**CSE 459: Cryptography and Network Security**

**Course Project**

**Submission Date: 08 / 04 / 2025**

***Project Title: 3D Chaos‑Enhanced Block‑Permutation & Diffusions***

**Group Members**:

1)AP22110010094, P Vishnu Vardhan, Vishnuvardhan\_p@srmap.edu.in

1. **Purpose of the project:**

Design and implement a lightweight yet secure encryption scheme for 256×256 grayscale images by combining 3D‑map–driven row/column rotations, intra‑block pixel shuffling, and final XOR diffusion

1. **Why it is relevant (explain with example):**

An unencrypted factory‑inspection camera feed can reveal proprietary component designs if intercepted. Encrypting each pixel globally and locally prevents both large uniform areas and fine details from leaking, safeguarding industrial secrets.

1. **How you will solve the problem:**

 **3D Chaotic Key Generation** – Iterate a 3D logistic map to produce three integer sequences: x\_key, y\_key, z\_key.

 **Row & Column Rotations** – Circularly shift each row by x\_key[i] (even→right, odd→left) and each column by y\_key[j] (even→up, odd→down).

 **Intra‑Block Permutation** – Split into 16×16 blocks; for block b, take z\_key[b·256…], derive a 256‑entry permutation via argsort, and reorder its pixels.

 **XOR Diffusion** – Reshape z\_key into 256×256 and XOR with the permuted image to erase residual patterns.

1. **What are the other possible ways (if any) to solve it:**

* **AES/DES** – Secure but heavy on CPU and memory, and ECB mode may leak block patterns.
* **Selective Transform‑Domain** – Encrypt DCT/DWT coefficients; efficient but risks leakage in unencrypted bands.
* **Basic Chaos‑Based Permutation** – Full‑image pixel shuffle; fast but lacks diffusion of value changes.

1. **Advantages of using the chosen approach:**

* **Multi‑stage confusion** at both global (rows/columns) and local (blocks) levels.
* **High diffusion** via final XOR, yielding NPCR ≈ 99.6 % and UACI ≈ 30 %.
* **Efficient** implementation: encryption ≈ 0.02 s, decryption ≈ 0.017 s on a standard desktop.