Image and Video Encryption

From Digital Rights Management to Secured Personal Communication

Advances in Information Security

Sushil Jajodia
Consulting editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers as well as developers are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

INTRUSION DETECTION AND CORRELATION: Challenges and Solutions by Christopher Kruegel, Fredrik Valeur and Giovanni Vigna; ISBN: 0-387-23398-9
THE AUSTIN PROTOCOL COMPILER by Tommy M. McGuire and Mohamed G. Gouda; ISBN: 0-387-23227-3
ECONOMICS OF INFORMATION SECURITY by L. Jean Camp and Stephen Lewis; ISBN: 1-4020-8089-1
PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC KEY CRYPTOGRAPHY by Song Y. Yan; ISBN: 1-4020-7649-5
SYNCHRONIZING E-SECURITY by Godfried B. Williams; ISBN: 1-4020-7646-0
INTRUSION DETECTION IN DISTRIBUTED SYSTEMS: An Abstraction-Based Approach by Peng Ning, Sushil Jajodia and X. Sean Wang ISBN: 1-4020-7624-X
SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4
SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
APPLICATIONS OF DATA MINING IN COMPUTER SECURITY, edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3
MOBILE COMPUTATION WITH FUNCTIONS by Zeliha Dilsun Kırlı, ISBN: 1-4020-7024-1

Additional information about this series can be obtained from
http://www.wkap.nl/prod/s/ADIS

Image and Video Encryption
From Digital Rights Management to Secured Personal Communication

by

Andreas Uhl
Andreas Pommer
Salzburg University, Austria

Springer

eBook ISBN: 0-387-23403-9
Print ISBN: 0-387-23402-0

Created in the United States of America

I dedicate this book to my wife Jutta – thank you for your understanding and help in my ambition to be both, a loving and committed partner and father as well as an enthusiastic scientist.

Andreas Uhl

I dedicate this book to all the people with great ideas who make the net an enjoyable place.

Andreas Pommer

Contents

Dedication v

List of Figures ix

List of Tables xiii

Preface xv

Acknowledgments xvii

1. INTRODUCTION 1

2. VISUAL DATA FORMATS 11
   1 Image and Video Data 11
   2 DCT-based Systems 12
   3 Wavelet-based Systems 14
   4 Further Techniques 18

3. CRYPTOGRAPHY PRIMER 21
   1 Introduction, Terminology 21
   2 Secret key vs. Public key Cryptography 22
   3 Block Ciphers 23
   4 Stream Ciphers 27
   5 Hybrid Algorithms, some Applications 28
   6 Cryptanalysis Overview 29
   7 Further Information 30

4. APPLICATION SCENARIOS FOR THE ENCRYPTION OF VISUAL DATA 31
   1 Security provided by Infrastructure or Application 31
   2 Full Encryption vs. Selective Encryption 32
   3 Interplay between Compression and Encryption 37

5. IMAGE AND VIDEO ENCRYPTION 45
1 DCT-based Techniques 47
2 Wavelet-based Techniques 82
3 Further Techniques 115
4 Transparent Encryption 127
5 Commercial Applications and Standards 129

6. CONCLUSIONS 135

Appendices 137
A Copyrighted sections 137
B Test Images and Videos 139
1 Cover Page 139
2 Test Images 139
3 Sequence 1 — Bowing 141
4 Sequence 2 — Surf Side 141
5 Sequence 3 — Coast Guard 141
6 Sequence 4 — Akiyo 142
7 Sequence 5 — Calendar 142
C Authors' Biographies 143

References 145

Index 159

List of Figures

2.1 Frame-structure of video (football sequence) 11

2.2 Block-Matching motion estimation 13

2.3 1-D and 2-D wavelet decomposition 15

2.4 Comparison of DCT-based and wavelet-based compression schemes 16

2.5 Spatial Orientation Tree 17

2.6 JPEG 2000 coding pipeline 18

4.1 Runtime analysis of JJ2000 compression for increasing image size 36

4.2 Testimages used to evaluate the rate distortion performance. 39

4.3 Rate-distortion performance of JPEG and JPEG 2000. 39

4.4 Time demand. 40

4.5 Wireless connections, AES encryption. 42

4.6 Wired connections (ethernet), AES encryption 42

5.1 VLC encryption results 63

5.2 MB permutation results 65

5.3 DCT block permutation results 66

5.4 Motion vector permutation results 67

5.5 Results of motion vector prediction sign change 68

5.6 Results of motion vector residual sign change 68

5.7 DCT coefficient sign change results 69

5.8 I-frame sign change results 70

5.9 I-frame + I-block sign change results 70

5.10 DC and AC coefficient mangling results 71

5.11 DC and AC coefficient mangling results 72

5.12 DC and AC coefficient mangling results 72

5.13 Modified Scan Order (example) 73

5.14 Zig-zag order change results 74

5.15 Compression performance — baseline and progressive JPEG 79

5.16 Lena image; a three level pyramid in HP mode is used with the lowest resolution encrypted 79

5.17 Mandrill image; SS mode is used with DC and first AC coefficient encrypted 80

5.18 Subjective quality of reconstructed Lena image 82

5.19 Images from Fig. 5.18 median filtered (3x3 kernel) and blurred (5x5 filter). 83

5.20 Compression performance, Lena image 512 x 512 pixels 86

5.21 Reconstruction using random filters 89

5.22 Reconstructed image where the heuristic failed at the finest level of decomposition 89

5.23 Reconstructed image where the heuristic failed at 3 out of 5 levels 89

5.24 Quality of JPEG 2000 compression 91

5.25 Attack against a 1-D parameter scheme 92

5.26 Quality of attacked images 93

5.27 Attack against a 2-D parameter scheme 94

5.28 Quality of attacked images 95

5.29 Quality values for $K = 0$. 97

5.30 Parameterised biorthogonal 4/8 filters. 98

5.31 Frequency response 98

5.32 minimum and maximum level of decomposition influencing the quality 100

5.33 Various weight factors for the decomposition decision 101

5.34 All parameters of figures 5.32(a), 5.32(b), 5.33(a), 5.33(b) in one plot 102

5.35 Variance for increasing number of coefficients 104

5.36 Reconstruction using a wrong decomposition tree 105

5.37 Comparison of selective encryption 110

5.38 Angiogram: Comparison of selective encryption 110

5.39 Comparison of selective encryption 111

5.40 Comparison of selective encryption 112

5.41 Angiogram: PSNR of reconstructed images after replacement attack 113
5.42 PSNR of reconstructed images after replacement attack 113
5.43 Visual quality of reconstructed Angiogram after replacement 114
5.44 Visual quality of reconstructed Lena after replacement attack 115
5.45 Baker Map (1/2,1/2). 116
5.46 Baker Map (1/2,1/2) applied to Lena. 118
5.47 Visual examples for selective bitplane encryption, direct reconstruction. 119
5.48 Further visual examples for selective bitplane encryption. 120
5.49 Visual examples for encryption of MSB and one additional bitplane. 121
5.50 Visual examples for the efficiency of the Replacement Attack. 122
5.51 MSB of the Lena image and reconstructed Bitplane. 123
5.52 Combination of two half-images after Reconstruction Attack. 124
5.53 Example for leaf ordering I and II. 125

List of Tables

4.1 Number of basic operations for AES encryption 35

4.2 Magnitude order of operations for wavelet transform 35

4.3 Numbers of instructions for wavelet decompositions 36

5.1 Overall assessment of the Zig-zag Permutation Algorithm 49

5.2 Overall assessment of Frequency-band Coefficient Shuffling 49

5.3 Overall assessment of Scalable Coefficient Encryption (in coefficient domain) 50

5.4 Overall assessment of Coefficient Sign Bit Encryption 51

5.5 Overall assessment of Secret Fourier Transform Domain 51

5.6 Overall assessment of Secret Entropy Encoding 52

5.7 Overall assessment of Header Encryption 52

5.8 Overall assessment of Permutations applied at the bitstream level 54

5.9 Overall assessment of One-time pad VEA 56

5.10 Overall assessment of Byte Encryption 56

5.11 Overall assessment of VLC Codeword encryption 57

5.12 Overall assessment of I-frame Encryption 59

5.13 Overall assessment of Motion Vector Encryption 60

5.14 Objective quality (PSNR in dB) of reconstructed images 81

5.15 Overall assessment of Coefficient Selective Bit Encryption 84

5.16 JPEG 2000/SPIHT: all subbands permuted, max. observed file size increase at a medium compression rate ranging from 25 up to 45 86

5.17 Overall assessment of Coefficient Permutation 87

5.18 Overall assessment of Coefficient Block Permutation and Rotation 88
5.19 Overall assessment of Secret Wavelet Filters 90
5.20 Overall assessment of Secret Wavelet Filters: Parametrisation Approach 99
5.21 Overall assessment of Secret Subband Structures 107
5.22 Overall assessment of SPIHT Encryption 108
5.23 Overall assessment of JPEG 2000 Encryption 114
5.24 Overall assessment of Permutations 116
5.25 Overall assessment of Chaotic Encryption 117
5.26 PSNR of images after direct reconstruction 120
5.27 Number of runs consisting of 5 identical bits 121
5.28 Overall assessment of Bitplane Encryption 124
5.29 Overall assessment of Quadtree Encryption 126
5.30 Overall assessment of Encrypting Fractal Encoded Data 126
5.31 Overall assessment of the Virtual Image Cryptosystem 127

Preface

Contrasting to classical encryption, security may not be the most important aim for an encryption system for images and videos. Depending on the type of application, other properties (like speed or bitstream compliance after encryption) might be equally important as well. As an example, the terms “soft encryption” or “selective encryption” are sometimes used as opposed to classical “hard” encryption schemes like full AES encryption in this context. Such schemes do not strive for maximum security and trade off security for computational complexity. They are designed to protect multimedia content and fulfil the security requirements for a particular multimedia application. For example, real-time encryption for an entire video stream using classical ciphers requires much computation time due to the large amounts of data involved, on the other hand many multimedia applications require security on a much lower level (e.g. TV broadcasting) or should protect their data just for a short period of time (e.g. news broadcast). Therefore, the search for fast encryption procedures specifically tailored to the target environment is mandatory for multimedia security applications. The fields of interest to deploy such solutions span from digital rights management (DRM) schemes to secured personal communication.

Being the first monograph exclusively devoted to image and video encryption systems, this book provides a unified overview of techniques for the encryption of visual data, ranging from commercial applications in the entertainment industry (like DVD or Pay-TV DVB) to more research oriented topics and recently published material. To serve this purpose, we discuss and evaluate different techniques from a unified viewpoint, we provide an extensive bibliography of material related to these topics, and we experimentally compare different systems proposed in the literature and in commercial systems. Several techniques described in this book can be tested online, please refer to `http://www.ganesh.org/book/`. The cover shows images of the authors which have been encrypted in varying strength using techniques described in section 1.3.8 (chapter 5) in this book.

The authors are members of the virtual laboratory "WAVILA" of the European Network of Excellence ECRYPT, which focuses on watermarking technologies and related DRM issues. National projects financed by the Austrian Science Fund have been supporting the work in the multimedia security area. Being affiliated with the Department of Scientific Computing at Salzburg University, Austria, the authors work in the Multimedia Signal Processing and Security research group, which will be organising as well the 2005 IFIP Communications and Multimedia Security Conference CMS 2005 and an associated summerschool. For more informations, please refer to the website of our group at `http://www.scicomp.sbg.ac.at/research/multimedia.html` or at `http://www.ganesh.org/`.

Acknowledgments

This work has been partially funded by the Austrian Science Fund FWF, in the context of projects no. 13732 and 15170. Parts of the text are copyrighted material. Please refer to the corresponding appendix to obtain detailed information.