Report

by Darshan Holla

Submission date: 06-Nov-2023 05:25PM (UTC+0800)

Submission ID: 2219191080

File name: 210953009_210953044_210953052_210953216.pdf (256.83K)

Word count: 1885

Character count: 10348

V Semester B.Tech. (CCE)

ICT 3172: INFORMATION SECURITY

IMPLEMENTATION REPORT

VISUAL CRYPTOGRAPHY

submitted by

Darshan Holla M	210953009
Manik Baboria	210953044
Harshith Nagaraj	210953052
Pranith Kanakagiri	210953216

Introduction:

These days, we often send multimedia files over the Internet. As online business becomes more important, keeping our data safe is a big concern. To protect our data, we use traditional encryption methods. These methods jumble up the data so that it's unreadable. But, we can unjumble it using the right key. Without that key, even if someone unauthorized gets the data, they can't make sense of it.

In 1994, Naor and Shamir introduced a new field called visual cryptography. It has a unique feature —it can reveal a hidden image without using any complex calculations. Instead, it relies on the human visual system to decipher the secret message from a set of overlapping shares. This approach eliminates the need for complicated computations often required in traditional cryptography. Visual cryptography becomes even more versatile with threshold schemes. For example, in a "*t out of n*" scheme (where *t* is less than or equal to *n*), a manager creates *n* transparent copies based on a secret image, one for each group member. If *t* or more of these transparent copies are stacked together, the secret image becomes visible. However, if there are fewer than *t* copies stacked, the secret content remains hidden.

Visual cryptography is a cryptographic technique that allows for the encryption of visual information (images or text) into shares, such that decryption can be performed by the human visual system without the need for complex cryptographic algorithms or computers. It's a method for distributing a secret image or message into multiple shares or transparencies, which individually reveal no information about the original message but collectively can be used to reconstruct the secret. Visual cryptography is often used for secure transmission of sensitive visual information or for secure multi-party computations. It's particularly useful in scenarios where security and privacy are essential, and it doesn't require computational complexity for encryption and decryption.

Methodology:

The basic idea of visual cryptography is as follows:

i. Secret Sharing: A secret image or message is divided into multiple shares or transparencies, each containing a seemingly random pattern of black and white pixels.

ii. Distribution: These shares are distributed to different parties or participants. In a 2-out-of-2 visual cryptography scheme, two shares are needed to reveal the secret, but neither alone can provide any information about the secret. A "2-out-of-2" scheme refers to a specific threshold scheme where the secret information is divided into two shares, and both shares are required to reveal the secret. In other words, for the secret to be reconstructed, both shares must be combined or overlaid.

iii. Reconstruction: To reveal the secret, the participants simply overlay the shares by stacking them on top of each other. When the shares are superimposed, the secret image becomes visible.

Project Overview:

The primary goal of this project is to implement a visual cryptography system that allows for secure image sharing and retrieval over the internet. The steps followed are as follows:

1. Image Processing techniques used:

   i. Image Upload: Users can upload an image of their choice using the File Upload widget.

   ii. Grayscale Conversion: The uploaded image is converted to grayscale using OpenCV (cv2) to simplify processing.

   iii. Binary Half-Tone Conversion: A binary half-tone image is created by thresholding the grayscale image, resulting in a black-and-white representation.

   iv. Master Grid Generation: A master grid is generated with 50% randomly distributed black (0) and white (255) pixels.

   v. Encoding Process: The encoding process involves comparing the binary half-tone image with the master grid. For each pixel in the binary image, if it's black (0), the corresponding pixel in the encoded grid takes the value from the master grid; if it's white (255), it takes the complementary value.

   vi. Reconstruction: The secret image is reconstructed by performing an XOR operation between the master grid and the encoded grid.

2. Components of the User Interface:

   i. File Upload: Users upload their image through the File Upload widget.

   ii. Output Display: The Output widget displays the processed and reconstructed images.

   iii. Buttons: Users interact with buttons to trigger specific actions:

      - "Show Half-Tone": Displays the binary half-tone image.
      - "Show Master Grid": Displays the master grid.
      - "Show Encoded Grid": Displays the encoded grid.
      - "Show Reconstructed Image": Displays the final reconstructed image.

3. Technical Details:

- **OpenCV (cv2):** The code utilizes the OpenCV library for image processing tasks.
- **Binary Data Storage:** Processed images are stored in a global dictionary (stored_images) for efficient display.
- **Thresholding:** Thresholding is used to create the binary half-tone image by distinguishing black and white pixels.

4. User Interaction with the system:

- Users upload an image via the File Upload widget.
- They trigger the display of specific images by clicking the corresponding buttons.

Implementation and Results:

1. Grayscale conversion is performed for the following reasons:

- Simplification of Data: Grayscale conversion reduces the image's color information to shades of gray, simplifying the data. This simplification is particularly useful when working with binary visual cryptography, where the information is encoded using only black and white (0 and 255) pixels. Grayscale images are essentially single-channel images, whereas color images have multiple channels (e.g., RGB or CMYK), which can complicate the encoding process.
- Uniform Data Representation: In visual cryptography, the source image is typically binary, with white and black pixels representing the two states (0 and 255). Grayscale conversion ensures that all the pixels in the source image are uniformly represented as gray levels, where 0 represents white and 255 represents black.
- Consistency with Encoded Information: When encoding the source image into shares, having a grayscale representation ensures that the encoded shares are also grayscale images. This consistency simplifies the encoding and decoding process, making it easier to implement the visual cryptography scheme.
- Improved Human Visual Interpretation: Grayscale images are easier for humans to interpret and visualize. In some applications of visual cryptography, such as watermarking and secure image sharing, it's beneficial to have a grayscale representation for better human visual perception. This can be important when combining shares to reveal the original image.
- Efficiency: Grayscale images have only one channel (intensity), which can make image processing more efficient in terms of memory and computation. In visual cryptography, this efficiency is

desirable, as it simplifies the manipulation of image data and can lead to faster encoding and decoding processes.

2. The Binary Half-Tone Conversion is performed for the following reasons:

- Simplification of Information: The binary half-tone conversion is performed to prepare the source image for encoding and sharing using visual cryptography. It simplifies the source image by reducing it to a binary representation, where each pixel is either fully black or fully white. This simplification is a fundamental step in visual cryptography, which works with binary data (0s and 1s) for efficient sharing.

- Enhancing Security: Binary half-toning transforms the source image into a form that is more resilient to unauthorized access. The binary representation ensures that the secret content of the image remains hidden until the shares are combined.

- Visual Clarity: Binary images have a strong visual contrast, making it easier for human observers to visualize the result. In some applications of visual cryptography, such as secure image sharing, visual clarity is essential.

- Efficiency: Binary images are computationally efficient, as they consist of only two pixel values (0 and 255). This efficiency is valuable in the context of visual cryptography, where the encoding and decoding processes involve simple mathematical operations on binary data.

- Thresholding: The conversion begins with a grayscale image where each pixel has a specific intensity value ranging from 0 (black) to 255 (white). Thresholding is applied to classify each pixel into one of two categories: black or white. This is done by selecting a threshold value, often set at 128, which divides the grayscale range into two halves. Pixels with intensity values below the threshold are assigned to the black category, while those above the threshold are assigned to the white category.

3. Master Grid Generation:

Visual cryptography is a cryptographic technique that allows for the secure sharing of a secret image among multiple participants. The goal is to distribute shares to these participants, and only when a sufficient number of shares are combined can the secret image be reconstructed. The master grid is a fundamental component of this process and is performed for the following reasons:

- Randomization: The master grid is a random pattern of black and white pixels. It introduces an element of randomness and complexity to the process. Without the master grid, the shares might not be secure because they could potentially be derived from a simple pattern or the original image itself. The master grid ensures that the shares are not individually revealing.

- Secrecy: The master grid is not shared with participants. Instead, it is used by the person generating the shares (often referred to as the "manager") to create the shares from the secret image. This ensures that the manager does not know the secret image but can create shares that, when combined, reveal it.

4. Encoding Process (Share Generation):

The encoding process involves pixel-wise comparison between the binary half-tone image and the master grid. For each pixel in the binary image:

If the pixel in the binary image is black (0), the corresponding pixel in the encoded share takes the value from the master grid at the same position. This is done through the XOR operation, which results in the same value (0 or 255) as the master grid for that pixel.

If the pixel in the binary image is white (255), the corresponding pixel in the encoded share takes the complementary value to the master grid. In other words, if the master grid has a white pixel (255), the encoded share will have a black pixel (0) at the same position, and vice versa.

5. Reconstruction:

The reconstruction process combines the information from the master grid and encoded grid to recover the original binary half-tone image. This is achieved by performing an XOR operation pixel by pixel.

Results:

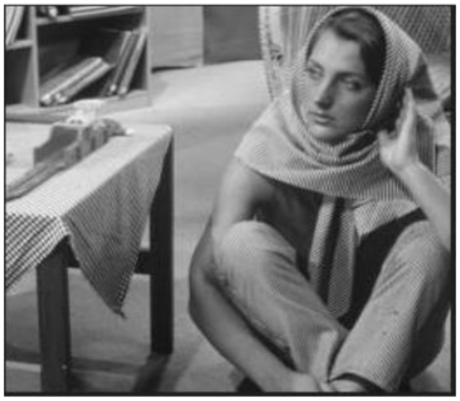

Fig 1: Secret Image

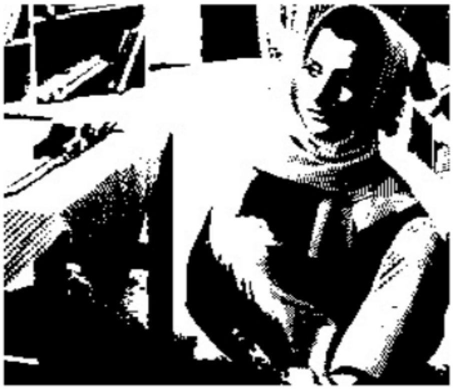

Fig 2: Halftone Image

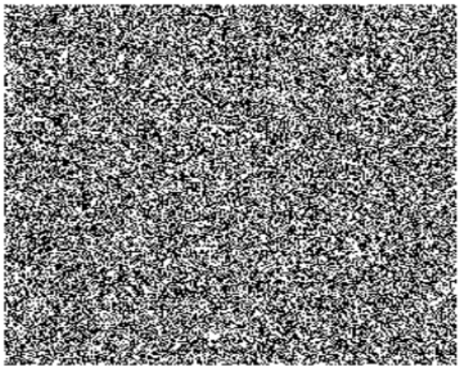

Fig 3: Master Grid

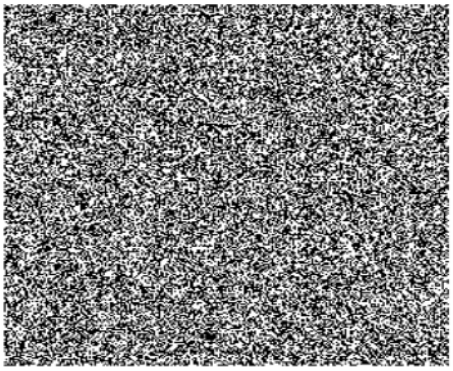

Fig 4: Encoded Grid

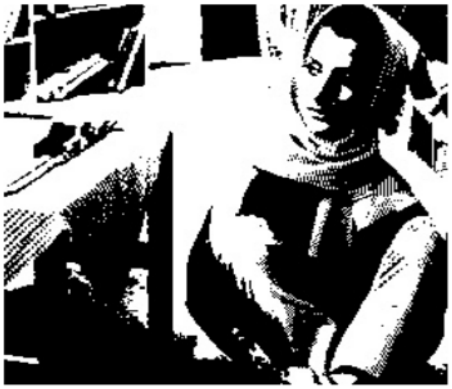

Fig 5: Reconstructed Image

Conclusion:

The project introduces a practical implementation of visual cryptography, offering a secure and user-friendly method for sharing and recovering images. The process involves converting an uploaded image into a binary half-tone format and generating a random master grid that serves as a key for encoding. Encoding relies on the binary image, where each pixel's value in the encoded grid is determined. The final image is reconstructed through XOR operations with the master grid.

The project provides a graphical user interface (GUI) for users to easily upload images and visualize each step of visual cryptography, including the binary half-tone image, master grid, encoded grid, and reconstructed image. This implementation has significant implications for data security and privacy, particularly in scenarios where sensitive images need to be securely shared and recovered without complex cryptographic computations, making it a valuable tool for various applications.

References:

[1] Hou, Young-Chang. "Visual cryptography for color images." *Pattern recognition* 36.7 (2003): 1619-1629.

Report

ORIGINALITY REPORT

7%	5%	4%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ijsrcseit.com Internet Source	2%
2	archive.org Internet Source	1%
3	www.bongos.net.au Internet Source	1%
4	Submitted to University of Anbar Student Paper	1%
5	Submitted to ABV-Indian Institute of Information Technology and Management Gwalior Student Paper	1%
6	Surya Sarathi Das, Kaushik Das Sharma, Jayanta K. Chandra, Jitendra Nath Bera. "Quantum signal processing-based visual cryptography with unexpanded shares", Journal of Electronic Imaging, 2015 Publication	1%
7	www.comm.utoronto.ca Internet Source	1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		