

RESILIENCE OF DIGITAL WATERMARKS UNDER TRANSFORMATION ATTACKS

Srilal Buddika T.M.

Registration No. : 138204V



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk
Degree of Master of Science

Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

April 2015

RESILIENCE OF DIGITAL WATERMARKS UNDER TRANSFORMATION ATTACKS

Srilal Buddika T.M.

Registration No. : 138204V



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Dissertation submitted in partial fulfillment of the requirements for the
degree Master of Science in Computer Science

Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

April 2015

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Candidate

.....

Date

.....

T.M.S. Buddika

The above candidate has carried out research for the Masters Dissertation under my supervision.

Supervisor

.....

Date

.....

Dr. Chandana Gamage

Acknowledgments

I offer my sincerest gratitude to my research supervisor Dr. Chandana Gamage, who gave endless support and encouragement to me during the research work and thesis preparation. His supervision has always inspired me to improve my writing skills and to produce quality work on this thesis.

I would like to extend my gratitude to my wife and family for providing assistance, support, encouragement and inspiration during the writing of this dissertation. I greatly appreciate their support and commitment in making this thesis a success.



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Abstract

Digital watermarking of electronic data has become a popular research area over last several years. The research work presented in this thesis blends a more practical perspective of digital watermarking schemes against transformation/geometric attacks with theoretical studies presented in past literature. Main objective of this dissertation is to come up with an attack success/failure evaluation metric against chosen watermarking schemes and with set of attacks. “Success” or “Failure” is defined as per given criteria: If there is a legitimate owner for the image, *success* of image attack would be determined if recovery of the watermark is denied given the fact that attacked image lies within the perceptual range. Otherwise it would be depicted as a *failure* of image attack.

In this thesis, limits that preserve perceptual quality of subjected images were analyzed for different types of attacks. Both PSNR and Histogram Analysis provide a foundation for meaningful measurement. We have shown that coupling such measurements with a perceptual quality measurement provide meaningful values for effectiveness of a watermarking scheme.

Table of Contents

Declaration	i
Acknowledgments	ii
Abstract	iii
List of Figures	vi
List of Tables	x
List of Equations	xi
1 Introduction	1
1.1 Origin of Information Hiding	2
1.2 Watermarking, Steganography and Cryptography	3
1.3 Digital Image Watermarking Applications	3
1.4 Digital Image Watermarking Techniques	4
1.5 Attacks on Digital Image Watermarks	6
1.6 Research Objective	13
2 Literature Review	14
2.1 Generic Watermarking System	15
2.1.1 Steps of Image Watermark Encoding	16
2.1.2 Steps of Image Watermark Decoding	16
2.2 Spatial Domain based Image Watermarking	17
2.2.1 LSB Watermarking Schemes	17
2.2.2 Patchwork based Watermarking Schemes	19
2.2.3 Correlation based Watermarking Schemes	21
2.2.4 Other Spatial Domain Watermarking Schemes	23
2.3 Transform Domain based Image Watermarking	24
2.3.1 Discrete Fourier Transform (DFT) based Schemes	24
2.3.2 Discrete Cosine Transform (DCT) based Schemes	25
2.3.3 Discrete Wavelet Transform (DWT) based Schemes	29
2.3.4 Hybrid Watermarking Schemes	34
2.4 Summary of Transform Domain	37
3 Research Methodology	39
3.1 Selection of Watermarking Schemes	39

TABLE OF CONTENTS

3.2	Selection of Transformation and Geometric Attacks	40
3.3	Selection of Images	48
3.4	Development of an Attack Success/Failure Evaluation Metric	49
4	Testing and Evaluation	50
4.1	Post Attack Evaluation on Watermarking Schemes	50
4.2	Summary of Test and Evaluation	59
5	Analysis and Conclusion	60
5.1	Distortion Analysis	60
5.2	Conclusion	69
	References	72
	Appendix	78



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

List of Figures

1.1	History of Steganography 5 th Century	2
1.2	Digital Image Watermark Classification	5
1.3	Generic Watermark Embedding Process	5
1.4	Watermark Recovery/Detection process	6
1.5	Two-Dimensional True Image Compression	9
1.6	Image Rotation Attack	10
1.7	Image Cropping Attack	10
1.8	Image Resize Attack	11
1.9	Image Enhancement Techniques: Filters and Histogram Equalization . .	12
1.10	Image Noise Attack	13
2.1	Digital Watermarking Hierarchy	15
2.2	Image Watermark Encoding	16
2.3	Image Watermark Decoding	17
2.4	Image Comparison-LSB Watermarking	18
2.5	Recovered Message Image	19
2.6	Image Comparison-LSB Watermarking	20
2.7	Histogram Comparison-LSB Watermarking	20
2.8	Watermark Encoding-Correlation Scheme	21
2.9	Image converted into DCT domain	26
2.10	Watermark Insert and Extract in Transform Domain	26
2.11	Original Image and Histogram-DCT	27
2.12	DCT Domain Watermarked Image and Histogram	27
2.14	Two-Dimensional Discrete Wavelet Transform	29
2.15	DWT watermark embedding block diagram	31
2.16	DWT watermark decoding block diagram	31
2.17	Original Image and Histogram-DWT	32
2.18	DWT Domain Watermarked Image and Histogram	32
2.19	Image Differences w.r.t Original Image-DWT	32
2.20	Resulting DWT Decomposed Image: Peppers	33
2.21	DWT block tree organization	33
2.22	Block-based hybrid method	35
2.23	Hybrid watermarked still image: Lena	37

LIST OF FIGURES

3.1	Block Diagram of Visible Differences Predictor	41
3.2	Cropped Lena Image	42
3.3	Cropped Peppers Image	42
3.4	Cropped OldLady Image	42
3.5	Image Flip Attack on Peppers Image	43
3.6	Image Resize Attack on Lena Image:ScaleUp	44
3.7	Image Resize Attack on OldLady:ScaleDown	44
3.8	Image JPEG Compression StirMark Attack on OldLady	45
3.9	Image Noise StirMark Attack on OldLady	46
3.10	Removal Attack on Peppers	46
3.11	Lowpass Filter Attack on OldLady	47
3.12	Lena	48
3.13	Peppers	48
3.14	OldLady	48
4.1	Watermark Detection after Crop Attack	51
4.2	Rotation:COX Scheme (Method:Bicubic)	52
4.3	Rotation:COX Scheme (Method:Nearest)	52
4.4	Watermark Detection after Flip Attack	53
4.5	Resize:WANG Scheme (Scale Down)	54
4.6	Resize:WANG Scheme (Scale Up)	54
4.7	JPEG Compression:KUCH Scheme	55
4.8	JPEG Compression:KUNDUR Scheme	56
4.9	Noise Attack:COX Scheme	56
4.10	Noise Attack:KUNDUR Scheme	57
4.11	Removal Attack:WANG Scheme	57
4.12	Removal Attack:KUNDUR Scheme	58
4.13	Filter Attack:XIA Scheme	59
4.14	Filter Attack:KUNDUR Scheme	59
5.1	Histogram Comparison of Lena (Flip Attack)	61
5.2	Histogram Comparison of Peppers (Flip Attack)	61
5.3	Histogram Comparison of OldLady (Flip Attack)	61
5.4	Histogram Comparison of Lena:Kundur (Filter Attack)	62
5.5	Histogram Comparison of Peppers:Kundur (Filter Attack)	62
5.6	Histogram Comparison of OldLady:Kundur (Filter Attack)	62
5.7	Histogram Comparison of Lena:Xia (Filter Attack)	63
5.8	Histogram Comparison of Peppers:Xia (Filter Attack)	63
5.9	Histogram Comparison of OldLady:Xia (Filter Attack)	63
5.10	Histogram Comparison of Lena:Kundur (StirMark JPEG Attack)	64
5.11	Histogram Comparison of Peppers:Kundur (StirMark JPEG Attack)	64

LIST OF FIGURES

5.12	Histogram Comparison of OldLady:Kundur (StirMark JPEG Attack) . .	64
5.13	Histogram Comparison of Lena:Kundur (StirMark Noise Attack)	65
5.14	Histogram Comparison of Peppers:Kundur (StirMark Noise Attack) . .	65
5.15	Histogram Comparison of OldLady:Kundur (StirMark Noise Attack) . .	65
5.16	Histogram Comparison of OldLady:Kundur (StirMark Removal Attack)	66
5.17	Histogram Comparison of Peppers:Kundur (Scale Down Attack)	66
5.18	Histogram Comparison of Lena:Kundur (Scale Up Attack)	66
5.19	Histogram Comparison of OldLady:Kundur (Rotate Attack)	67
5.20	PSNR Comparison:Kundur (Rotate Attack)	68
5.21	PSNR Comparison (Flip Attack)	68
5.22	Rotation:COX Scheme(Method:Bicubic)	78
5.23	Rotation:COX Scheme(Method:Nearest)	79
5.24	Rotation:WANG Scheme(Method:Bicubic)	79
5.25	Rotation:WANG Scheme(Method:Nearest)	79
5.26	Rotation:KUNDUR Scheme(Method:Bicubic)	80
5.27	Rotation:KUNDUR Scheme(Method:Nearest)	80
5.28	Rotation:XIA Scheme(Method:Bicubic)	80
5.29	Rotation:XIA Scheme(Method:Nearest)	81
5.30	Rotation:KOCH Scheme(Method:Bicubic)	81
5.31	Rotation:KOCH Scheme(Method:Nearest)	81
5.32	Resize:COX Scheme(Scale Down)	82
5.33	Resize:COX Scheme(Scale Up)	82
5.34	Resize:WANG Scheme(Scale Down)	83
5.35	Resize:WANG Scheme(Scale Up)	83
5.36	Resize:KUNDUR Scheme(Scale Down)	83
5.37	Resize:KUNDUR Scheme(Scale Up)	84
5.38	Resize:XIA Scheme(Scale Up)	84
5.39	Resize:XIA Scheme(Scale Up)	84
5.40	Resize:KOCH Scheme(Scale Down)	85
5.41	Resize:KOCH Scheme(Scale Up)	85
5.42	JPEG Compression:COX Scheme	86
5.43	JPEG Compression:WANG Scheme	86
5.44	JPEG Compression:KUNDUR Scheme	87
5.45	JPEG Compression:XIA Scheme	87
5.46	JPEG Compression:KOCH Scheme	87
5.47	Noise Attack:COX Scheme	88
5.48	Noise Attack:KUNDUR Scheme	88
5.49	Noise Attack:WANG Scheme	89
5.50	Noise Attack:XIA Scheme	89
5.51	Noise Attack:KOCH Scheme	89

LIST OF FIGURES

5.52 Removal Attack:COX Scheme	90
5.53 Removal Attack:WANG Scheme	90
5.54 Removal Attack:KUNDUR Scheme	91
5.55 Removal Attack:XIA Scheme	91
5.56 Removal Attack:KOCH Scheme	91
5.57 Filter Attack:COX Scheme	92
5.58 Filter Attack:WANG Scheme	92
5.59 Filter Attack:KUNDUR Scheme	93
5.60 Filter Attack:XIA Scheme	93
5.61 Filter Attack:KOCH Scheme	93
5.62 Histogram Comparison of Lena:Kundur(StirMark Removal Attack) . . .	94
5.63 Histogram Comparison of Peppers:Kundur(StirMark Removal Attack) .	94
5.64 Histogram Comparison of OldLady:Kundur(StirMark Removal Attack) .	94
5.65 Histogram Comparison of Lena:Kundur(Scale Down Attack)	95
5.66 Histogram Comparison of Peppers:Kundur(Scale Down Attack)	95
5.67 Histogram Comparison of OldLady:Kundur(Scale Down Attack)	95
5.68 Histogram Comparison of Lena:Kundur(Scale Up Attack)	96
5.69 Histogram Comparison of Peppers:Kundur(Scale Up Attack)	96
5.70 Histogram Comparison of OldLady:Kundur(Scale Up Attack)	96
5.71 Histogram Comparison of Lena:Kundur(Rotate Attack)	97
5.72 Histogram Comparison of Peppers:Kundur(Rotate Attack)	97
5.73 Histogram Comparison of OldLady:Kundur(Rotate Attack)	97
5.74 PSNR Comparison(Flip Attack)	98
5.75 PSNR Comparison:Kundur(JPEG Attack)	98
5.76 PSNR Comparison:Kundur(Filter Attack)	99
5.77 PSNR Comparison:Xia(Filter Attack)	99
5.78 PSNR Comparison:Kundur(Noise Attack)	100
5.79 PSNR Comparison:Kundur(Removal Attack)	100
5.80 PSNR Comparison:Kundur(Scale Down Attack)	101
5.81 PSNR Comparison:Kundur(Scale Up Attack)	101
5.82 PSNR Comparison:Kundur(Rotate Attack)	102

List of Tables

3.1	Selected Transformation and Geometric Attacks	41
3.2	Rotation Angles for Rotate Attack	43
3.3	Scale Factors for Resize Attack	43
3.4	Quality Levels of JPEG Compression Attack	45
3.5	Selected Images for Evaluation	48
5.1	Attack Success/Failure Summary	69



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

List of Equations

2.1	Watermarking Encoding Process	16
2.2	Watermarking Decoding Process with Original Image	16
2.3	Watermarking Decoding Process without Original Image	17
2.4	Watermark Encoding - Correlation Scheme	21
2.5	Edge-enhancing finite impulse response (FIR) filter	22
2.6	Spatial Domain Watermark Detection - Extended Method	23
2.7	DFT-1D Transformation	24
2.8	DFT-2D Transformation	24
2.9	DFT-2D Transformation-Magnitude and Phase	25
2.10	Discrete Cosine Transformation	28
2.11	Inverse of Discrete Cosine Transformation	28
2.12	DWT Embedding Procedure	30
2.13	DWT Extraction Procedure	30
2.14	Signature Function	30
2.15	DWT signal decomposition Level-1	34
2.16	DWT Signal Reconstruction Level-1	34
2.17	DWT and IDWT Orthogonality	34
2.18	Equation for modified DCT coefficients	38
2.19	Calculate Correlation Factor	38
2.20	PSNR Calculation	38
2.21	Mean Square Error Calculation	38