Digital Watermarking and Steganography

Second Edition

Ingemar J. Cox Matthew L. Miller Jeffrey A. Bloom Jessica Fridrich Ton Kalker





Contents

			XV
			ix
Exam	ple Wate	rmarking Systems	Хi
СНА	PTER 1	Introduction	1
1.1	Informa	ition Hiding, Steganography, and Watermarking	4
1.2		of Watermarking	6
1.3	-	of Steganography	9
1.4			11
1.5			12
СНА	PTER 2	Applications and Properties	15
2.1			16
	2.1.1		16
	2.1.2	8	19
	2.1.3		21
	2.1.4		23
	2.1.5		25
	2.1.6		27
	2.1.7	. .	31
	2.1.8		32
2.2		· .	34
4.2	2.2.1		34
	2.2.2		35
2.3			36
	2.3.1	- ·	37
	2.3.2		37 37
	2.3.3	•	38
	2.3.4	•	39
	2.3.5		39
	2.3.6		40
	2.3.7		41
	2.3.8		43
	2.3.9	* · · · · · · · · · · · · · · · · · · ·	45
	2.3.10	<u> </u>	46
2.4			46
-	2.4.1	0 7	4 7
	2.4.2		47
	2.4.3		48

vii

2.5	Proper	ties 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
2.6	Evaluat	ting and Testing Steganographic Systems	55
2.7		ary	56
СНА	PTER :	3 Models of Watermarking	61
3.1		on	62
3.2		unications	63
J.=	3.2.1	Components of Communications Systems	63
	3.2.2	Classes of Transmission Channels	64
	3.2.3	Secure Transmission	65
3.3		unication-Based Models of Watermarking	67
3.5	3.3.1	Basic Model	67
	3.3.2	Watermarking as Communications with Side	Ů,
	3.3.=	Information at the Transmitter	75
	3.3.3	Watermarking as Multiplexed Communications	78
3.4	•	etric Models of Watermarking	80
J	3.4.1	Distributions and Regions in Media Space	81
	3.4.2	Marking Spaces	87
3.5		ing Watermark Detection by Correlation	95
3.7	3.5.1	Linear Correlation	96
	3.5.2	Normalized Correlation	97
	3.5.3	Correlation Coefficient	100
3.6		ary	102
~ 11 A	DWED	A. Dowin Magazara Cladina	10=
		4 Basic Message Coding	105
4.1		ng Messages into Message Vectors	106
	4.1.1	Direct Message Coding	106
4.0	4.1.2	Multisymbol Message Coding	110
4.2		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	Detecti	ing 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	Summa	ury	134
СНА	PTER 9	5 Watermarking with Side Information	137
5.1		ed Embedding	139
J.1	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	141
	5.1.5	Robustness	147
5.2	Watom		
5.2		narking 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	4.50
		Signals	158
	5.2.6	Understanding Shannon's Theorem	159
	5.2.7	Correlated Gaussian Signals	161
5.3	•	aper 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	Summa	ıry	181
СНА	PTER (6 Practical Dirty-Paper Codes	183
6.1	Practic	al 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	-	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		nenting DM with a Simple Lattice Code	189
6.4	-	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
	0.4.4	Didici	17)

6.5	Coding with Better Lattices	7
	6.5.1 Using Nonorthogonal Lattices	7
	6.5.2 Important Properties of Lattices	9
	6.5.3 Constructing a Dirty-Paper Code from E ₈ 20	1
6.6	Making Lattice Codes Survive Valumetric Scaling 20	4
	6.6.1 Scale-Invariant Marking Spaces	15
	6.6.2 Rational Dither Modulation	7
	6.6.3 Inverting Valumetric Scaling	8
6.7	Dirty-Paper Trellis Codes	8
6.8	Summary	2
	PTER 7 Analyzing Errors 21	_
7.1	Message Errors	
7.2	False Positive Errors	
	7.2.1 Random-Watermark False Positive	
	7.2.2 Random-Work False Positive	
7.3	False Negative Errors	
7.4	ROC Curves	
	7.4.1 Hypothetical ROC	_
	7.4.2 Histogram of a Real System 23	
	7.4.3 Interpolation Along One or Both Axes 23	
7.5	The Effect of Whitening on Error Rates	
7.6	Analysis of Normalized Correlation	
	7.6.1 False Positive Analysis	
	7.6.2 False Negative Analysis	
7.7	Summary	2
СНА	PTER 8 Using Perceptual Models 25	5
8.1	Evaluating Perceptual Impact of Watermarks	
0.1	8.1.1 Fidelity and Quality	
	8.1.2 Human Evaluation Measurement Techniques 25	
	8.1.3 Automated Evaluation	
8.2	General Form of a Perceptual Model	
	8.2.1 Sensitivity	
	8.2.2 Masking	
	8.2.3 Pooling	
8.3	Two Examples of Perceptual Models	
	8.3.1 Watson's DCT-Based Visual Model	
	8.3.2 A Perceptual Model for Audio	
8.4	Perceptually Adaptive Watermarking	
	8.4.1 Perceptual Shaping	
	8.4.2 Optimal Use of Perceptual Models	
8.5	Summary	

CHA	PTER 9	Robust Watermarking	297
9.1	Approa	ches	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	Robustr	ness 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	Robustr	ness 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	Summa	ry	332
CHA	PTER 1	0 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	Waterm	ark 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 S	ignificant 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	Summa	ry	373

CHA	PTER 11 Content Authentication	375
11.1	Exact Authentication	377
	11.1.1 Fragile Watermarks	377
	11.1.2 Embedded Signatures	378
	11.1.3 Erasable Watermarks	379
11.2	Selective Authentication	395
	11.2.1 Legitimate versus Illegitimate Distortions	395
	11.2.2 Semi-Fragile Watermarks	399
	11.2.3 Embedded, Semi-Fragile Signatures	404
	11.2.4 Telltale Watermarks	409
11.3	Localization	410
	11.3.1 Block-Wise Content Authentication	411
	11.3.2 Sample-Wise Content Authentication	412
	11.3.3 Security Risks with Localization	415
11.4	Restoration	419
	11.4.1 Embedded Redundancy	419
	11.4.2 Self-Embedding	420
	11.4.3 Blind Restoration	421
11.5	Summary	422
CHA	PTER 12 Steganography	425
12.1	Steganographic Communication	427
	12.1.1 The Channel	428
	12.1.2 The Building Blocks	429
12.2	Notation and Terminology	433
12.3	Information-Theoretic Foundations of Steganography	433
	12.3.1 Cachin's Definition of Steganographic Security	434
12.4	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
12.5	Minimizing the Embedding Impact	449
	12.5.1 Matrix Embedding	450
	12.5.2 Nonshared Selection Rule	45 7
12.6	Summary	467
CIET A	DTED 12 Stogonolygic	460
	PTER 13 Steganalysis	469
13.1	Steganalysis Scenarios	469
	13.1.1 Detection	470
	13.1.2 Forensic Steganalysis	475
12.2	13.1.3 The Influence of the Cover Work on Steganalysis	476
13.2	Some Significant Steganalysis Algorithms	477
	13.2.1 LSB Embedding and the Histogram Attack	478

	13.2.2	Sample Pairs Analysis
	13.2.3	Blind Steganalysis of JPEG Images Using Calibration
	13.2.4	Blind Steganalysis in the Spatial Domain
13.3	Summa	ry
APP	ENDIX	A Background Concepts
A.1	Informa	ation Theory
	A.1.1	Entropy
	A.1.2	Mutual Information
	A.1.3	Communication Rates
	A.1.4	Channel Capacity
A.2	Coding	Theory
	A.2.1	Hamming Distance
	A.2.2	Covering Radius
	A.2.3	Linear Codes
A.3	Crypto	graphy
	A.3.1	Symmetric-Key Cryptography
	A.3.2	Asymmetric-Key Cryptography
	A.3.3	One-Way Hash Functions
	A.3.4	Cryptographic Signatures
		71 0 1
APP	ENDIX	B Selected Theoretical Results
B.1		ation-Theoretic Analysis of Secure Watermarking
		and O'Sullivan)
	B.1.1	Watermarking as a Game
	B.1.2	General Capacity of Watermarking
	B.1.3	Capacity with MSE Fidelity Constraint
B.2	-	robabilities Using Normalized Correlation Detectors
D.2		and Bloom)
B.3		of Quantization Noise on Watermarks (Eggers and Girod) .
D .5	B.3.1	Background
	B.3.2	Basic Approach
	B.3.3	Finding the Probability Density Function
	B.3.4	Finding the Moment-Generating Function
	B.3.5	Determining the Expected Correlation for a Gaussian
	ע.ע.	Watermark and Laplacian Content
		watermark and Laplacian Content
APPI	ENDIX	C Notation and Common Variables
C.1		e Naming Conventions
C.2		ors
C.3		on Variable Names
C.4		on Functions
U.T	Commit	m runctions

Glossary 533 References 549 Index 575

591

About the Authors