

Contents

38		3.4 In-camera processing	107
39	7.1	3.5 Noise	801
44	7.1.1	Summary	801
45	7.1.2	Exercises	110
45	7.2	Steganography by minimizing natural	411
47	7.2.1	Steganographic channel	411
50	7.2.2	Steganography by cover selection to minimize the	711
51	7.3	Steganography by cover modification	611
53	7.3.1	Steganography by cover modification	611
56	7.3.2	Summary	611
57		Exercises	611
		<i>Preface</i>	page xv
		<i>Acknowledgments</i>	xxiii
59		Naive steganography	31
61	1	Introduction	1
64	1.1	Steganography throughout history	3
66	1.2	Modern steganography	7
68	1.2.1	The prisoners' problem	9
68	1.2.2	Steganalysis is the warden's job	10
69	1.2.3	Steganographic security	11
70	1.2.4	Steganography and watermarking	12
72		Summary	13
73	2	Digital image formats	15
76	2.1	Color representation	15
78	2.1.1	Color sampling	17
78	2.2	Spatial-domain formats	18
81	2.2.1	Raster formats	18
82	2.2.2	Palette formats	19
83	2.3	Transform-domain formats (JPEG)	22
85	2.3.1	Color subsampling and padding	23
88	2.3.2	Discrete cosine transform	24
89	2.3.3	Quantization	25
91	2.3.4	Decompression	27
92	2.3.5	Typical DCT block	28
93	2.3.6	Modeling DCT coefficients	29
95	2.3.7	Working with JPEG images in Matlab	30
97		Summary	30
98		Exercises	31
100	3	Digital image acquisition	33
102	3.1	CCD and CMOS sensors	34
103	3.2	Charge transfer and readout	35
103	3.3	Color filter array	36

3.4	In-camera processing	38
3.5	Noise	39
	Summary	44
	Exercises	45
4	Steganographic channel	47
4.1	Steganography by cover selection	50
4.2	Steganography by cover synthesis	51
4.3	Steganography by cover modification	53
	Summary	56
	Exercises	57
5	Naive steganography	59
5.1	LSB embedding	60
5.1.1	Histogram attack	64
5.1.2	Quantitative attack on Jsteg	66
5.2	Steganography in palette images	68
5.2.1	Embedding in palette	68
5.2.2	Embedding by preprocessing palette	69
5.2.3	Parity embedding in sorted palette	70
5.2.4	Optimal-parity embedding	72
5.2.5	Adaptive methods	73
5.2.6	Embedding while dithering	75
	Summary	76
	Exercises	76
6	Steganographic security	81
6.1	Information-theoretic definition	82
6.1.1	KL divergence as a measure of security	83
6.1.2	KL divergence for benchmarking	85
6.2	Perfectly secure steganography	88
6.2.1	Perfect security and compression	89
6.2.2	Perfect security with respect to model	91
6.3	Secure stegosystems with limited embedding distortion	92
6.3.1	Spread-spectrum steganography	93
6.3.2	Stochastic quantization index modulation	95
6.3.3	Further reading	97
6.4	Complexity-theoretic approach	98
6.4.1	Steganographic security by Hopper <i>et al.</i>	100
6.4.2	Steganographic security by Katzenbeisser and Petitcolas	101
6.4.3	Further reading	102
	Summary	103
	Exercises	103

7	Practical steganographic methods	107
7.1	Model-preserving steganography	108
7.1.1	Statistical restoration	108
7.1.2	Model-based steganography	110
7.2	Steganography by mimicking natural processing	114
7.2.1	Stochastic modulation	114
7.2.2	The question of optimal stego noise	117
7.3	Steganalysis-aware steganography	119
7.3.1	± 1 embedding	119
7.3.2	F5 embedding algorithm	119
7.4	Minimal-impact steganography	122
7.4.1	Performance bound on minimal-impact embedding	124
7.4.2	Optimality of F5 embedding operation	128
	Summary	130
	Exercises	131
8	Matrix embedding	135
8.1	Matrix embedding using binary Hamming codes	137
8.2	Binary linear codes	139
8.3	Matrix embedding theorem	142
8.3.1	Revisiting binary Hamming codes	144
8.4	Theoretical bounds	144
8.4.1	Bound on embedding efficiency for codes of fixed length	144
8.4.2	Bound on embedding efficiency for codes of increasing length	145
8.5	Matrix embedding for large relative payloads	149
8.6	Steganography using q -ary symbols	151
8.6.1	q -ary Hamming codes	152
8.6.2	Performance bounds for q -ary codes	154
8.6.3	The question of optimal q	156
8.7	Minimizing embedding impact using sum and difference covering set	158
	Summary	162
	Exercises	163
9	Non-shared selection channel	167
9.1	Wet paper codes with syndrome coding	169
9.2	Matrix LT process	171
9.2.1	Implementation	173
9.3	Wet paper codes with improved embedding efficiency	174
9.3.1	Implementation	177
9.3.2	Embedding efficiency	179
9.4	Sample applications	179
9.4.1	Minimal-embedding-impact steganography	179
9.4.2	Perturbed quantization	180

107	9.4.3	MMx embedding algorithm	183
108	9.4.4	Public-key steganography	184
108	9.4.5	$e + 1$ matrix embedding	185
110	9.4.6	Extending matrix embedding using Hamming codes	186
114	9.4.7	Removing shrinkage from F5 algorithm (nsF5)	188
118		Summary	189
117		Exercises	190
119	10	Steganalysis	193
119	10.1	Typical scenarios	194
122	10.2	Statistical steganalysis	195
124	10.2.1	Steganalysis as detection problem	196
128	10.2.2	Modeling images using features	196
130	10.2.3	Optimal detectors	197
131	10.2.4	Receiver operating characteristic (ROC)	198
132	10.3	Targeted steganalysis	201
132	10.3.1	Features	201
137	10.3.2	Quantitative steganalysis	205
139	10.4	Blind steganalysis	207
142	10.4.1	Features	208
144	10.4.2	Classification	209
144	10.5	Alternative use of blind steganalyzers	211
144	10.5.1	Targeted steganalysis	211
145	10.5.2	Multi-classification	211
149	10.5.3	Steganography design	212
151	10.5.4	Benchmarking	212
152	10.6	Influence of cover source on steganalysis	212
154	10.7	System attacks	215
156	10.8	Forensic steganalysis	217
158		Summary	218
162		Exercises	219
163	11	Selected targeted attacks	221
167	11.1	Sample Pairs Analysis	221
169	11.1.1	Experimental verification of SPA	226
171	11.1.2	Constructing a detector of LSB embedding using SPA	227
173	11.1.3	SPA from the point of view of structural steganalysis	230
174	11.2	Pairs Analysis	234
177	11.2.1	Experimental verification of Pairs Analysis	237
179	11.3	Targeted attack on F5 using calibration	237
179	11.4	Targeted attacks on ± 1 embedding	240
179		Summary	247
180		Exercises	247

12	Blind steganalysis	251
	12.1 Features for steganalysis of JPEG images	253
	12.1.1 First-order statistics	254
	12.1.2 Inter-block features	255
	12.1.3 Intra-block features	256
	12.2 Blind steganalysis of JPEG images (cover-versus-all-stego)	258
	12.2.1 Image database	258
	12.2.2 Algorithms	259
	12.2.3 Training database of stego images	259
	12.2.4 Training	260
	12.2.5 Testing on known algorithms	261
	12.2.6 Testing on unknown algorithms	262
	12.3 Blind steganalysis of JPEG images (one-class neighbor machine)	263
	12.3.1 Training and testing	264
	12.4 Blind steganalysis for targeted attacks	265
	12.4.1 Quantitative blind attacks	267
	12.5 Blind steganalysis in the spatial domain	270
	12.5.1 Noise features	271
	12.5.2 Experimental evaluation	273
	Summary	274
13	Steganographic capacity	277
	13.1 Steganographic capacity of perfectly secure stegosystems	278
	13.1.1 Capacity for some simple models of covers	280
	13.2 Secure payload of imperfect stegosystems	281
	13.2.1 The SRL of imperfect steganography	282
	13.2.2 Experimental verification of the SRL	287
	Summary	290
	Exercises	291
A	Statistics	293
	A.1 Descriptive statistics	293
	A.1.1 Measures of central tendency and spread	294
	A.1.2 Construction of PRNGs using compounding	296
	A.2 Moment-generating function	297
	A.3 Jointly distributed random variables	299
	A.4 Gaussian random variable	302
	A.5 Multivariate Gaussian distribution	303
	A.6 Asymptotic laws	305
	A.7 Bernoulli and binomial distributions	306
	A.8 Generalized Gaussian, generalized Cauchy, Student's t -distributions	307
	A.9 Chi-square distribution	310
	A.10 Log-log empirical cdf plot	310

B	Information theory	313
	B.1 Entropy, conditional entropy, mutual information	313
	B.2 Kullback–Leibler divergence	316
	B.3 Lossless compression	321
	B.3.1 Prefix-free compression scheme	322
C	Linear codes	325
	C.1 Finite fields	325
	C.2 Linear codes	326
	C.2.1 Isomorphism of codes	328
	C.2.2 Orthogonality and dual codes	329
	C.2.3 Perfect codes	331
	C.2.4 Cosets of linear codes	332
D	Signal detection and estimation	335
	D.1 Simple hypothesis testing	335
	D.1.1 Receiver operating characteristic	339
	D.1.2 Detection of signals corrupted by white Gaussian noise	339
	D.2 Hypothesis testing and Fisher information	341
	D.3 Composite hypothesis testing	343
	D.4 Chi-square test	345
	D.5 Estimation theory	347
	D.6 Cramer–Rao lower bound	349
	D.7 Maximum-likelihood and maximum a posteriori estimation	354
	D.8 Least-square estimation	355
	D.9 Wiener filter	357
	D.9.1 Practical implementation for images	358
	D.10 Vector spaces with inner product	359
	D.10.1 Cauchy–Schwartz inequality	361
E	Support vector machines	363
	E.1 Binary classification	363
	E.2 Linear support vector machines	364
	E.2.1 Linearly separable training set	364
	E.2.2 Non-separable training set	366
	E.3 Kernelized support vector machines	369
	E.4 Weighted support vector machines	371
	E.5 Implementation of support vector machines	373
	E.5.1 Scaling	373
	E.5.2 Kernel selection	373
	E.5.3 Determining parameters	373
	E.5.4 Final training	374
	E.5.5 Evaluating classification performance	375

<i>Notation and symbols</i>	377
<i>Glossary</i>	387
<i>References</i>	409
<i>Index</i>	427

Steganography is another term for covert communication. It works by hiding messages in inconspicuous objects that are then sent to the intended recipient. The most important requirement of any steganographic system is that it should be impossible for an eavesdropper to distinguish between ordinary objects and objects that contain secret data.

Steganography in its modern form is relatively young. Until the early 1990s, this unusual mode of secret communication was used only by spies. At that time, it was hardly a research discipline because the methods were a mere collection of clever tricks with little or no theoretical basis that would allow steganography to evolve in the manner we see today. With the subsequent spontaneous transition of communication from analog to digital, this ancient field experienced an explosive rejuvenation. Hiding messages in electronic documents for the purpose of covert communication seemed easy enough to those with some background in computer programming. Soon, steganographic applications appeared on the Internet, giving the masses the ability to hide files in digital images, audio, or text. At the same time, steganography caught the attention of researchers and quickly developed into a rigorous discipline. With it, steganography came to the forefront of discussions at professional meetings, such as the Electronic Imaging meetings annually organized by the SPIE in San Jose, the IEEE International Conference on Image Processing (ICIP), and the ACM Multimedia and Security Workshop. In 1996, the first Information Hiding Workshop took place in Cambridge and this series of workshops has since become the premier annual meeting place to present the latest advancements in theory and applications of data hiding.

Steganography shares many common features with the related but fundamentally quite different field of digital watermarking. In late 1990s, digital watermarking dominated the research in data hiding due to its numerous lucrative applications, such as digital rights management, secure media distribution, and authentication. As watermarking matured, the interest in steganography and steganalysis gradually intensified, especially after concerns had been raised that steganography might be used by criminals.

Even though this is not the first book dealing with the subject of steganography [22, 47, 51, 123, 142, 211, 239, 250], as far as the author is aware this is the first self-contained text with in-depth exposition of both steganography and