UNIVERSITI PUTRA MALAYSIA

DEVELOPMENT OF A ROBUST BLIND DIGITAL VIDEO WATERMARKING ALGORITHM USING DISCRETE WAVELET TRANSFORM

AHMED A. BAHA'A AL-DEEN

DEVELOPMENT OF A ROBUST BLIND DIGITAL VIDEO WATERMARKING ALGORITHM USING DISCRETE WAVELET TRANSFORM

AHMED A. BAHA'A AL-DEEN

MASTER OF SCIENCE
UNIVERSITI PUTRA MALAYSIA

2007

DEVELOPMENT OF A ROBUST BLIND DIGITAL VIDEO WATERMARKING ALGORITHM USING DISCRETE WAVELET TRANSFORM

By

AHMED A. BAHA'A AL-DEEN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

September 2007

DEDICATION

To my wonderful Grandfather, who has always encouraged me to continue my studies

To my great Father, for his prayers and endless support

To my beloved Mother, none of this would be possible without your love and moral support

Ahmed '07

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

DEVELOPMENT OF A ROBUST BLIND DIGITAL VIDEO WATERMARKING ALGORITHM USING DISCRETE WAVELET TRANSFORM

By

AHMED A. BAHA'A AL-DEEN

September 2007

Chairman: Associate Professor Abdul Rahman Ramli, PhD

Faculty: Engineering

Video watermarking technology enables us to hide an imperceptible, robust, and secure data in digital or analog video. This data can be used for tracking, fingerprinting, copyright infringement detection or any other application that requires some hidden data. Video watermarking can be achieved by either applying still image technologies to each frame of the movie or by using dedicated methods which exploit inherent features of the video sequence.

There is a complex trade-off between three requirements in digital watermarking: robustness against noise and attacks, imperceptibility or invisibility, and capacity, which represent the amount of data, i.e., the number of bits encoded by the watermark. However, these three requirements conflict with each other. Increasing the watermark strength makes the system more robust but unfortunately decreases the perceptual quality. Whereas, increasing the capacity of the watermark decreases the robustness.

In the production chain, video compression is usually applied before broadcasting or before transferring the video to other devices. In order to be robust against format conversions, the watermark has to be inserted before compression. Therefore, uncompressed video format has been used in the research undertaken. On the other hand, a random key is used to choose the frames to be watermarked to increase the security level of the algorithm and discourage piracy.

The aim of this research is to develop a video watermarking algorithm to embed a binary image inside the uncoded video stream that acts as a logo. A mid-band discrete wavelet transform coefficients of the selected frames are chosen to be the hosted region in the frequency domain. An inverse transformation should be taken in order to get the desired watermarked video shot. In extraction process the watermark is extracted from the marked video directly without access to the original video.

The experiment results showed that the proposed scheme provides better quality watermarked videos in term of watermark invisibility to human eyes. Results also indicated that obtaining average peak signal to noise ratio (PSNR) equals 41.59dB as compared with 38.48dB in the case of direct embedding. In addition, the scheme is robust against video processing operations, such as MPEG compression which could be successfully recovered.

In conclusion, modifying the wavelet coefficients depending only on the logo object's pixels highly improve the invisibility and at the same time providing a good robustness level.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PEMBANGUNAN ALGORITMA VIDEO TERA AIR DIGITAL JAGUR MENGGUNAKAN TRANSFORMASI WAVELET DISKRIT

Oleh

AHMED A. BAHA'A AL-DEEN

September 2007

Pengerusi: Profesor Madya Abdul Rahman Ramli, PhD

Fakulti: Kejuruteraan

Teknologi video tera air membolehkan kita menyembunyikan data yang tahan lasak dan selamat dalam video digital atau analog. Data ini boleh digunakan untuk pengesanan cap jari, pengesanan perlanggaran akta hak cipta atau aplikasi lain yang memerlukan data yang tersembunyi. Video tera air dapat dicapai dengan menggunakan teknologi imej pegun kepada setiap kerangka video atau menggunakan kaedah yang mengeksploitasikan ciri inheren jujukan video.

Didapati satu keseimbangan yang kompleks di antara tiga keperluan dalam tera air digital: kekuatan terhadap hingar dan gangguan, keadaan yang tidak jelas dan bilangan data atau nombor bit yang dikodkan oleh tera air. Ketiga – tiga keperluan adalah bertentangan di antara satu sama lain. Peningkatan daya tera air menyebabkan sistem lebih kukuh tetapi mengurangkan kualitinya. Manakala, kenaikan keupayaan tera air boleh mengurangkan kekuatannya.

Dalam rantaian pengeluaran, pemampatan video selalu digunakan sebelum penyiaran atau penukaran video kepada peranti lain. Tera air perlu dimasukkan sebelum pemampatan demi kekuatan terhadap penukaran format. Dengan ini, format video yang tidak termampat akan digunakan dalam kajian ini. Selain ini, satu kunci rawak akan digunakan untuk memilihk kerangka tera air untuk meningkatkan tahap keselamatan algoritma dan mengawal kegiatan cetak rompak.

Tujuan kajian ini adalah untuk membangunkan algoritma video tera air dan membenamkan imej nombor binari dalam video tidak dikodkan yang bertindak sebagai logo. Peliali jalur tengah penjelanaan wavelet diskrit pada kerangka terpilih alam ditempatkan dalam domain frekuensi. Perijelaraan balikam perlu dibuat untuk mendapatkan video tera air. Dalam proses penyarian, tera air disari secara terus dari pada video tertanda tanpa ambil daripada video asal.

Hasil eksperimen ini telah menunjukkan skim yang dicadangkan boleh meningkatkan kualiti video dari segi ketidak-lihatan tera air pada mata manusia. Keputusan nisbah isyarat kepada bisnigan sebanyak 41.59dB berbanding dengan. Pegekodan secara langsung yang sebanyak 38.48dB. Pada masa yang sama, skim ini adalah kukuh terhadap operasi proses video seperti pemampatan MPEG yang berjaya dipulihkan.

Kesimpulannya, pengubahsuaian pekali wavelet yang bergantung kepada piksel logo objek akan meningkatkan ketidak-lihatan dan memberikan tahap keselamatan yang kukuh.

ACKNOWLEDGEMENTS

All praise to Supreme Almighty ALLAH s.w.t the only Creator, Cherisher, Sustainer and Efficient Assembler of the world and galaxies whose blessings and kindness have enabled the author to accomplish this project successfully.

The author gratefully acknowledges the guidance, support and encouragement received from his supervisor, Assoc. Prof. Dr. Abdul Rahman Ramli whose constant advice and comments throughout the project helped to turn it into a real success.

Great appreciation is expressed to Dr. Mohammad Hamiruce b. Marhaban for reviewing the work from time to time, his valuable remarks, helpful advice and encouragement.

Thanks are due to Mr. Ahmed M. Mharib for his encouragement and support. He was always available to help when it was needed the most. His patience is greatly acknowledged.

Also appreciations are due for the Faculty of Engineering in providing the facilities and components required for undertaking this project.

I certify that an Examination Committee has met on 6th September 2007 to conduct the final examination of Ahmed A. Baha'a Al-Deen on his Master of Science thesis entitled "Development of a Robust Blind Digital Video Watermarking Algorithm Using Discrete Wavelet Transform" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the student be awarded the degree of Master of Science.

Members of the Examination Committee were as follows:

Norman Mariun, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

M. Iqbal Saripan, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Adznan Jantan, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Dzulkifli Mohamad, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Teknologi Malaysia
(External Examiner)

_____

HASANAH MOHD GHAZALI, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 29 January 2008

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Abdul Rahman Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Mohammad Hamiruce Marhaban, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 21 February 2008

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

_____

AHMED A. BAHA'A AL-DEEN

Date: 15 December 2007

TABLE OF CONTENTS

			Page
DEDICATION			ii
ABSTRACT			iii
ABSTRAK			v
ACKNOWLEDGEMENTS			vii
APPROVAL			viii
DECLARATION			x
LIST OF TABLES			xiii
LIST OF FIGURES			xiv
LIST OF ABBREVIATIONS			xvi
CHAPTER			
1	**INTRODUCTION**		
	1.1	Background	1.1
	1.2	Statement of the Problem	1.4
	1.3	Thesis Objectives	1.4
	1.4	Scope of Work	1.5
	1.5	Contribution	1.7
	1.6	Motivation	1.7
	1.7	Thesis Organization	1.7
2	**LITERATURE REVIEW**		
	2.1	Introduction	2.1
	2.2	Historical Watermarking	2.1
	2.3	Digital Watermarks Types	2.3
		2.3.1 Blind and Non-blind Techniques	2.4
		2.3.2 Visible vs. Invisible Watermarks	2.5
		2.3.3 Fragile or Robust	2.5
	2.4	Watermarking Techniques	2.6
		2.4.1 Spatial Domain Watermarking	2.7
		2.4.2 Frequency Domain Watermarking	2.8
	2.5	DCT Domain Watermarking	2.9
	2.6	DWT Domain Watermarking	2.10
		2.6.1 Wavelet Transform (Theory)	2.11
		2.6.2 Characteristics of DWT	2.14
		2.6.3 DWT over DCT	2.15
		2.6.4 DWT Watermarking Survey	2.16
	2.7	Classification and Requirements	2.18
	2.8	A General Watermarking Framework	2.20
		2.8.1 Watermark Encoding	2.21
		2.8.2 Watermark Decoding	2.22
	2.9	Video Watermarking	2.22
	2.10	Video Watermarking Applications	2.23
		2.10.1 Copy Control	2.24
		2.10.2 Broadcast Monitoring	2.26

2.10.3 Fingerprinting 2.27
2.10.4 Video Authentication 2.29
2.10.5 Copyright Protection 2.30
2.10.6 Enhanced Video Coding 2.31
2.11 The Major Trends in Video Watermarking 2.32
2.12 Possible Attacks on Video Watermarking 2.33
2.12.1 Nonhostile Video Processing 2.33
2.12.2 Resilience against Collusion 2.35
2.12.3 Real-time Watermarking 2.36
2.11 Conclusion 2.37

3 METHODOLOGY
3.1 Introduction 3.1
3.2 MATLAB 3.2
3.2.1 M-files 3.2
3.3 Common Intermediate Format (CIF) 3.3
3.4 YUV Colour Space 3.3
3.5 The Video Watermarking Procedure 3.4
3.6 Watermark Object 3.7
3.7 Watermark Embedding Process 3.9
3.8 Watermark Extraction Process 3.15
3.9 Evaluation of the System Performance 3.18
3.9.1 Visual Quality Metrics 3.18
3.9.2 Robustness Evaluation 3.19

4 RESULTS AND DISCUSSION
4.1 Introduction 4.1
4.2 Experimental Setup 4.1
4.3 Video Frames Selection 4.4
4.4 Subband Energy Calculation 4.5
4.5 Watermark Embedding and Invisibility Measures 4.7
4.6 Watermark Extraction and Robustness Measures 4.9
4.6.1 MPEG Compression 4.10
4.6.2 Filtering 4.13
4.6.3 Noise Addition 4.14

5 CONCLUSION AND SUGGESTIONS
5.1 Conclusions 5.1
5.2 Future Work 5.3

REFERENCES R.1
BIODATA OF THE AUTHOR D.1
LIST OF PUBLICATION P.1

LIST OF TABLES

Table		Page
2.1	List of DWT based blind and non-blind watermarking algorithms.	2.17
2.2	Video watermarking: applications and associated purpose.	2.23
2.3	Advantages and disadvantages of the video watermarking approaches.	2.32
2.4	Examples of nonhostile video processing.	2.34
3.1	Bit rates for uncompressed frames.	3.3
4.1	List of the video clips used for experiments.	4.2
4.2	Energy distribution in the detail subbands of the original 1st frame of the test clips.	4.6
4.3	Invisibility results of the test clips.	4.8
4.4	Similarity measures in case of no attacks.	4.9
4.5	Similarity measures in case of MPEG.	4.12
4.6	Similarity measures in case of LPF	4.14
4.7	Similarity measures in case of noise addition	4.15

LIST OF FIGURES

Figure		Page
2.1	Types of watermarks.	2.4
2.2	Classification of watermarking algorithms based on domain used for the embedding process.	2.7
2.3	LSB watermarking.	2.8
2.4	Two stages discrete wavelet transform.	2.13
2.5	DWT two-level decomposition of an image by Haar filter.	2.14
2.6	Generic video watermarking scheme.	2.20
2.7	Watermark encoding example.	2.21
2.8	Watermark decoding example.	2.22
2.9	DVD copy-protection system.	2.24
2.10	Alternative watermarking strategies for video streaming.	2.28
2.11	Original and tampered video scenes.	2.29
3.1	Proposed video watermarking (embedding process).	3.5
3.2	Proposed video watermarking (extraction process).	3.6
3.3	Ideal watermark object vs. object with 25% additive Gaussian noise.	3.8
3.4	Watermark embedding process.	3.11
3.5	Watermark extraction process.	3.16
4.1	Binary images used as watermarks.	4.4
4.2	The first frame from original mobile video sequence.	4.7
4.3	The first frame from watermarked mobile video sequence.	4.7
4.4	Original vs. extracted watermark in case of no attacks.	4.10
4.5	The effect of MPEG compression.	4.11

4.6	The video watermarking system in the uncoded and decoded domain.	4.11
4.7	Extracted watermark for the proposed method after MPEG coding.	4.12
4.8	The effect of low pass filter.	4.13
4.9	Extracted watermark for the proposed method after LPF.	4.14
4.10	Extracted watermark for the proposed method after noise addition.	4.15

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
BER	Bit Error Rate
CIF	Common Intermediate Format
CPTWG	Copy Protection Technical Working Group
dB	Decibel
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DVD	Digital Versatile Disc
DWT	Discrete Wavelet Transformation
FFT	Fast Fourier Transformation
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transformation
IEEE	Institute of Electrical and Electronic Engineers
ISBN	International Standard Book Number
ISRC	International Standard Recording Code
ITU	International Telecommunication Union
JPEG	Joint Picture Experts Group
LPF	Low Pass Filter
LSB	Least Significant Bit
LZW	Lempel-Ziv-Welch
MB	Mega Byte
Mbps	Mega bit per second
MPEG	Motion Picture Experts Group

MSE	Mean Square Error
PC	Personal Computer
PPV	Pay-Per-View
PSNR	Peak Signal-to-Noise Ratio
QCIF	Quarter Common Intermediate Format
TV	Television
USD	United States dollar
VBI	Vertical Blanking Interval
VHS	Video Home System
VIVA	Visual Identity Verification Auditor
VOD	Video-On-Demand

CHAPTER 1

INTRODUCTION

1.1 Background

Digital Television offers many potential benefits in picture quality as it is able to store and copy material without losing the quality or fidelity; hence resulting in superior quality as compared to the analog form due to its noise-free transmission. At the same time, there has been tremendous growth in both network and performance of computers, which directly increases considerable challenges for copyright enforcement.

However, the fact that an unlimited number of perfect copies can be illegally produced is a serious threat to the rights of the content owners. As such, there is a great desire for copyright system that can preserve both the economic value of digital data and the rights of the owners.

Until recently, the primary tool available to protect the content owners' rights has been encryption. Encryption protects the content during the transmission of the video stream from the sender to the receiver by encrypting the video using a secret key. Nevertheless, this technique has one significant disadvantage, i.e., encryption does not offer any protection once the encrypted video has been decrypted. This is a

significant limitation and encryption alone may not be sufficient for any copyright protection. In fact, it is mainly concerned with secure communication but not the copyright protection (Lin *et al.*, 2005).

Digital watermarks have been proposed as a way to handle this challenging issue. A watermark can act as an invisible signature to discourage copyright violation. This may help to determine the authenticity and ownership of the copyrighted video, even when data has been decrypted.

The invisible watermark has many applications including the copyright protection, video authentication, copy control, broadcast monitoring, fingerprinting, enhanced video coding and many other applications which are yet to be imagined. However, digital television systems also offer many potential challenges to the usefulness of a watermark (Huggett and Stubbings, 2000).

Watermarking compliments (and does not replace) encryption. A digital watermark is a piece of information that is hidden directly in the media content, in such a way that it is imperceptible to a human visual system (HVS) and always remains present, but easily detected by a computer. The principal advantage of this is that the content is inseparable from the watermark. This makes watermarks suitable for several applications (Parhi and Nishitani, 1999).

Watermark embedding techniques apply minor modifications to the host video in a perceptually invisible manner, where the modifications are related to the watermark information. The watermark information can be retrieved afterwards from the

watermarked video by detecting the presence of these modifications. A wide range of modifications in any domain can be used for watermarking techniques. Prior to embedding or extracting a watermark, the host video can be converted, for instance, to the spatial, the Fourier, the wavelet, the discrete cosine transform or even the fractal domain, where the properties of the specific transform domains can be exploited (Langelaar *et al.*, 2000).

In general, to give the video a sense of ownership or authenticity, the desirable properties of watermarking scheme should comply with the following requirements (Hartung and Girod, 1996):

- The digital watermark embedded into the video data should be invisible or at least hardly perceptible.
- A digital watermark should be statistically invisible so it cannot be removed by intentional or unintentional operations on the bitstream or on the decoded video without degrading the perceived quality of the video too much that it makes the video without any commercial value. This requirement is called robustness.
- Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation.
- Watermarking in the bitstream domain may not increase the bit-rate (at least for constant bit-rate applications).
- It can be assumed that incorporating a watermark into a compressed video has to obey much more constraints than incorporating a watermark into uncompressed video. Therefore, it is advantageous to do so in the domain of uncompressed video wherever possible.

- The watermark should be able to determine the true owner of the video.
- The watermark can only be extracted by privileged individuals who are given the security key.

1.2 Statement of the Problem

Video watermarking stands for the method of imperceptibly altering that video in order to embed a message, referred to as mark or watermark. Imperceptibility or invisibility is one of the most important requirements in watermarking for video copyright protection i.e., a perceptible watermark may decrease the commercial value of the video. A binary image (logo) with the specified dimension embedded into video frame will make a high modification to the host data for each bit of watermark by increasing the watermark strength. However, this large modification will be perceptible or slightly visible.

1.3 Thesis Objectives

The aim of the project is to embed meaningful data in the form of logo image in digital video, considering the most desirable requirements of invisibility and robustness. It must also be able to guarantee the security of the embedded watermark by developing a method for video watermarking scheme based on the discrete wavelet transform (DWT) applied on the pre-selected frames. Later, the watermark from the video that has probably been attacked or damaged is extracted. This will

help to achieve the legal DVD and video products while at the same time, prove the production companies and Hollywood studios ownership.

The objectives of this work are as follows:

- To study the available watermarking techniques.
- To implement the DWT-based watermarking algorithm in the digital video.
- To improve the imperceptibility of the DWT video watermarking in terms of Peak Signal to Noise Ratio.
- To test and evaluate the imperceptibility and robustness of the proposed watermarking algorithm.

1.4 Scope of Work

By using a random key, a number of an uncompressed video frames are selected to be watermarked; and this secret key will increase the security level of the algorithm and discourage piracy. Then, a 3-level discrete wavelet transformation is applied on the Luminance colour component (Y) of the CIF/QCIF frame to obtain ten sub-bands in the frequency domain. The energy of each sub-band is calculated in order to choose the one with the lowest value to ensure the best invisibility; and this sub-band is the region where the watermark is placed.

A binary image with a dimension of $M \times N$ pixel is to be embedded by modifying the coefficients in the centre of the selected sub-band. The contribution is made by

doing this modification depending on the pixels of the object (usually black) in the binary image, which almost stands for either a text identifies the owner or a logo of a company; whereas the other pixels (usually white) present the background. This will decrease the modification to about the half or even less while keeping the robustness in a good level.

The watermarked Y component is achieved by applying inverse discrete wavelet transform (IDWT) to the wavelet coefficients. The Y, U and V colour components are then concatenated together for each watermarked frame. Saving the whole frame in a new video file is the final step. Peak signal to noise ratio (PSNR) and mean square error (MSE) are calculated to evaluate the imperceptibility.

Watermark detection process is an inverse procedure of the watermark embedding process. The extraction process requires the key used for selecting frames, the wavelet transform filter, and the channel in which the watermark is inserted. The watermark is finally extracted by defining a threshold region T which detects the existence of the video watermark and reconstruct the watermark image. The bit error rate (BER) is used to evaluate the robustness of the scheme. The proposed algorithm extracts the watermark directly from the decoded video without any access to the original video (blind mode).

The proposed algorithm can offer a better watermarked video in term of quality (invisibility) with high robustness. The scheme of this work has been designed by using the MATLAB 6 software applied on CIF/QCIF raw video sequences, which can exploit other media-like another video format or digital images as well.