ROBUST AND IMPERCEPTIBLE DIGITAL VIDEO WATERMARKING TECHNIQUES

by

SADIK ALI MURSHID AL-TAWEEL

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosphy

February 2011

ACKNOWLEDGEMENTS

Although this thesis represents an achievement that bears my name, it would not have been possible without help of others whom I would like to thank. First, and for most, I thank Allah (SWT) for all his blessings and guidance.

I would like to express my sincere thanks and deepest gratefulness to my supervisor Assoc. Prof. Dr. Putra Sumari for his supervision, encouragements, guidance, insightful criticism, and for all of his help during my research work and preparation for this thesis. I would also seize this opportunity to express my special thanks to the School of Computer Sciences, USM, for all the facilities and support in this research.

I am also grateful to my parents for being there for me, and I dedicate this work to the soul of my father who waited long for this day to come and Almighty Allah (SWT) chose him to be closer to his mercy and blessings.

And last, but not least I am deeply grateful to my wife, for her prayers, love and care for her support and encouragement, and my kids for the time deducted from theirs to give me a time to finish this thesis.

TABLE OF CONTENTS

CHAPTER 2 – BACKGROUND

CHAPTER 3 – LITERATURE REVIEW

CHAPTER 4 – FREQUENCY DOMAIN SPREAD SPECTRUM WATERMARKING SCHEME

CHAPTER 5 – 3D WAVELET-BASED WATERMARKING SCHEME

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CMS	Computer Mediated System
3D-DWT	Three Dimensional Discrete Wavelet Transform
B0	Band-pass
B-pictures	Bidirectionally-predictive pictures
CDMA	Code-Division Multiple Access
CIF	Common intermediate format
CR	Collusion Resistant
Cr	Chip- rate
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DVD	Digital Video Disc
DWT	Discrete Wavelet Transform
FFT	Fast Fourier Transform
GOP	Group of pictures
H0	High-pass
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
I-pictures	Intra pictures

ISBN	International Standard Book Number
ISRC	International Standard Recording Code
JPEG	Joint Photographic Experts Group
KD	Key Detection
KE	Key Embedded
L0	Low-pass
LSB	Least Significant Bit
MPEG	Moving Picture Experts Group
MRA	Multi-resolution approximation
MRR	Multi-resolution representation
MSE	Mean square errors
NC	Normalized correlation
NCC	Normalized correlation coefficients
OEM	Original equipment manufacturer
PN	Pseudo-random noise
P-pictures	Predictive pictures
PSNR	Peak signal to noise ratio
PW	Perceptual watermarking
RBEM	Region Based Energy modification
SVD	Singular Value Decomposition

TEKNIK PENANDAAN-AIR VIDEO DIGITAL YANG TEGUH DAN TIDAK BOLEH DITANGGAP

ABSTRAK

Pengeluaran bahan video dan imej yang banyak dalam sistem berperantaraan komputer di Internet telah memberikan cabaran besar dalam bidang perlindungan hak milik. Banyak cetakan yang tidak sah telah dibuat dan usaha untuk membuktikan perlindungan hak milik terpelihara terhadap bahan media berkenaan adalah satu tugas yang mencabar. Penandaan-air digital merupakan salah satu penyelesaian yang boleh membuktikan hak milik dengan cara membenamkan satu penanda (mengandungi maklumat pemilik) ke dalam imej atau video berkenaan. Penanda berkenaan akan digunakan sebagai bahan bukti terhadap usaha membuktikan tuntutan hak milik. Oleh sebab itu, penanda yang dibenamkan seharusnya teguh dan tidak boleh ditanggap terhadap sebarang percubaan untuk membuang dan mengubahsuainya. Walau bagaimanapun, memastikan penanda berkenan selamat daripada sebarang percubaan pengubahsuaian untuk tujuan mengekalkan keasliannya merupakan halangan utama dalam pembangunan sistem penandaan-air video digital. Penanda yang dibenamkan di dalam imej dan video mudah di terubahsuai hasil daripada kegiatan seperti manipulasi geometri, proses pemprosesan imej, proses pemampatan dan hingar. Ini (yang juga dipanggil serangan) telah menyebabkan penanda tersebut tidak lagi serupa dengan yang asli dan ini akan menggagalkan proses tuntutan hak milik. Kajian ini mempersembahkan empat teknik sistem penandaan-air yang teguh dan tidak boleh ditanggap terhadap serangan. Skim pertama dipanggil domain frekuensi spektrum rebak. Skim ini menggunakan jujukan rebak modulasi dalam mewakili penanda. Dalam proses pembenamannya pula, dua domain proses pembenaman domain frekuensi dipanggil transformasi kosain diskret spektrum rebak (SSDCT) dan tranformasi wavelet spektrum rebak (SSDWT) dipersembahkan. Kedua-dua skim ini membenamkan penanda koefisien yang ditransformasikan ke dalam rangka terpilih yang mempunyai frekuensi tinggi. Skim ketiga dipanggil skim penandaan-air berasaskan wavelet 3-D. Skim ini mentransformasikan rangka kepada tiga paras dan bit penanda yang telah dimodulasikan dibenamkan ke dalam koefisien terisih yang tertinggi . Skim terakhir dipanggil skim penanda-air spatial teguh (RSS). Skim ini merupakan pendekatan domain spatial dengan penanda dalam bentuk bit pseudo-rawak dibenamkam ke dalam piksel menggunakan modulasi XOR secara bait. Pretasi skim diukur berdasarkan keteguhan dan kebolehtanggapan terhadap empat jenis serangan: serangan geometri, serangan pemprosesan imej, serangan pemampatan hilang dan serangan hingar. Keputusan menunjukkan bahawa skim-skim berkenaan menambah baik keteguhan dan keupayaan tidak boleh ditanggap terhadap empat jenis serangan tersebut dari segi PNSR dan korelasi yang baik berbanding dengan skim-skim lain yang serupa.

ROBUST AND IMPERCEPTIBLE DIGITAL VIDEO WATERMARKING TECHNIQUES

ABSTRACT

The massive production of image and video materials on the Computer Mediated Systems (CMS) over the Internet has created a challenge in the area of copyright protection. Numerous illegal copies have been made and efforts on proving the owner copyright of those media are indeed a challenging task. Digital watermarking is a solution that can be used to prove the ownership/copyright by embedding watermark (owner, information) into the image/video. Later, the embedded watermark is used as a proof and evidence for the real ownership. Thus, the embedded watermark should be robust and imperceptible against any attempt of removing and alteration on it. However, guaranteeing against any alteration as to preserve the originality is one of the major hurdles in image and video watermarking system. The embedded watermark in the image is easily distorted / altered from activities such as geometric manipulation, image processing process, compression process and noises within the image. Those (also being referred to as attacks) has caused the extracted watermark not similar to the original one and thus denying ownership claiming. This study presents four watermarking techniques that are robust and imperceptible against attacks. The first scheme is called Spread Spectrum Frequency Domain. This scheme uses modulated spread spectrum sequence in representing the watermark. In the embedding process, two frequency domain embedding process called Spread Spectrum Discrete Cosine transform (SSDCT) and Spread Spectrum Wavelet transform (SSDWT) are presented. Both schemes embedded the transformed coefficients watermark into the high frequency of transform coefficient of the selected frames. The third scheme is called 3-D wavelet based watermarking scheme (3D-DWT). The scheme transforms the frame into three levels and the modulated watermark bits are embedded in the highest sorted coefficients. The final scheme is called Robust Spatial Watermarking Scheme (RSS). This is a spatial domain approach in which the watermark in the form of pseudo-random bit is embedded within pixels of selected frame using XOR bit wise modulation. The performance of the schemes is measured based on its robustness and imperceptibility against four types of attacks: geometric attack, image processing attack, lossy compression attack and noise attack. The results have shown that the schemes have improved the robustness and imperceptibility against those four types of attacks in term of good PNSR and correlation compared to other similar existing schemes.

CHAPTER 1

INTRODUCTION

Today, we see that multimedia data such as video, music, text, and image are growing at a very fast rate. One of the characteristics of these data is that they can be transferred and copied easily to any storage medium anyplace and anytime. This has raised many issues such as illegal copying and piracy. Japan ranks high among the countries dealing with illegal copying over the internet. The number of users of file-sharing software such as "Winny" is estimated to be about 1.75 million, with most of the files exchanged using illegal copies of the software (Cooper, 2008). A brief six-hour survey conducted by a copyright organization monitoring the Internet found approximately 3.55 million examples of illegally copied gaming software, worth about 9.5 billion yen, at standard software prices. Furthermore, 610,000 illegally copied music files worth 440 million yen could freely be downloaded into personal computers by means of such software. This survey alone, estimated damages worth 10 billion yen (Cooper, 2008). Another survey conducted by International Intellectual Property Alliance (Eric H. Smith, 2010) on the statistics of copyright piracy in 2009 of video in Argentina, Canada, Chile, Costa Rica, India, Indonesia, Mexico, Philippines, China, Russian, and Italy revealed the losses as shown in Figure(1.1) and estimated damages worth (1, 966, 6 billion USD) (Eric H. Smith, 2010; IIPA, 2009).

The motion picture industry has also been affected by the growing online piracy crisis. Approximately, 90% of the pirated DVDs and other optical media products sold by street vendors, or internet auction sites, originate either from illegal uploads by peer to peer networks (p2p) or from illegal imports. In spite of the criminal conviction of the developer of "Winny" p2p

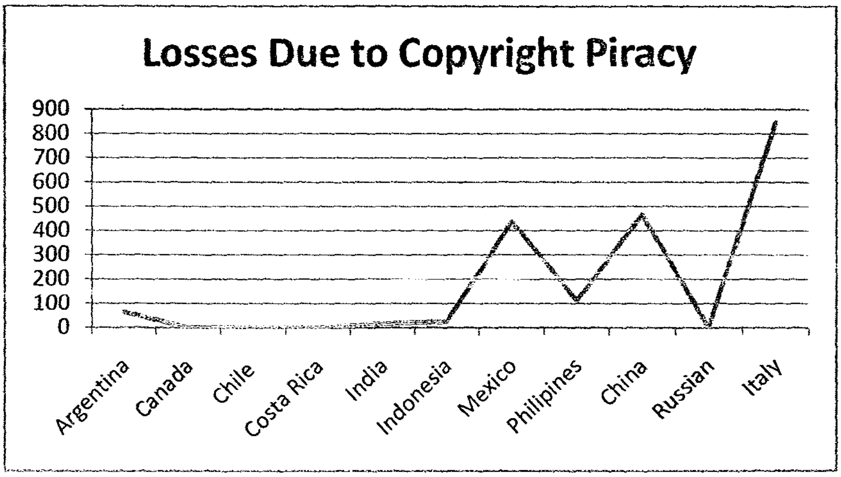


Figure 1.1: Losses of Copyright Piracy 2009 (Eric H. Smith, 2010)

file sharing system in 2006, it still remains in operation and is a source of online piracy (IIPA, 2009).

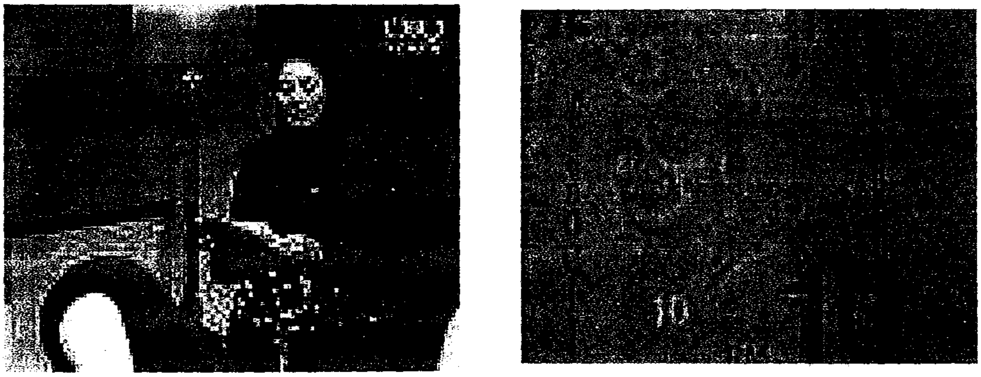
Digital watermarking has recently become a popular area of research due to the proliferation of digital data (image, audio, or video) on the internet and the need to find a way to protect the above issues. Numerous digital watermarking algorithms are also developed to help protect the copyright of digital video and to verify the multimedia data integrity (Liui and Zhao, 2009).

1.1 Digital Watermarking

Digital watermark is a signal (e.g. symbol, ownership information) that is securely, imperceptibly, and robustly embedded into innocent-looking host such as an image, a video, or an audio signal. The watermark can contain information that can be used for proof of ownership or tamper proving (Hussein, 2010). It is a one-to-many communication and the signal should be robust against an attempt on removing it (Aliwa et al., 2009).

Different watermarking applications exhibit different requirements such as fingerprinting, copy protection, data authentication and copyright protection. In case of fingerprinting, the copyholder (the seller of a digital data, for example) might also want to know which customer has leaked an unauthorized copy of data. Here, fingerprinting and distribution tracking techniques are used to identify not only the seller but also the buyer of a digital data (Karzenbeisser and Perircolas, 2000). However, copy protection means disallowing unauthorized copying of digital data. In open systems like the Internet, it is very difficult to achieve copy protection but, it is possible to enforce copy protection in a controlled system like the DVD player (Meerwald, 2001; Loo and Kingsbury, 2000). The objective of authentication applications is to detect any modifications on the data (Fridrich, 1999; Kundur and Hatzinakos, 1998). Fragile watermarks can be used to check the authenticity of the data. If the data, for example, are modified maliciously, the watermark will be destroyed. If the watermark can be retrieved by the recipient, the data is considered to be authentic. Otherwise, it should be discarded.

The most popular application of watermarking is copyright protection, i.e., embedding copyright statements that prove the ownership of original data clearly. Digital watermarks can be visible and invisible. We see visible watermarks every day, such as tv station logos as shown in Figure 1.2a and we also see invisible watermarks in banknotes and passports. Figure 1.2b shows an invisible watermark of a banknote. The copyright information should resist any modifications and/or manipulations that may alter the original information (Loo and Kingsbury, 2000; Neil et al., 2000; Fu, 1998).



(a) Visible watermark

(b) Invisible watermark

Figure 1.2: Types of watermark

The owner of digital data can quickly extract the watermark in order to proof ownership (Meerwald, 2001). This will prevent other parties from claiming the copyright of the data. Thus, this application requires a very high level of robustness. Note that watermarks for copyright protection do not prevent any person from copying the digital data. They simply exist as a means for owners to declare ownership over some digital data (Karzenbeisser and Perircolas, 2000). In this case, the author or originator integrates a watermark with his own intellectual property signature into the original document and delivers it as usual. By doing this, he can prove his intellectual creation later on, for instance, in a legal proceeding and has the possibility to assert entitlement to the restricted use (Seitz, 2005).

Although, copyright legislation does not define digital materials (Multimedia or Websites) as separate categories, these media platforms comprise one or more elements which can be protected by copyright. These media platforms include digital images, digital sound recordings, films, digital broadcasts and e-books, which can be classified according to the existing definitions of works and are protected by copyright as shown in Figure 1.3.

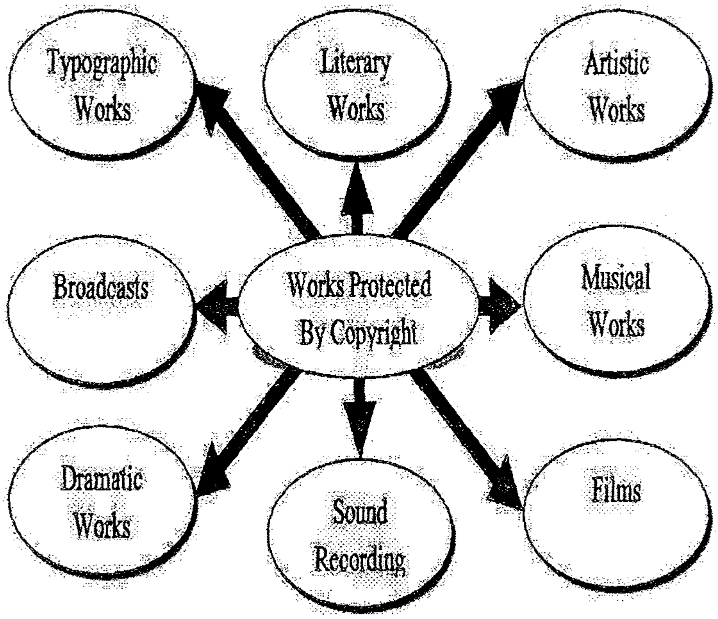


Figure 1.3: Elements which will be protected by copyright protection

A survey in October 2008 by IIPA (2009) indicated that nearly two-third of mobile phone users are in their early teens, and more than one-third of all the users are engaged in unauthorized music downloads. Unauthorized file sharing on PCs reached an estimated level of 84 million tracks in 2008, which outstripped the legal market nearly 2 to 1. It is encouraging that three arrests were made during October and November of 2008 of those operating, uploading, and hosting mobile music piracy sites, yet far greater efforts are required to save the market from being lost to piracy (IIPA, 2009).

1.2 Watermarking Objectives and Requirements

An effective watermark should have several properties whose importance varies depending on the application. These properties are described in the following subsections.

1.2.1 Robustness

Robustness here refers to the resistance of the watermarked message towards any form of malicious distortion which does not render the digital data useless. Robustness is the most fundamental for watermarking. The data after being embedded into cover-media, and after compression or other processing must also be recoverable from watermarking. It must be able to resist lossy data compression, filtering and other kinds of destruction without losing its function.

1.2.2 Imperceptibility

To conserve the quality of the marked document, the watermark should not obviously distort the original document. Ideally, the original and marked documents should be perceptually matching (Hartung et al., 1999). The embedded data should depend on the application and purpose of the watermarking system and should be minimally perceptible by the human visual or auditory systems (Bender et al., 1996).

Robustness and imperceptibility are the most important requirements for an effective watermarking system. Unfortunately, these requirements are in conflict and all watermarking algorithms involve determining a trade off between these two conflicting requirements. Using a good perceptual model will allow us to maximize the energy of watermark while keeping its visibility to a minimum (Busch et al., 1999; Sowers and Yousef, 1998).

1.2.3 Capacity

Capacity refers to the maximum amount or size of the information that can be embedded in a cover-media. A capacity of one bit (one = allow/zero = reject) seems to be sufficient in digital watermarking for simple copy control applications. For example, intellectual property applications require at least 60 to 70 bits information capacity to embed data about copyright, authors, limitations, International Standard Recording Code (ISRC), or International Standard Book Number (ISBN), or original equipment manufacturer (OEM) and other information (Seitz, 2005).

1.2.4 Security

The attacker is supposed to have some knowledge about the practical watermark process, but, the secret key is not known to him. As a result, an attacker will try to operate the data to destroy the watermark. Therefore, unauthorized parties should not be able to read or alter the watermark. Security should be assured for most watermarking applications such as the copyright protection. Sometimes, a secret key has to be used for the embedding and extraction processes. It is not possible for a user to find out whether a piece of data is watermarked until he or she has this (private) key. In other words, watermarking algorithms based on a secret key and this makes a major problem; they do not allow a public recovery of the watermark to work properly. In order to overcome this problem, public key watermarking algorithms have been proposed. Such algorithms consist of two keys; a public key and a private key. An image, for example, can be watermarked using the private key, whereas the public key is used to verify the mark (Seitz, 2005; Karzenbeisser and Perircolas, 2000). Some public keys watermarking algorithms are discussed in Meerwald (2001); Karzenbeisser and Perircolas (2000); Qiao and Nahrstedt (1999).

1.2.5 Low Cost

One of the most important features of the watermarking algorithm is that it should have low complexity and perform simple operations (Hartung et al., 1999; Darmstaedter et al., 1998). The speed of watermarking embedding and recovery processes is important for some applications like video applications because of the large amount of data to be processed.

1.3 Watermark Attacks

The following sections highlights the four groups of attacks related to the robustness, imperceptibility, capacity, security and cost. They are geometric attacks, lossy compression attack, image processing attacks, and noise attacks.

1.3.1 Geometric Attacks

Geometric attack of watermarked images and videos refers to downscaling, cropping, rotation and frame dropping and is the major disadvantage of image and video watermarking system. These operations are not aimed at removing the watermark, but try to either destroy it or disable its detection(Li and Kwong, 2005). Furthermore, geometric attack destroys the embedding, the detection process and the synchronisation of watermarking.

1.3.2 Lossy Compression attack

Lossy compression is an algorithm that compresses a file (such as image or video), in order to reduce the size of the file, but may not maintain the integrity of the original file. This can impact negatively on any hidden data in the image or frame of video. This algorithm may "loose" unnecessary data and provides a close approximation to high-quality file, but not exactly the original. Lossy compression involves general processing which does not specifically aim to embed watermark but may accidentally destroy or damage it (Xiaojing, 2006).

1.3.3 Image processing attack

The three filters in image processing attacks consist of low-pass filter, median filter and Wiener filter. A low-pass filter passes low-frequency signals and apart from that it also reduces the extent of signals with frequencies higher than the cut-off frequency. Furthermore, an important role is played by low-pass filters in signal processing which is identical to moving averages in some other fields, such as finance. Median filtering is a non-linear digital filtering technique which is used to remove noise from images or other signals. Furthermore, it is also an important step in image processing and is used to reduce speckle noise. It replaces a pixel with the median of all the pixels in the neighbourhood. The function of the Wiener filter is to filter out noise which has corrupted a signal by removing desired frequencies. Image processing attack, for instance doesn't introduce considerable degradation in watermarked frames, but can dramatically affect the performance (Bovik, 2005).

1.3.4 Noise attack

Gaussian noise is a random signal with a given distribution added to the image unintentionally. In certain applications, Gaussian noise may originate from digital to analogue and analogue to digital converters, or as a consequence of transmission errors. Salt and Pepper noise is a type of noise usually seen on images or frames of video. It represents itself as randomly occurring white and black pixels and it has been sprinkled on the image. Noise attack may introduce perceptually shaped noise with the maximum unnoticeable power. This will typically force the threshold at which the correlation detector operates to increase. Also watermark distortion is caused by Gaussian noise and Salt and Pepper noise (Bovik, 2005).

1.4 Research Motivation

It is important for digital data and multimedia, such as video, image, and music, to have digital watermarking. The importance of digital watermarking stems from the fact that digital data can be easily transformed through the Internet. In spite of the existence of watermarking technique for all kinds of digital data, most of the literature address the watermarking of still images for copyright protection and only some are extended to the temporal domain for video watermarking. There has been much emphasis on the robustness of watermarking against signal processing operations. However, it has become clear that a very small geometric distortion can prevent the detection of a watermark in many watermarking techniques. This problem is more pronounced for digital video watermark detection.

In order for a watermark to be useful, it must be perceptually invisible and robust against any possible attack and image processing by those who seek to corsair the material (Voloshynovskiy et al., 2001).

The wider applications for video watermarking have also created some additional difficulties in the two fundamental requirements of watermarking, namely robustness and imperceptibility (Koz and Alatan, 2008). There has been much emphasis on the robustness of watermarking against signal processing operations, and geometric attack is known as the most crucial issue to handle in watermarking. Moreover, a video watermarking scheme should be resistant to a number of hostile attacks, such as image processing attack and noise attack.

1.5 Problem Statement

Digital watermarking is a general solution that can be used to identify illegal copying and ownership, authentication, or other applications by inserting information into the digital data in visible, or an invisible way Dugelay and Petitcolas (2000). The huge production of media in the Computer Mediated Systems (CMS) or over the net has created the complexity of protecting media. One of the major obstacles in image and video watermarking system is geometric attacks of watermarked images or video. Geometric attack means that a small amount of rotation or scaling could disable the receiver from detecting the watermark (Seitz, 2005).

Generally, the lack of synchronisation that is essential for watermarking detection makes geometric attacks more difficult to handle than numerical processing in watermarking. For this reason, it is still in high demand to find a watermarking method that is robust against geometric attacks. Because of these difficulties that watermarking faces, it remains one of the most difficult areas of watermarking that needs to be solved. Its difficulties also encompass still images in addition to the video. The poor performance, computational complexity and the difficulty in the implementation are the main factors in the unresolved issues in geometric attacks (Wang and Pearmain, 2006; Seitz, 2005).

Additional developments in watermarking methods are aimed at improving the security, and detection performance of these watermarks. Furthermore, the work also aims at resisting a combination of watermark attack, geometric attack, lossy compression, image processing attack and noise attack. Thus, these will be the major challenges in video watermarking.

1.6 Objectives of the Thesis

It can be observed that perceptual transparency, robustness, capacity and security are very important elements and they should be included in the performance criteria for the quality of watermarking. Imperceptibility is the degree of invisibility of the embedded watermark when the watermarked signal is displayed. Robustness is the resilience of the embedded watermark against removal of watermarking information using signal processing.

This research aims to improve existing digital video watermarking technique and design and implementation of two robust watermarking techniques based on wavelet transform and spatial domain. The main objectives of this thesis are:

- To propose digital video watermarking algorithms that support robustness and imperceptibility.
- To ensure that the proposed algorithms are more robust against the following attacks:

  1. Geometric (downscaling, rotation, cropping, and frame dropping).
  2. Lossy compression (JPEG compression)
  3. Image processing (low pass filtering, Median filtering, and Wiener filtering).
  4. Noise (Gaussian noise, Salt and Pepper noise).

1.7 Scope and Limitation

The scope of this thesis is to develop the watermarking requirements like robustness and imperceptible hiding. The majority of current data hiding researches are concerned with robust and imperceptible watermarking. As mentioned earlier, robustness refers to the resistance of the watermarked data towards any form of malicious distortion which does not render the digital data useless. The data after being embedded into video, and after compression or other processing must also be recoverable from watermarking. It must be able to resist geometric attacks, lossy data compression, filtering, and noise attacks without losing its function.

The embedding system needs to modify the data in such a way that the changes are visually imperceptible. Imperceptibility retains the perceptual quality and value of the multimedia sources. A visually meaningful grey image, such as a logo, is embedded in video, which is essentially a video editing or copyright protection. In addition, the modification is modulated by a random sequence to make it difficult to systematically remove invisible marks via an automated algorithm.

1.8 Research Approach

In order to investigate the improvement on the robustness and imperceptibility of video watermarking as well as to accomplish the research objectives, the steps involved in this research are as shown in Figure 1.4

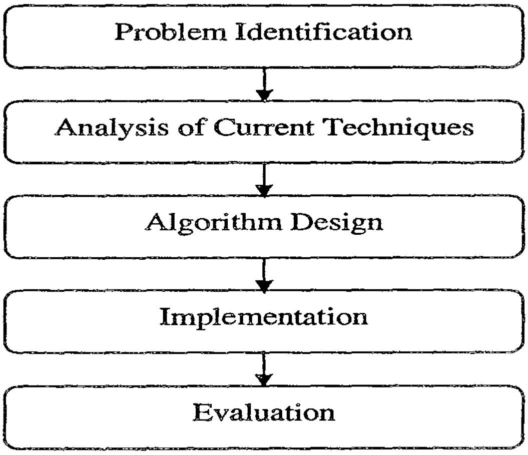


Figure 1.4: Research Approach

1.8.1 Problem Identification

Even with the challenges encountered with robust and imperceptibility digital video watermarking techniques, it remains an active topic for research. From the literature, problem identification is carried out with the aim of addressing many issues. The first issue of video watermarking is geometric attacks, which could disable the receiver from detecting the watermark. The second issue is the poor performance in the implementation of the methods in geometric attacks. The third issue is the problems of improving the security and detection performance in watermarking. Lastly, the problem of resisting a combination of watermark attacks.

1.8.2 Analysis of Current Techniques

This step focuses on current methods and algorithms, and is concerned with the robustness and invisibility. In particular, this research focuses on the robust and imperceptibility digital video watermarking. In robustness, the researchers are concerned with geometric attacks, image processing attacks, lossy compression attack, and noise attacks. Based on the literature review, there are limitations in the existing methods. Therefore, the current research will address these limitations.

1.8.3 Algorithm Design

In this step the proposed algorithms will be designed to improve the watermarking process in terms of robustness and invisibility in order to achieve the objectives of the research. Therefore, in this research, the proposed methods improve over Hartung and Girod (1998) watermarking technique by moving it to frequency domain using discrete cosine transform (DCT) and discrete wavelet transform (DWT). The current watermarking techniques have weaknesses when geometric attacks are involved. Hence, the researchers propose two new algorithms (3D-DWT and RSS) that have more resistance to geometric attacks. The study in this thesis focuses on the design of a system against any possible attacks such as geometric attacks, lossy compression attacks, image processing attacks, and noise attacks. The watermark is embedded in I, B, and P-frame to counter the frame dropping attack because embedding the watermark in P-frame and B-frame have less capacity since they are highly compressed by motion compensation.

1.8.4 Implementation

In this step, the proposed methods will be implemented using MATLAB version 7.5 and the experiments will be performed on a Pentium 4 PC running Windows XP. The four proposed algorithms that will improve the robustness and imperceptibility will be implemented in order to achieve the objectives of the research.

1.8.5 Evaluation

This step is concerned with examining the performance efficiency of the proposed methods through evaluation of the results of the proposed methods for video watermarking algorithm with respect to two metrics: imperceptibility and robustness. The metrics were evaluated using video clips: "Susi on the phone", "Flower", "Football", "Mobile", "Tempte", and "Table Tennis" with frame count of 450,150, 150, 450, 149, and 150 frames, with each frame having a resolution of 352 × 240, 352 × 240, 704 × 480, 704 × 480, 352 × 288, and 352 × 240 pixels respectively.

Imperceptibility: The results of the experiment are presented in the context of peak signal to noise ratio (PSNR) to estimate the performance of the invisibility and the detection ratio of the watermarks.

Robustness: is a measurement of the invulnerability of a watermark against the attempts to remove or degrade it by different types of digital signal processing attacks. The similarity between the original and extracted watermarks is measured using the correlation factor with a range between 0 and 1.

1.9 Thesis Contributions

1. A new spread spectrum watermarking in discrete cosine transform domain called SS-DCT. SSDCT improved an existing technique i.e. Hartung and Girod (1998).
2. A new spread spectrum watermarking in discrete wavelet transform domain called SS-DWT. SSDWT improved an existing technique i.e. Hartung and Girod (1998).
3. A new wavelet-based watermarking algorithm (3DDWT). This algorithm has high invisibility and robustness.
4. A new robust spatial watermarking algorithm (RSS). The more interesting part of this method is that it attempts to realize a good trade-off between robustness and quality of the embedding.

1.10 Thesis organisation

The organisation of the rest of the thesis is as follows: Chapter Two gives a brief introduction to digital video watermarking and its attack which is the core of this thesis.

Chapter Three presents several techniques related to video watermarking. These techniques are classified in this chapter according to the domain they operate in. A comparative analysis of different video watermarking techniques is also presented. Finally, this chapter discusses the limitations of the existing approaches that motivate this research.

Chapter Four proposed two new spread spectrums watermarking in frequency domain, namely SSDCT and SSDWT. The performance evaluation of the SSCT and SSDWT algorithms have been evaluated on the basis of the imperceptibility and robustness. The experimental result is then discussed and the improved method (Hartung and Girod, 1998) is compared with the proposed methods and shows the significant effect of the SSDCT and SSDWT is then discussed.

In Chapter Five, a new multi-resolution wavelet-based watermarking technique 3DDWT is proposed. Robustness against frame dropping is proposed. Then, performance evaluation on the basis of imperceptibility and robustness, performance comparison, experimental results are reviewed.

In Chapter Six, a new robust spatial watermarking scheme called RSS is presented. The performance evaluation of the RSS algorithm has been evaluated on the basis of imperceptibility and robustness. Performance comparison, experimental results are also used to demonstrate the performance of the proposed technique.

The focus of Chapter Seven is on the overall comparison performance of all the proposed schemes. Therefore, this chapter presents experiment setup, imperceptibility, robustness, and the simulation results of performance measurement for the evaluation of the proposed methods (SSDCT, SSDWT,3DDWT, and RSS). Experiment setup presents the performance of the proposed methods. Imperceptibility shows the quality for the watermarked frames. The robustness section explains various types of attacks and measures the proposed methods against these attacks. The quality of the watermarked video is presented and the proposed methods are compared with the existing methods.

Finally Chapter Eight concludes the thesis and suggests future work.

CHAPTER 2

BACKGROUND

2.1 Introduction

This chapter provides an overview of the fundamental concept of digital watermarking, particularly for videos. This chapter provides background knowledge and focus to the work presented in this thesis. This chapter describes watermarking terminology, basic watermark schemes, type of attacks on watermarks, pseudo-random number generators, and finally MPEG video.

2.2 Watermarking Terminology

Numerous names have been used to describe and classify watermarking techniques. In this work the following terms are used as follows:

Host is the piece of digital data in which the information is hidden, whereas payload refers to the hidden information.

Visible watermarks are visual patterns like logos, which are inserted into the digital data that can be seen by human eyes. While invisible watermarks are watermark that cannot be seen by human eyes.

Non-blind watermarking schemes are those which permit the extraction of the embedded information with the aid of the original, unwatermarked data. Its counterpart is known as blind watermarking scheme. A key to enforce security is used by some watermarking schemes. Watermarking techniques are usually referred to as secret or public watermarking techniques due to the use of a secret or public key respectively.

Fragile watermarks are watermarks that have only very limited robustness. They are used to detect modifications of the watermarked data rather than extract non-erasable information (Marini et al., 2007; Karzenbeisser and Perircolas, 2000; Delaigle:, 2000; Qiao and Nahrstedt, 1999).

2.3 Basic Watermarking Schemes

All watermarking schemes consist of three stages, namely the embedding stage (Figure 2.1), the recovery stage or extraction stage (Figure (2.2) and finally the decision stage. The embedding stage as shown in Figure (2.1), blends together the host, the payload and a public/secret key to produce the watermarked data. The secret key is used to make the watermark robust against replacement or removal of watermarked data. The recovery stage is the process of getting back the payload. The process takes watermarked data (which may be modified by a third party), the secret key and payload, and returns either the payload or a confidence measure of how probable the presence of a specific watermark is (Karzenbeisser and Perircolas, 2000; Delaigle:, 2000).

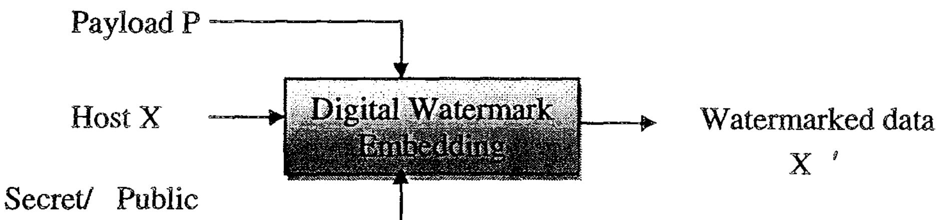


Figure 2.1: The generic watermark embedding process

In the decision stage, watermarking system analyses the extracted data (payload). Depending on the type of the application, the decision stage can produce a number of different outputs. For copyright protection, the output of the system can give from simple to more complicated answers. In the simplest case, the result is just a yes/no decision indicating if the copyright

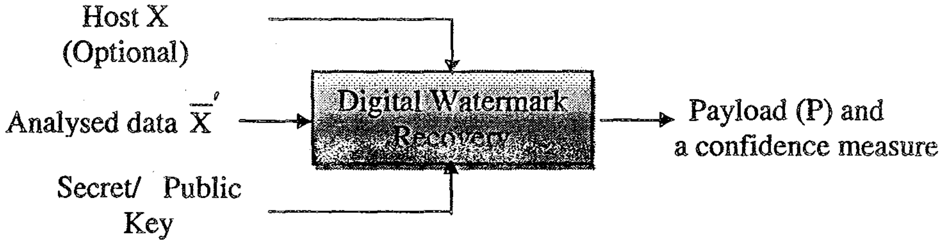


Figure 2.2: The generic watermark recovery process

holder's mark (payload) has been found in the host. The detection process uses the similarity measurement which measures the similarity between the extracted payloads against the original payload.

A widely used similarity measure that is used for the original watermark and the extracted watermark, is the normalised correlation coefficients (NCC) as shown in Gonzalez (2002).

$$NCC = \frac{\sum_X \sum_Y (W-\overline{W})(W^*-\overline{W}^*)}{[\sum_X \sum_Y (W-\overline{W})^2 \sum_X \sum_Y (W^*-\overline{W}^*)^2]^{1/2}} \tag{2.1}$$

where W and W^*refers to the original watermark and the extracted watermark respectively, and are the average value of the embedded and extracted watermark respectively, and X and Y represent the dimensions of the watermark. Another widely used measure is the normalised correlation as shown in Equation 2.2(NC) Neil et al. (2000).

$$NC = \frac{\sum_X \sum_Y W \times W^*}{\sum_X \sum_Y W.W} \tag{2.2}$$

The similarity values vary in the interval [-1,1]; a value well above 0 and close to 1 indicates that the extracted sequence W^* matches the embedded sequence W. Then, it can be concluded that the video has been watermarked with W.

A detection threshold T can be used to make the detection decision. If the value of NC or NCC for example is greater than T, the watermark is considered detected. The detection threshold can be derived experimentally Cox et al. (1997) or analytically Meerwald (2001). An experimental detection threshold can be derived by calculating the correlation between many randomly generated watermarks (for example 1000) and the original embedded one as shown Figure 2.3. Analytical threshold can be defined as Equation 2.3.

$$T = \frac{a}{S*N}|f^*| \tag{2.3}$$

where S, is the standard deviation which is either 2 or 3,f^* is the data coefficients that carry the watermarked information, N is the length of data coefficients, and a is the strength of the watermark. Several authors have attempted to draw general models of watermarking. Cox et al. (1999), proposed a general model, which describes watermarking as a communication problem. A message has to be hidden (watermarked) in a digital media such as an image. In the proposed 3DDWT method, the logo is encoded in two steps before being embedded. First, it is encrypted by using stream cipher (RC4) and thus becomes more robust. In the second step, it is modulated and takes an appropriate shape to be later added to the frame of the video. This can be a real value to be added to pixels or transformed coefficients to be added into another domain. This happens in watermark embedding.

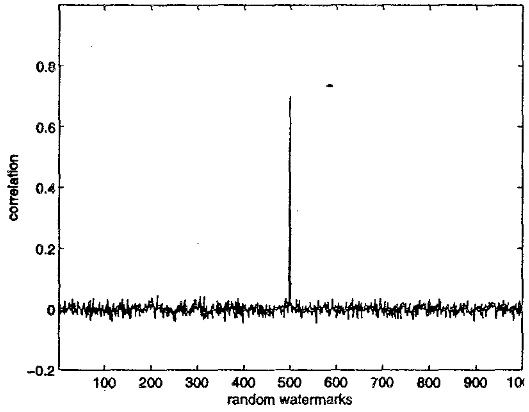


Figure 2.3: Experimental Detection

At the receiver side, the watermarked frame of the video is analysed and an estimation of the watermark is extracted and then demodulated in order to produce a bit stream. This stream inputs into a channel decoder, which finally produces the watermark message.

A widely used imperceptibility measure that is used for the original frame and the watermarked frame, is the Peak-Signal-to-Noise-Ratio (PSNR). PSNR is derived by setting the mean squared error (MSE) in relation to the maximum possible value of the luminance (for a typical 8-bit value this is 255) as follows:

$$MSE = \frac{1}{M.N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|X(i,j)-X^{*}(i,j)|^{2} \tag{2.4}$$

$$PSNR = 10\log(255^{2}/MSE) \tag{2.5}$$

where, X is the coefficients of the original video, X^{*} represents the coefficients of the watermarked video, while M and N are the height and width of the frame respectively. Typical values for the PSNR in video compression is between 30 and 50 dB, where higher is better.

2.4 Transform Techniques (DCT and DWT)

The transform technique is one of the watermarking techniques which embeds a message by modulating coefficients in a transform domain, such as the discrete cosine transform (DCT), or discrete wavelet transform (DWT). Transform techniques can offer superior robustness against lossy compression because they are designed to resist or exploit the methods of popular lossy compression algorithms. The DCT domain permits a host signal (image or video) to be divided into different frequency bands, facilitating the embedding of watermark information into the middle frequency bands. These bands avoid the most visually important parts of the host signal without over-exposing themselves to their elimination through noise attacks and compression (high frequencies). Therefore, the middle frequency bands are selected to provide additional resistance to lossy compression techniques. Avoiding the most visually important parts of the host signal (low frequencies) without over-exposing themselves to their elimination through noise attacks and compression (high frequencies). The original signal is divided into 8 × 8 blocks of pixels, and the 2-D DCT is applied independently to each block. The two dimensional DCT pair is given by Equations 2.6 and 2.7.

$$C(0,0) = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \tag{2.6}$$

$$C(u,v) = \frac{1}{2N^3}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)[cos(2x+1)u\pi])[cos(2y+1)v\pi] \tag{2.7}$$

for $U,V = 1,2...,N-1$ where C (u, v) is the DCT coefficient in row and column, and $f(x,y)$ is the intensity of the pixel in row and column. The inverse DCT is given by Equation 2.8.

$$f(x,y) = \frac{1}{N}C(0,0) + \frac{1}{2N^3}\sum_{U=0}^{N-1}\sum_{V=0}^{N-1} C(U,V)[cos(2x+1)u\pi][cos(2y+1)v\pi] \tag{2.8}$$

The base of Discrete Wavelet Transform (DWT) goes back to 1976 when Croiser, Esteban, and Galand derived a technique to decompose discrete time signals. Crochiere, Weber, and Flanagan did related work on the coding of speech signals in the same way; their analysis scheme was termed as Subband coding. In 1983, Burt termed it pyramidal coding which is also known as multi-resolution analysis (Yan and Gao, 2009; Pajares and de la Cruz, 2004; Leavey et al., 2003).

The fundamental idea of DWT for a one dimensional signal is as follow. A signal is split into two parts, generally high frequency and low frequency. The edge components of the signal are largely restricted in the high frequency part. The low frequency part is split again into two parts of high and low frequency. This process is continued until the signal has been entirely decomposed or stopped before the application is at hand. For compression and watermarking application, usually no more than five decomposition steps are computed. Furthermore, from the discrete wavelet transform (DWT) coefficients, the original signal can be reconstructed. The reconstruction process is called the inverse DWT (IDWT). Mathematically, the DWT and IDWT can be stated as follows:

$$H(w) = \sum_{k} h_k . e^{-jkw} \tag{2.9}$$

and

$$G(w) = \sum_{k} g_k . e^{-jkw} \tag{2.10}$$

where $H(w)$ is a low-pass filter and $G(w)$ is a high-pass filter respectively, which satisfy certain conditions for the reconstruction. A discrete signal,(n) can be decomposed recursively by using Equation (2.11).

$$f_{j-1}^{low}(k) = \sum_{n} h_{n-2k} \times f_j(n) \tag{2.11}$$

and

$$f_{j-1}^{high}(k) = \sum_{n} g_{n-2k} \times f_j(n) \tag{2.12}$$

This applies to $J = J+1, J, \ldots, J_0$ where $f_{J+1} = F(f), k \in Z.J+1$ is the highest resolution level index and j_0 is the low resolution level index. The coefficients $f_{J_0}^{low}(k), f_{J_0}^{high}(k)$,$f_{J_{0+1}}^{high}(k), f_{J}^{high}(k)$ are called the DWT of the signal F (n), where $f_{J_0}^{low}(k)$ is the lowest resolution part of F(n) (the approximation)and the $f_{J}^{high}(k)$ are the details of F (n) at various bands of frequencies. Furthermore, the signal F(n) can be reconstructed from its DWT coefficients recursively as follows:

$$f_{j}^{low}(n) = \sum_{k} h_{n-2k} \times f_{j-1}^{low}(k) + \sum_{k} g_{n-2k} \times f_{j-1}^{high}(k) \tag{2.13}$$

and

$$|H(w)|^2 + |G(w)|^2 = 1 \tag{2.14}$$

An example of such $H(w) and G(W)$ is given by:

$$H(w) = \frac{1}{2} + \frac{1}{2} \times e^{-} jw \tag{2.15}$$

and

$$G(w) = \frac{1}{2} - \frac{1}{2} \times e^{-} jw \tag{2.16}$$

which is known as the Haar wavelet filter. Other common filters used in image processing are the family of Daubechies orthogonal (D-4, D-6, D-8, D-10, D-12) and bi-orthogonal (B-5/3, B-7/9) filters. The DWT and IDWT for a two dimensional image $F(m,n)$ can be similarly defined by implementing the one dimensional DWT and IDWT for each dimension m and n separately as shown in Figure (2.4). The resulting pyramidal representation of the image is shown in Figure (2.5). The Discrete Wavelet Transforms (DWT) provides us with one part of multiresolution approximation (MRA) and three parts of multiresolution representation (MRR) (Mallat, 1989). It is similar to the hierarchical subband system, where the subbands are logarithmically spaced in frequency. The subband LL1 (that is MRA) is further decomposed and critically subsampled. The subbands labelled as LH1, HL1, and HH1 of MRR represent the first scale wavelet coefficients which are used to get the next coarser scale of wavelet coefficients (Inoue et al., 1999).

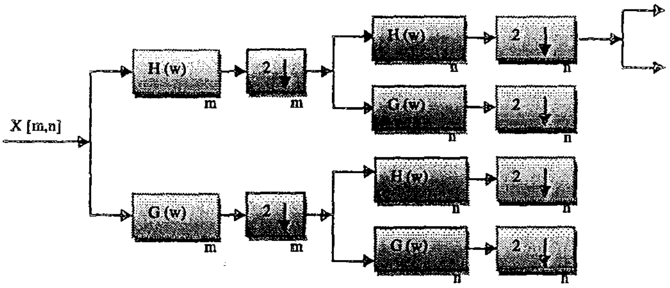


Figure 2.4: DWT for two dimensional images.