

# Contents

<b>1</b>	<b>General Introduction</b> . . . . .	1
1.1	Forewords . . . . .	1
1.2	Notations . . . . .	1
1.3	Watermarking and Security. . . . .	2
1.3.1	The Needs for Watermarking Security . . . . .	3
1.3.2	Who Are the Adversaries? . . . . .	5
1.3.3	Standardising Watermarking Security. . . . .	6
1.3.4	Security or Robustness? . . . . .	9
1.3.5	The Stakes Behind Watermarking Security . . . . .	10
	References . . . . .	11
<b>2</b>	<b>A Quick Tour of Watermarking Techniques</b> . . . . .	13
2.1	Basic Principles. . . . .	13
2.1.1	Watermarking Constraints . . . . .	13
2.1.2	Zero-Bit and Multi-bit Watermarking. . . . .	14
2.1.3	A Processing View . . . . .	14
2.1.4	The Geometrical View. . . . .	15
2.1.5	Three Fundamental Constraints . . . . .	16
2.2	Spread Spectrum and Improved Spread Spectrum . . . . .	18
2.2.1	Improved Spread Spectrum. . . . .	20
2.3	Correlation Based Zero-Bit Watermarking . . . . .	22
2.4	Watermarking Based on Dirty Paper Codes . . . . .	24
2.4.1	Distortion Compensated Quantisation Index Modulation (DC-QIM) . . . . .	25
2.4.2	Scalar Costa Scheme (SCS) . . . . .	27
2.4.3	Trellis-Based Watermarking . . . . .	29
2.5	Conclusions of the Chapter. . . . .	30
	References . . . . .	30

<b>3</b>	<b>Fundamentals</b>	33
3.1	Introduction: Information Theoretical Approaches	33
3.2	Watermarking Security Classes	35
3.2.1	Embedding Security Classes	35
3.3	Measuring Watermarking Security Using the Effective Key Length	39
3.3.1	How to Define the Secret Key in Watermarking?	39
3.3.2	The Effective Key Length	40
3.3.3	Definition of the Effective Key Length	41
3.3.4	Mathematical Expressions of the Effective Key Length for ISS	45
3.3.5	Practical Effective Key Length Computations	49
3.3.6	Security Analysis of Watermarking Schemes	52
3.4	Conclusions of the Chapter	59
	References	60
<b>4</b>	<b>Secure Design</b>	63
4.1	Secure Spread-Spectrum Embedding	63
4.1.1	Natural Watermarking	63
4.1.2	Circular Watermarking	65
4.1.3	Distribution Matching and Distortion Minimization	67
4.1.4	Informed Secure Embedding for Gaussian Hosts	69
4.2	Secure Quantization Based Embedding	73
4.2.1	Scalar Costa Scheme	74
4.2.2	Soft Scalar-Costa-Scheme	76
4.2.3	Embedding Computation and Decoding	78
4.2.4	Performance Analysis	79
4.3	Applied Watermarking Security	82
4.3.1	Four Nested Spaces	83
4.3.2	Embedding and Detection	86
4.3.3	Proportional Embedding	94
4.3.4	Experimental Investigations	96
4.3.5	Counter-Attacks	97
4.4	Conclusions of the Chapter	101
	References	101
<b>5</b>	<b>Attacks</b>	103
5.1	SS-Based Embedding Security	103
5.1.1	Attacks Using Independent Component Analysis	103
5.1.2	A Subspace Estimation Approach for Broken Arrows	106

- 5.2 Attacks on Dirty Paper Trellis Schemes . . . . . 112
  - 5.2.1 DPT Parameters Estimation . . . . . 114
  - 5.2.2 Patterns Estimation Using a Clustering Method. . . . . 114
- 5.3 Conclusions of the Chapter. . . . . 121
- References . . . . . 122
- 6 Conclusions and Open Problems . . . . . 123**
  - References . . . . . 124



<http://www.springer.com/978-981-10-0505-3>

Watermarking Security

Bas, P.; Furon, T.; Cayre, F.; Doërr, G.; Mathon, B.

2016, IX, 125 p. 70 illus., 29 illus. in color., Softcover

ISBN: 978-981-10-0505-3