DIGITAL WATERMARKING AND STEGANOGRAPHY SYLLABUS

Module 1: Fundamentals of Digital Watermarking

- Importance of Watermarking
- Applications and Properties of Watermarking
- Models of Watermarking
- Basic Message Coding: Mapping Message into Message Vectors, Error Correction Coding
- Watermarking with Side Information
- Analyzing Errors

Module 2: Digital Watermarking Schemes

- Spatial Domain: Correlation-Based Watermarking, Least Significant Bit Watermarking
- Frequency Domain: Discrete Wavelet Transform Watermarking, Discrete Fourier Transform Watermarking, Discrete Cosine Watermarking, Quantization Watermarking, Haar Transform Watermarking, Hadamard Transform Watermarking
- Robust Watermarking
- Fragile and Semi-Fragile Watermarking

Module 3: Digital Watermarking Security and Authentication

- Watermarking Security: Security Requirements, Watermark Security and Cryptography, Watermarking Attacks and Tools
- Content Authentication: Exact Authentication, Selective Authentication, Localization, Restoration

Module 4: Steganography

- Basics and Importance of Steganography
- Applications and Properties of Steganography
- Steganography Techniques: LSB Embedding, Steganography in Palette Images
- Steganography in JPEG Images: JSteg Data Hiding in Spatial and Transform Domain
- Steganography Security

Module 5: Audio and Video Steganography

- Audio Steganography: Temporal Domain Techniques, Transform Domain Techniques, Cepstral Domain
- Video Steganography: Introduction to Video Streams, Substitution-Based Techniques, Transform Domain Techniques, Adaptive Techniques, Format-Based Techniques
- Cover Generation Techniques
- Video Quality Metrics
- Perceptual Transparency Analysis
- Robustness Against Compression and Manipulation

Module 6: Wet Paper Code

- Random Linear Codes
- LT Codes
- Perturbed Quantization
- Matrix Embedding: Matrix Embedding Theorem
- Binary Hamming Codes
- Q-Ary Case
- Random Linear Codes for Large Payloads

Module 7: Steganalysis

- Steganalysis Principles
- Statistical Steganalysis: Steganalysis as Detection Problem, Modeling Images Using Features, Receiver Operating Characteristics
- Targeted Steganalysis: Sample Pair Analysis, Targeted Attack on F5 Using Calibration, Targeted Attack on ± Embedding
- Blind Steganalysis: Features for Steganalysis of JPEG Images (Cover vs Allstego and One-Class Neighbor Machine)