



DATA HIDING FUNDAMENTALS AND APPLICATIONS

Content Security in Digital Multimedia

Husrev T. **Sencar**
Mahalingam **Ramkumar**
Ali N. **Akansu**

Contents

Preface xiii

CHAPTER 1

Introduction

- 1.1 What Is Data Hiding? 1
- 1.2 Forms of Data Hiding 2
 - 1.2.1 Relative Importance of Cover Signals 3
 - 1.2.2 Nature of Content 4
 - 1.2.3 Oblivious and Nonoblivious 4
 - 1.2.4 Synchronous and Asynchronous 4
 - 1.2.5 Active and Passive Wardens 5
- 1.3 Properties of Steganographic Communications 5
 - 1.3.1 Multimedia Data Hiding 6
- 1.4 The Steganographic Channel 8

CHAPTER 2

Frameworks for Data Hiding

- 2.1 Signal Processing Framework 14
- 2.2 Data Hiding from a Communications Perspective 15
- 2.3 Relationship Between Communications and Signal Processing Frameworks 17
- 2.4 A Review of Data Hiding Methods 20

CHAPTER 3

Communication with Side Information and Data Hiding

- 3.1 Costa's Framework 27

3.2	A Framework Based on Channel Adaptive Encoding and Channel Independent Decoding	30
3.2.1	Highlights of the CAE-CID Framework	34
3.3	On the Duality of Communications and Data Hiding Frameworks	35
3.4	Codebook Generation for Data Hiding Methods	40

CHAPTER 4

Type I (Linear) Data Hiding

4.1	Linear Data Hiding in Transform Domain	50
4.2	Problem Statement	51
4.3	Capacity of Additive Noise Channels	52
4.4	Modeling Channel Noise	58
4.4.1	Modeling Image Noise	59
4.4.2	Modeling Processing Noise	59
4.5	Visual Threshold	61
4.6	Channel Capacity vs. Choice of Transform	63
4.7	Some Capacity Results and Discussions	66
4.8	The Ideal Decomposition	74
4.9	Factors Influencing Choice of Transform	76

CHAPTER 5

Type II and Type III (Nonlinear) Data Hiding Methods

5.1	Type II Embedding and Detection	79
5.2	Type III Embedding and Detection Methods	83
5.2.1	Postprocessing Types	85
5.2.1.1	Vectorial Embedding and Detection	86
5.2.1.2	Scalar Embedding and Detection	87
5.2.2	Forms of Demodulation	87
5.2.2.1	Minimum Distance Decoding	88
5.2.2.2	Maximum Correlation Rule	90
5.2.3	Optimization Criteria for Embedding and Detection Parameters	91
5.2.3.1	Optimization of Parameters for Vectorial Embedding and Detection	91
5.2.3.2	Optimization of Parameters for Scalar Embedding and Detection	92
5.2.3.3	Maximizing Correlation	95
5.2.3.4	Minimizing Probability of Error	96
5.2.3.5	Maximizing Mutual Information	98
5.3	Performance Comparisons	98

Advanced Implementations

- 6.1 Spread Transforming 108
- 6.2 Multiple Codebook Data Hiding 113
 - 6.2.1 A Channel Model for Multiple Codebook Data Hiding 119
 - 6.2.2 Single Codebook Data Hiding Based on the Maximum Correlation Criterion 125
 - 6.2.2.1 Distribution of ρ_{ind} 127
 - 6.2.2.2 Distribution of ρ_{dep} 128
 - 6.2.3 Multiple Codebook Data Hiding Using the Maximum Correlation Criterion 130
 - 6.2.3.1 Distribution of $\rho_{m,j}^i$ 132
 - 6.2.3.2 Distribution of ρ_{max} 133
 - 6.2.4 Single Codebook Hiding Using the Minimum Distance Criterion 134
 - 6.2.4.1 Distribution of d_{ind} 135
 - 6.2.4.2 Distribution of d_{dep} 136
 - 6.2.5 Multiple Codebook Hiding Using the Minimum Distance Criterion 137
 - 6.2.5.1 Distribution of $d_{m,j}^i$ 139
 - 6.2.5.2 Distribution of d_{min} 139
 - 6.2.6 Comparisons 139
 - 6.2.7 Implementation and Simulation Results 147

Major Design Issues

- 7.1 DFT-Based Signaling 154
 - 7.1.1 Conventional Signaling 154
 - 7.1.2 FFT-Based Signaling 155
 - 7.1.2.1 Cyclic All-Pass Sequences 155
 - 7.1.2.2 Signal Constellation 157
 - 7.1.2.3 Redundant Signaling 158
- 7.2 Synchronization 160
 - 7.2.1 Autocorrelation for Restoring the Cropped Signal 162
 - 7.2.2 Practical Concerns 165
 - 7.2.2.1 Watermark Signal Design 165
 - 7.2.2.2 Cyclic Autocorrelation 165
 - 7.2.3 Synchronization 167
 - 7.2.4 Results 167
- 7.3 Perceptual Constraints 170
- 7.4 Attacks on Data Hiding Systems 172
 - 7.4.1 Removal Attacks 173
 - 7.4.1.1 Blind Attacks 173
 - 7.4.1.2 Estimation Attacks 174

7.4.2	Desynchronization Attacks	175
7.4.2.1	Geometric Attacks	175
7.4.2.2	Mosaic Attack	175
7.4.2.3	Template and Periodicity Removal	175
7.4.3	Security/Cryptographic Attacks	176
7.4.4	Protocol Attacks	176
7.4.4.1	Invertible Watermarks	176
7.4.4.2	Copy Attack	176
7.4.5	Future Direction in Attack Design	176

CHAPTER 8

Data Hiding Applications

8.1	Design of Data Hiding Methods Robust to Lossy Compression	179
8.1.1	Data Hiding for Secure Multimedia Delivery	180
8.1.2	Compression and Data Hiding	182
8.1.2.1	Data Hiding with Known Compression	183
8.1.2.2	Simultaneous Robustness to Multiple Compression Techniques	185
8.1.2.3	Robustness to Unknown Compression Methods	187
8.1.3	Utilizing the "Hole" in Compression Techniques	187
8.1.4	The Data Hiding Scheme	191
8.2	Type III Hiding for Lossy Compression	194
8.2.1	Joint Embedding and Compression	195
8.2.2	Results for JPEG Compression	197
8.3	Watermarking for Ownership	199
8.3.1	Counterfeit Attacks on Watermarks	201
8.3.1.1	Freedom in Choosing	202
8.3.1.2	Detection Statistic	203
8.3.1.3	Fake Originals	205
8.3.1.4	Multiple Watermarks	205
8.3.2	Watermarking Algorithms	206
8.3.3	Overcoming Attacks on Watermarks	207
8.3.4	Restrictions on Choice of Signature	209
8.3.5	Attacking Scheme III (Craver's Protocol)	210
8.3.6	Quasi-Oblivious Watermarking	211
8.3.7	Detection Statistic for Quasi-Oblivious Watermarking	213
8.3.8	Suggested Protocol	214
8.3.9	An Example of a Watermarking Scheme	216

APPENDIX A

CAE-CID Framework under Varying Channel Noise

221

**Statistics of $\rho_{dep}|P$
and $d_{dep}|P$ 223**

Mathematical Proofs

- C.1 Proof of Eq. (7.7) 229
C.2 Proof of Eq. (7.10) 230

Bibliography 231

Index 239