Cryptography and Applications Lab - CS352

Cryptography Project Report

Implementation and Analysis of various Visual Cryptographic Methods

K Krishna Swaroop (181CO125) and Shreeraksha R Aithal (181CO149)

Overview

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decrypted information appears as a visual image.

One of the best-known techniques has been credited to Moni Naor and Adi Shamir who developed it in 1994. They demonstrated a visual secret sharing scheme wherein an image was broken up into n shares and only someone with **all n shares** could decrypt the image. Any combination of n-1 shares revealed zero information about the original image.

Problem Statement

Given an image, build several secure (N, N) Visual Cryptography Sharing Scheme image encryption techniques, which is robust to various cryptographic attacks and compare the efficiency of encryption and decryption methods in extracting the original image.

Implementation

All the implemented algorithms are (2, 2) Visual Cryptography Sharing Scheme image encryption technique. However, most of them can be extended to the (N, N) Sharing Scheme. Following is the list of Visual Cryptographic algorithms implemented in this project.

1. Pixel Expansion algorithm

In this algorithm, each pixel is divided into subpixels and the original image is split into 2 shares which are then overlapped to get the final decrypted image. Each collection of subpixels will have an equal number of black and white subpixels. The colors of the sub-pixels are assigned in such a way that when the two shares are overlapped, the previously black-colored pixel will still have all its sub pixels black, and the previously white-colored pixel will have half of its subpixels black. We have implemented the algorithm where each pixel is divided into 4 subpixels. This would result in the share images being double the size of the original image. Since there are six different blocks (4C2 options for subpixels collection) for each pixel in a share that are randomly chosen, decryption with a single share is impossible, taking 6^(m*n) states (m * n is the size of the original image) for a brute force attack to decrypt the secret from a single share. We have followed two ways to decrypt : Overlap (decrypted image is twice the size of original image, hence it is resized to half to match with original image), Extraction (only pixels which has all its sub pixels as black is termed as black, else it is white).

Advantage:

- Proven to be one of the best and oldest image-encryption techniques.
- Applicable to binary images of any size.

Disadvantage:

- Computation costs are high.
- Decrypted image is not fully the same as the original image. Hence the algorithm is a lossy loss encryption-decryption method.

2. CMYK Decomposition algorithm

Visual cryptography was developed in the early times for only binary images, although recent works have been it's usages in grayscale and color images. One method is where the color image is decomposed to Cyan, Magenta, Yellow and Black. Using the first three images, we use halftone conversions for each of the monotone images. We then use

nearest neighbor interpolation to generate the three shares. We later combine the three shares to get the output image file.

Advantage :

- Applicable to Color images of any size
- Can be easily extended to n-shares

Disadvantage :

- Computation Costs are high
- Since we use halftone, there is lossy decryption resulting in some visual information being lost

3. XOR Image encryption algorithm

This encryption technique is very similar to encrypting a number using XOR with a secret number. This idea is extended to make it work for each pixel value in an image. The original image is XORed with k share images (where k>1) of the same size to form a secret image. This secret image is then XORed with the k share images to obtain back the original image. This algorithm is an (N, N) Sharing scheme, meaning all k share images along with the secret image is required to decrypt the image. Even if one share image is missing, it would require 2^(m*n) states (m * n is the size of the original image) to retrieve the final image where each state is equiprobable, making it hard to decrypt.

Advantage :

- Easier to build the encryption-decryption system
- Computation cost is very low.
- Can be used to encrypt-decrypt any kind of image.

Disadvantage :

- An attacker having access to the system can easily track the secret images as he/she can run the system once to decipher the equivalent share image.

- The encryption-decryption method is very similar to One-time Pad and hence is not secure. Same key (image shares) cannot be used multiple times.

4. Modular Arithmetic Image encryption algorithm

This encryption technique uses the idea of modular arithmetic and its cyclic ring nature. Since the value of each pixel is between 0-255, taking modulo 256 works. The original image is added to k share images (where k>1) of the same size taken to modulo 256 to form a final secret image. To decrypt, each k share image is subtracted from the secret image taken modulo 256 to get the final decrypted image. This algorithm is an (N, N) Sharing scheme, meaning all k share images along with the secret image is required to decrypt the image. Even if one share image is missing, it would require 256^(m*n) states (m * n is the size of the original image) to retrieve the final image where each state is equiprobable, making it hard to decrypt.

Advantage :

- Easier to build the encryption-decryption system
- Computation cost is very low.
- Can be used to encrypt-decrypt any kind of image.

Disadvantage :

- An attacker having access to the system can easily track the secret images as he/she can run the system once to decipher the equivalent share image.
- The encryption-decryption method is very similar to One-time Pad and hence is not secure. Same key (image shares) cannot be used multiple times.

5. Bit Level Decomposition algorithm

This algorithm is an extension of Pixel-Expansion to work on Grayscale images[2]. The input grayscale image is split into binary images on which the Pixel-expansion algorithm is applied. The resultant two sets of binary images are combined to form two grayscale

shares. The same logic is applied to decrypt the image. Since each pixel value in the image varies from 0-255, the original image is split into 8 binary images. Value in the corresponding binary image is the same as what value is present in the pixel in that bit. Eg : (i, j)th pixel in kth binary image will contain the kth bit of the (i, j)th pixel value in the original image. We have followed two ways to decrypt due to the usage of Pixel-Expansion algorithm : Overlap (decrypted image is twice the size of original image, hence it is resized to half to match with original image), Extraction (only pixels which has all its sub pixels as black is termed as black, else it is white).

Advantage :

- Applicable to grayscale images of any size.
- Since it is an extension to Pixel expansion, its efficiency is the same as that of Pixel Expansion.

Disadvantage :

- Computation costs are high.
- Decrypted image is not fully the same as the original image. Hence the algorithm is a lossy loss encryption-decryption method.

6. AES Image encryption algorithm

With the rapid development of the internet around us, there is an increasing need to securely transfer images between two (in)secure systems. To tackle this problem, many visual encryption algorithms have been developed, but we propose a unique image encryption algorithm that uses a mix of AES and Visual Cryptographic techniques to protect the image.

In short, we have encrypted the image using our own implementation of AES and encoded the secret key into shares based on visual cryptography techniques discussed above.

Advantage :

- Works for various sizes of images and different key sizes

- Secret Image is retrieved with low losses and the visual quality is intact

Disadvantage :

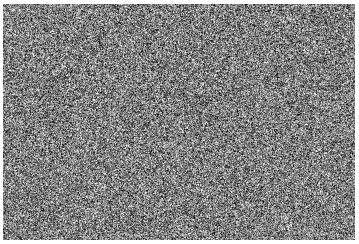
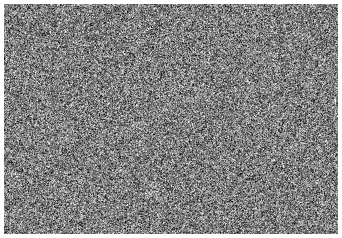
- Takes significant time for encryption and decryption
- Computation costs are high

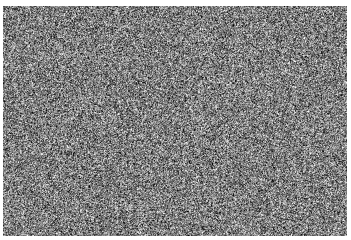
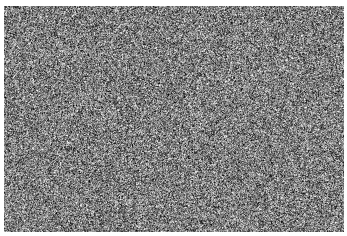
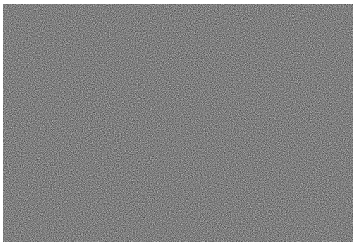
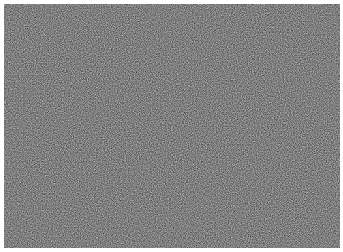
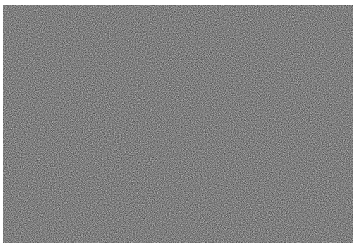
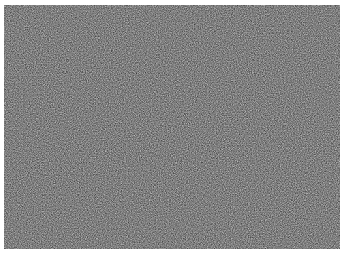
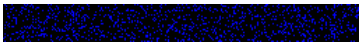
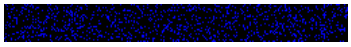
Observation

The algorithms mentioned in the previous section have been crafted to work for different kinds of images (Binary, Grayscale and Colored). Following is the observation that we could get from the implementation of the algorithms.

1. Algorithms for Binary Images

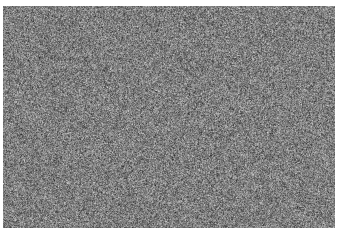
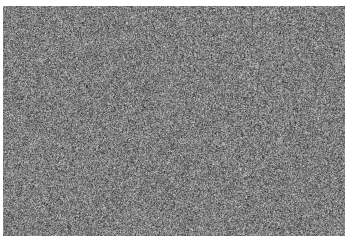
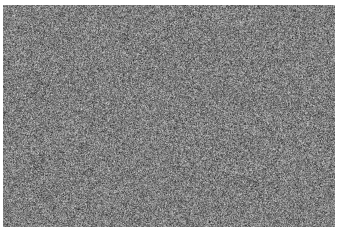
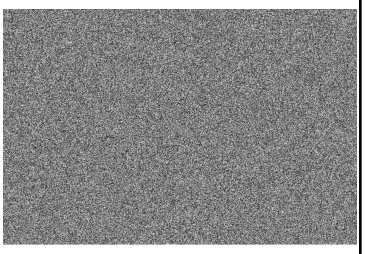
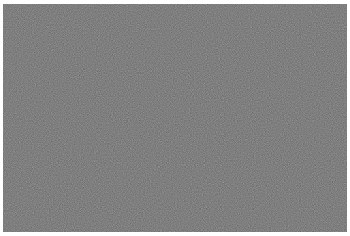
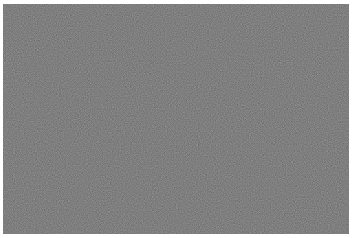
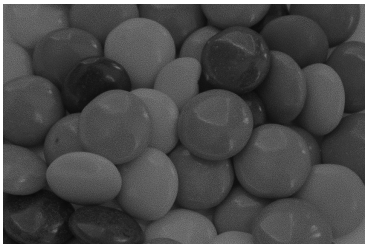
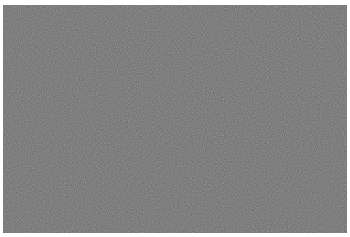
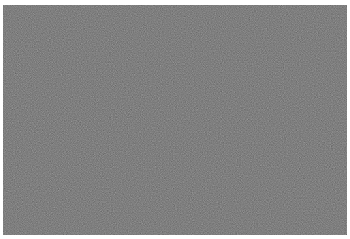
Input Image :

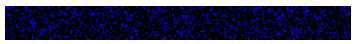
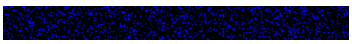
Algorithm Name	***Share 1***	***Share 2***	***Final Decrypted Image***
Modular Arithmetic Image Encryption			

XOR Image Encryption			
Pixel Expansion Image encryption (Overlap)			
Pixel Expansion Image encryption (Extraction)			
AES Image encryption			

2. Algorithms for GrayScale Images

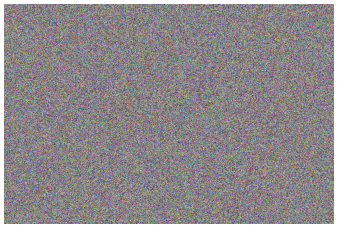
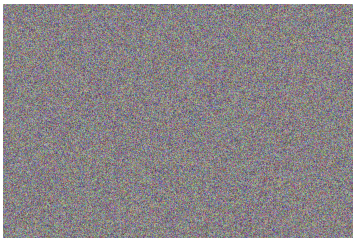
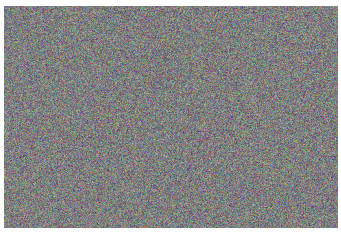
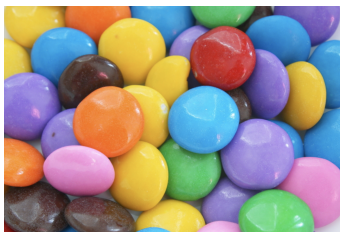
Input Image :

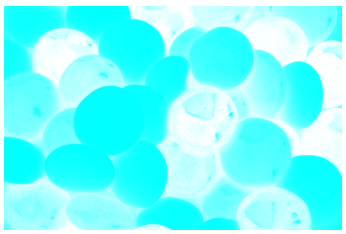
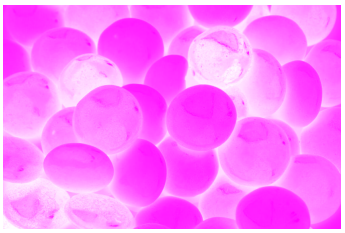
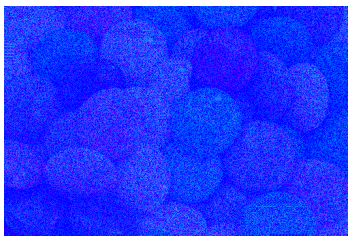
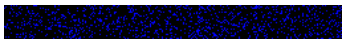
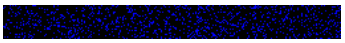
Algorithm Name	***Share 1***	***Share 2***	***Final Decrypted Image***
Modular Arithmetic Image Encryption			
XOR Image Encryption			
Bit-Level Decomposition Image encryption (Overlap)			
Bit-Level Decomposition Image encryption (Extraction)			

AES Image encryption			

3. Algorithms for Colored Images

Input Image :

Algorithm Name	***Share 1***	***Share 2***	***Final Decrypted Image***
Modular Arithmetic Image Encryption			
XOR Image Encryption			

Halftone CMYK Decomposition Image encryption		 	
AES Image encryption			

Result

The algorithms mentioned in the previous section have been crafted to work for different kinds of images (Binary, Grayscale and Colored). Following is the observation that we could get from the implementation of the algorithms.

1. Algorithms for Binary Images

Algorithm Name	***Peak signal-to-noise ratio (PSNR)***	***Mean Normalised Cross Correlation***
Modular Arithmetic Image Encryption	100 dB	0.0060369955
XOR Image Encryption	100 dB	0.0060369955
Pixel Expansion Image encryption (Overlap)	28.153 dB	0.0084041602

Pixel Expansion Image encryption (Extraction)	100 dB	0.0060369955
AES Image encryption	100 dB	0.0060369955

2. Algorithms for Grayscale Images

Algorithm Name	***Peak signal-to-noise ratio (PSNR)***	***Mean Normalised Cross Correlation***
Modular Arithmetic Image Encryption	100 dB	0.0296635942
XOR Image Encryption	100 dB	0.0296635942
Bit - Level Decomposition Image encryption (Overlap)	27.475 dB	0.0277611896
Bit - Level Decomposition Image encryption (Extraction)	100 dB	0.0296635942
AES Image encryption	100 dB	0.0296635942

3. Algorithms for Colored Images

Algorithm Name	***Peak signal-to-noise ratio (PSNR)***	***Mean Normalised Cross Correlation***
Modular Arithmetic Image Encryption	100 dB	0.0169427971
XOR Image Encryption	100 dB	0.0169427971
Halftone CMYK Decomposition Image encryption	27.981	-0.077237

AES Image encryption	100 dB	0.0169427971

Conclusion

Visual Cryptography provides one of the most secure ways to transfer images on the internet. The main advantage visual cryptography has over conventional cryptographic techniques is that the decryption happens almost instantaneously via the naked eye. Unlike most existing literatures which have advances in grayscale and black and white images, this project takes it a step forward and explores and exploits various algorithms for coloured images as well.

In all, we have done a comprehensive analysis of various image encryption algorithms for grayscale, binary and color images and also reported metrics such as Peak Signal to Noise Ratio and Mean normalised cross correlation to understand the security of these algorithms.

References

[1] Moni Naor and Adi Shamir, *"Visual Cryptography"* (1994)

[2] D. Taghaddos and A. Latif, *"Visual Cryptography for Gray-scale Images Using Bit-level"* (2014)

[3] Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan, *"A novel image encryption algorithm using AES and visual cryptography"* (2016)

[4] Archana B. Dhole and Prof. Nitin J. Janwe, *"Visual Cryptography in Gray Scale Images"* (2013)

[5] Young-Chang Hou, "*Visual cryptography for color images*" (2002)