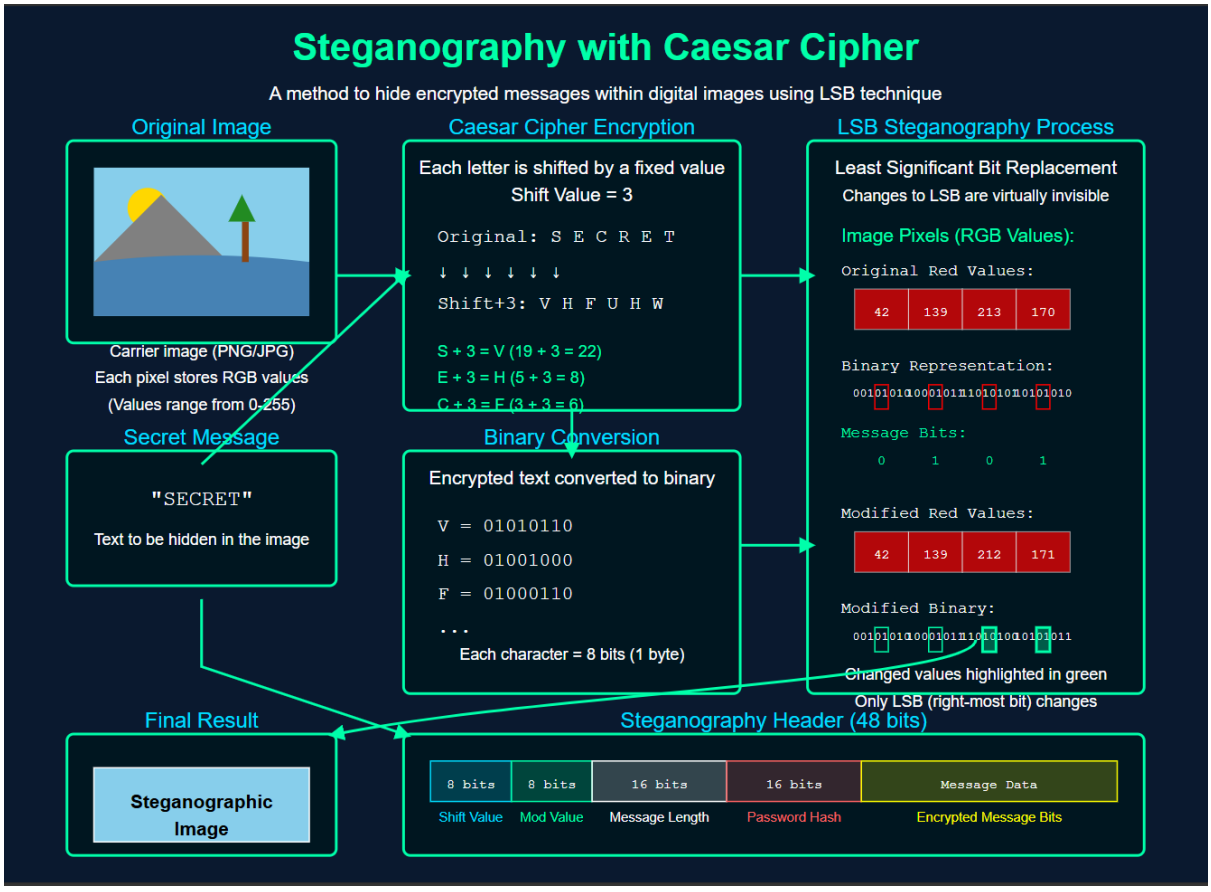
M.KUMARASAMY COLLEGE OF ENGINEERING, KARUR
Department of Freshmen Engineering
PROJECTEXPO'25

Title: Steganography with caesar cipher

Team Members

Section Roll Number	Branch	Name
A531	IT	K.MUTHUVEL MUKESH
A526	IT	P.MADHAVAN
A521	IT	M.S.KAMARASAR

Steganography with Caesar Cipher



Overview

This document presents a comprehensive web-based steganography application that combines classical cryptography with modern digital steganography techniques. The system enables users to hide encrypted messages within image files using the least significant bit (LSB) method while implementing multiple layers of security.

Encryption Components

The application implements a multi-layered security approach:

1. Caesar Cipher Ecryption:
   - Customizable shift value (1-25)
   - Adjustable modulus value (default: 26)
   - Character-by-character transformation

2. Binary Conversion and Header Structure:

   - 8 bits for shift value
   - 8 bits for modulus value
   - 16 bits for message length
   - 16 bits for password hash

3. LSB Steganography Implementation:

LSB steganography involves hiding secret data within an image by replacing the least significant bit (LSB) of each pixel's color values with the bits of the secret message

4. Security Features

-Password Protection: 4-digit numeric password with simple hash verification
- XOR Encryption: Optional bitwise XOR operations using the password as a key
- Image Noise Addition: Random pixel value modifications to mask steganographic changes
- Stealth Mode: Option to hide canvas visualization during the encoding process
- Capacity Analysis: Automatic calculation of maximum message capacity based on image dimensions

Decryption process

Image as decryption tool:

When the recipient receives the image, they display or analyze it to retrieve the key and mod value.
This can be automated via a script that extracts the key from the image data or by manually checking metadata.

Reverse Caesar cipher

The recipient uses the extracted key and mod value to reverse the Caesar Cipher and decrypt the text, restoring the original message.

User Experience Elements

- The application features a cybersecurity-themed aesthetic with:
    - Animated Matrix-style falling characters background
    - Interactive cursor trails with occasional "glitch" effects
    - Real-time console logging of operations
    - Threat scanning simulation with randomized results

The implementation serves as both a functional steganography tool and an educational platform for demonstrating concepts in information security, cryptography, and digital steganography.