HIDING AND EXTRACTION OF BINARY IMAGE USING ADVANCED VISUAL CRYPTOGRAPHY

Srishti Bhugra¹, Pardeep Tyagi², Abhinav Juneja³

¹M.tech Student, DCRUST University, B.M.I.T, Sonipat
²Assistant Professor, MDU, Rohtak, A.I.T.M, Palwal.
³Associate Professor, GGSIPU, Delhi

Abstract—It is now common to transfer multimedia data via the Internet. There is a need to solve the problem of ensuring information safety in today’s increasingly open network environment. Visual Cryptography (VC) is a special cryptographic technique where decryption is done by an authorized user by simply overlaying the shares. It uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot observe any clues about a secret image from individual cover images. So, there is a need to design a method by which a binary image could be encrypted and decrypted easily in a secure manner. Watermarking is a potential method for protection of ownership rights on digital audio, image, and video data. It helps to identify the true owner of the digital information. This technology is one of the possible methods to protect digital information. In the field of communication, security is an important issue nowadays. Digital communication has seen exponential growth in the past few decades. As a result, the security of digital data has become a field of extensive research since piracy and unauthorized use of such data is common because of the ease with which data can be replicated or tampered. This work will focus on designing for the efficient visual crypto system. The key concept of proposed system is based upon visual cryptography. Proposed cryptography method will encrypt secret information into two pieces (on the bases of white and black colour) called as shares. These two shares are operations together by logical operation to disclose the original secret. Proposed visual cryptography will encrypts the secret in various levels. The encryption will be expansion less. The original secret size will be retained in the shares at all levels.

Keywords: Visual Cryptography, Watermarking, Cryptography

1. INTRODUCTION

The basic principle of the Visual Cryptography Scheme (VCS) was first introduced by Naor and hamir [3] [2]. Visual cryptography (VC) is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Colour visual cryptography encrypts a colour secret message into a colour half-tone image shares [5]. The basic idea of the visual cryptography scheme is to split a secret image into number of random shares which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the shares [3].

It is now common to transfer multimedia data via the Internet. There is a need to solve the problem of ensuring information safety in today’s increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become chaotic after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

There is a general method for Visual Cryptography scheme based on general access structure [5]. The access structure is a specification of the qualified and forbidden subsets of shares. The participants in the qualified subsets can recover the secret image while the participants in forbidden subsets cannot. The VC scheme concept has been extended to gray scale share images rather than binary image shares. Although the secret image is gray scale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

The encrypting technologies of traditional cryptography are usually used to guard information security. With such technologies, the data become chaotic after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data [6]. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography [6].

Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography useful especially for the low computation load requirement [3].

1.2. BASIC THEOREM OF VISUAL CRYPTOGRAPHY

Because the output media of visual cryptography are transparencies, we treat the white pixels of black-and-white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into a 2x2 block in the two transparencies according to the rules in Fig. 1. When a pixel is white, the method chooses one of the two combinations for white pixels in Fig. 1 to form the content of the block in the two transparencies; when a pixel
is black, it chooses one of the other two combinations. Then, the characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white. Therefore, when stacking two transparencies, the blocks corresponding to black pixels in the secret image are full black, and those corresponding to white pixels are half-black-and-half-white, which can be seen as 50% gray pixels [6].

<table>
<thead>
<tr>
<th>Secret image</th>
<th>Share1</th>
<th>Share2</th>
<th>Stacked image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

Fig.1: Sharing and stacking scheme of black and white pixels [6]

### 1.3. VISUAL SECRET SHARING SCHEME

Visual Secret Sharing is based on the access structure schemes specified as follows:

- **k out of n Scheme:**
  - The 2-out-of-2 VSS scheme demonstrated above is a special case of the k-out-of-n VSS scheme. An access structure is a specification of all the qualified and forbidden subsets of shares. The participants in qualified subsets can recover the secret image while the participants in a forbidden subset cannot [4].

### 1.3.1. VISUAL CRYPTOGRAPHY BASED IMAGE WATERMARKING SCHEMES

Watermarking in images can be done both in spatial and transform domains. Spatial domain techniques though computationally less complex, are less resilient to attacks. Transform domain techniques, on the other hand, are more robust in comparison to spatial domain techniques since they modify the coefficients of the transform of the pixel values. Discrete wavelet transform (DWT), discrete cosine transform (DCT) and discrete Fourier transform (DFT) based transformed domain techniques have been found to be more robust than spatial domain techniques particularly in attacks like lossy compression, rescaling, rotation, noise addition etc [8].

### 1.3.2. VISUAL CRYPTOGRAPHY BASED VIDEO WATERMARKING SCHEMES

A video is nothing but a sequence of images yet image watermarking techniques cannot be directly applied to videos owing to their three dimensional characteristics. In addition to their special preprocessing techniques, the temporal nature of videos has to be taken into account [8]. Redundancy between frames and a large volume of data makes it all the more difficult to perform watermarking in videos. Some common forms of attack on videos are frame swapping, frame averaging, frame dropping, statistical analysis, interpolation etc. which are unknown to the domain of image watermarking. Inter-video collusion attacks and intra-video

Collusion attacks are also issues which need to be addressed. Real time implementations of video watermarking techniques are generally much more complex than that of image watermarking which becomes an important issue.

Video watermarking schemes are used for various video applications such as copyright protection, copy control, fingerprinting, broadcast monitoring, video authentication, enhanced video coding etc. Some traditional video watermarking schemes attempt to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer.

### 1.4. VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the secret image that appears on the stacked shares [1].

Fig 2 shows the working of visual cryptography. We can achieve this by using one of following access structure schemes [7].

1: (2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encodes it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2: (2, n) – Threshold VCS: This scheme encodes the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3: (n, n) – Threshold VCS: This scheme encodes the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants [7].

4: (k, n) – Threshold VCS: This scheme encodes the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

![Fig.2: Working of visual cryptography [7]](image-url)
other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. Decoding can be done by simply stacking subset $s$ of those $n$ shares. In their technique $n-1$ shares reveals no information about the original image.

An example of traditional $(2,2)$-VCS is shown in Fig. 3. In the scheme of Fig. 3, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after stacking shares (a) and (b), the secret image can be observed visually by the participants. VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field [3].

![Fig. 3: Example of traditional (2,2)-VCS with image size 128*128](image)

### 1.4.1. VCS ALGORITHMS

VCS Scheme involves two algorithms:
1. Algorithm for creating shares
2. Algorithm for combining shares

VCS algorithm’s efficiency is very important factor and the reliability and level of security are some more parameter which we need to consider while designing a VCS algorithm [1]. The VCS system should be reliable enough such a way that intruders are not able to read the original image. One important functional requirement of any VCS system is size of shares which should be same as that of original image to prevent doubt for unauthorized user.

#### 1.4.1.1. Algorithm for creating shares:
- It divides secret image into $n$ number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted separately through communication network, security is achieved [1].

#### 1.4.1.2. Algorithm for combining shares:
- This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input [1].

### 1.4.2. APPLICATION OF VISUAL CRYPTOGRAPHY-WATERMARKING

With data and multimedia taking on digital format, there is a need to protect digital property. There are two ways of accomplishing this: encryption and watermarking. Encryption protects information during transmission, but after its arrival at its destination, it is decrypted and is no longer protected. Watermarking is meant to compliment encryption in an effort to protect data after it has been decrypted.

Watermarking is the technique of embedding a secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are: hard to perceive, resists ordinary distortions, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Water marks.

---

### 2. PROPOSED METHODOLOGY

All the simulation work has been implemented in MATLAB environment 2013 using general MATLAB toolbox and Image processing toolbox. We have taken an input gray scale image “watermark128.bmp” as test image for cryptography and applied the following steps:

- Reading of noisy RGB image
- Conversion of colour RGB image into gray-scale image
- Calculation of threshold level from gray-scale image using otsu method
- Conversion of gray-scale image into binary image using threshold level
- Removal of noise from binary image
- Calculation of size of input Binary Secret image
  - Creation of share 1 according to the size of input Binary Secret image having all elements equal to zero
  - Creation of share 2 according to the size of input Binary Secret image having all elements equal to zero

#### 2.1 White Pixel share combinations

- Finding of white pixel indices in input Binary Secret image
- Calculation of number of rows of white pixel
- Random permutation the share generation
- Updating of share 1 and share 2 randomly for white pixel
2.2 Black Pixel share combinations

2.3 EXPERIMENTAL RESULTS

All simulation work has been implemented in the MATLAB environment 2013 using general MATLAB toolbox and Image processing toolbox. We have taken a noisy RGB input image “7.bmp” as test image for cryptography as shown in fig. 4. The size of input image is 768 KB and dimension of pixels is 512 X 512. This image is then converted into grayscale and then into binary image according Otsu threshold level, as shown in fig. 5. The noise has been removed from noisy binary image, as shown in fig. 6. This is the final representation of input image in binary form. According to the size of this image Share1 and share 2 images has been prepared just contacting zeros as all the elements. These zero elements will be updated or modified by random permutation according to white and black pixel positions of binary input image for both the shares. These updated shares i.e. share 1 and share 2 are shown in fig. 7 and fig. 8 respectively. Finally after over lapping of both the shares using logical OR operation we traced the secret binary input image as shown in fig. 9. Also, we have evaluated and analyzed the performance of a proposed methodology using PSNR as output parameter. PSNR of both shares has been calculated which is 51.1750 db (for both). The PSNR of our method is compared by that of [3]. The size of test image used by [3] is 2.95KB and dimension is 512 X 512. The PSNR of its share is 9.93db and 5.53db. Bar chart of their comparison has been shown in fig. 10.
4. CONCLUSION & FUTURE SCOPE

Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. It provides one of the secure ways to transfer images on the Internet. The main advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. A new advanced visual cryptographic technique has been introduced in this present research work. This proposed work contains some details about Visual Cryptographic Scheme. This work rectifies the problem of security of encoded images i.e. share 1 and share 2 as impositor can access all communication channels but can't reconstruct the secret image random permutation is used for creation of shares. Proposed method also overcomes pixel expansion problem. In this proposed work the concept of random permutation along with traditional VCS is combined to give a secured image sharing system. As we have compared the performance of proposed method with that of existing method in terms of PSNR. It can be concluded that proposed method is performing much better than the existing one, by comparing the PSNR of both shares. The proposed method not only improves the PSNR but also increases the visual quality as compared to other methods. The performance analysis of the proposed method reveals that the proposed encryption method is ideal. The proposed system can be extended such that it can be applied to all types of image formats.

REFERENCES