

Data Compression and Cryptography

IT 803A

Credit: 3

Introduction [4L]: Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification.

Methods of Data Compression [8L]: Data compression-- Lossless & Lossy; Entropy encoding-- Repetitive character encoding, Run length encoding, Zero/Blank encoding; Statistical encoding-- Huffman, Arithmetic & Lempel-Ziv coding; Source encoding-- Vector quantization(Simple vector quantization & with error term); Differential encoding—Predictive coding, Differential pulse code modulation, Delta modulation, Adaptive differential pulse code modulation; Transform based coding : Discrete cosine transform & JPEG standards; Fractal compression.

Introduction To Security [5L]: Need for security, Security approaches, Principles of security, Types of attacks.

Cryptographic Techniques [5L]: Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key range & Size.

Symmetric & Assymmetric Key Cryptography [8L]: Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Assymmetric key together, Digital signature, Knapsack algorithm.

User Authentiction Mechanism [4L]: Authentication basics, Passwords, Authentication tokens, Certificate based & Biometric authentication, Firewall .

Case Studies Of Cryptography [5L]: Deniel of service attacks, IP spoofing attacks, Secure inter branch payment transactions.