

University of Wollongong - Research Online

Thesis Collection

Title: Contributions to image encryption and authentication

Author: T Uehara

Year: 2003

Repository DOI:

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Research Online is the open access repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

2003

Contributions to image encryption and authentication

T. Uehara

University of Wollongong, takeyuki@uow.edu.au

Follow this and additional works at: <https://ro.uow.edu.au/theses>

University of Wollongong

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Uehara, Takeyuki, Contributions to image encryption and authentication, PhD thesis, Department of Computer Science, University of Wollongong, 2003. <http://ro.uow.edu.au/theses/430>

NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.



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

Abstract	iii
Acknowledgments	iv
1 Introduction	1
1.1 Motivation	1
1.2 Objective	4
1.3 Contributions	4
1.3.1 Image Encryption	4
1.3.2 Image Authentication	5
1.3.3 Organization of Thesis	5
1.4 Images	6
1.5 Notations	7
2 Background	10
2.1 Introduction	10
2.2 Information Theory	10
2.3 Data Compression	12
2.3.1 Source Coding	12
2.3.2 Optimal Codes	12
2.3.3 Constructions of Optimal Codes	13
2.4 Security Systems	17
2.4.1 Symmetric Key Encryption	17
2.4.2 Public Key Cryptography	17
2.4.3 Authentication	18
2.4.4 Digital Signature	18
2.4.5 Message Authentication Codes	19
2.4.6 Attacks against Encryption Systems	19

2.4.7	Attacks against Authentication Systems	20
2.4.8	Redundancy of a Language	21
2.4.9	Unicity Distance	21
2.4.10	Data Compression and Security	22
2.5	Image Compression	22
2.5.1	Transform	23
2.5.2	Quantization	26
2.5.3	JPEG	28
2.5.4	JPEG2000	29
2.5.5	MPEG	30
2.6	Conclusion	31
3	Review of Image Encryption and Image Authentication Systems	32
3.1	Introduction	32
3.2	Arithmetic Coding Encryption Systems	32
3.2.1	Model-based Schemes	33
3.2.2	Coder-based Schemes	33
3.2.3	Effect on Data Compression Performance	34
3.2.4	Security	34
3.3	Image Encryption	35
3.3.1	Elementary Cryptographic Operations	35
3.3.2	Selective Encryption	37
3.3.3	Compression Performance of Encryption Systems	40
3.3.4	Security	41
3.3.5	Concluding Remarks	42
3.4	Image Authentication	43
3.4.1	Watermarking Systems	44
3.4.2	Signature Systems	47
3.4.3	Evaluation	52
3.4.4	Concluding Remarks	53
3.5	Conclusion	54
4	Attacks on Image Encryption Systems	55
4.1	Introduction	55
4.2	Chosen DCT Coefficients Attack on MPEG Encryption Schemes	55
4.2.1	Encryption Using Random Permutation	56

4.2.2	Chosen DCT Coefficients Attack	57
4.2.3	Concluding Remarks	60
4.3	Recovering the DC Coefficient in Block-based Discrete Cosine Transform	60
4.3.1	Properties of DCT Coefficients	61
4.3.2	Recovering the DC Coefficients in a Block-based DCT	64
4.3.3	Experiment Results	70
4.3.4	Another Application of DC Recovery	72
4.3.5	Concluding Remarks	74
4.4	Conclusion	75
5	JPEG Encryption	77
5.1	Introduction	77
5.2	JPEG Compression	78
5.2.1	Huffman Coding in JPEG	79
5.3	JPEG Stream	82
5.3.1	JPEG Data Components	82
5.4	Encrypting Markers	87
5.5	Encryption of JPEG Components	87
5.5.1	Encrypting Headers	88
5.5.2	Encrypting Quantization Table Specifications	90
5.5.3	Encrypting Huffman Table Specifications	90
5.6	Security of Huffman Code	91
5.6.1	Complexity of Recovering the Huffman Table Using Exhaustive Search	92
5.6.2	Security Analysis : Using the Information from Similar Images .	94
5.6.3	Huffman Coding and Arithmetic Coding	98
5.6.4	Chosen plaintext and ciphertext attacks	98
5.7	Experiments	98
5.7.1	Tables with Different Smoothness	99
5.7.2	Tables with Different Quality Levels	101
5.7.3	Probability Distribution of Binary Symbols	102
5.7.4	Modification of Quantization Table Specifications	103
5.7.5	Modification of Huffman Table Specifications	105
5.7.6	Encryption of Huffman Table Specification	106
5.8	Distribution of Differential DC Values	106
5.8.1	Huffman Table Specifications of Various Images	108

5.8.2	Conclusion	120
6	Wavelet Compression and Encryption	121
6.1	Introduction	121
6.2	Encryption with Discrete Wavelet Transform	121
6.2.1	Wavelet Image Compression	122
6.2.2	Encryption Using Random Permutation	123
6.2.3	Chosen Plaintext Attack	124
6.2.4	Enhancing Security	125
6.2.5	Experiments	126
6.2.6	Compression Rate	128
6.2.7	Concluding Remarks	129
6.3	A JPEG2000 Encryption System	129
6.3.1	JPEG2000 Compression System	130
6.3.2	Encryption Using Random Permutation Lists	134
6.3.3	Security of JPEG2000 Encryption	135
6.3.4	Experiments	139
6.3.5	Compression Rate	141
6.3.6	Concluding Remarks	143
6.4	Conclusion	144
7	Image Authentication	151
7.1	Introduction	151
7.2	Preliminaries	152
7.2.1	JPEG Compression	152
7.2.2	SARI Authentication System	153
7.3	New Attacks against the SARI System	155
7.3.1	Attacks	156
7.3.2	Improvement	162
7.3.3	Concluding Remarks	163
7.4	A Secure and Flexible Authentication System for Digital Images	163
7.4.1	A Secure and Flexible Authentication Scheme	164
7.4.2	Designing a Message Authentication Code	176
7.4.3	Constructing Groups	180
7.4.4	Evaluation of the MAC	181
7.4.5	Experiments	185

7.4.6	Quantization Error Distribution	188
7.4.7	Concluding Remarks	190
7.5	Conclusion	190
8	Conclusion	194
8.1	Introduction	194
8.2	Image Encryption	194
8.2.1	Encryption Using Elementary Cryptographic Operations	195
8.2.2	Selective Encryption	196
8.3	Image Authentication	198
8.4	Further Research	198
8.4.1	Image Encryption	198
8.4.2	Image Authentication	199
	Bibliography	201

List of Tables

1.1	The sizes of gray scale images.	6
1.2	The sizes of color images.	6
2.1	Example of LZ77 encoding.	15
3.1	PSNR of reconstructed images lena , mandoril and peppers by sorting DCT coefficients : using largest 16 coefficients and 64 coefficients. . . .	41
4.1	Quality of the recovered images using the method in Section <i>Estimating the DC coefficient of a block</i>	71
4.2	Image quality of the recovered images using the method in Section <i>Improving the algorithm</i>	73
4.3	Quality of the recovered images with half of the DC coefficients in the image.	73
4.4	The sizes of the JPEG file and encoded differential DC values in the file for image quality=50%.	73
4.5	The sizes of the JPEG file and encoded differential DC values in the file for image quality=75%.	76
4.6	The sizes of the JPEG file and encoded differential DC values in the file for image quality=90%.	76
5.1	Table of category numbers and index numbers.	80
5.2	The high-level structure of the JPEG stream.	83
5.3	Frame header.	84
5.4	Scan header.	85
5.5	Quantization table specification (<i>o</i> is the number of quantization tables in the quantization table specifications).	86
5.6	Huffman table specification.	87
5.7	Examples of sizes of encrypted Huffman table specifications.	91

5.8	Variances of probabilities for n bit symbols.	104
6.1	Compression rate and PSNR with permuted subbands when the target compression rate is specified to 8:1.	127
6.2	Compressed file sizes of the random permutation list encryption. . . .	147
6.3	PSNRs of decrypted images using wrong secret keys.	148
7.1	Number of coefficients per group and the MAC size.	187
7.2	Precisions for linear sums ($m = 8$).	187
7.3	DCT coefficients of modified 8×8 block of lena (top) and those of the original (bottom).	188
7.4	Detection of lena's beauty mark (top) and detection of lena modified by a median filter with 3×3 , 5×5 , 7×7 and 9×9 window sizes (bottom). .	192
7.5	Tolerance values for linear sums of $m = 8$ (left) and $m = 16$ (right). . .	192
7.6	Tolerance values for linear sums of $m = 32$ (left) and $m = 64$ (right). .	193
7.7	Tolerance values for linear sums ($m = 128$).	193
7.8	Detection of lena with an 8×8 block at (264,272) position, modified by a median filter with 3×3 , 5×5 , 7×7 and 9×9 window sizes.	193

List of Figures

1.1	Gray scale images : (a) <code>airfield.pgm</code> , (b) <code>airplane.pgm</code> , (c) <code>lena.pgm</code> , (d) <code>mandoril.pgm</code> , and (e) <code>peppers.pgm</code>	8
1.2	Color images : (a) <code>lena.ppm</code> , (b) <code>mandoril.ppm</code> , and (c) <code>peppers.ppm</code>	9
2.1	Communication system.	10
2.2	Example of a Huffman code.	14
2.3	Data compression model.	16
2.4	Model of symmetric encryption system.	17
2.5	Model of public key encryption system.	18
2.6	Wavelet transform (left) and its inverse transform (right).	25
2.7	Wavelet decomposition of an image.	26
2.8	Wavelet decomposition of <code>lena.pgm</code>	27
3.1	Zig-zag scan of 8×8 DCT coefficients in JPEG.	36
3.2	Reconstructed images using sorted largest 16 coefficients : <code>lena</code> (a), <code>mandoril</code> (b) and <code>peppers</code> (c).	42
3.3	Reconstructed images using sorted 64 coefficients : <code>lena</code> (a), <code>mandoril</code> (b) and <code>peppers</code> (c).	42
4.1	Gray scale Lena picture.	65
4.2	Possible pixels patterns at the border in the case of a pair of horizontally neighboring blocks.	66
4.3	The distribution of differences of neighboring pixels in <code>airfield256x256.pgm</code> (left top), <code>mandoril.pgm</code> (right top), <code>lena.pgm</code> (left bottom), and <code>peppers.pgm</code> (right bottom).	71
4.4	The images recovered by the method in Section <i>Estimating the DC co- efficient of a block</i> . <code>airfield256x256.pgm</code> (top left), <code>mandrill.pgm</code> (top right), <code>lena.pgm</code> (bottom left) and <code>peppers.pgm</code> (bottom right).	72

4.5	The images recovered by the method in Section <i>Improving the algorithm</i> . <code>airfield256x256</code> (top left), <code>mandrill</code> (top right), <code>lena</code> (bottom left) and <code>peppers</code> (bottom right).	74
4.6	The images recovered from the half of DC signals by the method in <i>Improving the algorithm</i> . <code>airfield256x256.pgm</code> (top left), <code>mandrill.pgm</code> (top right), <code>lena.pgm</code> (bottom left) and <code>peppers.pgm</code> (bottom right).	75
5.1	Distribution of index numbers for four Huffman codes.	98
5.2	The image with the Huffman AC chrominance table of the image with smoothing.	101
5.3	74% quality image with 75% quality Huffman AC tables.	102
5.4	Probability distribution of one bit binary symbols (left) and two bit binary symbols (right).	103
5.5	Probability distribution of three bit binary symbols (left) and four bit binary symbols (right).	103
5.6	Probability distribution of five bit binary symbols (left) and six bit binary symbols (right).	104
5.7	<i>Decoding with different quantization tables: the original image (left) and recovered image using different quantization tables (right).</i>	105
5.8	<i>Destruction of Huffman table: Viewing the original image (left) and the image with “corrupted” Huffman table (right) using xv.</i>	106
5.9	<i>Distributions of differential DC values of <code>lena.pgm</code> (left) and <code>pepper.pgm</code> (right).</i>	107
5.10	<i>Distributions of differential DC values of <code>lena.pgm</code> (left) and <code>pepper.pgm</code> (right) for $Q_1=2$.</i>	107
5.11	<i>Distributions of differential DC values of <code>lena.pgm</code> (left) and <code>pepper.pgm</code> (right) for $Q_1=8$.</i>	108
5.12	<i>Distributions of differential DC values of <code>lena.pgm</code> (left) and <code>pepper.pgm</code> (right) for $Q_1=16$.</i>	108
5.13	<i>Distributions of differential DC values of <code>lena.pgm</code> (left) and <code>pepper.pgm</code> (right) for $Q_1=32$.</i>	109
5.14	<i>Distributions of differential DC values of <code>lena.pgm</code> (left) and <code>pepper.pgm</code> (right) for $Q_1=80$.</i>	109
6.1	The original image (left) and the recovered image without inverse-permutations when the image is encoded with subband 0 permuted (right).	128

6.2	The recovered image without inverse-permutations when the image is encoded with subband 15 permuted (left) and the recovered image without inverse-permutations when the image is encoded with subbands 0 to 15 permuted (right).	128
6.3	The recovered image without inverse-permutations when the image is encoded with subbands 0 to 7 permuted (left) and the recovered image without inverse-permutations when the image is encoded with subbands 8 to 15 permuted (right).	129
6.4	Code-block and bit-planes : A quantized coefficient consists of bits and A code-block consists of $m \times n$ quantized coefficients. The i th bit-plane is the collection of i th significant bits of the $m \times n$ quantized coefficients. The bits in a bit-plane are scanned as shown by the arrows.	133
6.5	Encrypting subband 0 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). The color spots correspond to low subband coefficients. The encryption decreased the image quality but the details (i.e. edges) are visible.	139
6.6	Encrypting subband 7 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). The encryption decreased the quality less compared to encrypting low subbands. The images are recognizable.	140
6.7	Encrypting subband 13 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). Some noise can be found in the active regions but the encryption did not decrease the quality very much. The images are similar to the original ones.	140
6.8	Encrypting subband 1, 2, and 3 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). The quality drop due to the encryption is large but the edges are visible.	141
6.9	Encrypting subband 7, 8, and 9 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). The encryption has a similar effect to “oil painting”. It may be visually disturbing but the images remain recognizable.	141
6.10	Encrypting subband 13, 14, and 15 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). Some noise can be found in the active regions but the quality drop is small.	142
6.11	Encrypting all subbands (0 to 15) : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right). The images are not comprehensible.	142

6.12	Encrypting bit-plane 0 of subbands 1, 2 and 3 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	143
6.13	Encrypting bit-plane 1 of subbands 1, 2 and 3 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	143
6.14	Encrypting bit-plane 2 of subbands 1, 2 and 3 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	144
6.15	Encrypting bit-plane 0 of subbands 7, 8 and 9 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	144
6.16	Encrypting bit-plane 1 of subbands 7, 8 and 9 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	145
6.17	Encrypting bit-plane 2 of subbands 7, 8 and 9 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	145
6.18	Encrypting bit-plane 0 of subbands 13, 14 and 15 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	146
6.19	Encrypting bit-plane 1 of subbands 13, 14 and 15 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	146
6.20	Encrypting bit-plane 2 of subbands 13, 14 and 15 : <code>lena.ppm</code> (left), <code>mandoril.ppm</code> (middle) and <code>peppers.ppm</code> (right).	146
6.21	Frequencies of 10 <i>contexts</i> in the encoding of <code>lena.ppm</code> , <code>mandoril.ppm</code> and <code>peppers.ppm</code> without encryption (left column) and with encryption (right column).	149
6.22	Frequencies of pairs of <i>contexts</i> and <i>decision</i> in the encoding of <code>lena.ppm</code> , <code>mandoril.ppm</code> and <code>peppers.ppm</code> without encryption (left column) and with encryption (right column).	150
7.1	Pattern “8” (left) and a pattern similar to \nearrow (right).	158
7.2	Example: Original image (left) and close up (right).	159
7.3	Close up of the modified image (left) and difference between the original and modified images (right). The large gray region, the darker part and the brighter part correspond to $\delta^{(i,j)} = 0$, $\delta^{(i,j)} < 0$ and $\delta^{(i,j)} > 0$, respectively.	159
7.4	Original license plate.	160
7.5	Removal experiments of “9” (left) and “5” (right).	160
7.6	The two images will be authenticated with the coefficients 0-10 (left) and 0-59 (right) protected.	162
7.7	MAC generation and JPEG compression.	165

7.8	MAC verification and JPEG decompression.	165
7.9	Encoding of $Y_j^{(u,v)}$ and error tolerance.	174
7.10	Lena with a beauty mark (left) and close-up of the modified region (right).	186
7.11	Lena using a median filter. 3×3 (a), 5×5 (b), 7×7 (c) and 9×9 (d) window sizes.	186
7.12	Close up of the right eye of lena. The center 8×8 block is at position (264,272) modified by a median filter with 9×9 window sizes.	188
7.13	Distribution of errors : lena	189
7.14	Distribution of errors : peppers	190
7.15	Distribution of errors : airplane	191