Visual Cryptography

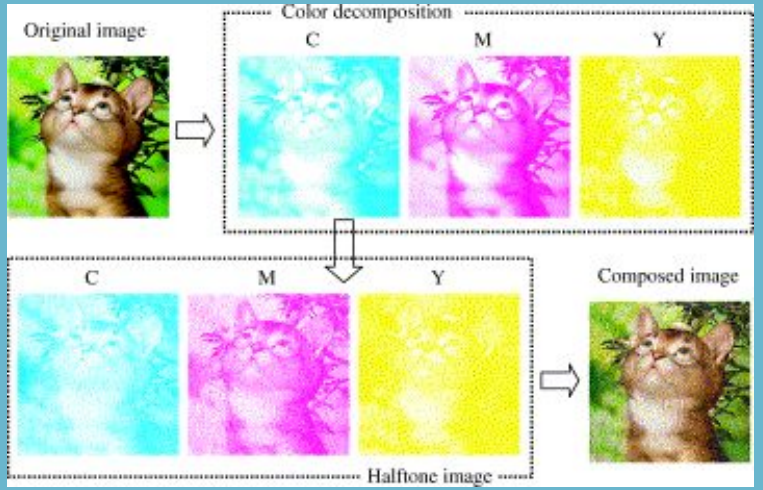
Submitted to:
Mrs. Mahalakshmi B S
(Assistant Professor)

By
Niranjan Hegde 1BM19IS103
Prashanth Jaganathan 1BM19IS115
Samartha S 1BM19IS219

A Comprehensive Study of Visual Cryptography

What is Visual Cryptography?

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image.



A Comprehensive Study of Visual Cryptography

How do you do Visual Cryptography?

- A binary image is divided into shares which can be stacked together to approximately recover the original image.
- A secret sharing scheme enables distribution of a secret amongst n parties, such that only predefined authorized sets will be able to reconstruct the secret.
- The secret, in terms of visual cryptography can be reconstructed visually by superimposing shares.

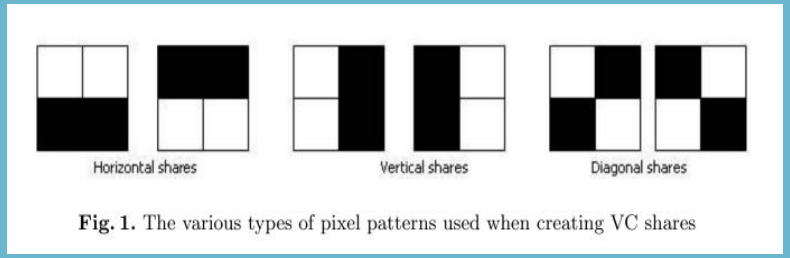


Fig. 1. The various types of pixel patterns used when creating VC shares

A Comprehensive Study of Visual Cryptography

Applications of Visual Cryptography

1. Watermarking
2. Anti - Phishing Systems
3. Human machine identification
4. Secure Banking Communication
5. Defense System
6. CAPTCHA
7. Offline QR Code Authorization

Visual Cryptography Schemes

1. 2 out of 2 scheme
2. K out of K scheme
3. General Access scheme
4. Halftone scheme
5. Color Images scheme
6. Extended scheme
7. Segment based scheme
8. Region incrementing scheme

Visual Cryptography Schemes

1. **2 out of 2 scheme:**
   - Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process.
   - This is equivalent to using the logical OR operation between the shares.

2. **K out of K scheme:**
- Similar to 2 out of 2, but for K share images.
- To reveal the encrypted image, we need to stack all K shares.

3. **Halftone Scheme:**
- When shares are created, the tone is continuously replicated, and these halftone cells are stored in each share.
- This helps in improving contrast and carrying more secret information.

Visual Cryptography Schemes

4. **Extended Scheme:**

-When there is more information in a particular share, it will have more noise and it will catch the attention of the hacker.

-This scheme will help in creating more uniform and meaningful shares.

5. **Segment based scheme:**

- Instead of creating shares based on pixels, this scheme works based on segments.
- It becomes very useful when dealing with symbols.

Role of Visual Cryptography in Information Security

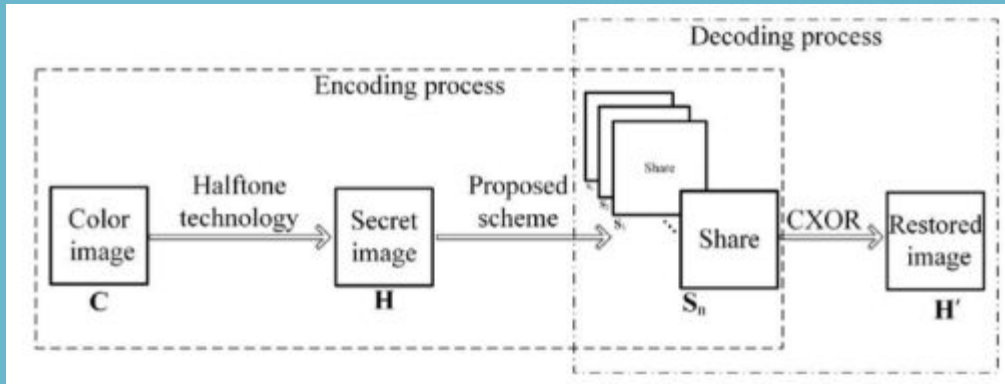
- Traditional cryptography relies on keys along with encryption and decryption algorithms, Thus, the security of the system mainly depends on the key.
- If the attacker obtains the key, our secret data is at risk.
- Visual cryptography does not require any complex encryption/decryption algorithms. It divides the key images into 2 or more noise-like images.
- And these shares are distributed in such a way that each participant gets only 1 share and to obtain the original message, all the shares must be stacked

Visual Cryptography for Color Images

- Until 1997, visual cryptography was done only on black and white images. Only in 1997, did they find techniques for dealing with color images.
- One technique that was proposed: each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identified from any one of these two shares alone.
- Another technique: The algorithm first creates a palette of a secret images and assigns a unique code to each color on the palette.

An examples of Visual Cryptography Algorithm

- The process of the proposed scheme is shown in the diagram The color image C is not encrypted by the proposed scheme directly. It needs to be converted to a halftone image H which is the secret image. H can be divided into n shares by the proposed scheme. All shares are performed XOR to restore the secret image. The restored image H' Is the same as H. The proposed scheme is the (n, n)-threshold scheme. The size of shares is the same as the secret image. The proposed scheme is pixel-non-expansible.



Research Papers Referred

1. A Comprehensive Study of Visual Cryptography
2. A REVIEW PAPER ON VARIOUS VISUAL CRYPTOGRAPHY SCHEMES
3. Schemes and Applications of Visual Cryptography
4. Role of Visual Cryptography Schemes in Information Security
5. Visual cryptography scheme for secret color images with color QR codes
6. Visual cryptography for color images

THANK YOU