26MA801 **Cryptography for Image Security** **4 0 0 4**

Prerequisites

Fundamentals of digital image processing and dynamical systems

Course Objectives:

To provide students with a comprehensive understanding of cryptographic principles, mathematical foundations, modern encryption algorithms, chaos-based techniques, and security analysis methods for designing, implementing, and evaluating secure digital image encryption systems.

Course Outcomes:

CO1: Explain the principles of classical and modern cryptography, including symmetric/asymmetric techniques
CO2: Analyze digital image characteristics and evaluate the suitability of modern cryptographic algorithms for image encryption.
CO3: Design and develop chaos-based image encryption schemes using chaotic maps, permutation–diffusion architectures, and keystream generation techniques.
CO4: Explain and apply cryptographic primitives such as S-boxes and hash functions.
CO5: Perform security evaluation and cryptanalysis using statistical, entropy, differential metrics, and attack models.

Course Content:

UNIT 1: Foundations of Cryptography for Image Security

Basics of Cryptography: Classical vs. Modern Cryptography, Symmetric & Asymmetric Cryptography, Shannon's Principles: Confusion & Diffusion.

Mathematical Foundations: Modular arithmetic, Number theory basics, Finite fields & matrix transformations, Randomness & entropy concepts.

Digital Image Fundamentals: Types of images: grayscale, RGB, medical, hyperspectral, Image properties influencing encryption, Pixel correlation, histogram characteristics.

UNIT 2: Modern Cryptography & Security Analysis for Images

Modern Cryptosystems: DES, AES, Blowfish, RSA, ECC basics, Stream ciphers vs block ciphers and their relevance to images.

Security Analysis Techniques: Key space analysis, Key sensitivity, Statistical analysis, Histogram analysis, Information entropy.

UNIT 3: Chaos-Based Cryptography for Image Encryption

Chaotic Maps: 1D map: Logistic, Tent, Bernoulli, Sine, 2D/3D maps: Lorenz, Chen, Lü, Rossler, Hyperchaotic systems & attractors.

Chaos-Based Encryption Design: Permutation–Diffusion architecture, Pixel-level scrambling, Chaotic keystream generation, Color channel encryption.

UNIT 4: Cryptographic S-boxes & Hash-Based Image Encryption
S-box Theory: Properties: nonlinearity, bijectivity, algebraic degree, Designing chaos-based S-boxes, Dynamic S-box generation for image encryption
Hash-Based Encryption: SHA-256, SHA-512, Hash-driven key generation, Image-dependent hashing for resisting CPA/CCA attacks

UNIT 5: Research Trends, Implementation & Attack Models
Cryptanalysis & Attack Models: Brute-force attacks, Known-plaintext attack (KPA), Chosen-plaintext attack (CPA), Chosen-ciphertext attack (CCA), Differential attacks: NPCR, UACI

Text Books:

1. Cryptography Foundations,– Cryptography and Network Security, William Stallings, 8th Edition, Pearson — Best foundational text for Shannon principles, S-boxes, AES, DES.
2. Applied Cryptography, Bruce Schneier, Wiley,— Authoritative reference on classical and modern cryptographic techniques.
3. Introduction to Modern Cryptography, Jonathan Katz & Yehuda Lindell, CRC Press.

Reference Books:

1. **Modern Cryptography: Theory and Practice,** Wenbo Mao, Pearson
2. **Secure Image Communication,** Jayanta Mukhopadhyay, CRC Press
3. **Chaos and Nonlinear Dynamics,** Robert Hilborn, Oxford University Press
4. **Nonlinear Dynamics and Chaos,** Steven Strogatz, CRC Press
5. **Cryptanalysis: A Study of Ciphers and Their Solution,** Helen Fouché Gaines