

**Robust and Adaptive Watermarking Technique for Secure
Authorship of Digital Images**

**Prepared by
G.W.R. Sandaruwan
149231R**

**Faculty of Information Technology
University of Moratuwa**

May 2017

**This thesis submitted in partial fulfillment of the requirement for the degree of MSc
in IT of University of Moratuwa**

Declaration

I, GALLENA WATTHAGE REKA SANDARUWAN declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research. This research work not been submitted for a degree in any other university/institution before.

I confirm that:

1. This work was done wholly or mainly while in candidature for a Master Degree at this University.
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
3. Where I have consulted the published work of others, this is always clearly attributed.
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
5. Either none of this work has been published before submission.

G.W.R. Sandaruwan:

Date: / /

Dr. Lochandaka Ranathunga:

Date: / /

(Head of Department / Senior Lecturer)

B.Sc. Sp(Hons), M.Sc., PGDip in DEd. (IGNOU),

PhD (Malaya), MIPSIL, MCSSL

Dedicated to

Dr. Lochandaka Ranathunga

Acknowledgments

I would like to express my sincere gratitude to My Supervisor Dr. Lochandaka Ranathunga Head of Department of Information Technology & Senior Lecture of University of Moratuwa for the continuous support of my M.Sc. study and related research, for his thought fullness, experience, patience, motivation, and immense knowledge. His guidance helped me in all the time of conduct the research and exposure My knowledge of research aria. I could not have imagined better advisor and mentor rather than Dr. Lochandaka Ranathunga in my whole life.

I would also like to acknowledge the rest of lectures in Faculty of Information Technology: Mr. D.K. Withanage (Former Dean of FIT), Mr. Saminda Premarathna (Senior Lecture), Mr. B.H. Sudantha (Course Coordinator), Mr. C.P. Wijesiriwardhana (Senior Lecture) for their insightful comments and encouragement.

Last but not the least, I would like to thank My colleagues and family: My parents and family members for supporting me spiritually throughout and my life in general.

G.W.R. Sandaruwan.

Abstract

There has been an increase in the broadcasting media since the last thirty years. The Tera Byte level multimedia data has been created, copied and transmitted via Internet every second. The access, sharing, replication and manipulation of images have become daily needs. Originators mind has a fear of illegal distribution and violation of copyright protection by malicious users. Hidden digital watermarking techniques have come to the rescue as a powerful solution to such potential problems. Several hidden type watermarking techniques have been proposed with a variety of their usage, complexity and security which are the primary concerns of such technique.

Digital watermarking describes methods and technologies that embed hidden information in digital media, such as images, video, audio or any other kind of multimedia object. Hidden digital watermarking techniques have many more challenges such as robustness, fidelity, extraction, and capacity. Robustness is a considerable feature of hidden watermarking techniques. This feature refers to the ability to detect the watermark after some signal processing operation, for example rotation, scaling, compression, noise adding, and image cutting. Resistance against several types of attacks is a real challenge for researcher's long years back. The robustness feature of hidden digital watermark will give huge benefits. Fidelity requirement of watermarking could be called invisibility. Fidelity feature preserves the similarity between the watermarked image and the original image according to human perception. The watermark must remain invisible notwithstanding the occurrence of small degradations in image features, contrast and brightness. Meeting the psycho-visual fidelity criteria is very important to every digital watermarking technique. Psycho-visual fidelity, is a huge challenging research gap of digital watermarking. Several previous researches have shown the evidence that invisibility and robustness are both very difficult to maintain mutually in available watermarking methodologies. Adaptive extraction feature determines, which resources are necessary for the analysis to extract the watermark from the watermarked image. Resource requirement should be minimized by a good watermark detection technique. The number of bits that can be inserted through watermark embedding process is a considerable research challenge to hidden digital watermarking. Increasing capacity of watermarking methods and fidelity of watermark can be conflicting. These two goals of watermarking

techniques should be balanced without any conflict.

This thesis describes a novel approach to hidden digital watermarking, based on low level features of digital image. It was hypothesized that, the above problem can be solved by a novel method of invisible watermarking of the digital images, based on low level features of the image and transform domain techniques. Corners are the salient feature of digital image. Corner detection is very important to the image processing operation. The Harris operator has been widely used for corner detection. This thesis has proposed a novel corner detector which is an extended and improved version of Harris operator. Novel operator is a step by step process, which improves corner detection ability and scale invariant property. The novel solution proposed in this thesis will giving the guarantee of features which robustness, fidelity, capacity and adaptive extraction. Proposed method in this thesis is to divide the entire process in to three major parts which are the analysis of the low-level features of image and detecting of the corner points in original or host image, watermark embedding into detected corner points, and adaptive watermark extraction. This study has abstracted a novel model by supporting Sobel operator of edge detection and Laplacian of Gaussian (LoG) filter. Using Sobel operator x-direction, y-direction and diagonal directions over host image, having improved edge detection ability of novel operator. LoG filter has provided a smoothing property and it's less sensitive to noise. LoG filter has improved scale invariant property of novel operator. Proposed watermarking solution can be used on color images and watermark object also can be small color images. Recover data matrix have generated by analyzing and comparing features of host image and intensity values of watermark image. Thus, recover data is generated dynamically. Generated recover data has been embedded in to host image at the prominent corner points of host image. Corner points are immutable points of image against many types of image processing operation. Specially corners provide good surveillance against rotation operations. Novel operator of this thesis has used LoG filter for the purpose of smoothing the host image. Thus, it has provided a good surveillance against scaling operation. Generated recover data are light weight. Due to the recover data generation process, it compares the host image and watermark object. Embedding process achieves the minimum degradation to original image. Thus, the novel approach of watermarking has guaranteed robustness and fidelity characteristics.

After embedding the recover data into host image, it produces uncompressed watermarked image. Study has proposed, represent watermarked image in a more efficient transferable and store-able manner. For the purpose of efficient representation, row-watermarked object has been converted into encoded format. Discrete Cosine Transformation (DCT) has been used to encode the row watermarked object. Other major function of watermarking system is an extracting watermark from watermarked object. Extraction process also has used low level features of watermarked image. Proposed extraction method of thesis is an adaptive process. It required minimum number of inputs included in watermarked image and meta data of watermark only. Extraction process has never required original image.

Comprehensive experiments have been conducted for the testing of novel watermarking approach. Study has used common data set widely used in image processing experiments. Experimental environment was a prototype application developed in C/C++ programming language. Evaluation process has been designed by covering all characteristics of watermarking algorithm. This thesis represents a complete evaluation of novel proposed solution by using a large data set. The thesis has represented test data results and analysis of results according to major characteristics of watermarking systems.

Evaluation has given evidence, that novel feature detection operator and watermark embedding algorithm provide higher robustness against rotation, scaling, filtering and noise adding attacks. The experimental results have given evidence that novel approach of digital watermarking can balance in between robustness and fidelity vis versa. Extraction method proposed by this thesis is a minimum number of inputs and it never required original image. Conclusion is that the proposed approach of digital watermarking gives many advantages over available methods.

Table of contents

Chapter 1 – Introduction	01
1.1 Introduction	01
1.2 Background & Motivation	01
1.3 Problem Statement	03
1.4 Hypothesis	04
1.5 Objectives	04
1.6 Low Level Features & DCT Base Approach	04
1.7 Structure of thesis	05
1.8 Summary	05
Chapter 2 – Review of Literature	06
2.1 Introduction	06
2.2 Classification of Watermark	06
2.2.1 Robustness	07
2.2.2 Fidelity	09
2.2.3 Capacity	09
2.2.4 Embedding	10
2.2.5 Detection types	10
2.3 Watermarking in Spatial Domain	11
2.4 Watermarking in Transform Domain	14
2.5 Feature Base Watermarking	20
2.6 Steganography Methods Used in Watermarking	22
2.7 Evaluation of watermark algorithms	24
2.8 Problem Definition	27
2.9 Summary	28
Chapter 3 – Methodology of Watermarking	29
3.1 Introduction	29
3.2 Pixel Based Techniques	30
3.2.1 Pixel Based Embedding	30
3.2.1.1 Random Insertion	34

3.2.1.2	Insertion into Less Sensitive Pixel to Human Vision	34
3.2.1.3	Insertion in to Less Significant Point of JPEG Macro-block	35
3.2.2	Pixel Based Extraction	35
3.3	Feature Based Techniques	36
3.3.1	Feature Detection	38
3.3.1.1	Feature Detection using Harris Operator	39
3.3.1.2	Feature Detection using Novel Operator	40
3.3.2	Feature Based Watermark Generation	44
3.3.3	Feature Based Embedding	45
3.3.3.1	Insert Around a Single Corner	46
3.3.3.2	Insert into Multiple Corners	46
3.3.4	Feature Based Extraction	47
3.4	Encoder	48
3.5	Decoder	49
3.6	Summary	49
Chapter 4	– Experimental Design and Experimentation	51
4.1	Introduction	51
4.2	Implementation Techniques	51
4.3	Experimental Environment	53
4.4	Data set	53
4.5	Experiments of Pixel Based Watermarking Techniques	54
4.5.1	Watermark Generator of Pixel Based	54
4.5.2	Watermark Embedder of Pixel Based	55
4.5.3	Encode in Pixel Based	55
4.5.4	Watermark Extraction of Pixel Based	56
4.6	Experiments of Feature Based Watermarking Techniques	57
4.6.1	Feature Analyzer, Feature Detector & Watermark Generator	58
4.6.2	Watermark Embedder of Feature Based Method	58
4.6.2.1	Experiment using Harris Operator	59
4.6.2.2	Experiment using Novel Introduced Operator	60
4.6.3	Watermark Extraction of Feature Based Method	61
4.7	Summary	63

Chapter 5 – Evaluation of Novel Watermarking Approach	64
5.1 Introduction	64
5.2 Evaluate of the Robustness	64
5.3 Evaluate of the Fidelity	68
5.4 Evaluate of the Capacity	72
5.5 Summary	76
Chapter 6 – Conclusion	77
6.1 Introduction	77
6.2 Major Findings	78
6.3 Achievements	79
6.4 Future Work	80
6.5 Summary	80
References	81
Appendix A – Methodology	86
Appendix B – Experimental Design	90
Appendix C – Evaluation	96
Appendix D – Prototype System	109

List of Tables

Table I: Summary of literature of watermarking	27
Table II: Recover data matrix of pixel based methods	33
Table III: Recover data matrix of pixel based methods	45
Table IV: Embedding using random insertion	56
Table V: Extraction using common algorithm	57
Table VI: Embed using Harris corner detector	59
Table VII: Embed using novel corner detector	60
Table VIII: Extract using Harris corner detector	62
Table IX: Extract using novel corner detector	62
Table X: Sample evaluation results for the robustness	65
Table XI: Sample evaluation results for the fidelity	70
Table XII: Sample evaluation results for the capacity	73

List of Figures

Figure 3.1: High level design diagram of pixel base watermark embedding technique	31
Figure 3.2 High level design diagram of pixel base watermark extraction technique	35
Figure 3.3: High level design diagram of feature base watermark embedding technique	38
Figure 3.4: Watermark objects	47
Figure 4.1: High level design diagram of feature base watermark extraction technique	54
Appendix A, Figure 1: High level design diagram of pixel base watermarking system	86
Appendix A, Figure 2: High level design diagram of feature base watermarking system	87
Appendix A, Figure 3: Mexican hat operator with different sigma values	89
Appendix A, Figure 4: Encoder module	91
Appendix D, Figure 1: Main window of prototype system	112
Appendix D, Figure 2: Watermark embed & extraction window	112
Appendix D, Figure 3: Evaluation window	113

Abbreviations

LoG:	Laplacian of Gaussian
DCT:	Discrete Cosine Transformation
I-DCT:	Inverse Discrete Cosine Transformation
DWT:	Discrete Wavelet Transformation
MTWC:	Multi Threshold Wavelet Codec
JPEG:	Joint Photographic Experts Group
SVD:	Singular Value Decomposition
LWT:	Lifting Wavelet Transform
DFRNT:	Discrete Fractional Random Transform
FFT:	Fast Fourier Transform
RT:	Ridgelet Transform
EHD:	Edge Histogram Descriptor
LSB:	Least Significant Bit
ITU:	International Telecommunications Union
GCC:	GNU Compiler Collection
MSE:	Mean Square Error
PSNR:	Peak Signal to Noise Ratio
NCC:	Normalized Cross-Correlation
NAE:	Normalized Absolute Error
SSIM:	Structural Similarity Index Matrix
FSIM:	Feature Similarity Index Matrix
PVD:	Pixel Value Differencing
TPVD:	Try-way Pixel Value Differencing