



**MORGAN KAUFMANN PUBLISHERS**

An Imprint of Academic Press  
A Harcourt Science & Technology Company

# Digital Watermarking

Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom

*The Morgan Kaufmann Series in Multimedia and Information Science, Edward Fox, Series Editor*

**Forthcoming: September 2001; 450 pages; ISBN 1-55860-714-5; US \$64.95**

Digital watermarking has received more and more attention as the distribution of content over the Internet and proliferation of high-capacity, digital recording devices have fuelled increased concerns over copyright protection of content. Watermarks are a valuable mechanism for protecting audio, video, and data and they are also becoming an important tool in facilitating e-commerce. Any company that is serious about safely protecting and distributing their content and products will need to know about digital watermarks.

This book will provide readers with a knowledge of the principles and the practices of watermarking, and will include discussions about a wide variety of applications, theoretical principles, detection and embedding concepts, and the key issues of digital watermarks--robustness, fidelity, fragility, and tampering. *Digital Watermarking* will be the first book of its kind to reveal the principles and practices of watermarking in a unified way, which until now have remained buried in research papers and articles.

## Features:

- Focuses exclusively on digital watermarking and thoroughly discusses the key issues-robustness, fidelity, fragility, and tampering.
- Covers important standards that are being considered now for implementation in systems within the next year.
- Emphasizes the principles and practices of watermarking--concepts are illustrated through examples and algorithms.

## ORDERING INFORMATION

### Order from Morgan Kaufmann Publishers—US

**Mail:** Harcourt Inc., Attn. Order Fulfillment Dept., 6277 Sea Harbor Drive, Orlando, FL 32887,  
**Phone:** US/ Canada 800-745-7323 , 407-345-3800 (Intl.) **Fax:** 800-874-6418, 407-345-4060,  
**Email:** [orders@mkp.com](mailto:orders@mkp.com) **Web:** [www.mkp.com](http://www.mkp.com)

### Order from Harcourt—EU

[www.harcourt-international.com](http://www.harcourt-international.com)

# TABLE OF CONTENTS

1 Introduction	5 Basic Message Coding	8.2.1 Additive noise
1.1 Information hiding, steganography, and watermarking	5.1 Mapping Messages into Message Vectors	8.2.2 Amplitude changes
1.2 History of watermarking	5.1.1 Direct Message Coding	8.2.3 Linear Filtering
1.3 Importance of digital watermarking	5.1.2 Multi-Symbol Message Coding	8.2.4 Lossy compression
2 Applications and Properties	5.2 Error Correction Coding	8.2.5 Quantization
2.1 Applications	5.2.1 The Problem with Simple Multi-Symbol Messages	8.3 Robustness to Temporal and Geometric Distortions
2.1.1 Broadcast Monitoring	5.2.2 The Idea of Error-Correction Codes	8.3.1 Temporal and Geometric Distortions
2.1.2 Owner Identification	5.2.3 Example: Trellis Codes and Viterbi Decoding	8.3.2 Exhaustive Search
2.1.3 Proof of Ownership	5.3 Detecting Multi-Symbol Watermarks	8.3.3
2.1.4 Transaction Tracking	5.3.1 Detection by Looking for Valid Messages	8.3.4 Autocorrelation
2.1.5 Content Authentication	5.3.2 Detection by Detecting Individual Symbols	8.3.5 Invariant Watermarks
2.1.6 Copy Control	5.3.3 Detection by Comparing Against Quantized Vectors	8.3.6 Implicit Synchronization
2.1.7 Device Control	5.4 Summary	8.4 Summary
2.2 Properties	6 Watermarking with Side Information	9 Watermark Security
2.2.1 Embedding Effectiveness	6.1 Informed Embedding	9.1 Security requirements
2.2.2 Fidelity	6.1.1 Embedding as an Optimization Problem	9.1.1 Restricting watermark operations
2.2.3 Data Payload	6.1.2 Optimization with Respect to a Detection Statistic	9.1.2 Public and Private Watermarking Applications
2.2.4 Blind or Informed Detection	6.1.3 Optimization with Respect to an Estimate of Robustness	9.1.3 Categories of Attack
2.2.5 False Positive Rate	6.2 Informed Encoding	9.1.4 Assumptions About the Adversary
2.2.6 Robustness	6.2.1 Writing on Dirty Paper	9.2 Watermark Security and Cryptography
2.2.7 Security	6.2.2 A Dirty-Paper Code for a Simple Channel	9.2.1 Cryptographic Tools
2.2.8 Cipher and Watermark Keys	6.2.3 Dirty-Paper Codes for More Complex Channels	9.2.2 The Analogy Between Watermarking and Cryptography
2.2.9 Modification and Multiple Watermarks	6.3 Structured Dirty-Paper Codes	9.2.3 Preventing Unauthorized Detection
2.2.10 Cost	6.3.1 Lattice Codes	9.2.4 Preventing Unauthorized Embedding
2.3 Evaluating Watermarking Systems	6.3.2 Syndrome Codes	9.2.5 Preventing Unauthorized Removal
2.3.1 The Notion of "Best"	6.3.3 Least-Significant-Bit Watermarking	9.3 Some Significant Known Attacks
2.3.2 Benchmarking	6.4 Summary	9.3.1 Scrambling Attacks
2.3.3 Scope of Testing	7 Using Perceptual Models	9.3.2 Pathological Distortions
2.4 Summary	7.1 Evaluation	9.3.3 Copy Attacks
3 Models of Watermarking	7.1.1 Fidelity and Quality	9.3.4 Ambiguity Attacks
3.1 Notation	7.1.2 Human Evaluation Measurement Techniques	9.3.5 Sensitivity Analysis Attack
3.2 Communications	7.1.3 Automated Evaluation	9.3.6 Gradient Descent Attacks
3.2.1 Components of Communication Systems	7.2 General Form of a Perceptual Model	9.4 Summary
3.2.2 Classes of Transmission Channels	7.2.1 Sensitivity	10 Content Authentication
3.2.3 Secure Transmission	7.2.2 Masking	10.1 Exact Authentication
3.3 Communication-Based Models of Watermarking	7.2.3 Pooling	10.1.1 Fragile Watermarks
3.3.1 Basic Model	7.3 Two Examples of Perceptual Models	10.1.2 Embedded Signatures
3.3.2 Watermarking as Communication with Side Information at the Transmitter	7.3.1 Watson's DCT-Based Visual Model	10.1.3 Erasable Watermarks
3.3.3 Watermarking as Multiplexed Communications	7.3.2 A Perceptual Model for Audio	10.2 Selective Authentication
3.4 Geometric Models of Watermarking	7.4 Perceptually Adaptive Watermarking	10.2.1 Legitimate vs. Illegitimate Distortions
3.4.1 Distribution and Regions in Media Space	7.4.1 Perceptual shaping	10.2.2 Semi-Fragile Watermarks
3.4.2 Marking Spaces	7.4.2 Optimal use of perceptual models	10.2.3 Embedded, Semi-Fragile Signatures
3.5 Correlation-Based Watermarking Systems	7.5 Summary	10.2.4 Tell-Tale Watermarks
3.5.1 Linear Correlation	8 Robust Watermarking	10.3 Localization
3.5.2 Normalized Correlation	8.1 Approaches	10.3.1 Block-Wise Content Authentication
3.5.3 Correlation Coefficient	8.1.1 Redundant Embedding	10.3.2 Sample-Wise Content Authentication
3.6 Summary	8.1.2 Spread Spectrum Coding	10.3.3 Security Risks with Localization
4 Evaluation of Error Rates	8.1.3 Embedding in Perceptually Significant Coefficients	10.4 Restoration
4.1 Message Errors	8.1.4 Embedding in Coefficients of Known Robustness	10.4.1 Embedded Redundancy
4.2 False Positive Errors	8.1.5 Inverting Distortions in the Detector	10.4.2 Self-Embedding
4.2.1 Random-Watermark False Positives	8.1.6 Pre-inverting Distortions in the Embedder	10.4.3 Blind Restoration
4.2.2 Random-Work False Positives	8.2 Robustness to Valumetric Distortions	10.5 Summary
4.3 False Negative Errors		A Background Concepts
4.4 ROC Curves		A.1 Probability and Statistics
4.5 The Effect of Whitening on Error Rates		A.2 Information Theory
4.6 Application to Normalized Correlation		A.3 Cryptography
4.6.1 False Positive Analysis		A.4 Transforms and Filtering
4.6.2 False Negative Analysis		B. Selected Theoretical Results
4.7 Summary		C Source Code
		D Notation and Common Variables
		E Glossary