# Chaos based image cryptography

**Course objectives**

To introduce students

- Chaos theory and cryptography
- Various attacks and cryptanalysis
- Various compression schemes along with encryption
- Real time encryption

**UNIT-I**

Introduction to chaos- properties of chaos- One dimensional chaos maps- Complex behavior in one dimensional maps -Two dimensional chaos maps- Three dimensional chaos maps- Formation of High dimensional chaos maps- PRNG tests-NIST test

**UNIT-II**

Chaos and cryptography - Traditional ciphers- AES, DES, RSA, IDEA, Chaotic hash function- Fridrich's Image Cipher- Applying 1D, 2D, 3D and high dimensional chaotic maps to image encryption- Security analysis- Performance analysis

**UNIT-III**

Cryptanalysis of chaotic ciphers- Linear cryptanalysis-Differential cryptanalysis- Cryptanalysis of Fridrich's Image Cipher- Various attacks-Main Problems in Chaos-Based Cryptography-Problems with the Selection of the Chaotic System -Problems with the Encryption Architecture-Implementation Problems-Design rules for chaos based cryptography

**UNIT-IV**

Compression and encryption- ETC scheme- CTE scheme- Lossless compression - Lossy compression - Transform based methods- Chroma Subsampling -Transform Coding - Fractal Compression -Vector Quantization- Block Truncation- Prediction based methods- Compression performance- Reversible data hiding

**UNIT-V**

Hardware Implementation of Chaos Based Cipher- Digital Programmable Hardware Implementation Using FPGAs- FPGA Technology- PRNG design using FPGA- On the fly image encryption- Case study- Implementation of Lorenz's System using FPGA

**OUTCOMES**

Students will be able to

- Develop chaos based image encryption-compression algorithms.
- Develop data hiding algorithms for the specialized applications.
- Develop real time image encryption algorithm.

Senate