
Project Title:

Steganography-Based Secure Messaging System

Objective:

The primary objective of this project is to develop a secure messaging system using steganography techniques to conceal sensitive messages within digital media, ensuring confidentiality, authenticity, and protection against eavesdropping and cyber threats.

1. Problem Statement:

Traditional encryption can attract attention, making messages vulnerable to interception. A discreet approach like steganography enhances security by hiding messages within digital media.

2. Solution:

This project aims to implement a steganographic messaging system that embeds secret messages within digital media, such as images, audio, or video files, using advanced encoding techniques. By this steganography, the project ensures that communication remains hidden from potential attackers, providing an additional layer of security beyond traditional encryption methods.

3. Technologies to be Used:

- **Programming Languages:** Python (with libraries such as OpenCV, Pillow, and NumPy) and Deep Learning.
- **Steganography Techniques:** LSB (Least Significant Bit),
- **Cryptography:** AES (Advanced Encryption Standard)
- **Frameworks & Tools:** Stegano, Cryptography, PyCrypto

4. Methodology:

Step 1: Define the System Requirements

Step 2: Data Preprocessing & Encryption(AES)

Step 3: Embedding Data using Steganography(LSB)

Step 4: Extracting the Hidden Message(RCNN or CNN)

Step 5: Decrypt the Extracted Message

Step 6: User Interface & System Integration