SISTER NIVEDITA UNIVERSITY

School of Engineering

Subject	Project Abstract
Department	CSE
Program	B.Tech Computer Science and Engineering (AI & ML)
Section	5
Academic Year	2022-26

Mentor and team details

Name	Enrolment ID	Phone Number	Signature
Akash Chakraborty	2211200010026	7679406225	
Aparajito Ray Chaudhuri	2211200010046	9830373593	
Abhirup Samadder	2211200010066	7439995200	
Sanjukta Sarkar	2211200010004	9832075018	

Mentor Name	Mentor Signature
Prof. Atal Chaudhuri	

Approach Towards Copyright Protection for Images Using Sharing and Signature Embedding Technique

Abstract

With the rapid growth of digital content distribution, protecting intellectual property rights over multimedia—especially digital images—has become critical. Unauthorized copying, modification, and redistribution of images pose significant threats to content creators and rights holders. This project proposes a robust and secure framework titled **"Approach Towards Copyright Protection for Images Using Sharing and Signature Embedding Technique"** that leverages a combination of steganography, watermarking, cryptography, and secret sharing to enhance image authentication and ownership protection, in true sense of robust

Objectives

The main objectives of this project are:

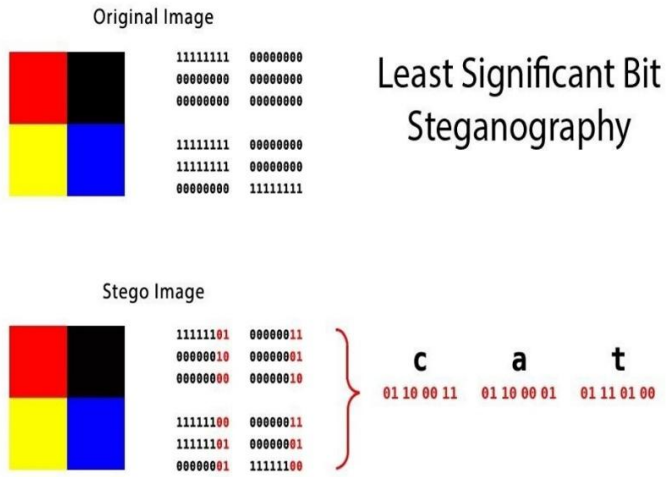
- To develop a secure mechanism for embedding a copyright signature within a digital image without perceptible distortion.
- To ensure the embedded signature can only be extracted and validated by authorized parties using password verification.
- To apply cryptographic and secret sharing techniques to increase the robustness and security of the embedded watermark against unauthorized tampering or removal.

Proposed Methodology

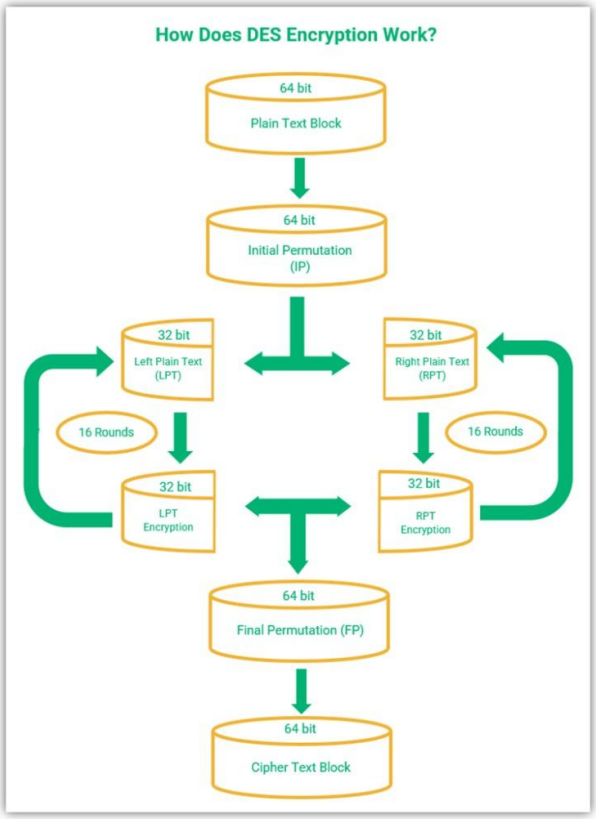
The approach combines three key techniques:

- **Least Significant Bit (LSB) Embedding:** The watermarking process involves embedding the copyright signature (such as an author's name or unique ID) into the image using the Least Significant Bit (LSB) technique. LSB replaces the least significant bits of selected image pixels with bits of the watermark. This method ensures minimal change in the image’s visual quality while storing the watermark data.

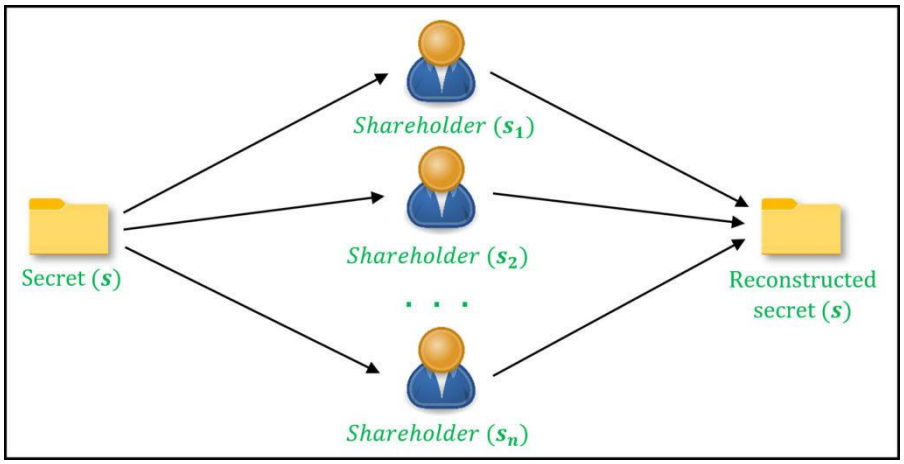
  For instance, in an 8-bit grayscale image pixel with binary value 11010110, replacing the least significant bit with a watermark bit 1 results in 11010111. The imperceptibility of changes in the LSB ensures a visually identical image, thereby maintaining user experience.



- **Data Encryption Standard (DES):** To prevent unauthorized detection or manipulation of the embedded signature, the watermark is first encrypted using the DES algorithm before LSB embedding. DES is a symmetric key block cipher that encrypts 64-bit blocks of plaintext using a 56-bit key through 16 rounds of complex substitution and permutation. Encrypting the signature ensures that even if the watermark is extracted, it cannot be interpreted without the decryption key.



- **Shamir's Secret Sharing Algorithm:** To further enhance security and support distributed verification, the encrypted watermark is divided into multiple shares using Shamir's Secret Sharing Scheme (SSSS). This technique is based on polynomial interpolation. A secret is split into n shares such that any k out of n shares can reconstruct the original secret (where k ≤ n), but fewer than k shares reveal nothing. This prevents single-point failure and allows collaborative authentication among multiple parties. The embedded watermark is thus encrypted using DES, split using Shamir's algorithm, and the shares are then embedded into the LSBs of the image.



Expected Outcomes

The implementation of the proposed methodology is expected to:

- Provide high imperceptibility and robustness of watermarking using the LSB technique.
- Ensure secure and confidential transmission of the watermark via DES encryption.
- Enable flexible and fault-tolerant recovery of the watermark using Shamir's algorithm.
- Prevent unauthorized extraction and counterfeiting of the digital image signature.

This approach will allow for reliable copyright verification without affecting image quality and will make ownership claims legally and technically enforceable.

Potential Future Scope

- The framework can be extended in multiple directions:
- Use of more advanced encryption techniques such as AES or RSA for higher security.
- Incorporation of biometric-based watermarking for author verification.
- Machine learning for watermark detection and authentication to automate verification.
- Application to other multimedia formats such as video or audio.
- Blockchain integration to store encrypted watermarks immutably for decentralized verification.