifies the dynamic range and contrast of an image so that its intensity histogram has a desired shape. The watermarked image WM1 is histogram equalized by making use of a non-linear mapping which re-assigns the intensity values so that the attacked image (Figure 7.14) has a flat histogram. Figure 7.16 shows the detector's response. Though the detection value is not high, it is still above the threshold.

7.3.7 Intensity adjustment

The watermarked image is attacked by intensity adjustment. Intensities between 0.2×256 and 0.8×256 are mapped to intensities between 0 and 1×256 using a gamma correction value of 1.4 which means that the mapping is weighted toward

Figure 7.9: Watermarked image under noise attack(strength=30)

Figure 7.10: Watermarked image after being median filtered(5×5)

darker output values. The attacked image is shown in Figure 7.17. From Figure 7.18, we can see that the watermark is still detectable.

7.4 Summary

The problem of joint ownership for digital images has not been noticed and addressed so far. The two proposed watermarking algorithms in this chapter first resolve this problem by introducing Shamir's secret sharing scheme to the watermarking system. The first algorithm embeds a watermark determined by the two keys to all middle bands in the wavelet domain of the image so that only when the two keys are put together can the ownership be verified. Any one of the keys alone can not be used to verify the ownership. The second algorithm is a modification of the first one. Three random watermarks are embedded to different locations in the wavelet domain of an image. For the watermark detection, two thresholds are set, so the watermark

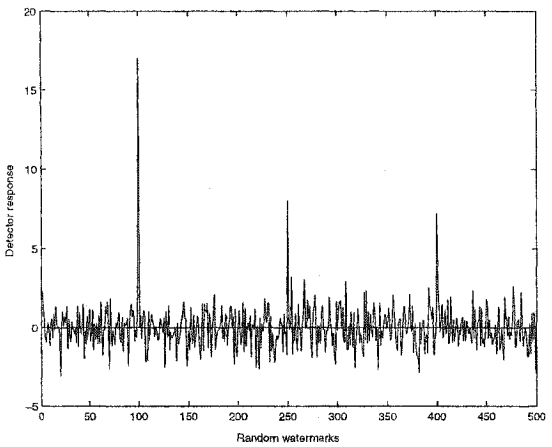


Figure 7.11: Detector's response to watermarked image after additive white noise attack(algorithm 2)

detector can verify partial ownerships as well as full ownership. Experimental results show that both algorithms have the desired properties: invisibility, robustness and reliable detection.

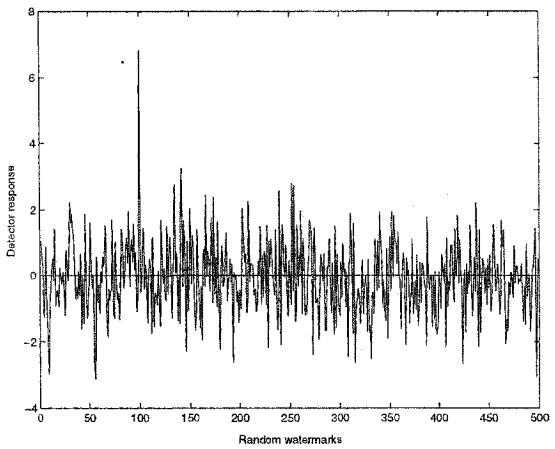


Figure 7.12: Detector's response to median filtered watermarked image

Figure 7.13: Watermarked image after cropping

Figure 7.14: Watermarked image after Histogram Equalization

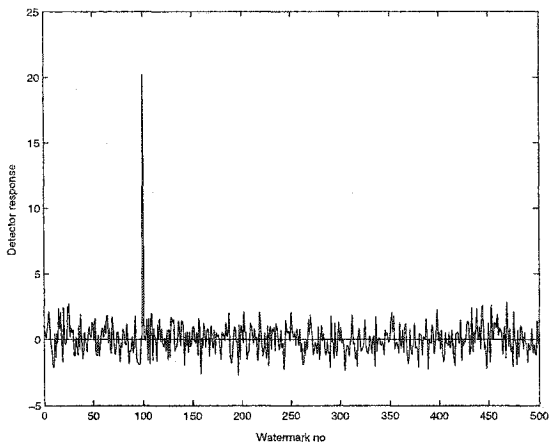


Figure 7.15: Detector's response to cropped watermarked image

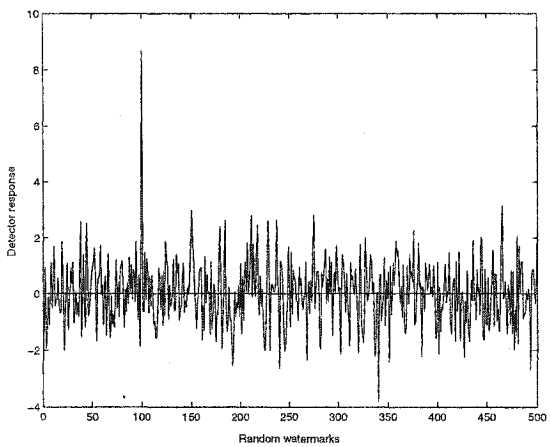


Figure 7.16: Detector's response to watermarked image after histogram equalization

Figure 7.17: Watermarked image after adjusting intensity

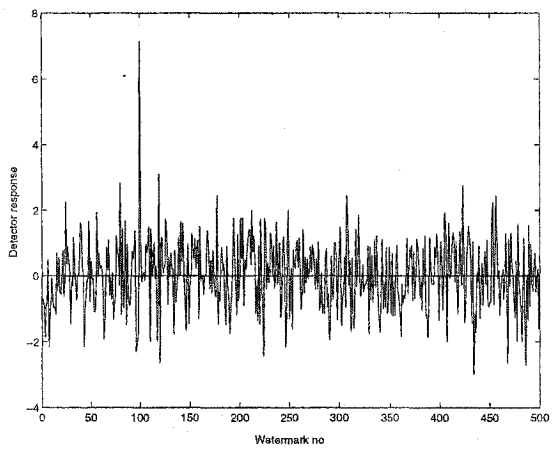


Figure 7.18: Detector's response to watermarked image after adjusting intensity

Chapter 8

Flexible Joint Ownership Verification for Digital Images

8.1 Introduction

In the digital image watermarking community, the problem of joint ownership has not been adequately addressed as we described previously. In our work in chapter 7, two watermarking algorithms based on Shamir's secret sharing schemes were proposed to address the problem of joint ownership verification. The problem is that, in the proposed scheme, it is assumed that every owner is equally important. Thus, the access structure of which owners can recover the embedding secret jointly is very strict. In reality, there are many situations where it is expected to have a more flexible arrangement for reconstructing the embedding secret. It is desirable that in

a watermarking scheme, given n owners, one can designate certain authorized groups of owners instead of any $t(t < n)$ owners who can use their shares to recover the key.

In this chapter, a novel algorithm that makes use of a generalized secret sharing scheme in cryptography to is proposed to address this problem. Given that multiple owners create an image jointly, distinct keys are given to only an authorized group of owners so that only when all the members in the group present their keys, can the ownership of the image be verified. Any owner alone can not verify the image ownership. In the proposed algorithm for joint ownership verification, there are three watermarks, the secrete key related watermark is more important the other two share related watermarks. The share related watermarks are equally important. Duo to the different importance of the three watermarks, the original is DWT transformed into several sub-images, the LL band is most significant, so the most important watermark is put in this sub-band. The other two watermarks are put in the LH and HL sub-bands, respectively. Experimental results show that the proposed algorithm is more robust than the algorithms in chapter 7.

8.2 Ito's generalized secret sharing scheme

Ito's generalized secret sharing scheme makes use of Shamir's threshold scheme to realize an arbitrary access structure [73]. An access structure is a family of sets of participants who are authorized to recover the secret, denoted by Γ. Any set from $\bar{\Gamma}$ presents a collection of participants who are unauthorized to recover the secret.

The family of maximal sets in Γ is denoted by $\delta^+\Gamma$. The scheme works as follows: Let Γ be an access structure. The dealer gets $t = |\delta^+\bar{\Gamma}|$ and utilizes a Shamir (t, t) threshold scheme to generate t shares. Then, for any unauthorized set ξ, $\xi \in \delta^+\bar{\Gamma}$, it assigns a distinct share to all participants who are not in ξ. For every access set $\alpha \in \Gamma$, it is shown that the number of distinct shares given to the participants is equal to t, while for every unauthorized set, $\xi \notin \Gamma$, the number of different shares given to its members is less than t. That is, the scheme satisfies the requirement of a secret sharing scheme, since the knowledge of at least t shares enables to recover the secret. The knowledge of less than t shares , however, does not allow an unauthorized set to recover the secret. For example, suppose there are four participants: P_1, P_2, P_3 and P_4. The access structure Γ is defined as:

$$\Gamma = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_4\}\} \tag{8.1}$$

To share a secret, the dealer gets:

$$\delta^+\bar{\Gamma} = \{\{P_1, P_4\}, \{P_2, P_3\}, \{P_3, P_4\}\} \tag{8.2}$$

Since $|\delta^+\bar{\Gamma}| = 3$, he applies Shamir's (3,3) threshold scheme to generate three shares: s_1, s_2, s_3. Then he assigns share s_1 to P_2 and P_3 (that do not belong to the unauthorized set P_1, P_4). Similarly, he also assigns s_2 to P_1 and P_4, s_3 to P_1 and P_2. Thus, every authorized set of participants has enough shares to reconstruct the secret, while unauthorized sets can not do so.

8.3 Watermark embedding and detection

In our previous work [54], Shamir's threshold scheme was exploited. The secret is shared between n participants who create an image collaboratively and each participant is equally important so that the watermark detector can give a positive response only when any $t(t \leq n)$ shares are present. However, in some situations, the participants may not be equally important and we may wish a more flexible watermarking scheme in which any specified groups of participants are authorized to recover the secret embedding key. For example, suppose there are four participants $\{A, B, C, D\}$ and the threshold t is equal to 3. In our previous scheme, any three of the participants, that is any three participants from a subset of $\{\{A, B, C\}, \{A, B, D\}, \{A, C, D\}, \{B, C, D\}\}$ are authorized. So there is only one access structure and the scheme can not authorize participants only from a generalized access structure such as the authorized set $\{\{A, B, C\}, \{B, C, D\}\}$ or $\{\{A, B, C\}, \{A, B, D\}, \{B, C, D\}\}$.

In the following, a novel algorithm is introduced to address the problem of secretly sharing the embedding key flexibly in a watermarking scheme, which has not yet been addressed. The proposed algorithm applies Ito's generalized scheme (3,2) to a watermarking system and several distinct watermarks are embedded in the spectrum domain of an image. The watermark detector is designed so that partial ownership as well as full ownership can be verified.

8.3.1 Embedding

Before embedding, the access structure must be determined first. For simplicity, we assume that there are three participants involved, say $\{A, B, C\}$. The access structure is $\Gamma = \{\{A, B\}\}$ and $\bar{\Gamma} = \{\{A, C\}, \{B, C\}\}$, that is, only A and B can jointly verify the ownership and no others can do so. Since $t = |\delta^{+}\bar{\Gamma}| = 2$, the dealer needs to use Shamir's (2,2) threshold scheme to generate two shares k_1, k_2 and the corresponding watermark embedding key k. Then the two shares k_1 and k_2 are assigned to all participants who are not in sets of $\bar{\Gamma}$. Thus, k_1 is given to B since $B \notin \{A, C\}$ and k_2 is given to C. To construct a secret polynomial, the dealer also needs to choose a secret coefficient a. Then two public coefficients x_1 and x_2 are computed according to the following secret polynomial and are assigned to A and B respectively.

$$k_i = k + ax_i \bmod p \qquad 1 \leq i \leq 2 \tag{8.3}$$

where p is a prime number. For security reasons, p should be a large number. Since any secret numbers are from Z_p and all computations are done in Z_p, if p is not large enough, the secrets can be easily found by attackers through a simple brute force attack.

Now, participants A and B hold a pair (x_i, k_i), in which $x_i s$ are public and $k_i s$ are private. Later, when there is a need to verify the ownership, both k_1 and k_2 must be present to get the secret k.

The image to be watermarked is l-level discrete wavelet transformed to the spectrum domain using Haar wavelets. The wavelet transform separates an image into several sub-images corresponding to horizontal (LH), vertical (HL) and diagonal detail (HH) sub-images and a coarse sub-image (LL). Since the wavelet coefficients are still correlated, Discrete Cosine Transform (DCT) is applied to all the sub-images except the HH sub-image. Then three i.i.d gaussian watermarks W_h, W_v and W_l, of which the lengths are N_h, N_v and N_l; are generated according to k_1, k_2 and the secret key k. Each watermark will make a contribution to the correlation value of the watermark detector so that both full ownership (both shares are present) and partial ownership (only on share is present) can be verified. The three watermarks will be embedded to the DCT domain of LH, HL and LL sub-images. To make a better tradeoff of the invisibility and the robustness, the watermarks are placed on a number of coefficients of high magnitude in the middle frequency bands in each sub-image (LL,LH,HL).

First, in each sub-image, the $(N_{l|h|v} + M_{l|h|v})$ largest coefficients are selected and grouped into vectors $X_i = (x_{i_1}, \ldots, x_{i_{M_i}}, x_{i_{M_i+1}}, \ldots, x_{i_{M_i+N_i}}), \qquad i = l, h, v$. Then, the corresponding watermark $W_i = (w_{i_1}, \ldots, w_{i_{M_i}})$ is embedded to X_i in a similar way as in [21]:

$$x'_{i_j} = \begin{cases} x_{i_j}(1 + \alpha w_{i_j}) & \text{if } M_i < j \leq N_i + M_i \\ x_{i_j} & \text{if } 1 \leq j \leq M_i \end{cases}$$

where α is a factor that controls the strength of the watermark. The insertion procedure is nonlinear so that the energy of the added watermark is proportional to the coefficient's magnitude. Since three watermarks are embedded instead of one,

the strength factor and the length of each watermark have to be selected carefully. Besides, the M_i highest magnitude coefficients are skipped and only the rest of the coefficients are modified to make a tradeoff between visibility and robustness.

The watermarked image is then obtained by applying the inverse DCT to the modified DCT coefficients, followed by applying the inverse DWT.

8.3.2 Detection

To detect the watermark, both participants A and B have to pool their keys k_1 and k_2 to get the secret k. Then three corresponding watermarks $W_{l|h|v}$ are generated and grouped into a vector W.

$$W = \{W_l, W_h, W_v\} \tag{8.4}$$

Next, both the suspect image and the original image are 1-level wavelet transformed, followed by DCT on LL, LH and HL sub-images. The three possible embedded watermark $W'_{l|h|v}$ are extracted according to the inverse embedding formula and grouped into another vector W'.

$$W' = \{W'_l, W'_h, W'_v\} \tag{8.5}$$

The correlation value between W' and W is computed:

$$\begin{aligned} \delta &= \frac{W' * W}{|W'|} \\ &= \frac{\{W'_l, W'_h, W'_v\} * \{W_l, W_h, W_v\}}{|W'|} \end{aligned}$$

$$= \frac{W'_l * W_l + W'_h * W_h + W'_v * W_v}{|W'|} \tag{8.6}$$

Now, consider the following three situations:

1. Both k_1 and k_2 are available.

2. Neither of them is available

3. Either k_1 or k_2 is available .

In the first case, the secret k can be correctly reconstructed and the three embedded watermarks can be generated perfectly. So the correlation value δ becomes:

$$\begin{aligned}
\delta_1 &= \frac{W'_l * W_l + W'_h * W_h + W'_v * W_v}{|W'|} \\
&= \frac{(W_l + N) * W_l + (W_h + N) * W_h + (W_v + N) * W_v}{|W'|} \\
&= \frac{W_l * W_l + W_h * W_h + W_v * W_v + N * W_l + N * W_h + N * W_v}{|W'|} \\
&\simeq \frac{W_l * W_l + W_h * W_h + W_v * W_v}{|W'|}
\end{aligned} \tag{8.7}$$

where N is the distortion the watermarked image suffers during the process of transmission. For simplicity, N is viewed as random noise. Since $W_l|h|v$ is i.i.d gaussian distributed, the correlation value between N and $W_l|h|v$ is close to zero. We can see that the correlation value will be high since all three watermarks contribute to it.

In the second case, suppose two people present two random numbers. For sure, the number that is computed from the two random numbers is not equal to k .

Accordingly, the three generated watermarks are random and the correlation value δ_2 should be small. Thus, the watermark detector will give a negative response and the two people are not the owners.

In the third case, suppose one of the keys, k_1, is present. k can not be found from it alone either. So the two watermarks W_l and W_v are random. The correlation value δ becomes:

$$\begin{aligned} \delta_3 &= \frac{W'_l * W_l + W'_h * W_h + W'_v * W_v}{|W'|} \\ &\simeq \frac{W'_h * W_h}{|W'|} \\ &\simeq \frac{W_h * W_h}{|W'|} \end{aligned} \tag{8.8}$$

The reason δ_3 is approximated the way it is is that k_1 is completely different from k, and hence the corresponding watermarks are not correlated.

In the above equation, since only one watermark contributes to the correlation value, δ_3 will be greater than δ_2 but less than δ_1.

As we see, in the proposed algorithm, three watermarks are embedded to give more information about the owners. If we only want to verify full ownership, we can only embed one watermark determined by the secret k and set a threshold T. The watermark detector can give positive responses only in the above first case with $\delta > T$. Thus, the last two cases can not be differentiated and partial ownership can not be verified. But for joint ownership verification, we may wish to differentiate the above last two cases so that we can know whether a key holder is one of the owners or

is not related to the suspect image at all. Thus, three watermarks are embedded and from the watermark detector's response to the above different cases, two thresholds T_1 and T_2 ($T_1 < T_2$) are set. The watermarking detector takes the following decision rules:

1. If $\delta < T_1$, the two people who present their keys are not the owners at all.
2. If $T_1 < \delta < T_2$, the person who gives the key that contributes to the high detection value is one of the owners and s/he only partially owns the image.
3. If $\delta > T_2$, the two people are the owners and they fully own the image.

Thus the watermark detector in the proposed algorithm can verify full ownership as well as partial ownership.

8.4 Experimental results

In this section, some experimental results are demonstrated to show the effectiveness of the proposed watermarking schemes. Figure 8.1 shows the test image used in the experiments. The size of the image is 256×256. Figure 8.2 is the watermarked image. The watermark strength α is set to 0.15 for the LL watermark and 0.3 for the other two watermarks, and the watermark lengths of the three watermarks are all set to 1000. Clearly, the watermarked image looks almost the same as the original one, which shows that the embedded watermarks are invisible. As to the robustness test, since the framework of the proposed scheme is different from that of other watermarking

Figure 8.1: Original image

Figure 8.2: Watermarked image (PSNR = 40.43)

schemes, well known benchmark tools such as Stirmark [137, 136] are not applicable and are not used in the test.

8.4.1 Verifying joint ownership

To demonstrate that the proposed schemes can verify the joint ownership, Figure 8.3 shows the detector's response under different conditions. In this figure, the 200th watermark is the watermark determined by the two shares and the detection value is high enough for a positive response, which means that the holders of the two keys are the joint owners. The 500th and the 800th watermarks are the watermarks from only one of the two shares alone. The detection values are lower than that of the first one but much higher than that of other random watermarks. This means that the right key holder is only one of the owners and he does not fully own the image.

Here, an important problem is how to set the thresholds. In conventional watermarking systems, there is only one threshold. Thus, we only need to set one suitable

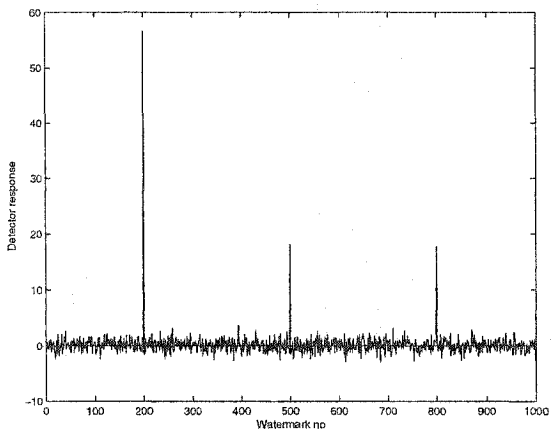


Figure 8.3: Detector's response to watermarked image

threshold to minimize the false negative alarms (no watermarks detected where a watermark is embedded) and false positive alarms (detecting a watermark where no watermarks are embedded). In the proposed scheme, a concept of joint ownership is introduced. To differentiate partial ownership and full ownership, two thresholds T_1 and T_2 are set. Thus, in addition to the above two mentioned false alarms, there are also other possible false alarms:

1. Both owners present two keys, but $T_1 < \delta < T_2$. This indicates that only one of the two people partially owns the image, where they are true owners. We call this a false FO negative alarm.

2. Only one owner presents a right key, but $\delta > T_2$. The owner only partially owns the image where the detector response indicates that he fully owns the image. We call this false PO positive response.

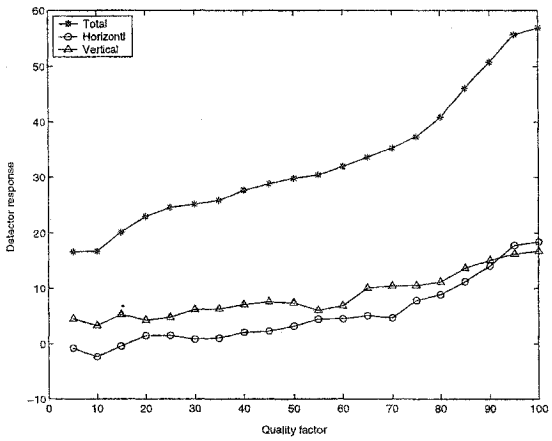


Figure 8.4: Detector's response to watermarked image after JPEG compression

To set the thresholds properly, in addition to minimizing the two conventional alarms, we also need to minimize the above two new alarms. Experimentally, the two thresholds are set to 17 and 8 respectively.

8.4.2 JPEG compression

The two watermarked images are JPEG compressed with different quality factors. Figure 8.4 shows the plot of detection value versus the quality factor. Obviously, for full ownership verification, even if the quality factor is equal to 5 when the watermarked image is seriously distorted, the corresponding correlation value is still above T_2. But for partial ownership verification, we can not expect the same robustness. From Figure 8.4, we can see that when the quality factor is greater that 40, partial ownership verification will be passed and the two kinds of curves can also be well separated.

8.4.3 Additive white Gaussian noise

White Gaussian noise of different strengths is added to the watermarked images to test the robustness of the methods, Figure 8.11 shows the results. We can see that even for stronger noise (Figure 8.5), the embedded watermark has a high correlation value. Both full and partial ownership assertion can be passed and separated. This shows that the proposed scheme is rather robust to Gaussian attacks.

Figure 8.5: Watermarked image under Gaussian noise attack(strength=40)

Figure 8.6: Watermarked image after being median filtered(5×5)

8.4.4 Additive salt & pepper noise

Salt & Pepper noise is added to the watermarked images. Figure 8.7 shows the attacked image under intensity value of 0.4. The intensity value specifies the percentage of image pixel values that are affected by the noise. From the figure, we can see that the watermarked image is highly noised. Figure 8.9 shows the detection results. Again, both full and partial ownership assertion can be passed.

Figure 8.7: Watermarked image under salt & pepper noise attack(intensity=0.4)

Figure 8.8: Watermarked image under multiplicative speckle noise attack(noise variance=0.1)

8.4.5 Multiplicative speckle noise

We now put the watermarked image under another kind of noise attack: multiplicative speckle noise attack. This attack adds the speckle noise to the watermarked image in a multiplicative way rather than an additive way in the two above mentioned noise attacks. Figure 8.8 shows the attacked image where the noise variance is 0.1. Figure 8.10 shows the results. We can see that both kinds of ownership can be verified.

8.4.6 Median filtering

Figure 8.12 shows the test results of median filtering. We can see that the full ownership verification can still be passed even after the watermarked image is 5×5 median filtered (Figure 8.6). But for partial ownership assertion, when the window size is greater that 2, it failed. How to improve its robustness is still under study.

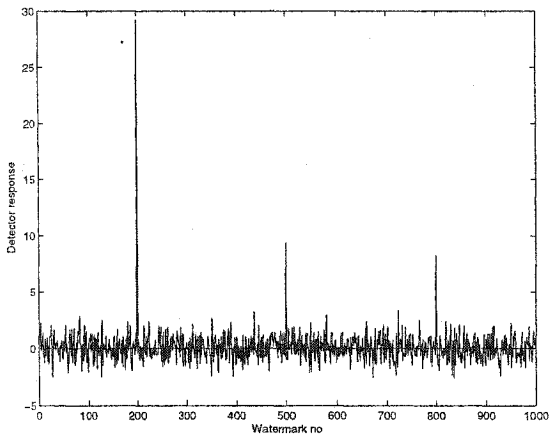


Figure 8.9: Watermarked image after additive salt & pepper noise attack

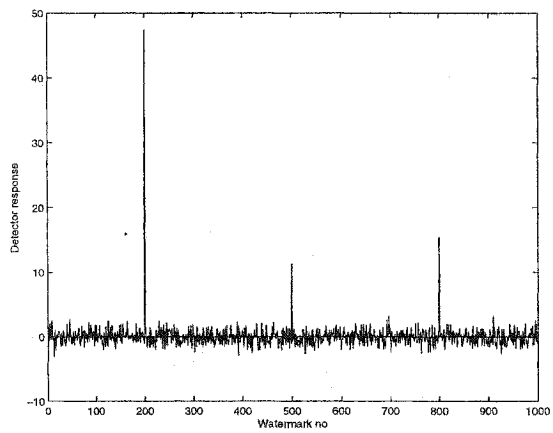


Figure 8.10: Watermarked image after multiplicative speckle noise attack

8.4.7 Histogram equalization

The watermarked image is histogram equalized by making use of a non-linear mapping which re-assigns the intensity values so that the attacked image (Figure 8.14) has a flat histogram. Figure 8.16 shows the detector's response. The detection values are very high and can be separated.

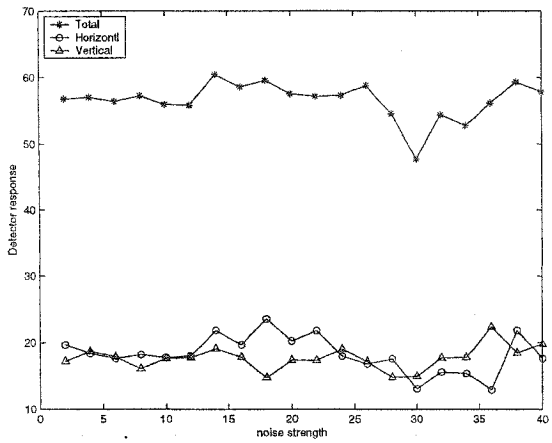


Figure 8.11: Detector's response to watermarked image after additive white noise attack

8.4.8 Intensity adjustment

The watermarked image is attacked by intensity adjustment. Intensities between 0.2 x 256 and 0.8 x 256 are mapped to intensities between 0 and 1 x 256 using a gamma correction value of 1.4 which means that the mapping is weighted toward darker output values. The attacked image is shown in Figure 8.17. From Figure 8.19, we can see that the watermark is still detectable.

8.4.9 Cropping

Figure 8.13 shows a cropped version of the watermarked image , in which only the central part of the image remains. Figure 8.15 shows the corresponding detector's response and we can see the watermarks can be detected and separated.

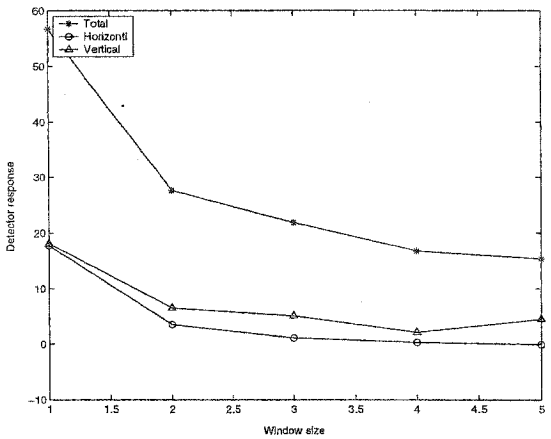


Figure 8.12: Detector's response to median filtered watermarked image

Figure 8.13: Watermarked image after cropping

Figure 8.14: Watermarked image after Histogram Equalization

8.4.10 Scaling

Scaling is a kind of geometrical transformations. The watermarked image is scaled from 256 × 256 to 240 × 240 and then scaled back. Figure 8.18 shows the resulting image. From Figure 8.20, we can see that though the three detection values are not as high as those in the above tests, the watermarks are still detectable. However, for

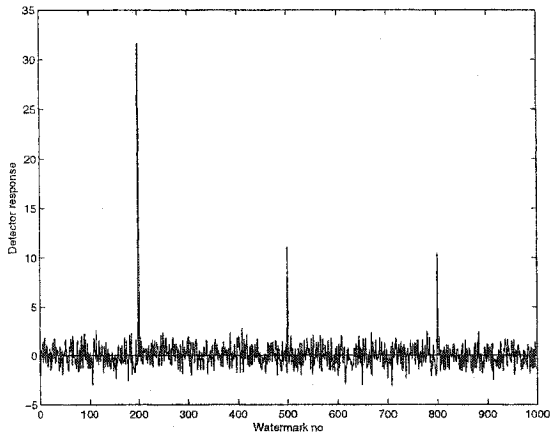


Figure 8.15: Detector's response to cropped watermarked image

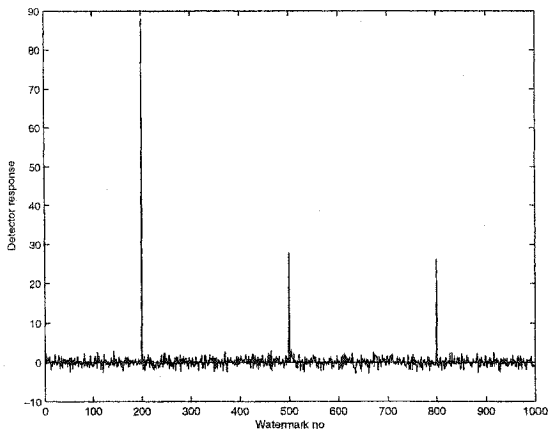


Figure 8.16: Detector's response to watermarked image after histogram equalization

large scale value, the test will fail. How to improve the robustness against this kind of attack is still under study.

8.4.11 Rotation

Rotation is another important kind of geometric transformations. Figure 8.21 shows the watermarked image after rotating counter clockwise by 0.1°. Though we can only see a little bit difference, only one watermark can be detected. In this case, we

Figure 8.17: Watermarked image after intensity adjustment

Figure 8.18: Watermarked image after scaling

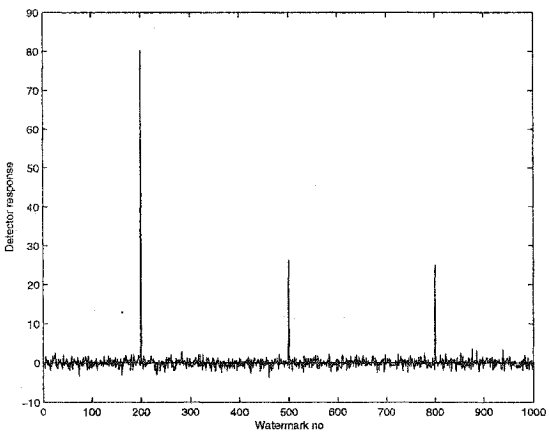


Figure 8.19: Detector's response to watermarked image after intensity adjustment

can only verify full ownership. Future work will focus on how to verify the partial ownership in this case.

8.5 Summary

In this chapter, a novel watermarking algorithm is proposed to address the problem of flexible joint ownership verification for digital images, which has been seldom noticed

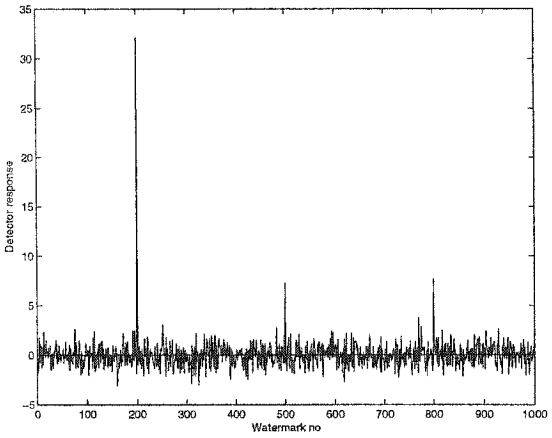


Figure 8.20: Detector's response to scaled watermarked image

Figure 8.21: Watermarked image after rotation

and addressed so far. By introducing Ito's generalized (3,2) secret sharing scheme to the watermarking system, the access structure can be arbitrarily specified so that the secret embedding key can be shared by several participants in a more flexible way. For the watermark embedding, three random watermarks of equal length are embedded to the DCT domain of three 1-level wavelet transformed sub-images. For the watermark detection, two thresholds are set, so the watermark detector can verify partial ownerships as well as full ownership. Experimental results show that both

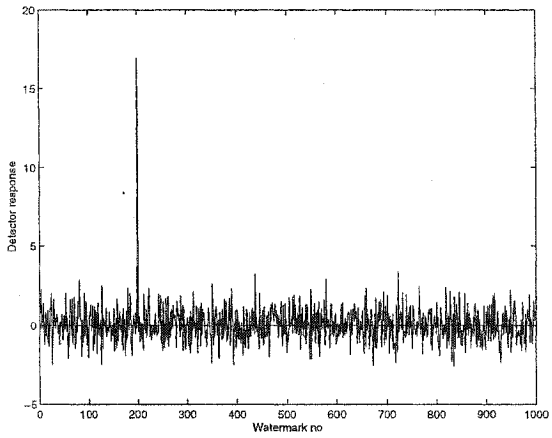


Figure 8.22: Detector's response to watermarked image after rotation

algorithms have the desired properties: invisibility, robustness and reliable detection. In the algorithm, there is a dealer involved. The dealer knows everything. Future work will focus on how to share the watermarking key without a dealer, as well as how to increase the robustness of partial ownership assertion.

Chapter 9

Conclusions

In this thesis, a couple of novel algorithms are proposed to address some problems of ownership verification for digital images. For single ownership verification, three watermarking schemes are proposed to address the problem of how to detect a watermark progressively while at the same time be robust to geometrical transformations, how to embed a watermark in the fractal domain and how to embed a watermark into an object in an image instead of into the whole image. For joint ownership verification which has never been noticed and addressed, a novel framework of the watermarking system that makes use of a secret sharing scheme is proposed. Based on this framework, several new watermarking algorithms are proposed where the secret watermark embedding key is split into shares and each owner holds one share. Multiple watermarks contributed by each owner are embedded into the spectrum domain of the image and multiple thresholds are set so that the watermark can verify joint ownership as well as partial ownership. To the best knowledge of the author,

the problems of joint ownership has not been addressed so far and the watermarking schemes proposed are the first ones to address them. Table 9.1 gives a summary of the robustness of the proposed watermarking schemes.

Table 9.1: Summary of the proposed algorithms' robustness

Watermarking Attacks	Single ownership			Joint ownership		
	1	2	3	1	2	3
Jpeg compression	√	√	√	√	√	√
Additive white Gaussian noise	√		√	√	√	√
Translation	√					
Rotation	√					
Cropping		√		√		√
Printing, photocoping and scanning		√				
Media filtering			√	√		√
Histogram equalization				√		√
Intensity adjustment				√		√
Additive salt & pepper noise						√
Multiplicative speckle noise						√
Scaling						√

Suggestions for further research:

1. **Secret sharing multiple watermarking keys**

   In some watermarking schemes, there may be multiple embedding secret keys involved. For example, one key is for generating a watermark and the other key is for randomizing the embedding locations. Both keys are required for watermark detection. If such watermarking schemes are used to resolve the problem of joint ownership, multiple secrets have to be shared among several participants. One possible solution is to apply Shamir's secret sharing scheme multiple times, so that each participant holds several shares for different secret

keys [9]. The problem with this solution is that each participant has to remember too much information. Also, lots of watermarks need to be embedded to the original image which may degrade the quality of the image. So it is preferable to devise a more advanced scheme in which each participant is assigned as few as possible shares while multiple secrets can be shared.

2. **JPEG2000 watermarking for joint ownership**

   JPEG2000 is the new compression standard for still images and it is very important to integrate a watermarking scheme with the JPEG2000 coding pipeline so that the watermarking scheme is more robust to JPEG2000 compression. Though such watermarking schemes have been proposed by some authors [157, 158, 113, 51], none of them can deal with the problem of joint ownership. The JPEG2000 watermarking algorithms for joint ownership are yet to be devised.

3. **Video watermarking for joint ownership**

   A lot of video watermarking algorithms have been proposed so far. Again, none of them addresses the problem of joint ownership. Usually, since there may be more participants involved in creating a video, the joint ownership problem is much more pronounced. So it is desirable to develop a digital video watermarking scheme that can resolve the problem of joint ownership.

4. **Digital watermarking for joint authentication.**

   One important application of digital watermarking is authentication. A fragile

or semi-fragile watermark is embedded into a digital image (or video) according to a key so that any illegal change of the digital image can render the watermark undetectable. Using the same embedding key, the watermark detector can decide whether the watermarked image is tempered or not. If the watermark is not detectable, the watermarked image is changed; otherwise, it is not. Now, consider such a scenario: Two persons, called them A and B, create an image collaboratively. They embed a watermark to the image and publish it, since they do not care that someone else will copy the image. What they are concerned mostly about is that the image will not be changed by others. Suppose A wants to change the content of the image on his behalf without B's permission. Since he knows the key, he can easily remove the watermark first, change the content of the image, and embed the same watermark to the changed image. When B finds out, he has nothing to prove that the image has been changed. This is indeed a problem of joint authentication which is yet to be addressed.

We do hope that this thesis will influence future watermarking standards.

Bibliography

[1] R.J. Anderson and F.A.P. Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications*, 16(4):474–481, May 1998.

[2] Anonymous. Introduction to penetrant testing (pt). http://www.cnde.iastate.edu/ncce/PT_CC/Sec.1.2.2/Sec.1.2.2.html.

[3] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci. A map identification criterion for dct-based watermarking. In *Proceedings of European Signal Processing Conference EUSIPCO 98*, pages 17–20, 1998.

[4] M. Barni, F. Bartolini, and A. Piva. Multichannel watermarking of color images. *IEEE Trans. on Circuits and Systems for Video Technology*, 12(3):142–156, March 2002.

[5] M. Barni, F. Bartolini, A. De Rosa, and A. Piva. Capacity of the watermark channel: how many bits can be hidden within a digital image. In *Proc. SPIE*, pages 437–448, 1999.

[6] M.F. Barnsley and L.P. Hud. *Fractal Image Compression.* AK Peters, Ltd., Wellesley, Massachusetts, 1993.

[7] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35(3/4):164–173, 1996.

[8] D. Benham, N. Memon, B.L. Yeo, and M.M. Yeung. Fast watermarking of dct-based compressed images. In *Inter. Conf. On Image Science, Systems, and Technology*, 1997.

[9] C. Blundo, A.D. Santis, G.D. Crescenzo, A.G. Gaggia, and U. Vaccaro. Multi-secret sharing schemes. In *Advances in Cryptology - Crypto'94(Lecture Notes in computer Science 839)*, pages 150–163, 1994.

[10] M. Celik, G. Sharma, E. Saber, and A. Tekalp. Hierarchical watermarking for secure image authentication with localization. *IEEE Trans. on Image Processing*, 11(6):585–595, June 2002.

[11] C.C. Chang, C.S. Tsai, and T.S. Chen. A new scheme for sharing secret color images in computer networks. In *Proc. 7th Int. Conf. On Parallel and Distributed Systems*, pages 21–27, 2000.

[12] B. Chen and G.W. Wornell. Dither modulation: a new approach to digital watermarking and information embedding. In *Proc. of SPIE Int. Conf. On Security and Watermarking Contents*, 342-353 1999.

[13] B. Chen and G.W. Wornell. Implementations of quantization index modulation methods for digital watermarking and information embedding of multimedia. *Journal of VLSI Signal Processing*, 27:7–33, Feb. 2001.

[14] B. Chen and G.W. Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. on Information Theory*, 47(4):1423–1443, May 2001.

[15] Q. Cheng and T.S. Huang. An additive approach to transform domain information hiding and optimum detection structure. *IEEE Trans. on Multimedia*, 3(3):273–278, September 2001.

[16] Q. Cheng and T.S. Huang. An image watermarking technique using pyramid transform. In *Proc. of the ACM Multimedia*, September 2001.

[17] C. Christopoulos, J. Askelof, and M. Larsson. Efficient methods for encoding regions of interest in the upcoming jpeg2000 still image coding standard. *IEEE Signal Processing Letters*, 7(9):247–249, September 2000.

[18] C. Christopoulos, A. Skodras, and T. Ebrahimi. The jpeg2000 still image coding system: An overview. *IEEE Transactions on Consumer Electronics*, 46(6):1103–1127, November 2000.

[19] M. Cooperman and S.A. Moskowitz. Steganographic method and device. United States Patent, No:5613004, 1997.

[20] M. Costa. Writing on dirty paper. *IEEE Trans. on Information Theory*, 29(3), May 1983.

[21] I.J. Cox, J. Kilian, T. Leighton, and T.G. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Trans. on Image Processing*, 6(12):1673–1687, 1997.

[22] I.J. Cox and M. Miller. A review of watermarking and the importance of perceptual modeling. In *Proc. of Electronic Imaging*, February 1997.

[23] I.J. Cox and M. Miller. The first 50 years of electronic watermarking. *Journal of Applied Signal Processing*, 2:126–132, 2002.

[24] I.J. Cox, M. Miller, and J. Bloom. Watermarking applications and their properties. In *Proc.of Int. Conf. Information Technology: Coding and Computing*, pages 6–10, March 2000.

[25] I.J. Cox, M. Miller, and J. Bloom. *Digital Watermarking*. Morgan Kaufmann, 2001.

[26] I.J. Cox, M. Miller, and A. McKellips. Watermarking as communications with side information. *Proc. of the IEEE*, 87(7):1127–1141, 1999.

[27] S. Craver, N. Memon, and B.L. Yeo. can invisible watermarks resolve rightful ownerships? In *Proc. SPIE Storage and Retrieval for Strill Image and Video Databaseds*, pages 310–321, Feb 1997.

[28] S. Craver, N. Memon, and B.L. Yeo. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications. *IEEE Journal on Selected Areas in Communications*, 16(4):573–586, May 1998.

[29] S. Craver, B.L. Yeo, and M. Yeung. Technical trials and legal tribulations. *Communications of the ACM*, 41(7):45–54, July 1998.

[30] G. Csurka, F. Deguillaume, J.O. Ruanaidh, and T. Pun. A bayesian approach to affine transformation resistant image and video watermarking. In *Information Hiding*, pages 270–285, 1999.

[31] J.F. Delaigle, C.De Vleeschouwer, and B. Macq. Watermarking algorithm based on a human visual model. *Signal Processing*, 66(3):319–335, May 1998.

[32] G. Depovere, T. Kalker, and J.P. Linnartz. Improved watermark detection reliability using filtering before correlation. In *IEEE Int. Conf. On Image Processing*, October 1998.

[33] Y. Desmedt. Some recent research aspects of threshold cryptography. In *The 1st International Workshop on Information Security, ISW'97*, pages 158–173, September 1997.

[34] J. Dittmann, M. Steinebach, and R. Steinmetz. Copyright protection in audio-visual digital libraries with digital watermarking. In *10th DELOS Workshop on Audio-Visual Digital Libraries, Santorini*, 1999.

[35] R. Dugad, K. Ratakonda, and N. Ahuja. A new wavelet-based scheme for watermarking images. In *IEEE Int. Conf. On Image Processing*, October 1998.

[36] J.J. Eggers and B. Girod. Quantization effects on digital watermarks. *Signal Processing*, 81(2):239–263, 1999.

[37] J.J. Eggers, J.K. Su, and B. Girod. Public key watermarking by eigenvectors of linear transforms. In *Proc. of European Signal Processing Conference*, September 2000.

[38] J.J. Eggers, J.K. Su, and B. Girod. Robustness of a blind image watermarking scheme. In *Proc. Of Int. Conf. on Image Processing*, 2000.

[39] C. Fei, D. Kundur, and R.H. Kwong. The choice of watermark domain in the presence of compression. In *Proc. IEEE Int. Conf. on Information Technology: Coding and Computing*, pages 79–84, April 2001.

[40] E. Ferrill and M. Moyer. A survey of digital watermarking. http://elizabeth.ferrill.com/papers/watermarking.pdf, 1999.

[41] Y. Fisher. *Fractal image compression: Theory and Application.* Springer Verlag, New York, 1995.

[42] International Organization for Standardization. Coding of moving pictures and audio mpeg4 , video verification model version 16.0. IOS/IEC JTC1/SC29/WG11 N3312, 2000.

[43] J. Fridrich, A.C. Baldoza, and R.J. Simard. Robust digital watermarking based on key-dependent basis functions. In *Proc.of Int. Conf. On Imaging Science,Systems and Technology*, June 1999.

[44] J. Fridrich and M. Du. Images with self-correcting capabilities. In *Proc. of the IEEE Inter. Conf. On Image Processing*, pages 792–796, 1999.

[45] J. Fridrich, M. Goljan, and M. Du. Invertible authentication. In *Proc. Of SPIE, Security and Watermarking of Multimedia Contents*, 2001.

[46] M.S. Fu and O.C. Au. Data hiding watermarking for halftone images. *IEEE Trans. on Image Processing*, 11(4):477–484, April 2002.

[47] T. Furon and P. Duhamel. An asymmetric public detection watermarking technique. In *The Third Int. Workshop on Information Hiding*, 1999.

[48] M. George. Spread spectrum watermarking for images and video. Master's thesis, University of Ottawa, 1999.

[49] J. Glas. *Non-Cellular Wireless Communication Systems.* PhD thesis, Delft University of Technology, 1996.

[50] M. Goljan, J. Fridrich, and R. Du. Distortion-free data embedding for images. In *Fouth International Information Hiding Workshop*, 2001.

[51] R. Grosbois and T. Ebrahimi. Watermarking in the jpeg 2000 domain. In *Proceedings of the IEEE Workshop on Multimedia Signal Processing (MMSP),Image/Video watermarking*, pages 339–344, October 2001.

[52] R. Grosbois, P. Gerbelot, and T. Ebrahimi. Authentication and access control in the jpeg 2000 compressed domain. In *Proc. of the SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV*, 95-104 2001.

[53] H. Guo and N.D. Georganas. Digital image watermarking for arbitrarily shaped objects. In *21st Biennial Symp. on Communications*, June 2002.

[54] H. Guo and N.D. Georganas. Digital image watermarking for joint ownership. In *Proceedings of ACM Multimedia 2002*, Dec 2002.

[55] H. Guo and N.D. Georganas. Multiresolution image watermarking scheme in the spectrum domain. In *Canadian. Conf. on Elec. And Comp. Eng*, May 2002.

[56] H. Guo and N.D. Georganas. A spread spectrum domain watermarking scheme in fractal domain. In *21st Biennial Symp. on Communications*, June 2002.

[57] H. Guo and N.D. Georganas. Digital image watermarking for joint ownership verification without a trusted dealer. In *International Conf. on Multimedia and Expo(ICME)*, July 2003.

[58] H. Guo and N.D. Georganas. Joint ownership verification for an image using digital watermarking. In *International Conf. on Information Technology: Coding and Computing*, April 2003.

[59] H. Guo and N.D. Georganas. Joint ownership verification for digital images. In *Canadian. Conf. on Elec. And Comp. Eng*, May 2003.

[60] H. Guo and N.D. Georganas. A novel approach to digital image watermarking based on a generalized secret sharing scheme. *ACM Multimedia Systems Journal*, Fall 2003.

[61] H. Guo and N.D. Georganas. Jointly verifying ownership of an image using digital watermarking. *International Journal of Multimedia Tools and Applications*, Accepted.

[62] F. Hartung and B. Girod. Watermarking of uncompressed and compressed video. *Signal Processing*, 66:283–301, May 1998.

[63] F. Hartung, J.K. Su, and B. Girod. Spread spectrum watermarking: Malicious attacks and counterattacks. In *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents*, January 1999.

[64] J. He and E. Dawson. Multistage secret sharing based on one-way function. *Electronics Letters*, 30(19):1591–1592, September 1994.

[65] J. Hernandez, M. Amado, and F. Perez-Gonzalez. Dct-domain watermarking techniques for still images detector performance analysis and a new structure. *IEEE Trans. on Image Processing*, 1(9):55–68, Jan 2000.

[66] J. Hernandez, M. Amado, and F. Perez-Gonzalez. Approaching the capacity limit in image watermarking: A perspective on coding techniques for data hiding applications. *Signal Processing*, 81(6):1215–1238, June 2001.

[67] J. Hernandez, F. Perez-Gonzalez, and J. Rodriguez. The impact of channel coding on the performance of spatial watermarking for copyright protection. In

Proceedings of the IEEE Inter. Conf. On Acoustics, Speech and Signal Processing, pages 2973–2976, 1998.

[68] M. Holliman and N. Memon. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. *IEEE trans. on Image Processing*, 9(3):432–441, March 2000.

[69] Y.C. Hou and P.M. Chen. An asymmetric watermarking scheme based on visual cryptography. In *Proc. of the IEEE Inter. Conf. On Signal Processing*, pages 992–995, 2000.

[70] C.T. Hsu and J.L. Wu. Multiresolution watermarking for digital images. *IEEE Trans. on Circuits and Systems Part II: Analog and Digital Signal Processing*, 45(8):1097–1101, August 1998.

[71] X.S. Hua, J.F. Feng, and Q.Y. Shi. Public multiple watermarking resistant to cropping. In *The Sixth International Conference Pattern Recognition and Information Processing*, 2001.

[72] I. Ingemarsson and G.J. Simmons. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. In *Advances in Cryptology - Crypto'90(Lecture Notes in computer Science)*, pages 266–282, 1990.

[73] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *Proceedings of IEEE Global Telecommun. Conf., Globecom'87*, pages 99–102, 1987.

[74] W.A. Jackson, K.M. Martin, and C.M.O Keefe. Efficient secret sharing without a mutually trusted authority. In *Advances in Cryptology - Crypto'95(Lecture Notes in computer Science*, pages 183–193, 1995.

[75] A.E. Jacquin. Image coding based on a fractal theory of iterated contractive image transformations. *IEEE Transactions on Image Processing*, 1:18–30, January 1992.

[76] A.K. Jain. *Fundamentals of Digital Image Processing.* Printice Hall, 1989.

[77] T. Kalker, G. Depovere, J. Haitsma, and M. Maes. Video watermarking system for broadcast monitoring. In *SPIE Int. Conf. On Security and Watermarking of Multimedia Contents*, January 1999.

[78] S. Katzenbeisser and F.A.P. Petitolas. *Infromation Hiding Techniques for Steganography and Digtital Watermarking.* Artech Hourse, 2000.

[79] K. Kobara and H. Imai. Limiting the visible space visual secret. In *Advances in Cryptology - Crypto'96(Lecture Notes in computer Science 1163)*, pages 185–195, 1996.

[80] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *IEEE Inter. Workshop on Nonlinear Signal and Image Processing*, pages 452–455, June 1995.

[81] D. Kundur. *Multiresolution Digital Watermarking:Hiding: Algorithms and Implications for Multimedia Signals.* PhD thesis, University of Toronto, 1999.

[82] D. Kundur and D. Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. In *Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing*, pages 2969–2972, May 1998.

[83] D. Kundur and D. Hatzinakos. Towards a telltale watermarking technique for tamper-proofing. In *Proc. IEEE Int. Conf. On Image Processing*, pages 409–413, October 1998.

[84] D. Kundur and D. Hatzinakos. Attack characterization for effective watermarking. In *Proc. IEEE Int. Conf. On Image Processing*, pages 240–244, October 1999.

[85] D. Kundur and D. Hatzinakos. Diversity and attack characterization for improved robust watermarking. *IEEE Transactions on Signal Processing*, 29(10):2383–2396, October 2001.

[86] M. Kutter. Watermarking resistance to translation, rotation, and scaling. In *SPIE Conf. on Multimedia Systems and Applications*, 1998.

[87] M. Kutter. *Digital Image Watermarking:Hiding Information in Images.* PhD thesis, University of Rhode Island, 1999.

[88] M. Kutter and F.A.P. Petitcolas. A fair benchmark for image watermarking systems. In *SPIE International Conf. on Security and Watermarking of Multimedia Contents*, January 1999.

[89] M. Kutter and S. Winkler. A vision-based masking model for spread spectrum image watermarking. *IEEE Trans. on Image Processing*, 11(1):16–25, January 2002.

[90] G. Langelaar and R. Langendijk. Optimal differential energy watermaking of dct encoded images and video. *IEEE Trans. on Image Processing*, 10(1):159–163, January 2001.

[91] G. Langelaar, R. Langendijk, and J. Biemond. Watermarking by dct coefficient removal: A statistical approach to optimal parameter settings. In *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents*, pages 2–13, January 1999.

[92] G.C. Langelaar, I. Setyawan, and R.L. Lagendijk. Watermarking digital image and video data: A state-of-the-art overview. *IEEE Signal Processing Magazine*, 17(5):20–46, September 2000.

[93] S.K. Langford. Threshold dss signatures without a trusted party. In *Advances in Cryptology - Crypto'95(Lecture Notes in computer Science 963)*, pages 397–409, 1995.

[94] J. Lee and C.S. Won. Authentication and correction of digital watermarking. *Electronic Letters*, 35(11):886–887, 1999.

[95] J. Lee and C.S. Won. Image integrity and correction using parities of eooro control coding. In *IEEE Inter. Conf. On Multimedia and Expo.*, pages 1297–1300, 2000.

[96] C. Li and S. Wang. Digital watermarking using fractal image coding. *IEICE Trans. on Fundamentals*, E-83-A(6), June 2000.

[97] V. Licks. On digital image watermarking robust to geometric transformations. Master's thesis, University of New Mexico, 2000.

[98] V. Licks and R. Jordan. On digital image watermarking robust to geometric transformations. In *Proc. Of Int. Conf. on Image Processing*, 2000.

[99] C.-Y. Lin and S.-F. Chang. Issues and solutions for authenticating mpeg video. In *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents*, pages 25–29, January 1999.

[100] C.-Y. Lin and S.-F. Chang. Semi-fragile watermarking for authenticating jpeg visual content. In *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents*, January 2000.

[101] C.Y. Lin, M. Wu, Y.M. Lui, J.A. Bloom, M.L. Miller, and I. J. Cox. Rotation, scale, and translation resilient public watermarking for images. *IEEE Trans. On Image Processing*, 10(5):767–782, May 1999.

[102] E. Lin, C. Podilchuk, and E.J. Delp. Detection of image alterations using semi-fragile watermarks. In *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II*, January 2000.

[103] E.T. Lin and E.J. Delp. A review of fragile image watermarks. In *Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99)*, pages 25–29, January 1999.

[104] E.T. Lin, C.I. Podilchuk, T. Kalker, and E.J. Delp. Streaming video and rate scalable compression: What are the challenges for watermarking? In *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents III*, January 2001.

[105] J.P. Linnartz, T. Kalker, and G. Depovere. Modelling the false alarm and missed detection rate for electronic watermarks. In *Proc. Second International Workshop on Information Hiding*, pages 329–343, 1998.

[106] R. Liu and T. Tan. An svd-based watermarking scheme for protecting rightful ownership. *IEEE Trans. on Multimedia*, 4(1):121–128, March 2002.

[107] D.C. Lou and J.L. Liu. Fault resilient and compression tolerant digital signature for image authentication. *IEEE Trans. on Consumer Electronics*, 46(1):31–39, Feb 2000.

[108] C.S. Lu, S.K. Huang, C.J. Sze, and H.Y.M. Liao. Cocktail watermarking for digital image protection. *IEEE Trans. on Multimedia*, 2(4):209–224, December 2000.

[109] C.S. Lu, H.Y.M. Liao, and M. Kutter. Denoising and copy attacks resilient watermarking by exploiting prior knowledge at detector. *IEEE Trans. on Image Processing*, 11(3):280–292, 2002.

[110] M. Maes and C. Overveld. Digital watermarking by geometric warping. In *IEEE Int. Conf. on Image Processing*, pages 424–426, 1998.

[111] B. Mandelbrot. *The Fractal Geometry of Nature.* Freeman Co., San Francisco, 1982.

[112] P. Meerald. Digital image watermarking in the wavelet transform domain. Master's thesis, University of Salzburg, 2001.

[113] P. Meerwald. Quantization watermarking in the jpeg2000 coding pipeline. In *Communications and Multimedia Security Issues of The New Century, IFIP*

TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security, CMS '01, pages 69–79, May 2001.

[114] P. Meerwald and A. Uhl. A survey of wavelet-domain watermarking algorithms. In *Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III*, January 2001.

[115] N. Memon and P.W. Wong. Protecting digital medis content. *Communications of the ACM*, 41(7):35–43, July 1998.

[116] M.L. Miller, I.J. Cox, and J.A. Bloom. Informed embedding: Exploiting image and detector information during watermark insertion. In *IEEE Int. Conf. on Image Processing*, 2000.

[117] M.L. Miller, I.J. Cox, J.P.M. G. Linnartz, and T. Kalker. A review of of watermarking principles and practices. In *Digital Signal Processing for Multimedia Systems*, pages 461–485. IEEE, 1999.

[118] F. Mintzer and G.W. Branudaway. If one watermark is good, are more better? In *IEEE Inter. Conf. On Acoustics, Speech and Signal Processing*, pages 2067–2069, 1999.

[119] F. Mintzer, G.W. Braudaway, and A.E. Bell. Opportunities for watermarking standards. *Communications of the ACM*, 41(7):57–64, July 1998.

[120] S. Mohanty and K.R. Ramakrishnan. A dual watermarking technique for images. In *Proc. Of ACM Multimedia 1999*, 1999.

[121] S.A. Moskowitz and M. Cooperman. Method for human-assisted random key generation and application for digital watermark system. United States Patent,No:5822432, 1998.

[122] S.A. Moskowitz and M. Cooperman. Method and system for digital watermarking. United States Patent,No:5905800, 1999.

[123] S.A. Moskowitz and M. Cooperman. Optimization methods for the insertion, protection, and detection of digital watermarks in digitized data. United States Patent,No:5889868, 1999.

[124] S.A. Moskowitz and M.S. Cooperman. Z-transform implementation of digital watermarks. United States Patent, 2000.

[125] D. Mukherjee, J.J. Chae, and S.K. Mitra. A source and channel coding framework for vector based data hiding in video. *IEEE Trans. on Circuits and Systems for Video Technology*, 10(4):630–645, June 2000.

[126] M. Naor and B. Pinkas. Visual authentication and identification. In *Lecture notes in computer science: CRYPTO'97*, pages 322–336, 1997.

[127] M. Naor and A. Shamir. Visual cryptography. In *Lecture notes in computer science LNCS 950, Advances in cryptology:EUROCRYPT'94*, pages 1–12, 1994.

[128] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Signal Processing*, 66(3):385–403, 1998.

[129] J. Ohnishi and K. Matsui. Embedding a seal into a picture under orthogonal wavelet transform. In *Proc. Of the IEEE Conf. On Multimedia Computing and Systems*, pages 514–521, June 1996.

[130] J. Ohnishi and K. Matsui. A method of watermarking with multiresolution analysis and pseudo noise sequences. *Systems and Computers in Japan*, 29(5):11–19, May 1998.

[131] T.P. Pedersen. A threshold cryptosystem without a trusted party (extended abstract). In *Advances in Cryptology - EuroCrypt '91*, pages 522–526, 1991. Lecture Notes in Computer Science Volume 547.

[132] S. Pereira and T. Pun. Fast robust template matching for affine resistant image watermarking. In *International Workshop on Information Hiding*, pages 200–210, 1999.

[133] S. Pereira, J.K.O. Runaidh, F. Deguillaume, G. Csurka, and T.Pun. Template based recovery of fourier-bsed watermarks using log-polar and log-log maps. In *IEEE Int. Conf. On Multimedia Computing and Systems*, June 1999.

[134] S. Pereira, S. Voloshynovskiy, M. Madueno, S.M. Maillet, and T. Pun. Second generation benchmarking and application oriented evaluation. In *International Workshop on Information Hiding*, 2001.

[135] S. Pereira, S. Voloshynovskiy, and T. Pun. Effective channel coding for dct watermarks. In *IEEE Inter. Conf. On Image Processing*, pages 671–673, 2000.

[136] F.A.P. Petitcolas. Watermarking schemes evaluation. *IEEE Signal Processing*, 17(5):58–64, September 2000.

[137] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn. Attacks on copyright marking systems. In *Int. workshop on Information Hiding*, pages 219–239, 1998.

[138] I. Pitas. A method for signature casting on digital images. In *IEEE Int. Conf. on Image Processing*, pages 215–218, 1996.

[139] A. Piva, M. Barni, F. Berbolini, and V. Cappellini. Dct-based watermark recovery without resorting to the uncorrupted original image. In *Proc.of IEEE Int. Conf. on Image Processing*, Ocotber 1997.

[140] C.I. Podilchuk and W. Zeng. Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications*, 16(4):525–540, May 1998.

[141] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. In *Proc. of SPIE Photonics East Symposium*, 1996.

[142] L. Qiao and K. Nahrstedt. Watermarking methods for mpeg encoded video: Towards resolving rightful ownership. In *Inter. Conf. On Multimedia Computing and Systems*, pages 276–285, 1997.

[143] M. Ramkumar. *Data Hiding in Multimedia:Theory and Applications.* PhD thesis, New Jersey Institute of Technology, 1999.

[144] J. Ruanaidh and G. Csurka. A bayesian approach to spead spectrum watermark detection and secure copyright protection for digital image libraries. In *IEEE Conf. On Computer Vision and Pattern Recognition*, June 1999.

[145] J. Ruanaidh, W. Dowling, and F. Boland. Phase watermarking of digital image. In *IEEE International Conference on Image Processing*, pages 239–242, September 1996.

[146] J. Ruanaidh, W. Dowling, and F. Boland. Digital image watermarking by salient point modification practical results. In *SPIE Conf. On Security and Watermarking of Multimedia Content*, pages 273–282, 1999.

[147] J. Ruanaidh and T. Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66(3):303–317, May 1998.

[148] R.G. Schyndel, A.Z. Tirkel, and I.D. Svalbe. Key independent watermark detection. In *IEEE International Conference on Multimedia Computing Systems (ICMCS99)*, pages 580–585, June 1999.

[149] A. Sequeira and D. Kundur. Communication and information theory in watermarking: A survey. In *Multimedia Systems and Applications IV, Proc. SPIE (vol. 4518)*, pages 216–227, August 2001.

[150] I. Setyawan, G. Kakesand, and R.L. Lagendijk. Synchronization-insensitive video watermarking using structured noise pattern. In *SPIE Inter. Conf. On Security and Watermarking of Multimedia Contents IV*, pages 520–529, 2002.

[151] I. Setyawan and R.L. Lagendijk. Low bit-rate video watermarking using temporally extended differential energy watermarking (dew) algorithm. In *SPIE*

Inter. Conf. On Security and Watermarking of Multimedia Contents III, pages 73–84, 2001.

[152] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11), November 1979.

[153] N.P. Sheppard, R.S. Naini, and P. Ogunbona. On multiple watermarking. In *Proc. of ACM Multimedia 2001 Workshops on Multimedia and Security: New Challenges*, Oct. 2001.

[154] D.R. Stinson. *Cryptography: Theory and Practice.* CRC Press, 1995.

[155] D.R. Stinson. Visual cryptography and threshold schemes. *IEEE Potentials*, 18(1):13–16, Feb/Mar 1999.

[156] J.K. Su. Spread-spectrum watermarking. http://www.lnt.de/ su/research2-e.html, 2002.

[157] P.-C. Su, H.-J. Wang, and C.-C. Kuo. Digital watermarking on ebcot compressed images. In *Proc. Of SPIE's 44th Annual Meeting: Applications of Digital Image Processing XXII*, July 1999.

[158] P.-C. Su, H.-J. Wang, and C.-C. Kuo. An integrated approach to image watermarking and jpeg-200 compression. *Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, 27(1/2), February 2001.

[159] Q.B. Sun and S.F. Chang. Semi-fragile image authentication using generic wavelet domain features and ecc. In *Proc. of the IEEE Inter. Conf. On Image Processing*, Sept. 2002.

[160] Q.B. Sun, S.F. Chang, and M. Suto. A new semi-fragile image authentication framework combining ecc and pki infrastructures. In *Proc. of ISCA*, May. 2002.

[161] Q.B. Sun, P.R. Feng, and R. Deng. An optical watermarking solution for authenticating printed documents. In *Proc. of the IEEE Inter. Conf. On Information Technology: Coding and Computing*, pages 65–70, 2001.

[162] M.D. Swanson, B. Zhu,.B. Chau, and A.H. Tewfik. Multiresolution video watermarking using perceptual models and scene segmentation. In *Proc. Of the IEEE Inter. Conf. On Image Processing*, October 1997.

[163] M.D. Swanson, B. Zhu, and A.H. Tewfik. Multiresolution scene-based video watermarking using perceptual models. *IEEE Journal on Selected Areas in Communications*, 16(4):540–550, April 1997.

[164] K.J. Tan and H.W. Zhu. General secret sharing scheme. *Computer Communications*, 22(8):755–757, 2002.

[165] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding secret information into a dithered multilevel image. In *Proc. 1990 IEEE Military Communications Conference*, pages 216–220, 1990.

[166] D. Taubman. High performance scalable image compression with ebcot. *IEEE Transactions On Image·Processing*, 9(7):1158–1170, July 2000.

[167] A.H. Tewfik, M.D. Swanson, and B. Zhu. Digital watermarking to resolve multiple claims of ownership. United States Patent, N0:6272634, 1997.

[168] A.Z. Tirkel, G.A. Rankin, R.M. Schyndel, W.J. Ho, N. Mee, and C.F. Osborne. Electronic watermark. In *Digital Image Computing, Technology and Applications (DICTA'93)*, pages 666–673, 1993.

[169] P. Vandergheynst, M. Kutter, and S. Winkler. Wavelet-based contrast computation and application to digital watermarking. In *SPIE Int. Conf. on Wavelet Applications in Signal Processing and Image Processing*, 2000.

[170] C. Vleeschouwer, J. Delaigle, and B. Macq. Invisibility and application functionalities in perceptual watermarking - an overview. *Proceedings of the IEEE*, 90(1):64–77, January 2002.

[171] S. Voloshynovskiy, F. Deguillaume, and T. Pun. Content adaptive watermarking based on a stochastic multiresolution image modeling. In *Tenth European Signal Processing Conference*, September 2000.

[172] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun. Attack modeling: Towards a second generation benchmark. *Signal Processing*, May 2001.

[173] G. Voyatzis and I. Pitas. The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE*, 87(7):1197–1207, July 1999.

[174] C.C. Wang, S.C. Tai, and C.S. Yu. Repeating image watermarking technique by the visual cryptography. *IEICE Transaction on Fundamentals*, E83-A(8), August 2000.

[175] H. Watanable and T. Kasami. A secure code for recipient watermarking against conspiracy attacks by all users. In *Proc. Of Inter. Conf. On Information and Communications Security*, pages 437–441, Oct 1998.

[176] A.B. Watson. Dct quantization matrices optimized for individual images. In *SPIE Int. Conf. On Human Vision, Visual Processing, and Digital Display IV*, pages 202–216, 1993.

[177] R.B. Wolfgang and E.J. Delp. A watermark for digital images. In *IEEE Int. Conf. on Image Processing*, October 1996.

[178] R.B. Wolfgang and E.J. Delp. Overview of image security techniques with applications in multimedia systems. In *Proc. of the SPIE Conf. on Multimedia Networks: Security, Displays, Terminals, and Gatweys*, pages 297–308, November 1997.

[179] R.B. Wolfgang and E.J. Delp. A watermarking technique for digital imagery: further studies. In *Int. Conf. on Imaging, Systems, and Technology*, pages 279–287, July 1997.

[180] R.B. Wolfgang and E.J. Delp. Fragile watermarking using the vw2d watermark. In *SPIE Int. Conf. on Security and Watermarking of Multimedia Contents*, January 1999.

[181] R.B. Wolfhang, C. Podilchuck, and E.J. Delp. Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, 87(7):1108–1126, July 1999.

[182] P. Wong and O. Au. Data hiding and wtermarking in jpeg compressed domain by dc coefficient modification. In *SPIE Int. Conf. on Security and Watermarking of Multimedia Contents*, 2000.

[183] P.W. Wong. A public key watermark for image verification and authentication. In *Proc. Of Inter. Conf. On Image Processing*, Oct 1998.

[184] M. Wu, S. Craver, E. Felten, and B. Liu. Analysis of attacks on sdmi audio watermarks. In *IEEE Inter. Conf. on Acoustic, Speech, and Signal Processing (ICASSP'01)*, May 2001.

[185] M. Wu and B. Liu. Watermarking for image authentication. In *Proc. Of Inter. Conf. On Image Processing*, pages 437–441, Oct 1998.

[186] M. Wu, H. Yu, and A. Gelman. Multilevel data hiding for digital image and video. In *SPIE Photonics East*, 1999.

[187] L. Xiao, H. Heys, and J. Robinson. Visual cryptography: threshold schemes and information hiding. In *Newfoundland Electrical and Computer Engineering Conference*, November 2000.

[188] L. Xie and G.R. Arce. Blind wavelet based digital signaturefor image authentication. In *Proc. Of the 9th European Signal Processing Conference, EUSIPCO'98*, pages 21–24, September 1998.

[189] L. Xie and G.R. Arce. Joint wavelet compression and authentication watermarking. In *Proc. Of the IEEE Inter. Conf on Image Processing*, 1998.

[190] W. Zeng and B. Liu. A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. *IEEE Trans. on Image Processing*, 8(11):1534–1548, November 1999.

[191] J. Zhao and E. Koch. Embedding robust labels into images for copyright protection. In *Inter. Congress on Intellectual Property Rights for Specialzed Infromation,Knowledge and New Technologies*, pages 465–468, August 1995.

[192] Y. Zheng, T. Hardjono, and J. Seberry. Reusing shares in secret sharing schemes. *The Computer Journal*, 37(3):199–205, March 1994.

[193] W. Zhu, Z. Xiong, and Y.Q. Zhang. Multiresolution watermarking for images and video. *IEEE Trans. on circuits and system for video technology*, 9(4), June 1999.