
Contents

Preface to the First Edition	xv
Preface to the Second Edition	xix
Example Watermarking Systems	xxi
CHAPTER 1 Introduction	1
1.1 Information Hiding, Steganography, and Watermarking	4
1.2 History of Watermarking	6
1.3 History of Steganography	9
1.4 Importance of Digital Watermarking	11
1.5 Importance of Steganography	12
CHAPTER 2 Applications and Properties	15
2.1 Applications of Watermarking	16
2.1.1 Broadcast Monitoring	16
2.1.2 Owner Identification	19
2.1.3 Proof of Ownership	21
2.1.4 Transaction Tracking	23
2.1.5 Content Authentication	25
2.1.6 Copy Control	27
2.1.7 Device Control	31
2.1.8 Legacy Enhancement	32
2.2 Applications of Steganography	34
2.2.1 Steganography for Dissidents	34
2.2.2 Steganography for Criminals	35
2.3 Properties of Watermarking Systems	36
2.3.1 Embedding Effectiveness	37
2.3.2 Fidelity	37
2.3.3 Data Payload	38
2.3.4 Blind or Informed Detection	39
2.3.5 False Positive Rate	39
2.3.6 Robustness	40
2.3.7 Security	41
2.3.8 Cipher and Watermark Keys	43
2.3.9 Modification and Multiple Watermarks	45
2.3.10 Cost	46
2.4 Evaluating Watermarking Systems	46
2.4.1 The Notion of “Best”	47
2.4.2 Benchmarking	47
2.4.3 Scope of Testing	48

Properties of Steganographic and Steganalysis Systems	49
2.5.1 Embedding Effectiveness	49
2.5.2 Fidelity	50
2.5.3 Steganographic Capacity, Embedding Capacity, Embedding Efficiency, and Data Payload	50
2.5.4 Blind or Informed Extraction	51
2.5.5 Blind or Targeted Steganalysis	51
2.5.6 Statistical Undetectability	52
2.5.7 False Alarm Rate	53
2.5.8 Robustness	53
2.5.9 Security	54
2.5.10 Stego Key	54
Evaluating and Testing Steganographic Systems	55
Summary	56

TER 3 Models of Watermarking	61
Notation	62
Communications	63
3.2.1 Components of Communications Systems	63
3.2.2 Classes of Transmission Channels	64
3.2.3 Secure Transmission	65
Communication-Based Models of Watermarking	67
3.3.1 Basic Model	67
3.3.2 Watermarking as Communications with Side Information at the Transmitter	75
3.3.3 Watermarking as Multiplexed Communications	78
Geometric Models of Watermarking	80
3.4.1 Distributions and Regions in Media Space	81
3.4.2 Marking Spaces	87
Modeling Watermark Detection by Correlation	95
3.5.1 Linear Correlation	96
3.5.2 Normalized Correlation	97
3.5.3 Correlation Coefficient	100
Summary	102

TER 4 Basic Message Coding	105
Mapping Messages into Message Vectors	106
4.1.1 Direct Message Coding	106
4.1.2 Multisymbol Message Coding	110
Error Correction Coding	117
4.2.1 The Problem with Simple Multisymbol Messages	117
4.2.2 The Idea of Error Correction Codes	118
4.2.3 Example: Trellis Codes and Viterbi Decoding	119

4.3 Detecting Multisymbol Watermarks	124
4.3.1 Detection by Looking for Valid Messages	125
4.3.2 Detection by Detecting Individual Symbols	126
4.3.3 Detection by Comparing against Quantized Vectors	128
4.4 Summary	134

CHAPTER 5 Watermarking with Side Information	137
5.1 Informed Embedding	139
5.1.1 Embedding as an Optimization Problem	140
5.1.2 Optimizing with Respect to a Detection Statistic	141
5.1.3 Optimizing with Respect to an Estimate of Robustness	147
5.2 Watermarking Using Side Information	153
5.2.1 Formal Definition of the Problem	153
5.2.2 Signal and Channel Models	155
5.2.3 Optimal Watermarking for a Single Cover Work	156
5.2.4 Optimal Coding for Multiple Cover Works	157
5.2.5 A Geometrical Interpretation of White Gaussian Signals	158
5.2.6 Understanding Shannon's Theorem	159
5.2.7 Correlated Gaussian Signals	161
5.3 Dirty-Paper Codes	164
5.3.1 Watermarking of Gaussian Signals: First Approach	164
5.3.2 Costa's Insight: Writing on Dirty Paper	170
5.3.3 Scalar Watermarking	175
5.3.4 Lattice Codes	179
5.4 Summary	181

CHAPTER 6 Practical Dirty-Paper Codes	183
6.1 Practical Considerations for Dirty-Paper Codes	183
6.1.1 Efficient Encoding Algorithms	184
6.1.2 Efficient Decoding Algorithms	185
6.1.3 Tradeoff between Robustness and Encoding Cost	186
6.2 Broad Approaches to Dirty-Paper Code Design	188
6.2.1 Direct Binning	188
6.2.2 Quantization Index Modulation	188
6.2.3 Dither Modulation	189
6.3 Implementing DM with a Simple Lattice Code	189
6.4 Typical Tricks in Implementing Lattice Codes	194
6.4.1 Choice of Lattice	194
6.4.2 Distortion Compensation	194
6.4.3 Spreading Functions	195
6.4.4 Dither	195

Coding with Better Lattices	197
6.5.1 Using Nonorthogonal Lattices	197
6.5.2 Important Properties of Lattices	199
6.5.3 Constructing a Dirty-Paper Code from E_g	201
Making Lattice Codes Survive Valumetric Scaling	204
6.6.1 Scale-Invariant Marking Spaces	205
6.6.2 Rational Dither Modulation	207
6.6.3 Inverting Valumetric Scaling	208
Dirty-Paper Trellis Codes	208
Summary	212
APTER 7 Analyzing Errors	213
Message Errors	214
False Positive Errors	218
7.2.1 Random-Watermark False Positive	219
7.2.2 Random-Work False Positive	221
False Negative Errors	225
ROC Curves	228
7.4.1 Hypothetical ROC	228
7.4.2 Histogram of a Real System	230
7.4.3 Interpolation Along One or Both Axes	231
The Effect of Whitening on Error Rates	232
Analysis of Normalized Correlation	239
7.6.1 False Positive Analysis	240
7.6.2 False Negative Analysis	250
Summary	252
APTER 8 Using Perceptual Models	255
Evaluating Perceptual Impact of Watermarks	255
8.1.1 Fidelity and Quality	256
8.1.2 Human Evaluation Measurement Techniques	257
8.1.3 Automated Evaluation	260
General Form of a Perceptual Model	263
8.2.1 Sensitivity	263
8.2.2 Masking	266
8.2.3 Pooling	267
Two Examples of Perceptual Models	269
8.3.1 Watson's DCT-Based Visual Model	269
8.3.2 A Perceptual Model for Audio	273
Perceptually Adaptive Watermarking	277
8.4.1 Perceptual Shaping	280
8.4.2 Optimal Use of Perceptual Models	287
Summary	295

CHAPTER 9 Robust Watermarking	297
9.1 Approaches	298
9.1.1 Redundant Embedding	299
9.1.2 Spread Spectrum Coding	300
9.1.3 Embedding in Perceptually Significant Coefficients	301
9.1.4 Embedding in Coefficients of Known Robustness	302
9.1.5 Inverting Distortions in the Detector	303
9.1.6 Preinverting Distortions in the Embedder	304
9.2 Robustness to Valumetric Distortions	308
9.2.1 Additive Noise	308
9.2.2 Amplitude Changes	312
9.2.3 Linear Filtering	314
9.2.4 Lossy Compression	319
9.2.5 Quantization	320
9.3 Robustness to Temporal and Geometric Distortions	325
9.3.1 Temporal and Geometric Distortions	326
9.3.2 Exhaustive Search	327
9.3.3 Synchronization/Registration in Blind Detectors	328
9.3.4 Autocorrelation	329
9.3.5 Invariant Watermarks	330
9.3.6 Implicit Synchronization	331
9.4 Summary	332
CHAPTER 10 Watermark Security	335
10.1 Security Requirements	335
10.1.1 Restricting Watermark Operations	336
10.1.2 Public and Private Watermarking	338
10.1.3 Categories of Attack	340
10.1.4 Assumptions about the Adversary	345
10.2 Watermark Security and Cryptography	348
10.2.1 The Analogy between Watermarking and Cryptography	348
10.2.2 Preventing Unauthorized Detection	349
10.2.3 Preventing Unauthorized Embedding	351
10.2.4 Preventing Unauthorized Removal	355
10.3 Some Significant Known Attacks	358
10.3.1 Scrambling Attacks	359
10.3.2 Pathological Distortions	359
10.3.3 Copy Attacks	361
10.3.4 Ambiguity Attacks	362
10.3.5 Sensitivity Analysis Attacks	367
10.3.6 Gradient Descent Attacks	372
10.4 Summary	373

PART 11 Content Authentication	375
Exact Authentication	377
1.1.1 Fragile Watermarks	377
1.1.2 Embedded Signatures	378
1.1.3 Erasable Watermarks	379
Selective Authentication	395
1.2.1 Legitimate versus Illegitimate Distortions	395
1.2.2 Semi-Fragile Watermarks	399
1.2.3 Embedded, Semi-Fragile Signatures	404
1.2.4 Telltale Watermarks	409
Localization	410
1.3.1 Block-Wise Content Authentication	411
1.3.2 Sample-Wise Content Authentication	412
1.3.3 Security Risks with Localization	415
Restoration	419
1.4.1 Embedded Redundancy	419
1.4.2 Self-Embedding	420
1.4.3 Blind Restoration	421
Summary	422
PART 12 Steganography	425
Steganographic Communication	427
12.1.1 The Channel	428
12.1.2 The Building Blocks	429
Notation and Terminology	433
Information-Theoretic Foundations of Steganography	433
12.3.1 Cachin's Definition of Steganographic Security	434
Practical Steganographic Methods	439
12.4.1 Statistics Preserving Steganography	439
12.4.2 Model-Based Steganography	441
12.4.3 Masking Embedding as Natural Processing	445
Minimizing the Embedding Impact	449
12.5.1 Matrix Embedding	450
12.5.2 Nonshared Selection Rule	457
Summary	467
PART 13 Steganalysis	469
Steganalysis Scenarios	469
13.1.1 Detection	470
13.1.2 Forensic Steganalysis	475
13.1.3 The Influence of the Cover Work on Steganalysis	476
Some Significant Steganalysis Algorithms	477
13.2.1 LSB Embedding and the Histogram Attack	478

13.2.2 Sample Pairs Analysis	480
13.2.3 Blind Steganalysis of JPEG Images Using Calibration	486
13.2.4 Blind Steganalysis in the Spatial Domain	489
13.3 Summary	494

APPENDIX A Background Concepts **497**

A.1 Information Theory	497
A.1.1 Entropy	497
A.1.2 Mutual Information	498
A.1.3 Communication Rates	499
A.1.4 Channel Capacity	500
A.2 Coding Theory	503
A.2.1 Hamming Distance	503
A.2.2 Covering Radius	503
A.2.3 Linear Codes	504
A.3 Cryptography	505
A.3.1 Symmetric-Key Cryptography	505
A.3.2 Asymmetric-Key Cryptography	506
A.3.3 One-Way Hash Functions	508
A.3.4 Cryptographic Signatures	510

APPENDIX B Selected Theoretical Results **511**

B.1 Information-Theoretic Analysis of Secure Watermarking	
(Moulin and O'Sullivan)	511
B.1.1 Watermarking as a Game	511
B.1.2 General Capacity of Watermarking	513
B.1.3 Capacity with MSE Fidelity Constraint	514
B.2 Error Probabilities Using Normalized Correlation Detectors	
(Miller and Bloom)	517
B.3 Effect of Quantization Noise on Watermarks (Eggers and Girod)	522
B.3.1 Background	524
B.3.2 Basic Approach	524
B.3.3 Finding the Probability Density Function	524
B.3.4 Finding the Moment-Generating Function	525
B.3.5 Determining the Expected Correlation for a Gaussian Watermark and Laplacian Content	527

APPENDIX C Notation and Common Variables **529**

C.1 Variable Naming Conventions	529
C.2 Operators	530
C.3 Common Variable Names	530
C.4 Common Functions	532