2003

Contributions to image encryption and authentication

T. Uehara
University of Wollongong, takeyuki@uow.edu.au

Contributions to Image Encryption and Authentication

A thesis submitted in partial fulfillment of the
requirements for the award of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Takeyuki Uehara

Department of Computer Science
October 2003

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Takeyuki Uehara
October 21, 2003

Abstract

Advanced digital technologies have made multimedia data widely available. As multimedia applications become common in practice, security of multimedia data has become main concern. Digital images are widely used in various applications, that include military, legal and medical systems and these applications need to control access to images and provide the means to verify integrity of images.

Image encryption algorithms protect data against unauthorized access. In almost all cases image data is compressed before it is stored or transmitted because of the enormity of multimedia data and their high level of redundancy. Compressing plaintext before applying the encryption algorithm effectively increases security of the overall system. However direct application of encryption algorithms to image data *i*) requires high computational power and *ii*) introduces delay in real-time communication. If a data compression algorithm can be made to also provide security, less processing overhead could be expected as a single algorithm achieves two goals.

Image authentication provides the means to verify the genuineness of images. *Authentication codes* provide a method of ensuring integrity of data. The challenge in image authentication is that in many cases images need to be compressed and so the authentication algorithms need to be compression tolerant. Cryptographic authentication systems are sensitive to bit changes and so are not suitable for image authentication.

In this thesis, we study existing image encryption and authentication systems and demonstrate various attacks against these systems. We propose a JPEG encryption system that encrypts only part of the data, and a JPEG2000 encryption system that uses a simple operation, i.e. permutation, and show methods to minimize the computation cost for encryption. We also propose an image authentication system that remains tolerant to changes due to JPEG lossy compression.

Acknowledgments

I would like to thank my supervisor Dr. Rei Safavi-Naini and Dr. Philip Ogonbuna for guiding and encouraging me throughout this project. I would also like to thank Dr. Wanqing Li and Dr. Xing Zhang for their interest in this project. I would also like to thank my colleagues, Gareth Charles Beatt Brisbane, Chandrapal Kailasanathan, Dr. Nicholas Sheppard, Angela Piper, Vu Dong To, Qiong Liu, the people in Centre for Computer Security Research (CCSR) and Dr. John Fulcher. The work of the author is partially supported by Motorola Australian Research Centre (MARC).

Publications

The results of research in this thesis were published as follows.

- Takeyuki Uehara and Reihaneh Safavi-Naini, *Chosen DCT Coefficients Attack on MPEG Encryption Schemes*, Proc. of IEEE Pacific-Rim Conference on Multimedia, 316-319, 2000

- Takeyuki Uehara and Reihaneh Safavi-Naini and Philip Ogunbona, *Securing Wavelet Compression with Random Permutations*, Proc. of IEEE Pacific-Rim Conference on Multimedia, 332-335, 2000

- Takeyuki Uehara and Reihaneh Safavi-Naini, *On (In)security of "A Robust Image Authentication Method"*, Proc. of IEEE Pacific-Rim Conference on Multimedia (PCM 2002),1025-1032, 2002

- Takeyuki Uehara, Reihaneh Safavi-Naini and Philip Ogunbona, *A Secure and Flexible Authentication System for Digital Images*, ACM Multimedia Systems Journal to appear, 2003

Patent applications are as follows.

- JPEG2000 encryption system

  Takeyuki Uehara (University of Wollongong), Reihaneh Safavi-Naini (University of Wollongong), Philip Ogunbona (Motorola Australian Research Centre) and Motorola

- JPEG encryption system

  Takeyuki Uehara (University of Wollongong), Reihaneh Safavi-Naini (University of Wollongong), Philip Ogunbona (Motorola Australian Research Centre) and Motorola

Contents

List of Tables

List of Figures