

Contents

Foreword by Gildas Avoine	xi
Foreword by Cédric Richard	xiii
Preface	xv
William PUECH	
Chapter 1. How to Reconstruct the History of a Digital Image, and of Its Alterations	1
Quentin BAMMEY, Miguel COLOM, Thibaud EHRET, Marina GARDELLA, Rafael GROMPONE, Jean-Michel MOREL, Tina NIKOUKHAH and Denis PERRAUD	
1.1. Introduction	2
1.1.1. General context	2
1.1.2. Criminal background	3
1.1.3. Issues for law enforcement	4
1.1.4. Current methods and tools of law enforcement	5
1.1.5. Outline of this chapter	5
1.2. Describing the image processing chain	8
1.2.1. Raw image acquisition	8
1.2.2. Demosaicing	8
1.2.3. Color correction	10
1.2.4. JPEG compression	11
1.3. Traces left on noise by image manipulation	11
1.3.1. Non-parametric estimation of noise in images	11
1.3.2. Transformation of noise in the processing chain	13
1.3.3. Forgery detection through noise analysis	15

1.4. Demosaicing and its traces	18
1.4.1. Forgery detection through demosaicing analysis	19
1.4.2. Detecting the position of the Bayer matrix	20
1.4.3. Limits of detection demosaicing	23
1.5. JPEG compression, its traces and the detection of its alterations	23
1.5.1. The JPEG compression algorithm	23
1.5.2. Grid detection	25
1.5.3. Detecting the quantization matrix	27
1.5.4. Beyond indicators, making decisions with a statistical model	28
1.6. Internal similarities and manipulations	31
1.7. Direct detection of image manipulation	33
1.8. Conclusion	34
1.9. References	35
Chapter 2. Deep Neural Network Attacks and Defense: The Case of Image Classification	41
Hanwei ZHANG, Teddy FURON, Laurent AMSALEG and Yannis AVRITHIS	
2.1. Introduction	41
2.1.1. A bit of history and vocabulary	42
2.1.2. Machine learning	44
2.1.3. The classification of images by deep neural networks	46
2.1.4. <i>Deep Dreams</i>	48
2.2. Adversarial images: definition	49
2.3. Attacks: making adversarial images	51
2.3.1. About white box	52
2.3.2. Black or gray box	62
2.4. Defenses	64
2.4.1. Reactive defenses	64
2.4.2. Proactive defenses	66
2.4.3. Obfuscation technique	67
2.4.4. Defenses: conclusion	68
2.5. Conclusion	68
2.6. References	69
Chapter 3. Codes and Watermarks	77
Pascal LEFÈVRE, Philippe CARRÉ and Philippe GABORIT	
3.1. Introduction	77
3.2. Study framework: robust watermarking	78
3.3. Index modulation	81
3.3.1. LQIM: insertion	81
3.3.2. LQIM: detection	82

3.4. Error-correcting codes approach	82
3.4.1. Generalities	84
3.4.2. Codes by concatenation	86
3.4.3. Hamming codes	88
3.4.4. BCH codes	90
3.4.5. RS codes	93
3.5. Contradictory objectives of watermarking: the impact of codes	96
3.6. Latest developments in the use of correction codes for watermarking	98
3.7. Illustration of the influence of the type of code, according to the attacks	102
3.7.1. JPEG compression	103
3.7.2. Additive Gaussian noise	106
3.7.3. Saturation	106
3.8. Using the rank metric	108
3.8.1. Rank metric correcting codes	109
3.8.2. Code by rank metric: a robust watermarking method for image cropping	113
3.9. Conclusion	121
3.10. References	121

Chapter 4. Invisibility 129

Pascal LEFÈVRE, Philippe CARRÉ and David ALLEYSSON

4.1. Introduction	129
4.2. Color watermarking: an approach history?	131
4.2.1. Vector quantization in the RGB space	132
4.2.2. Choosing a color direction	133
4.3. Quaternionic context for watermarking color images	135
4.3.1. Quaternions and color images	135
4.3.2. Quaternionic Fourier transforms	137
4.4. Psychovisual approach to color watermarking	139
4.4.1. Neurogeometry and perception	139
4.4.2. Photoreceptor model and trichromatic vision	141
4.4.3. Model approximation	144
4.4.4. Parameters of the model	145
4.4.5. Application to watermarking color images	146
4.4.6. Conversions	147
4.4.7. Psychovisual algorithm for color images	148
4.4.8. Experimental validation of the psychovisual approach for color watermarking	151
4.5. Conclusion	155
4.6. References	157

Chapter 5. Steganography: Embedding Data Into Multimedia Content	161
Patrick BAS, Rémi COGRANNE and Marc CHAUMONT	
5.1. Introduction and theoretical foundations	162
5.2. Fundamental principles	163
5.2.1. Maximization of the size of the embedded message	163
5.2.2. Message encoding	165
5.2.3. Detectability minimization	166
5.3. Digital image steganography: basic methods	168
5.3.1. LSB substitution and matching	168
5.3.2. Adaptive embedding methods	169
5.4. Advanced principles in steganography	172
5.4.1. Synchronization of modifications	173
5.4.2. Batch steganography	175
5.4.3. Steganography of color images	177
5.4.4. Use of side information	178
5.4.5. Steganography mimicking a statistical model	180
5.4.6. Adversarial steganography	182
5.5. Conclusion	186
5.6. References	186
Chapter 6. Traitor Tracing	189
Teddy FURON	
6.1. Introduction	189
6.1.1. The contribution of the cryptography community	190
6.1.2. Multimedia content	191
6.1.3. Error probabilities	192
6.1.4. Collusion strategy	192
6.2. The original Tardos code	194
6.2.1. Constructing the code	195
6.2.2. The collusion strategy and its impact on the pirated series	195
6.2.3. Accusation with a simple decoder	197
6.2.4. Study of the Tardos code-Škorić original	199
6.2.5. Advantages	202
6.2.6. The problems	204
6.3. Tardos and his successors	205
6.3.1. Length of the code	205
6.3.2. Other criteria	205
6.3.3. Extensions	207
6.4. Research of better score functions	208
6.4.1. The optimal score function	208
6.4.2. The theory of the compound communication channel	209

6.4.3. Adaptive score functions	211
6.4.4. Comparison	213
6.5. How to find a better threshold	213
6.6. Conclusion	215
6.7. References	216
Chapter 7. 3D Watermarking	219
Sébastien BEUGNON, Vincent ITIER and William PUECH	
7.1. Introduction	220
7.2. Preliminaries	221
7.2.1. Digital watermarking	221
7.2.2. 3D objects	222
7.3. Synchronization	224
7.3.1. Traversal scheduling	224
7.3.2. Patch scheduling	224
7.3.3. Scheduling based on graphs	225
7.4. 3D data hiding	230
7.4.1. Transformed domains	231
7.4.2. Spatial domain	231
7.4.3. Other domains	232
7.5. Presentation of a high-capacity data hiding method	233
7.5.1. Embedding of the message	234
7.5.2. Causality issue	235
7.6. Improvements	236
7.6.1. Error-correcting codes	236
7.6.2. Statistical arithmetic coding	236
7.6.3. Partitioning and acceleration structures	237
7.7. Experimental results	238
7.8. Trends in high-capacity 3D data hiding	240
7.8.1. Steganalysis	240
7.8.2. Security analysis	241
7.8.3. 3D printing	242
7.9. Conclusion	242
7.10. References	243
Chapter 8. Steganalysis: Detection of Hidden Data in Multimedia Content	247
Rémi COGRANNE, Marc CHAUMONT and Patrick BAS	
8.1. Introduction, challenges and constraints	247
8.1.1. The different aims of steganalysis	248
8.1.2. Different methods to carry out steganalysis	249
8.2. Incompatible signature detection	250

8.3. Detection using statistical methods	252
8.3.1. Statistical test of χ^2	252
8.3.2. Likelihood-ratio test	256
8.3.3. LSB match detection	261
8.4. Supervised learning detection	263
8.4.1. Extraction of characteristics in the spatial domain	264
8.4.2. Learning how to detect with features	269
8.5. Detection by deep neural networks	270
8.5.1. Foundation of a deep neural network	271
8.5.2. The preprocessing module	272
8.6. Current avenues of research	279
8.6.1. The problem of <i>Cover-Source mismatch</i>	279
8.6.2. The problem with steganalysis in real life	279
8.6.3. Reliable steganalysis	280
8.6.4. Steganalysis of color images	280
8.6.5. Taking into account the adaptivity of steganography	281
8.6.6. Grouped steganalysis (batch steganalysis)	281
8.6.7. Universal steganalysis	282
8.7. Conclusion	283
8.8. References	283
List of Authors	289
Index	293