

Contents

Series introduction	iii
Preface	v
1 Introduction	1
1.1 Elements of a watermarking system	1
1.1.1 Information coding	3
1.1.2 Embedding	3
1.1.3 Concealment	5
1.1.4 Watermark impairments	6
1.1.5 Recovery of the hidden information	6
1.2 Protocol considerations	7
1.2.1 Capacity of watermarking techniques	10
1.2.2 Multiple embedding	11
1.2.3 Robustness	12
1.2.4 Blind vs. non-blind recovery	14
1.2.5 Private vs. public watermarking	15
1.2.6 Readable vs. detectable watermarks	15
1.2.7 Invertibility and quasi-invertibility	16
1.2.8 Reversibility	18
1.2.9 Asymmetric watermarking	18
1.3 Audio vs image vs video assets	19
1.4 Further reading	20
2 Applications	23
2.1 IPR protection	24
2.1.1 Demonstration of rightful ownership	24
2.1.2 Fingerprinting	25
2.1.3 Copy control	29
2.2 Authentication	31
2.2.1 Cryptography vs watermarking	31
	xi

2.2.2	A general authentication framework	33
2.2.3	Requirements of data-hiding-based authentication	36
2.3	Data hiding for multimedia transmission	37
2.3.1	Data compression	37
2.3.2	Error recovery	38
2.4	Annotation watermarks	40
2.4.1	Labelling for data retrieval	41
2.4.2	Bridging the gap between analog and digital objects	41
2.5	Covert communications	42
2.6	Further reading	43
3	Information coding	45
3.1	Information coding in detectable watermarking	47
3.1.1	Spread spectrum watermarking	47
3.1.2	Orthogonal waveforms watermarking	56
3.1.3	Orthogonal vs PN watermarking	58
3.1.4	Self-synchronizing PN sequences	62
3.1.5	Power spectrum shaping	63
3.1.6	Chaotic sequences	65
3.1.7	Direct embedding	68
3.2	Waveform-based readable watermarking	69
3.2.1	Information coding through M -ary signaling	69
3.2.2	Position encoding	71
3.2.3	Binary signaling	72
3.3	Direct embedding readable watermarking	75
3.3.1	Direct embedding binary signalling with bit repetition	75
3.4	Channel coding	76
3.4.1	Block codes	77
3.4.2	Convolutional codes	79
3.4.3	Coding vs bit repetition	81
3.4.4	Channel coding vs orthogonal signaling	83
3.4.5	Informed coding	83
3.5	Further reading	87
4	Data embedding	91
4.1	Feature selection	91
4.1.1	Watermarking in the asset domain	92
4.1.2	Watermarking in a transformed domain	96
4.1.3	Hybrid techniques	102
4.1.4	Watermarking in the compressed domain	110
4.1.5	Miscellaneous non-conventional choices of the feature set	112

4.2	Blind embedding	119
4.2.1	Additive watermarking	119
4.2.2	Multiplicative watermarking	126
4.3	Informed embedding	129
4.3.1	Detectable watermarking	135
4.3.2	Readable watermarking	142
4.4	Further reading	153
5	Data concealment	155
5.1	The Human Visual System	157
5.1.1	The Weber law and the contrast	160
5.1.2	The contrast sensitivity function	161
5.1.3	The masking effect	167
5.1.4	Mapping luminance to images	170
5.1.5	Perception of color stimuli	173
5.1.6	Perception of time-varying stimuli	184
5.2	The Human Auditory System (HAS)	187
5.2.1	The masking effect	188
5.3	Concealment through feature selection	190
5.4	Concealment through signal adaptation	192
5.4.1	Concealment through perceptual masks	192
5.4.2	Concealment relying on visibility thresholds	198
5.4.3	Heuristic approaches for still images	201
5.4.4	A theoretically funded perceptual threshold for still images	205
5.4.5	MPEG-based concealment for audio	209
5.5	Application oriented concealment	211
5.5.1	Video surveillance systems	212
5.5.2	Remote sensing images	214
5.6	Further reading	215
6	Data recovery	219
6.1	Watermark detection	220
6.1.1	A hypothesis testing problem	221
6.1.2	AWGN channel	225
6.1.3	Additive / Generalized Gaussian channel	238
6.1.4	Signal dependent noise with host rejection at the em- bedder	242
6.1.5	Taking perceptual masking into account	248
6.1.6	Multiplicative Gaussian channel	248
6.1.7	Multiplicative Weibull channel	259
6.1.8	Multichannel detection	271

6.2	Decoding	272
6.2.1	General problem for binary signalling	273
6.2.2	Binary signaling through AWGN channel	275
6.2.3	Generalized Gaussian channel	279
6.2.4	Multiplicative watermarking with Gaussian noise	280
6.2.5	Multiplicative watermarking of Weibull-distributed features	285
6.2.6	Quantization Index Modulation	288
6.2.7	Decoding in the presence of channel coding	296
6.2.8	Assessment of watermark presence	299
6.3	Further reading	304
7	Watermark impairments and benchmarking	307
7.1	Classification of attacks	308
7.2	Measuring obtrusiveness and attack strength	310
7.3	Gaussian noise addition	312
7.3.1	Additive vs multiplicative watermarking	312
7.3.2	Spread Spectrum vs QIM watermarking	317
7.4	Conventional signal processing	325
7.4.1	The gain attack	326
7.4.2	Histogram equalization	329
7.4.3	Filtering	331
7.5	Lossy coding	334
7.5.1	Quantization of the watermarked features	337
7.6	Geometric manipulations	344
7.6.1	Asset translation	345
7.6.2	Asset zooming	348
7.6.3	Image rotation	350
7.6.4	More complex geometric transformations	353
7.6.5	Countermeasures against geometric manipulations	354
7.7	Editing	362
7.8	Digital to analog and analog to digital conversion	364
7.9	Malicious attacks	365
7.10	Attack estimation	371
7.11	Benchmarking	371
7.11.1	Early benchmarking systems	372
7.11.2	StirMark	374
7.11.3	Improving conventional systems	378
7.11.4	A new benchmarking structure	381
7.12	Further reading	382

8	Security issues	385
8.1	Security by obscurity	388
8.2	The symmetric case	389
8.3	The asymmetric case	394
8.4	Playing open cards	401
8.5	Security based on protocol design	404
8.6	Further reading	406
9	An information theoretic perspective	409
9.1	Some historical notes	411
9.2	The watermarking game	412
9.2.1	The rules of the game	413
9.2.2	Some selected results	416
9.2.3	Capacity under average distortion constraints	420
9.3	The additive attack watermarking game	421
9.3.1	Game definition and main results	421
9.3.2	Costa's writing on dirty paper	424
9.4	Lattice-based capacity-achieving watermarking	427
9.5	Equi-energetic structured code-books	432
9.6	Further reading	433
	Bibliography	435
	Index	457