Introduction

Visual cryptography is a form of image-based encryption that allows a secret image to be split into multiple “shares” that individually appear as random noise, but reveal the secret when overlaid. Introduced by Naor and Shamir in 1994, the (2,2) visual cryptography scheme divides a binary (black-and-white) image into two shares such that neither reveals any information alone, yet both together visually reconstruct the original image without the need for computation.

This project implements both the classical (2,2) scheme for black-and-white images and extends it to handle color images securely. The work demonstrates how images can be securely shared between two parties and visually decrypted using only human vision.

Implementation

The core principle of visual cryptography relies on pixel expansion and random pattern encoding:

- The input image is first converted into black-and-white (binary).
- Each 1×1 pixel is expanded into a 2×2 block in both shares.
- For white pixels, both shares receive the same 2×2 random pattern.
- For black pixels, the second share receives a complementary pattern to the first.
- When both shares are stacked, black pixels become visually darker, while white pixels appear lighter or gray.

Two basic 2x2 patterns are used:

A: [1, 0] and B: [0, 1]
    [0, 1]   [1, 0]

Each pixel in the image is randomly assigned one of these patterns and handled based on whether it is black or white.

To extend visual cryptography to color images, the project implements an adapted scheme that preserves **perfect secrecy** while handling the Red, Green, and Blue (RGB) channels individually.

The secure color approach involves:

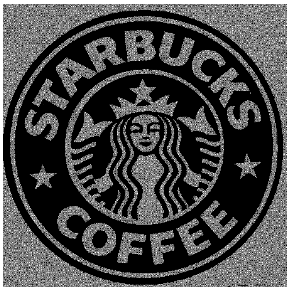
- Generating **pure random noise** for the first share (each pixel randomly selected from all possible RGB values).
- Calculating the second share such that when **added modulo 256** to the first share, it perfectly reconstructs the original image.

Mathematically, Share2_pixel = (Original_pixel − Share1_pixel) mod 256, and hence (Share1_pixel + Share2_pixel) mod 256 = Original_pixel

Each color channel (R, G, and B) is handled separately, ensuring full-color reconstruction while maintaining information-theoretic security.

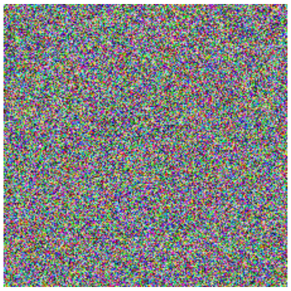
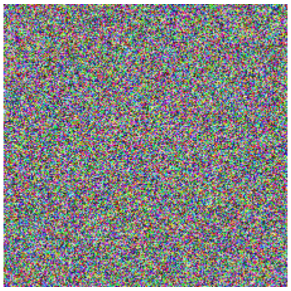
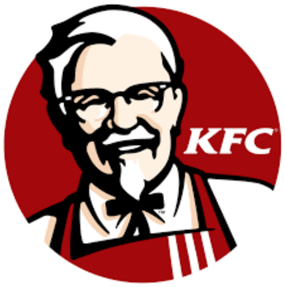
Results

The tool successfully produces two visually meaningless shares from a black-and-white input image. When viewed individually, the shares resemble random noise. When stacked, they reveal the original image clearly.

Input Image	Share 1	Share 2	Reconstructed Image
			

This confirms that the (2,2) visual cryptography scheme works effectively, preserving information-theoretic secrecy while enabling simple human-readable decryption.

Similarly, for color images, two fully random-looking color shares are produced. Each share individually appears as meaningless colored noise. Upon stacking (adding pixel values modulo 256), the original colored image is perfectly reconstructed.

Input Image	Share 1	Share 2	Reconstructed Image
			

This confirms that the color extension maintains the core idea of visual cryptography while allowing full-color secure sharing.

Security and Limitations

In both schemes, each individual share reveals no information about the original image. Even with unlimited computational power, an adversary cannot infer any part of the secret from just one share — satisfying information-theoretic security. However, this scheme is limited to black-and-white binary images, and resolution is reduced due to pixel expansion since the original image is enlarged 4x. It also does not scale well to color images without more advanced encoding.

Link to Lecture Concepts

- **Perfect Secrecy**
    - Visual cryptography satisfies the formal definition of perfect secrecy for each individual share, as given only one share, the distribution of pixel values is independent of the original message.
    - This aligns with the formal notion of perfect secrecy where for any ciphertext and any two messages, the probability of the ciphertext being observed is the same.
    - Mathematically, For all messages m0, m1 and ciphertext c, Pr[C=c | M=m0] = Pr[C=c | M=m1]
    - This is achieved because:
        - In black-and-white VC: random pattern selection ensures share randomness.
        - In color VC: random RGB noise ensures complete obfuscation of pixel values.
- **Information-Theoretic Security vs Computational Security**
    - Visual cryptography is secure regardless of the adversary's computational power, placing it in the class of information-theoretically secure schemes.
    - This contrasts with most modern cryptographic systems (e.g., RSA, AES) that rely on computational assumptions (e.g., hardness of factoring).
    - Even an adversary with unlimited computation cannot infer the original image from one share alone.
- **Secret Sharing Schemes**
    - The (2,2) visual cryptography scheme is a special case of a threshold secret sharing scheme: The secret (image) is divided into two parts, and both parts are required to reconstruct the secret; neither alone suffices.
    - This mimics Shamir's secret sharing in spirit, though visual cryptography doesn't use interpolation or modular arithmetic, it relies on visual overlap.
    - It satisfies:
        - Correctness: The original image is recovered when both shares are combined.
        - Privacy: No single share reveals anything about the original.

Link to Lecture Concepts

Through this project, I implemented and extended the classical (2,2) visual cryptography scheme to both black-and-white and color images. The results confirm the feasibility of using simple randomized methods to achieve perfect secrecy, supporting key cryptographic concepts such as information-theoretic security, secret sharing, and perfect secrecy. This project has deepened my understanding of how theoretical ideas from cryptography, such as the one-time pad and secret sharing, can be applied to practical and intuitive visual domains.