

<b>BCSE323L</b>	<b>DIGITAL WATERMARKING AND STEGANOGRAPHY</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
		<b>3</b>	<b>0</b>	<b>0</b>	<b>3</b>
<b>Pre-requisite</b>	<b>NIL</b>	<b>Syllabus version</b>			
		1.0			
<b>Course Objectives</b>					
<p>1. To understand the basic principles, characteristics, various approaches and applications of digital watermarking and steganography.</p> <p>2. To apply digital watermarking techniques as an authentication tool for distribution of content over the Internet and steganography techniques for covert communication.</p> <p>3. To impart knowledge on the basics of the counter measures like steganalysis for assessing the data hiding methods.</p>					
<b>Course Outcome</b>					
After completion of this course, the student shall be able to:					
<p>1. Learn the fundamental concepts, principles, characteristics and performance measures of digital watermarking and steganography.</p> <p>2. Acquire the various concepts of watermarking for digital authentication and authorization schemes related to electronic documents, image and video.</p> <p>3. Gathering the various concepts of steganography to access the sensitive information concealing of message, image, audio or video within another file.</p> <p>4. Design and implement efficient data hiding methods against steganalysis techniques.</p>					
<b>Module:1</b>	<b>Fundamentals of Digital Watermarking</b>	<b>6 hours</b>			
Importance of Watermarking - Application and Properties of Watermarking - Models of Watermarking - Basic Message Coding: Mapping Message into Message Vectors, Error Correction Coding - Watermarking with Side Information - Analyzing Errors.					
<b>Module:2</b>	<b>Digital Watermarking Schemes</b>	<b>7 hours</b>			
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.					
<b>Module:3</b>	<b>Digital Watermarking Security and Authentication</b>	<b>5 hours</b>			
Watermarking Security: Security Requirements, Watermark Security and Cryptography, Watermarking Attacks and Tools - Content Authentication: Exact Authentication, Selective Authentication, Localization, Restoration.					
<b>Module:4</b>	<b>Steganography</b>	<b>7 hours</b>			
Basics and Importance of Steganography - Applications and Properties of Steganography - Steganography: LSB embedding, Steganography in palette images -Steganography in JPEG images: JSteg data hiding in spatial and transform domain -Steganography Security.					
<b>Module:5</b>	<b>Audio and Video Steganography</b>	<b>6 hours</b>			
Audio Steganography: Temporal domain techniques, Transform domain techniques, Cepstral Domain - Video Steganography: Introduction 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.					
<b>Module:6</b>	<b>Wet Paper Code</b>	<b>6 hours</b>			
Random Linear Codes - LT Codes - Perturbed Quantization, Matrix Embedding - Matrix Embedding Theorem - Binary Hamming Codes - Q-Ary Case Random Linear Codes for Large Payloads.					
<b>Module:7</b>	<b>Steganalysis</b>	<b>6 hours</b>			
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 $\pm$ embedding - Blind Steganalysis: Features for steganalysis of JPEG images (cover vs all-stego and one class neighbor machine).			
<b>Module:8</b>	<b>Contemporary Issues</b>	<b>2 hours</b>	
		<b>Total Lecture hours:</b>	<b>45 hours</b>
<b>Text Book(s)</b>			
1.	Frank Y. Shih, Digital Watermarking and Steganography Fundamentals and Techniques, 2020, 2 <sup>nd</sup> Ed. CRC Press, United States. (ISBN No. : 9780367656430)		
2.	J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, 2010, 1 <sup>st</sup> Ed. Cambridge: Cambridge University Press, United Kingdom. (ISBN No.: 978-0-52-119019-0 )		
<b>Reference Books</b>			
1.	I. J. Cox, M. L. Miller, J. A. Bloom, T. Kalker, and J. Fridrich, Digital Watermarking and Steganography, 2008, 2 <sup>nd</sup> Ed. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-12-372585-1 )		
2.	P. Wayner, Disappearing Cryptography: Information hiding: Steganography and Watermarking, 2008, 3rd ed. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-08-092270-6 )		
Mode of Evaluation: CAT / Assignment / Quiz / FAT			
Recommended by Board of Studies		04-03-2022	
Approved by Academic Council		No.65	Date 17-03-2022