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

Contents

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 postgraduate 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

List of Tables