Encryption Theory

First Semester 2025-2026

Project One

Each group selects one classical technique you taught (LSB, Phase Coding, Text Synonym Stego, DCT Watermarking, etc.), then searches for a **recent research paper** that proposes a **new or improved version** of that technique.

- Work must be as a group, each group consists of two students only or individual.
- Each group must implement **the new technique** described in selected paper.
- Each group must compare it with the **original classical technique** you covered in class.
- Each group must prepare a report with results + analysis + comparison.
- Below is the **exact list of research directions** each group should explore or can select any other research paper in the field.
- Every group chooses a technique → searches for a recent paper that proposes **improvement, optimization, or a new variant**.
- Each group must submit documentation and source-code
- Each group information must be listed in this shared sheet GroupsInfo.xlsx
- **Deadline to submit your work by one of group members over ITC is 20/12/2025.**

Topics as follows:

Image Steganography (LSB Variants), Students must search for a modern paper that improves classical LSB.

Suggested research areas:

- Adaptive LSB. Uses statistical or perceptual characteristics of each pixel (such as texture strength, noise level) to decide where to embed bits. Complex regions hide more data; smooth areas hide less, improving imperceptibility and reducing detection.
- Edge-based LSB. Focuses embedding in edge pixels regions with sharp changes, because modifying them slightly is harder to detect. Algorithms that

detect edges (such as Sobel, Canny) and embed bits only in those areas to increase security.

- **Multi-bit LSB with distortion minimization.** Embeds more than one bit per pixel while controlling distortion. Uses cost functions or distortion models (such as HILL, S-UNIWARD variants) to decide which locations can safely host multiple bits without creating detectable artifacts.
- **LSB using deep learning for optimization.** Deep neural networks (CNNs or GANs) learn optimal embedding patterns to minimize detectable changes. The model identifies where modifications can be hidden or automatically generates stego images with reduced statistical anomalies.
- **Reversible LSB steganography.** Allows the receiver to fully restore the original image after extracting the secret message. Uses reversible difference expansion, histogram shifting, or prediction-based embedding to achieve lossless recovery.
- LSB with error correction or redundancy reduction. Integrates coding techniques (Hamming, BCH, Reed-Solomon, run-length reduction) so hidden data remains recoverable even if the image suffers noise or compression. Which will reduces redundancy to increase payload capacity.

Audio Steganography (Phase Coding Variants), Embeds data in the phase component of audio frames (typically via FFT). Because human hearing is less sensitive to phase differences, this method maintains high audio quality and is robust to many operations.

Advanced Audio Steganography (LSB Variants)

- LSB with error-resistant embedding. Adds redundancy, parity bits, or ECC so hidden audio survives noise, re-encoding, or channel distortion. Useful for low-quality transmission environments.
- Randomized sample selection LSB. Does not embed bits sequentially. Instead, it uses a key-based or pseudo-random index generator to choose sample positions, making statistical attacks far more difficult.

Text Steganography (Synonyms / Grammar / Semantic)

- Grammar structure–based embedding. Encodes bits by choosing between grammatically equivalent structures (active/passive voice, clause ordering, optional adjectives). Each structural choice represents a bit or bit-sequence.

- Unicode-based text stego. Hides data using Unicode zero-width characters, homoglyphs, similar-looking characters, or special Unicode control symbols. Difficult for the reader to notice but detectable by specialized text-forensics tools.

Image-Based Watermarking (DCT / DWT / SVD / Hybrid)

- DCT mid-frequency watermark but enhanced (robust or blind). Embeds watermark bits in mid-frequency DCT coefficients for better trade-off between invisibility and robustness. Enhanced techniques add quantization, adaptive gain, or blind extraction (no original image needed).
- Watermark resistant to geometric attacks (rotation, scaling, cropping). Designs watermarking schemes robust to rotation, scaling, cropping, translation (RST). Uses invariant features (SIFT/SURF), log-polar transforms, or template-based synchronization.
- Watermark with deep features (CNN-extracted features). Uses CNN feature maps as embedding domains or uses deep networks to decide embedding strength. Achieves high robustness against compression, noise, filtering, and geometric distortions.

Image Steganalysis (Statistical / Classical), Students search for modern Steganalysis papers that improve classical detection.

- Statistical LSB detection improvements. Enhances classical statistical tests (LSB histograms, pairwise analysis) to detect adaptive or multi-bit LSB more accurately.
- Chi-square based enhanced detectors.
- Texture and edge analysis. Detects Stego by analyzing high-frequency regions. Assumes embedding disrupts natural noise patterns in textured or edge-dense areas.
- Stego noise pattern analysis. Examines how embedding introduces unique “noise signatures.” Uses residual images, prediction errors, or noise filters to expose embedding patterns. Combines histogram irregularity detection with entropy-based metrics to catch both simple and adaptive embedding. Suitable for LSB and some transform-domain techniques.
- Histogram/entropy hybrid detectors.

- Feature extraction improvement methods. Uses improved handcrafted features (SPAM, SRM) or machine-learning feature selection to enhance steganalysis accuracy—sometimes combined with SVM or CNN classifiers.

How can work with selected topics if you select one of these?

If a student picks a topic like “Multi-bit LSB with distortion minimization”, they should locate a research paper titled or describing a method for multi-bit LSB embedding with distortion minimization, then implement that method (or a simplified version) and compare to standard multi-bit LSB embedding.

If group select as example “Watermark with deep features (CNN-extracted features)”, they should find a recent research article about watermarks that embed in deep-feature space (or use CNN features) and then implement some component of that method or adaptation, plus a baseline watermark in, say, DCT domain.

Each group is not required to implement all variations you listed under each category. Just choose one single topic variation (for example: “Randomized sample selection LSB” in audio stego) and focus on that variation.

You are free to use any programming language you prefer. There is no restriction on the language, framework, or tools, if Your code runs successfully and produces the required experiments (embedding, extraction, watermark attack tests, steganalysis evaluation, etc).