

Thesis:
**Multimedia Transaction Tracking from
a Mutual Distrust Perspective.**

by

Angela S. L. Wong

Thesis submitted for the degree of

Doctor of Philosophy

in

Electrical and Electronic Engineering
University of Adelaide

November 2007



© 2007
Angela S. L. Wong
All Rights Reserved



Contents

Contents	iii
Abstract	vii
Statement of Originality	ix
Acknowledgments	xi
Publications	xiii
List of Figures	xv
List of Tables	xxiii
Chapter 1. Introduction	1
1.1 Outline of Thesis	2
1.2 History	2
1.2.1 Watermarking	2
1.2.2 Cryptology	3
1.3 Assumptions	4
1.4 Background and Aim	5
1.5 Legal Issues	8
Chapter 2. A Review of the State of the Art	11
2.1 Watermarking Alone	12
2.2 Cryptography Alone	15
2.2.1 General Cryptosystems	16
2.2.2 Image- and Video-Specific Cryptosystems	17
2.3 Watermarking and Cryptography	20
2.4 Summary	21

Chapter 3. A Technical Background on Watermarking and Cryptography	23
3.1 Steganographic Watermarking	24
3.1.1 Watermarking Categories	26
3.1.2 Spread Spectrum Watermarking	27
3.1.3 Attacks and Defenses	28
3.2 Public Key Cryptography	32
3.2.1 RSA Cryptosystem	33
3.2.2 ElGamal Cryptosystem	34
3.2.3 Rabin Cryptosystem	35
3.2.4 Elliptic Curve Cryptography	37
3.2.5 Attacks on Cryptosystems	46
3.3 Pre- and Post-processing	47
3.3.1 Trade-offs: Capacity and Invisibility	47
3.3.2 Power Spectral Density (PSD)	48
3.3.3 Choice of watermark	48
3.3.4 Choosing document components to alter	49
3.3.5 Watermark detection	50
Chapter 4. Issues Associated with Mutual Distrust	53
4.1 The problem with trusting too much...	54
4.2 Significance of Research	54
4.3 Applications of Research Findings	55
4.4 Trusted Owner Party Scenario	56
4.5 The Staining Approach	58
4.5.1 Problems Anticipated with Staining	58
Chapter 5. Experimental Results	61
5.1 Test Work	62
5.2 XOR Cryptosystem	62
5.3 Block-based Cryptosystem	65
5.4 RSA Cryptosystem	68
5.5 Elliptic Curve Cryptosystem	94

Chapter 6. Summary	115
6.1 Discussion of Problems	116
6.1.1 The Exacting Nature of Cryptograms	116
6.1.2 Cryptosystem and Watermark Requirements	117
6.2 Conclusion	118
6.3 Summary of Contributions	119
6.4 Future Research	121
Appendix A. Acronyms, Abbreviations and Glossary	123
A.1 Acronyms	124
A.2 Abbreviations	125
A.3 Glossary	125
Appendix B. Paper-Pen Analyses	127
B.1 XOR Watermarking Algorithm	128
B.2 RSA Cryptosystem	130
B.3 Elliptic Curve Cryptography (ECC)	133
Appendix C. Codes	137
C.1 XOR	138
C.2 Block-Based	141
C.3 RSA	145
C.4 Menezes-Vanstone Elliptic Curve Cryptosystem	153
C.4.1 Truncation	153
C.4.2 JPEG Compression	159
C.4.3 Cropping and Replacing	166
C.4.4 Gaussian Noise Addition	172
C.4.5 Scaling and Rescaling	179
C.4.6 Combination Attacks: Rotate, Crop and Rescale	185
C.4.7 Combination Attacks: Crop and Rescale	192
C.4.8 Double Watermarking	198

Contents

C.5	Extraneous	205
C.5.1	POWMOD	205
C.5.2	RANDPRIME	206
C.5.3	EXTDEUC	207
	Bibliography	209

Abstract

In this thesis, we present a novel, elegant and simple method for secure transaction authentication and non-repudiation for trading multimedia content. Multimedia content can be video, images, text documents, music, or any form of digital signal, however here we will focus particular on still images with application to video.

We will provide proof that not only can receiving parties within a transaction be untrustworthy, but the owner, or members within an owning party, also cannot be trusted. Known as the *insider attack*, this attack is particularly prevalent in multimedia transactions. Thus the focus of the thesis is on the prevention of piracy, with particular emphasis on the case where the owner of a document is assumed to be capable of deceit, placing the system under the assumption of *mutual distrust*.

We will introduce a concept called *staining*, which will be used to achieve authentication and non-repudiation. Staining is composed of two key components: (1) public-key cryptography; and (2) steganographic watermarking. The idea is to watermark a multimedia document after encryption, thereby introducing a *stain* on the watermark. This *stain* is due to the non-commutative nature of the scheme, so that decryption will be imperfect, leaving a residue of the cryptographic process upon the watermark. Essentially, secrets from the owner (the watermark) and the receiver (the cryptographic key) are *entangled* rather than *shared*, as in most schemes.

We then demonstrate our method using image content and will test several different common cryptographic systems with a spread-spectrum type watermark. Watermarking and cryptography are not usually combined in such a manner, due to several issues such as the rigid nature of cryptography. Contrary to the expectation that there will be severe distortions caused to the original document, we show that such an entanglement is possible without destroying the document under protection. We will then attack the most promising combination of systems by introducing geometric distortions such as rotation and cropping, as well as compressing the marked document, to demonstrate that such a method is robust to typical attacks.

Statement of Originality

This work contains no material that has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of my thesis being available in the University Library.

The author acknowledges that copyright of published works contained within this thesis (as listed under Publications) resides with the copyright holder/s of those works.

Signed

Date

Acknowledgments

I am grateful to my supervisors, Dr. Matthew Sorell and Dr. Robert Clarke, for teaching me how to walk on water, and for their boundless patience and guidance over the course of my PhD. They have given me an incredible opportunity to study these fascinating fields of watermarking and cryptography, to which I could never express my gratitude enough. I am especially thankful for the care and speed with which they reviewed my original manuscript, considering Dr. Sorell has just had his second child and Dr. Clarke is in semi-retirement.

I would also like to thank the School of Electrical and Electronic Engineering of the University of Adelaide, including the lovely office ladies whom have made my post-graduate life easier, for all the resources that have been made available to aid me in my research. Furthermore, I would like to include in my acknowledgements all the members of the Centre for Internet Research (CIR), past and present, for making my postgraduate candidature an exceptional time in my life. Many of my colleagues have become very good friends of mine, especially one very witty and brilliant miss, who has been of great help over the years, and while I was writing this dissertation.

For all their love and encouragement, I would also like to acknowledge my friends and family, and in addition for his faith, my closest friend, Andrew Morris, as well as for his cheer: "You can do it, Gigi!", that has kept me going during some tough times. Infinitely, I would like to thank God, for listening to my worries, and giving me strength and clarity when I have needed them the most.

Finally, I would like to thank the anonymous reviewers, for taking the time to review this manuscript. Their constructive and insightful comments have been of tremendous value.

Publications

- Wong, A. S. L., Sorell, M. & Clarke, R. (2004). Transaction Tracking for Multimedia Content from a Mutual Distrust Perspective. International Symposium on Intelligent Multimedia, Video & Speech Processing (ISIMP2004), The Hong Kong Polytechnic University, Hong Kong, October 20–22.
- Wong, A. S. L., Sorell, M. & Clarke, R. (2005). Secure Mutual Distrust Transaction Tracking Using Cryptographic Elements, Lecture Notes for Computer Science, **No. 3710**, 4th International Workshop on Digital Watermarking (IWDW2005), Siena, Italy, September 13–15, pp. 459–469.
- Wong, A. S. L., & Sorell, M., (2007). Trading Multimedia Content Using Entangled Secrets, in Chang-Tsun Li (ed.), Multimedia Forensics and Security, Idea Group Inc. Pending Acceptance for Publication.

List of Figures

3.1	An example of fragile watermarking.	24
3.2	An example of robust watermarking.	25
3.3	The most general watermarking system.	25
3.4	Point addition of two unequal points in a real field.	39
3.5	Point addition of a point and its reflection in a real field.	41
3.6	Point doubling in a real field.	42

4.1	Trust-distrust copy transfer process.	57
4.2	Mutual distrust copy transfer process.	59

5.1	Lena image used in the testing of the implementations, courtesy of the Signal and Image Processing Institute at the University of Southern California.	62
5.2	Baboon image used in the testing of the implementations, courtesy of the Signal and Image Processing Institute at the University of Southern California.	63
5.3	Results for XOR encryption and spread spectrum watermarking scheme with $\alpha = 0.012$, (a) original image (Lena), (b) after encryption, (c) then watermarking, and finally (d) after decryption.	71
5.4	Results for matrix multiplication watermarking scheme, with encryption block size 8, and DCT watermarking block size 8, $\alpha 0.00043$, (a) original image (Lena), (b) after encryption, (c) then watermarking, and finally (d) after decryption.	72
5.5	Comparison for matrix multiplication watermarking scheme, with encrypted image at block sizes (a) 8, (b) 16, (c) 64, and (d) 512.	73

List of Figures

5.6	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, (a) original image (Lena), (b) after encryption, (c) then watermarking, and finally (d) after decryption.	74
5.7	The correlation of the decrypted image to 100 randomly watermarked decrypted images.	75
5.8	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: forcing to 8-bits, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	76
5.9	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: JPEG compressed by 50%, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	77
5.10	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: cropping 1 pixel from edges, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	78
5.11	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: cropping 50 pixel from edges, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	79
5.12	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: adding Gaussian noise with zero mean and standard variance 0.004, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	80
5.13	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: scaling by half and then doubling in size, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	81
5.14	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, after applying attack: cropping 1 pixel from edges and resizing to original size, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	82

5.15	Results of RSA encryption and DCT watermarking, first watermark $\alpha = 0.0005$, second watermark $\alpha = 0.0005$, after applying attack: double watermarking, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	83
5.16	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: forcing to 8-bits, where the original image has been subtracted from the attacked image, before correlating.	85
5.17	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: JPEG compressed by 50%, where the original image has been subtracted from the attacked image, before correlating.	85
5.18	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: cropping 1 pixel from edges, where the original image has been subtracted from the attacked image, before correlating.	86
5.19	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: cropping 50 pixel from edges, where the original image has been subtracted from the attacked image, before correlating.	86
5.20	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: adding Gaussian noise with zero mean and standard variance 0.004, where the original image has been subtracted from the attacked image, before correlating.	87
5.21	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: scaling by half and then doubling in size, where the original image has been subtracted from the attacked image, before correlating.	87
5.22	Results of RSA encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: cropping 1 pixel from edges and resizing to original size, where the original image has been subtracted from the attacked image, before correlating.	88

List of Figures

5.23	Results of RSA encryption and DCT watermarking, first watermark $\alpha = 0.0005$, second watermark $\alpha = 0.0005$, correlation after applying attack: double watermarking, where the original image has been subtracted from the attacked image, before correlating.	88
5.24	Results of RSA encryption and DCT watermarking, capacity analysis, with α varying from 0.0002 to 0.001, and for a range of prime keys, n , versus peak signal-to-noise ratio (PSNR).	89
5.25	Results of RSA encryption and DCT watermarking, capacity analysis, with α varying from 0.0002 to 0.001, and for a range of prime keys, n , versus peak signal-to-noise ratio (PSNR), lower-bound and best-fit. . .	90
5.26	Results of RSA encryption and DCT watermarking, capacity analysis, with α varying from 0.0002 to 0.001, versus a range of prime keys, n , versus peak signal-to-noise ratio (PSNR), upper-bound and surface-best-fit.	91
5.27	Results of RSA encryption and DCT watermarking, capacity analysis: individual upper-curve best-fits for α equal to (a) 0.0002, (b) 0.0003, (c) 0.0004, (d) 0.0005, (e) 0.0006, and (f) 0.0007.	92
5.28	Results of RSA encryption and DCT watermarking, capacity analysis: individual upper-curve best-fits for α equal to (a) 0.0008, and (b) 0.001.	93
5.29	Results of RSA encryption and DCT watermarking, capacity analysis: upper-curve percentage of PSNR below the JND threshold.	93
5.30	Results of Menezes-Vanstone EC encryption and DCT watermarking, $\alpha = 0.001$, (a) original image (Lena), (b) after encryption, (c) then watermarking, and finally (d) after decryption.	97
5.31	The correlation of the MVECC-encrypted and DCT-watermarked recovered watermark to 100 random watermarks.	98
5.32	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: forcing to 8-bits, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	99
5.33	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: JPEG compression to 10%, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	100

5.34	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: cropping 1 pixel from the edges and replacing from the original, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack. . .	101
5.35	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: cropping 50 pixel from the edges and replacing from the original, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack. . .	102
5.36	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: adding Gaussian noise with zero mean and standard variance 0.01, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	103
5.37	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: scaling by half and then doubling the size, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	104
5.38	Results of MV-ECC encryption and DCT watermarking, watermark at $\alpha = 0.001$, correlation after applying attack: cropping 1 pixel from edges and resizing to original dimensions, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	105
5.39	Results of MV-ECC encryption and DCT watermarking, first watermark $\alpha = 0.0005$ at index 27, second watermark $\alpha = 0.001$ at index 65, correlation after applying attack: double watermarking, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	106
5.40	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.005$, correlation after applying attack: rotating 1° clockwise, cropping 3 pixels from edges, and resizing to original size, where (a) before attack, (b) after attack, (c) correlation before attack, and (d) correlation after attack.	107
5.41	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: forcing to 8-bits, where the original image has been subtracted from the attacked image, before correlating.	108

List of Figures

5.42	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: JPEG compressed to 10%, where the original image has been subtracted from the attacked image, before correlating.	109
5.43	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: cropping 1 pixel from edges and replacing from original, where the original image has been subtracted from the attacked image, before correlating.	109
5.44	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: cropping 50 pixel from edges and replacing from original, where the original image has been subtracted from the attacked image, before correlating.	110
5.45	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: adding Gaussian noise with zero mean and standard variance 0.01, where the original image has been subtracted from the attacked image, before correlating.	110
5.46	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: scaling by half and then doubling in size, where the original image has been subtracted from the attacked image, before correlating.	111
5.47	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.001$, correlation after applying attack: cropping 1 pixel from edges and resizing to original size, where the original image has been subtracted from the attacked image, before correlating.	111
5.48	Results of MV-ECC encryption and DCT watermarking, first watermark $\alpha = 0.0005$, second watermark $\alpha = 0.001$, correlation after applying attack: double watermarking, where the original image has been subtracted from the attacked image, before correlating.	112
5.49	Results of MV-ECC encryption and DCT watermarking, $\alpha = 0.005$, correlation after applying attack: rotating 1° clockwise, cropping 3 pixels from edges, and resizing to original size, where the original image has been subtracted from the attacked image, before correlating.	112

List of Tables

3.1	Summary of Cox’s watermarking algorithm	28
3.2	Summary of RSA algorithm	35
3.3	Summary of ElGamal algorithm	36
3.4	Summary of Rabin algorithm	37
3.5	Summary of ElGamal-type ECC encryption algorithm	44
3.6	Summary of Menezes-Vanstone ECC encryption algorithm	45
5.1	Summary of XOR encryption algorithm	63
5.2	Summary of XOR watermarking algorithm	64
5.3	Summary of matrix multiplication watermarking algorithm	65
5.4	Correlation comparison for different encryption and watermarking block sizes for matrix multiplication watermarking scheme.	68
5.5	Summary of RSA watermarking algorithm	69
5.6	Summary of Menezes-Vanstone ECC watermarking algorithm	95

