Secure Image Sharing Using Threshold Cryptography and Visual Secret Sharing

S.Azhagesh- 23BCE1205

Giridharen Goguladhevan- 23BCE5043

Rohith Ganesh Kanchi - 23BCE5049

S.D. Madhumitha - 23BCE5058

This presentation details their approach leveraging Shamir’s Secret Sharing and other cryptographic techniques to enable secure, efficient, and robust image distribution with privacy guarantees based on threshold reconstruction.

Project Aim: Robust Threshold-Based Secure Image Sharing

Threshold Mechanism

Secret images are split into multiple shares such that only a minimum (threshold k) number reconstruct the original image; fewer shares reveal no information.

Security & Efficiency

Prioritizes security against unauthorized access and computational efficiency, making the solution scalable for large images.

Comparison

Evaluates Shamir's Secret Sharing (SSS) approaches versus Chinese Remainder Theorem (CRT) schemes for performance and security tradeoffs.

Proposed Solution: Shamir's Secret Sharing Variations for Secure Image Sharing

Basic SSS (Code 1)

Encodes each pixel as a polynomial constant in GF(257). Generates n shares by polynomial evaluation. Uses Lagrange interpolation for reconstruction.

SSS with N+1 Share (Code 2)

Adds an extra share based on pixel-wise sum modulo P=251. Allows reconstruction with any k shares out of n+1. Uses linear algebra if the extra share is involved.

Parallelized SSS (Code 3)

Improves efficiency by processing polynomial evaluations and reconstruction in parallel across image chunks using multiprocessing.

Encrypted Parallel SSS (Code 4)

Enhances security by encrypting the numerical shares using AES-GCM with keys derived from user passwords. Ensures secure storage against unauthorized access.

Key Definitions: Prime Modulus P in Shamir's Secret Sharing

Prime Modulus Role

Defines the finite field GF(P) where polynomial coefficients and operations occur, ensuring closure of arithmetic operations essential for SSS correctness.

Choice of P

P must be greater than pixel max value (255) for lossless recovery. P=257 used in Code 1 ensures exact recovery; P=251 used in other codes introduces minor loss for pixels 251-255.

Implications

Smaller prime values introduce modulo wrapping for some pixel intensities, resulting in minor, usually imperceptible distortions in the reconstructed image.

Detailed Procedure for Secure Share Generation and Reconstruction

1

Initialization

Load image, convert to grayscale array, select parameters n, k, and prime P; compute original image hash for integrity checking.

2

Share Creation

Generate random polynomials per pixel, evaluate shares-modulo P in parallel; compute additional share if specified; hash shares.

3

Secure Storage

Optionally encrypt numerical shares with AES-GCM using password-derived keys; save visual and numerical share files with hashes.

4

Reconstruction

Load k shares with verification; decrypt if necessary; reconstruct pixels using Lagrange interpolation or linear algebra depending on shares selected.

5

Verification & Display

Validate final image via hash comparison; display original, shares, and recovered image with timing metrics.

Sharing Phase and Participant-Increasing Method

Generating the (n+1)th Share

Combines original n shares pixel-wise modulo prime p=251, creating an additional share that enables participant increase without changing the threshold.

Loss vs Resolution Tradeoff

Using p=251 (less than 256) causes minor information loss in bright pixels but maintains high resolution compared to existing visual cryptography schemes.

Algorithm 1. The proposed participant increasing method in sharing phase

Input: k original secret shadow images $SC_1, SC_2, \cdots SC_n$
Output: 1 new shadow image SC_{n+1}

Step 1: For each position$(i,j) \in \{(i,j)|1 \leq i \leq M, 1 \leq j \leq N\}$, repeat Step 2.
Step 2: Set $SC_{n+1}(i,j) = (SC_1(i,j) + SC_2(i,j) + \cdots + SC_n(i,j)) \bmod p$
Step 3: Output the new shadow image SC_{n+1}

Recovery Phase and Polynomial Reconstruction

Algorithm 2. The proposed participants increasing method in recovery phase

Input: The $k(>k)$ shadow images which are randomly selected from $n+1$ shadow images $SC_1, SC_2, \cdots, SC_n, SC_{n+1}$
Output:The original secret image S

Step 1: Select $k(>k)$ shadows, and note down their lables x.
Step 2: For each position$(i,j) \in \{(i,j)|1 \le i \le M, 1 \le j \le N\}$, repeat Step 3-4.
Step 3: According to the k or more lables, Eq(1) and Eq(3), construct the k or more corresponding polynomials.
Step 4: Get the coefficient a_0 of $f(x)$ by solving polynomials, and set the pixel $S(i,j)$ as the value a_0.
Step 5: Output the secret image S

This algorithm represents the recovery phase and polynomial reconstruction.

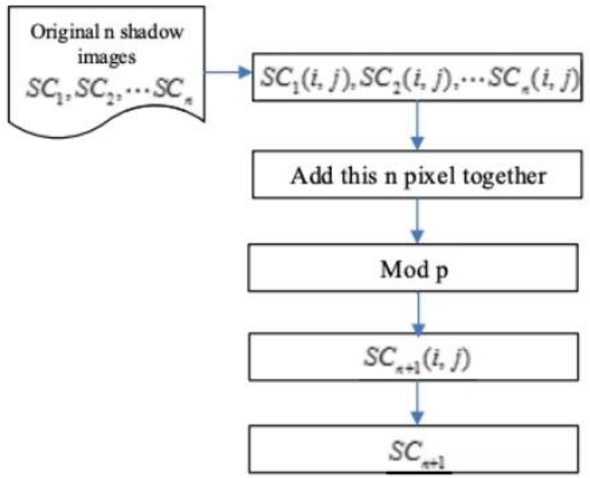

Figure 1. Design concept of the proposed method

Reconstruction Mechanism

When n+1th share is chosen, reconstruction requires solving linear equations modulo p using the polynomial sums; otherwise Lagrange interpolation applies.

Example Scenario

Extending a (2,2) to a (2,3) scheme allows flexible share combinations, with subtraction employed if n+1 share is involved for recovery.

The project also implemented visual cryptography and Chinese Remainder Theorem-based approaches, along with entropy and performance analyses.

Overview of Implemented Algorithms and Features

Shamir's Secret Sharing

Basic and enhanced schemes with polynomial shares, N+1 share extension, parallelization, and AES-GCM encryption for share security.

Visual Cryptography

Implemented 2-out-of-2 VC scheme for binary images, enabling pixel expansion and overlay reconstruction.

Chinese Remainder Theorem

Implemented Asmuth-Bloom CRT secret sharing with prime moduli selection and reconstruction using CRT conditions.

Max Flow Analysis

Conceptual network capacity checks to validate distribution feasibility, ensuring k-share delivery is possible.

Analysis & Insights from Experimental Results

Effectiveness & Security

- All schemes successfully masked image data; threshold shares reveal no info below k.
- Integrity verified by SHA-256 hashes, ensuring data correctness.

Entropy & Randomness

High Shannon entropy in SSS and CRT shares confirms robust randomization and strong secrecy.

CRT shares showed generally higher entropy due to number-theoretic complexity.

Performance

Parallelism in SSS notably accelerates share generation and reconstruction.

CRT shows trade-offs: slower for low k/n, faster for higher k/n, affecting usability.

VC & Max Flow

VC simple but limited by contrast loss and binary image requirement.

Max flow check verifies theoretical distribution network capacity for share delivery.

Limitations, Future Work, and Conclusion

Current Constraints

Loss from P=251 modulus, limited CRT parameterization, basic VC scheme, conceptual max flow, and simplistic password encryption.

Enhancement Opportunities

Guarantee lossless SSS with P>257, dynamic CRT prime generation satisfying Asmuth-Bloom, advanced VC schemes for color/grayscale.

Extend Max Flow to practical network path optimization, add GUI, asymmetric encryption, error correction, and hybrid cryptographic approaches.

Conclusive Summary

The project effectively implements and compares multiple threshold secret sharing schemes for secure image distribution with performance and security analyses. It lays groundwork for further research combining cryptography and image processing for practical, secure image sharing.