Preface

Multimedia Encoding Methodologies for Selective Access with Traitor Tracing

This book explores two very interesting but different problems in the emerging area of multimedia security. It has been well recognized that the traditional requirements of information security which are confidentiality, integrity and availability of information need to be augmented by the increasingly important requirements of privacy and accountability. In line with these trends, the main theme of this book is merging selective access with traitor tracing, which is presented in two parts.

Part-I: Joint Fingerprinting and Decryption

Inspired by the chameleon cipher, a joint fingerprinting and decryption (JFD) architecture is proposed for multicast content protection. Most ciphers have been constructed based on the two principles of confusion and diffusion, as originally proposed by Shannon in his 1949 paper "Communication theory of secrecy systems". While the process of diffusion disperses the statistics of the plaintext across the ciphertext, confusion makes the relationship between the keys and the ciphertext more complex. Integration of fingerprinting with decryption however enforces a softening of the encryption process and consequently a cipher with controlled confusion is deployed. In JFD, different decryption keys are derived from a single encryption key and this carefully orchestrated structural difference is responsible for casting a fingerprint at the receiver during the decryption process. Based on this methodology a DCT sign bit modulation and fingerprinting algorithm is proposed for protecting and tracking JPEG compressed images in a multicast environment.

An attack which can never be ignored in most fingerprinting applications is collusion. Pirates amongst legitimate subscribers to a video multicast, may choose to fuse several decryption keys or fingerprinted copies to remove traces of the fingerprint. Such attacks can be deterred by integrating anti-collusion codes (ACCs) into the decryption key design. ACCs create an intrinsic association between the keys, which must be preserved by the soft decryption process to enhance collusion resistance of the fingerprinted copies.

Amongst the different forms of collusion, linear collusion or averaging is the most common and effective approach, from the point of view of the traitors. To counteract this, the most fundamental unit of a fingerprint, which is a mark, is designed to be robust to single copy attacks but sensitive to multi-copy fusion. This semi-fragility creates a nexus between the collusion attack model, watermark modulation strategy and the mark distribution across users (controlled by the ACC). For sign modulated fingerprints, linear collusions can be characterized in the bit domain as a majority vote. This majority vote model serves as an excellent approximation for other forms

of collusion such as random mixing of data streams and other spatial domain collusion operations such as min, max and median pixel processing functions.

To construct the ACC, a graphical approach based on edge coloring is used to build a unique association between every K-subset of fingerprints for a total of $n > K$ users. The design ensures that a majority vote of K or fewer codewords out of n results in a unique bit pattern, which is necessary to counteract random mixing attacks. We also present an alternative and simpler construction based on Hadamard 2-designs, which is more compact but does not satisfy the uniqueness constraint for $n > 7, K > 3$.

Part-II: Anonymous Fingerprinting with Shared Access Control

Non-perfect secret sharing schemes open up the possibility of juggling with secrecy to control leakage of information between secrets and shares, thereby serving as a valve to balance anonymity with traceability.

As a first step in the investigation we propose a non-perfect secret sharing scheme called MIX-SPLIT, to explore the characteristics which accompany the sacrifice of information theoretic secrecy. Two independent but statistically identical sequences of random variables, are mixed and then split to produce a closely associated group of n shares. This statistical similarity allows the inheritance to be concealed and so each share can be treated as a traceable anonymous descendant of two parent secrets, a property, which can be used for constructing anonymous fingerprinting schemes.

The anti-collusion code which controls the mixing and splitting of the two secrets also satisfies the property of *closure*. That is, the construction also ensures that when these n shares are stacked, the two secrets can be retrieved by simply evaluating a majority bit vote and minority bit vote respectively.

This opens up the possibility of integrating joint access with traitor tracing, which can be applied towards the protection and tracking of highly sensitive medical records. Non-perfectness is an invitation to traitors, who do not know how close they will get to the original secret by colluding their shares and if the information leaked out by the coalition is sufficient to form a correct diagnosis. By design, any illegitimate fusion is expected to result in a distorted record which can also be traced.

Other applications which inherit some of the properties of MIX-SPLIT include selective access of strategic maps and distributed secure storage of biometric PINs.

Contents

Part I: Joint Fingerprinting and Decryption **1**

1 Multicast Content Protection **3**
1.1 Watermarking in a DRM system 4
1.2 Encryption in a broadcast environment 6
1.3 Multicast Environment 7
1.4 Multicast security issues 8
1.4.1 Authentication 9
1.4.2 Integrity 10
1.4.3 Confidentiality and key management 11
1.4.4 Content Identification through fingerprinting 14
1.5 Existing security architectures for multicast fingerprinting 15
1.5.1 Group based fingerprinting applied to multicast 17
1.5.2 Fingerprinting in trusted receiver devices 18
1.5.3 Distributed fingerprinting 19
1.5.4 Transmitter-side embedding coupled with selective decryption 19
1.6 Distributed fingerprinting: Watercasting and WHIM 20
1.6.1 Watercasting 20
1.6.2 WHIM 22
1.7 Problem definition and book outline 24
1.7.1 Outline 25

2 Joint Fingerprinting and Decryption **27**
2.1 Related work: Chameleon 27
2.2 JFD architecture 28
2.3 Design challenges 29
2.3.1 Imperceptibility versus secrecy 30
2.3.2 Collusion attack model and countermeasures 30
2.4 JFD implementation 32
2.4.1 Feature extraction for selective encryption 32
2.4.2 Decryption key design 33
2.5 Softening of the encryption process in JFD 35
2.6 Analytical model for JFD 36

2.6.1 Encryption . . . 36
2.6.2 Decryption key design and fingerprinting . . . 37
2.6.3 Capacity and perceptual constraints . . . 37
2.6.4 Secrecy and fingerprint capacity . . . 38
2.6.5 Salient features of the analytical model . . . 40

3 Sign bit embedding and detection 43
3.1 Life cycle of video security . . . 43
3.2 Sign bit encryption and embedding . . . 44
3.2.1 DCT and quantization . . . 44
3.2.2 Texture map creation . . . 47
3.2.3 Creation and compression of the encryption map $[B_E]$ . . . 48
3.2.4 Extraction of significant AC coefficients . . . 48
3.2.5 Encryption and decryption key generation . . . 48
3.2.6 Incorporating collusion resistance . . . 49
3.3 Detection of sign bit modulated fingerprints . . . 51
3.3.1 Detection of orthogonal fingerprints . . . 53
3.3.2 Noise model . . . 54
3.3.3 Detection threshold . . . 55
3.3.4 Simulation results for effect of compression on orthogonal fingerprints . . . 57
3.4 Detection of ACC encoded fingerprints . . . 57
3.5 Decryption key size and secrecy . . . 58

4 Anti-Collusion codes for Multimedia Forensics 61
4.1 Related literature . . . 62
4.1.1 Frameproof and collusion-secure codes of Boneh and Shah . . . 62
4.1.2 Traitor tracing by Chor, Fiat and Naor . . . 63
4.1.3 Code modulation and ACCs by Trappe et al. . . . 63
4.2 Effect of Linear collusion on sign bit modulated fingerprints . . . 64
4.3 ACC construction . . . 69
4.3.1 Detecting 2-collusions . . . 70
4.3.2 Detecting $K \leq 3$-collusions . . . 70
4.4 Construction by Edge Coloring . . . 71
4.4.1 Example: $n = 5, K \leq 3$ (fewer colors) . . . 72
4.5 Collusion invariants . . . 74
4.5.1 Algorithm . . . 75
4.6 Construction using symmetric block designs . . . 78
4.6.1 Balanced incomplete block designs (BIBDs) . . . 79
4.6.2 Symmetric design examples . . . 80
4.6.3 Construction of (v, v+1/2, v+1/4)-designs from Hadamard matrices . . . 81

4.7 Collusion attacks and traitor tracing . . . 81
4.7.1 Linear collusion with some pre-processing . . . 82
4.7.2 Non-linear collusion . . . 82
4.7.3 Fingerprint detection and traitor tracing . . . 82
4.7.4 Simulation results and analysis . . . 83

Part II: Anonymous Fingerprinting with Shared Access 90

5 MIX-SPLIT 93
5.1 Some perfect secret sharing schemes . . . 93
5.1.1 Shamir's scheme . . . 94
5.1.2 Blakeley's geometric secret sharing scheme . . . 94
5.1.3 Visual sharing by Naor and Shamir . . . 95
5.2 Non-perfect secret sharing . . . 95
5.3 Problem formulation . . . 96
5.4 MIX-SPLIT . . . 98
5.5 Codebook for MIX-SPLIT . . . 100
5.5.1 Codebook examples . . . 101
5.5.2 Association between shares . . . 102
5.5.3 Statistical Similarity . . . 102
5.5.4 Concealed Inheritance . . . 105
5.6 Secrecy and Privacy . . . 106
5.6.1 Anonymity with Traceability . . . 108
5.6.2 Scenarios . . . 110
5.7 Share collusion attack model . . . 112

6 Applications 117
6.1 Authentication and tracing of copies of a digital portrait . . . 117
6.1.1 Architecture . . . 118
6.2 Selective access . . . 119
6.2.1 Algorithm description . . . 120
6.2.2 Simulation . . . 121
6.3 Distributed and secure storage of biometrics . . . 122
6.3.1 Airport Security . . . 124
6.4 Joint access with tracing . . . 125
6.5 Implementation: Joint access with Tracing . . . 126
6.5.1 Sign encryption of medical images . . . 126
6.5.2 Decryption share generation . . . 127
6.5.3 Fingerprint detection . . . 127
6.5.4 Results for a 5-out-of-5 sharing scheme . . . 128

7 Conclusions and Future work **137**
7.1 Reducing side information in JFD 137
7.2 JFD based on wavelet packet decomposition 139
7.3 Non-perfect secret sharing methods for multicast fingerprinting? . . . 141
7.4 Contributions of this research 143

Bibliography **145**