Contents

Foreword by Gildas Avoine xi

Foreword by Cédric Richard xiii

Preface xv
William PUECH

Chapter 1. Biometrics and Applications 1
Christophe CHARRIER, Christophe ROSENBERGER and Amine NAIT-ALI

1.1. Introduction 1
1.2. History of biometrics 3
1.3. The foundations of biometrics 6
1.3.1. Uses of biometrics 7
1.3.2. Definitions 7
1.3.3. Biometric modalities 8
1.4. Scientific issues 10
1.4.1. Presentation attacks 10
1.4.2. Acquisition of new biometric data or hidden biometrics 12
1.4.3. Quality of biometric data 14
1.4.4. Efficient representation of biometric data 19
1.4.5. Protecting biometric data 22
1.4.6. Aging biometric data 24
1.5. Conclusion 25
1.6. References 26

Chapter 2. Protecting Documents Using Printed Anticopy Elements 31
Iuliia TKACHENKO, Alain TREMEAU and Thierry FOURNEL

2.1. Introduction 31
2.2. Document authentication approaches: an overview 33
2.3. Print test shapes 35
2.3.1. Print test signatures 36
2.3.2. Glyphs 38
2.3.3. Guilloches 39
2.4. Copy-sensitive graphical codes 41
2.4.1. Copy detection pattern 42
2.4.2. Two-level barcodes 44
2.4.3. Watermarked barcodes 47
2.4.4. Performance of CSGC authentication 48
2.5. Conclusion 52
2.6. References 52

Chapter 3. Verifying Document Integrity 59
Petra GOMEZ-KRÄMER

3.1. Introduction 59
3.2. Fraudulent manipulation of document images 62
3.2.1. Imitation 62
3.2.2. Copy-and-paste of a region from the same document 62
3.2.3. Copy-and-paste of a region from another document 63
3.2.4. Deleting information 63
3.3. Degradation in printed and re-scanned documents 64
3.3.1. Degradations linked to the print process 65
3.3.2. Degradations linked to scanning 66
3.3.3. Degradation models 67
3.4. Active approaches: protection by extrinsic fingerprints 68
3.4.1. Watermarking a document 68
3.4.2. Digital signatures 73
3.5. Passive approaches: detecting intrinsic characteristics 76
3.5.1. Printer identification 77
3.5.2. Detecting graphical clues 80
3.5.3. Other approaches 81
3.6. Conclusion 82
3.7. References 82

Chapter 4. Image Crypto-Compression 91
Vincent ITIER, Pauline PUTEAUX and William PUECH

4.1. Introduction 91
4.2. Preliminary notions 93
4.2.1. The JPEG image format 93
4.2.2. Introduction to cryptography 96
4.3. Image encryption 100
4.3.1. Naive methods 102
4.3.2. Chaos-based methods 104
4.3.3. Encryption-then-compression 105
4.4. Different classes of crypto-compression for images 106
4.4.1. Substitution-based crypto-compression 108
4.4.2. Shuffle-based crypto-compression 108
4.4.3. Hybrid crypto-compression 110
4.5. Recompressing crypto-compressed JPEG images 113
4.5.1. A crypto-compression approach robust to recompression 114
4.5.2. Recompression of a crypto-compressed image 117
4.5.3. Decoding a recompressed version of a crypto-compressed JPEG image 119
4.5.4. Illustration of the method 122
4.6. Conclusion 124
4.7. References 124

Chapter 5. Crypto-Compression of Videos 129
Cyril BERGERON, Wassim HAMIDOUCHE and Olivier DÉFORGES

5.1. Introduction 129
5.1.1. Background 129
5.1.2. Video compression 130
5.1.3. Video security 131
5.2. State of the art 131
5.2.1. Naive encryption 132
5.2.2. Partial encryption 133
5.2.3. Perceptual encryption 134
5.2.4. Crypto-compression methods 134
5.2.5. Selective encryption methods 135
5.3. Format-compliant selective encryption 136
5.3.1. Properties 136
5.3.2. Constant bitrate format compliant selective encryption 139
5.3.3. Standardized selective encryption 140
5.3.4. Locally applied selective encryption 143
5.3.5. Decrypting selective encryption 149
5.4. Image and video quality 150

5.4.1. Experiments on encryption solutions 151
5.4.2. Video quality: experimental results 154
5.4.3. CSE: a complete real-time solution 162
5.5. Perspectives and directions for future research 163
5.5.1. Versatile Video Coding 163
5.5.2. Immersive and omnidirectinal video 164
5.6. Conclusion 165
5.7. References 166

Chapter 6. Processing Encrypted Multimedia Data Using Homomorphic Encryption 173
Sébastien CANARD, Sergiu CARPOV, Caroline FONTAINE and Renaud SIRDEY

6.1. Context 173
6.2. Different classes of homomorphic encryption systems 176
6.2.1. Partial solutions in classic cryptography 176
6.2.2. Complete solutions in cryptography using Euclidean networks . . . 178
6.3. From theory to practice 181
6.3.1. Algorithmics 183
6.3.2. Implementation and optimization 183
6.3.3. Managing and reducing the size of encrypted elements 189
6.3.4. Security 191
6.4. Proofs of concept and applications 193
6.4.1. Facial recognition 193
6.4.2. Classification 196
6.4.3. RLE and image compression 201
6.5. Conclusion 207
6.6. Acknowledgments 207
6.7. References 207

Chapter 7. Data Hiding in the Encrypted Domain 215
Pauline PUTEAUX and William PUECH

7.1. Introduction: processing multimedia data in the encrypted domain . . 215
7.1.1. Applications: visual secret sharing 216
7.1.2. Applications: searching and indexing in encrypted image databases 217
7.1.3. Applications: data hiding in the encrypted domain 218
7.2. Main aims 219
7.2.1. Digital rights management 220
7.2.2. Cloud storage 220
7.2.3. Preserving patient confidentiality 220
7.2.4. Classified data 220
7.2.5. Journalism 220
7.2.6. Video surveillance 221

7.2.7. Data analysis . . . 221
7.3. Classes and characteristics . . . 221
7.3.1. Properties . . . 221
7.3.2. Classic approaches to encryption . . . 223
7.3.3. Evaluation criteria . . . 227
7.4. Principal methods . . . 231
7.4.1. Image partitioning . . . 231
7.4.2. Histogram shifting . . . 232
7.4.3. Encoding . . . 234
7.4.4. Prediction . . . 235
7.4.5. Public key encryption . . . 237
7.5. Comparison and discussion . . . 237
7.6. A high-capacity data hiding approach based on MSB prediction . . . 239
7.6.1. General description of the method . . . 239
7.6.2. The CPE-HCRDH approach . . . 243
7.6.3. The EPE-HCRDH approach . . . 245
7.6.4. Experimental results for both approaches . . . 249
7.7. Conclusion . . . 253
7.8. References . . . 253

Chapter 8. Sharing Secret Images and 3D Objects . . . 259
Sébastien BEUGNON, Pauline PUTEAUX and William PUECH

8.1. Introduction . . . 259
8.2. Secret sharing . . . 261
8.2.1. Classic methods . . . 262
8.2.2. Hierarchical aspects . . . 264
8.3. Secret image sharing . . . 272
8.3.1. Principle . . . 272
8.3.2. Visual cryptography . . . 273
8.3.3. Secret image sharing (polynomial-based) . . . 274
8.3.4. Properties . . . 275
8.4. 3D object sharing . . . 276
8.4.1. Principle . . . 276
8.4.2. Methods without format preservation . . . 276
8.4.3. Methods with format preservation . . . 277
8.5. Applications for social media . . . 280
8.6. Conclusion . . . 287
8.7. References . . . 288

List of Authors . . . 293

Index . . . 295