B.M.S College of Engineering

P.O. Box No.: 1908 Bull Temple Road,
Bangalore-560 019

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

Course – Cryptography and Network Security
Course Code – 20IS6PCCNS
AY 2021-2022

VISUAL CRYPTOGRAPHY

Submitted to – B S Mahalakshmi
(Assistant Professor)

Submitted by -
Niranjan Hegde 1BM19IS103
Prashanth Jaganathan 1BM19IS115
Samartha S 1BM19IS219

B.M.S College of Engineering
P.O. Box No.: 1908 Bull Temple Road,
Bangalore-560 019

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

BMS COLLEGE OF ENGINEERING

(Autonomous College under VTU)
Bull Temple Road, Basavanagudi, Bangalore – 560019

CERTIFICATE

This is to certify that the presentation entitled "**Visual Cryptography**" is a bona-fide work carried out by by **Niranjan Hegde**, **Prashanth Jaganathan and Samartha S** bearing USN: **1BM19IS103**, **1BM19IS115** and **1BM19IS219** respectively, in partial fulfillment of the requirements for the VI Semester degree in **Bachelor of Engineering in Information Science & Engineering** of **Visvesvaraya Technological University, Belgaum** as a part of for the **course Cryptography and Network Security, Course Code - 20IS6PCCNS** during academic year 2021-2022

Faculty Name: B S Mahalakshmi

Designation: Assistant Professor

Signature:

Table of Contents

Abstract

In today's world handling and security of information from attacks becomes a very important aspect for the individuals. Researchers are innovating new techniques to secure the information from unwanted intrusions. Various cryptography techniques are discovered and many are yet to be revealed. Here we are going to review an advanced method of information hiding i.e. Visual Cryptography. Visual Cryptography emerged as a special encryption technique for information hiding using images. In a way that encrypted image can be decrypted by the human vision if the correct image key is used. By this cryptographic technique we can encrypt visual information (pictures, text, etc.) in a way that a human visual system can perform decryption of encrypted information & no aid of computers needed. In visual cryptography a secret image is transformed into several shared images. These shared images are meaningful but noisy or distorted images. Combination of these shared images can reveal the original secret image. This report covers the progress of visual cryptography, along with the current trends and the various applications for visual cryptography.

INTRODUCTION

Visual cryptography is a powerful technique which combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. A binary image can be 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.

Visual cryptography allows the transmission of visual information and many aspects of this area are covered, including its inception to the current techniques being employed and actively researched today. This survey covers the progress of VC, along with the current trends and the various applications for VC.

Having the ability to hide information such as personal details is very desirable. When the data is hidden within separate images (known as shares), it is completely unrecognizable. While the shares are separate, the data is completely incoherent. Each image holds different pieces of the data and when they are brought together, the secret can be recovered easily. They each rely on one another in order to obtain the decrypted information. There should be no way that anyone could decipher the information contained within any of the shares.

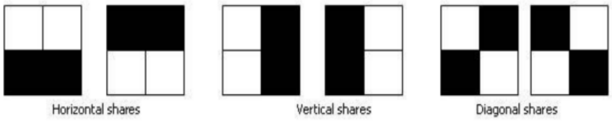


Fig. 1. The various types of pixel patterns used when creating VC shares

When the shares are brought together, deciphering is possible when the shares are placed over one another. At this point, the information becomes instantly available. No computational power is required at all in order to decrypt the information. All decryption is performed by the human visual system (HVS). This kind of problem is formally referred to as a secret sharing problem.

APPLICATIONS OF VISUAL CRYPTOGRAPHY

Visual cryptography method is proved to be a secure and reliable cryptographic method and hence application of this method has increased. Here we are discussing some of the applications.

- **Watermarking**

  Watermarking process includes the technique of visual cryptography. Process consists of two steps.

  - Watermark embedding:
  - Watermark retrieving.

  In the process of embedding splits the watermark into shares with the help of visual cryptography technique. After this the host image and one share is embedded together on the basis of the frequency domain of the host image, and another share is kept by the owner. To claim the original image, the owner has to extract another share from the image. The combination of extracted share and owner's share generates the original image.

- **Anti-Phishing System.**

  Credential information such as security pins, debit credit card numbers and passwords are crucial information and can be stolen by intruders. And phishing is used highly to steal secret credentials from their owners. To save from phishing attacks cryptography techniques can be applied. Use of visual cryptography provides the confidence of security to users while using any website. By imposing the two shares, one received from the server site and second his own share, the user can ensure a website without phishing.

- **Human Machine Identification**

  Kim et al. proposed human/terminal machine identification techniques. A more generalized form was extended by Kim after Katoh and Imai's scheme.

- **Secure Banking Communication**

  In a core banking industry, there's an opportunity of encountering forged signatures for transactions. And in the web banking system, the password of the client is also hacked and exploited. A scheme is proposed for securing the client information and to stop the doable forgery of password hacking. The idea of image processing in visual cryptography is employed.

- **Defense System**

  Visual Cryptography scheme is an encryption technique that uses combinatorial techniques to code secret written materials. This can be terribly helpful in a defense system to guard terribly sensitive data. Once information like secret code is to be transferred from one place to another so that secret data can be hidden in cover image, the share of the image is to be regenerated into shares. Those multiple shares are unbroken with multiple partners. any one partner cannot retrieve the secret code from the one share he has, all the shares from all the partners are needed to retrieve secret data hidden within the image. so information is safe in the hands of all the partners.

- **CAPTCHA**

CAPTCHA was proposed as a technique for authentication supported Visual Cryptography. It stands for completely automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

Their method consists of 3 processes:

1. Share Creation Process
2. Hash Code Generation
3. Authentication Process

- **Offline QR Code Authorization**

Fang proposed an algorithmic rule for the authentication of offline QR (Quick Response) code. He used the Visual Secret Sharing Scheme for the authentication. A QR code is a matrix barcode that is readable by specific readers dedicated to QR code. The code consists of a white background on which black modules are organized in an exceedingly square pattern. The information that's encoded in an exceedingly QR code will be any text or URL or the other information.

There are five vital options of a QR code:

1. High capability coding of data.
2. Tiny output signal size.
3. Dirt and harm resistance.
4. Readable from any direction in
5. A structure append feature.

VISUAL CRYPTOGRAPHY SCHEMES

Some of the most popular visual cryptography schemes are:

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

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.

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.

Halftone Scheme:

- In this process of share creation it replicates the tone continuously to image. They are called halftone cells and these cells are stored in each and every ‘n’ share. By the usage of halftone cells with a particular size, then the halftone shares will be obtained. And this technique increases the quality and makes a good contrast to the shares.

Extended Scheme:

- The share which has noise will get the attention of hackers and the hacker who identifies this noise in share may suspect that there is a content in the noise like image. This may lead to security issues. And maintaining the noise like images is also a risk.
- To overcome this risk Yamaguchi, Y. developed the extended Scheme. This scheme helps to create meaningful shares and it helps to ignore noise problems.

Segment based scheme:

- This is a new scheme in Visual Cryptography, and it was proposed by Bernd Borchert to overcome the limitation of pixel-based VCS loss its contrast while decrypted or restored image which is directly proportional to the expansion of pixel.
- This scheme does not use pixels, but it works based on segments. This scheme is very useful to encrypt a message which contains symbols with text that can be represented in segment display. The advantage of this scheme is that secret symbols and images are shown easily.

ROLE OF CRYPTOGRAPHY IN INFORMATION SECURITY

To secure important information, different techniques are used. Traditional cryptography is playing an important role to do this work. Security through a typical cryptographic system, relies on certain keys along with the complex encryption and decryption algorithm. Thus, the security of information mainly depends on the security of the key due to which, relying on the information kept on a single channel (person, physical entity etc.) is not secure. These problems are elegantly controlled by visual cryptography schemes.

Generally, encryption techniques such as DES, AES, and ECC are used for information security. In these cryptographic technologies, data becomes disordered after the encryption phase. To retrieve the data, we require large quantities of computation with the complex decryption algorithm and right keys. Also to retrieve original data from encrypted data without the correct key is very difficult. If adversaries get a secret key by any means they can retrieve the message without longing. Thus, the security of information mainly depends upon the security of the key.

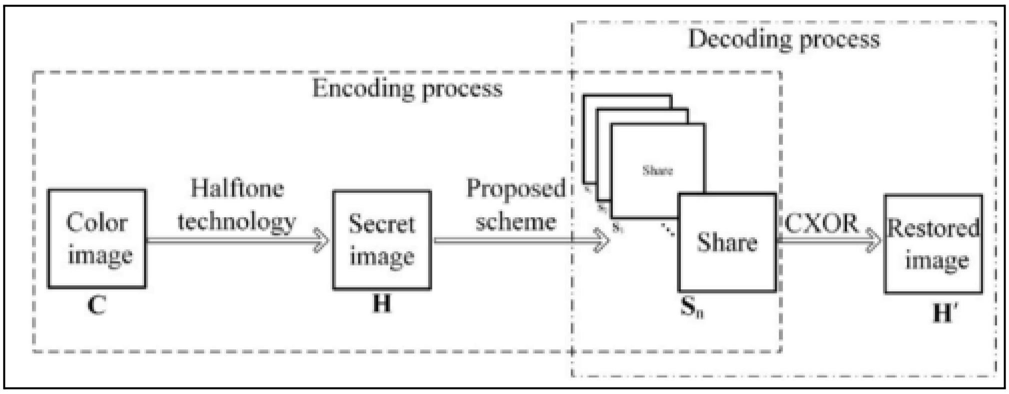
Visual cryptography is a secret sharing technique which facilitates the security of information. It neither requires complex encryption, decryption algorithms nor large amounts of computing power to retrieve the secret information. Visual cryptography basically divides key messages into two or more noise-like images. These noisy images are known as shares and distributed to the same number of participants in such a way that each participant receives only one share. Individual shares convey no clue about the original secret message. Secret messages can be retrieved by the human visual system by stacking shares printed on transparencies. This allows us to decode secrets without the knowledge of cryptography.

VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

Rijmen and Preneel have proposed a visual cryptography approach for color images. In their approach, 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, respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. Rijman and Preneel claimed that there would be 24 possible combinations according to the permutation of the four colors. Because human eyes cannot detect the color of a very tiny subpixel, the four-pixel colors will be treated as an average color. When stacking the corresponding blocks of the two shares, there would be 242 variations of the resultant color for forming a color image.

Another method uses a procedure to transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images is expanded into a 2×2 block to which a color is assigned. Every block of the sharing images therefore includes two transparent (white) pixels and two color pixels so that the entropy reaches its maximum to conceal the content of the secret image. Furthermore, they have design a half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

Another one of the proposed schemes 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 CXOR 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.



REFERENCES

1. A Comprehensive Study of Visual Cryptography
2. Visual Cryptography: A Review
3. A Review Paper On Various Visual Cryptography Schemes
4. Schemes and Applications of Visual Cryptography
5. Role of Visual Cryptography Schemes in Information Security: A Review
6. Visual cryptography for color images
7. Visual cryptography scheme for secret color images with color QR codes