AN INTRODUCTION TO DIFFERENT TYPES OF
VISUAL CRYPTOGRAPHY SCHEMES

Néelima. Guntupalli
Assistant Professor
CSE Department
Acharya Nagarjuna University
Email: neelima_raju2003@yahoo.co.in

Mr. P.D. Ratna Raju
Associate Professor
CSE Department
Priyadarshini Instt Of Tech&Science
Email: ratnaraju.daniel@gmail.com

Mr. Suresh Cheekaty
Assistant Professor
CSE Department
Priyadarshini Instt Of Tech&Science
Email: cheekaty.cse@gmail.com

Abstract:
Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by the human visual system. Security has become an inseparable issue as Information Technology is ruling the world now. Cryptography in the study of mathematical techniques related aspects of information security such as confidentiality, data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. Visual cryptography can be applied for copy right for images, access control to user images, visual authentication and identification any kind images of images like (normal or digital). Visual cryptography is a new technique which provides information security which user simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows visual information (pictures, text, etc.) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This technique encrypts a secret image into shares such that stacking sufficient number of shares reveals the secret image. Shares are visually presented in transparencies.

In this paper we provide an analysis of the emerging visual cryptography (VC) and related security research work done in this area.

Keywords: Pixels, Contrast, Secret sharing, Shares, Stacking, Analysis.

Introduction:
The basic model of visual cryptography proposed by Naor and Shamir [1] accepts binary image ‘I’ as secret image, which is divided into ‘n’ number of shares. Each pixel of image ‘I’ is represented by ‘m’ sub pixels in each of the ‘n’ shared images. The resulting structure of each shared image is described by Boolean matrix ‘S’. Where S=[Sij] an [n x m] matrix Sij=1 if the jth sub pixel in the ith share is black Sij=0 if the jth sub pixel in the ith share is
white. When the shares are stacked together, a secret image can be seen but the size is increased by ‘m’ times. The grey level of each pixel in the reconstructed image is proportional to the Hamming weight $H(V)$ of the OR-ed Vector ‘V’, where vector ‘V’ is the stacked sub-pixels for each original pixel. A solution of the ‘n’ out of ‘n’ visual secret sharing consists of two collections of n x m Boolean Matrices $C_0$ and $C_1$. To share a white pixel, randomly choose one of the matrices from $C_0$, and to share a black pixel, randomly choose one of the matrices from $C_1$. The following conditions are considered for the construction of the matrices:

1. For any ‘S’ in $C_0$, the OR-ed ‘V’ of ‘n’ rows satisfies $H(V) \leq m$.
2. For any ‘S’ in $C_1$, the OR-ed ‘V’ of any ‘n’ rows satisfies $H(V) = n$.

By stacking fewer than ‘n’ shares, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black. Let us describe the construction of matrix for (n, n) visual cryptography for n=3. $C_0 = \{\text{all the matrices obtained by permuting the columns complement of } [B1]\}$ $C_1 = \{\text{all the matrices obtained by permuting the columns of } [B1]\}$ Where, $B$ is the matrix of order n x (n-2) which contains only ones $I$ is the identity matrix of order n x n. The basic model was then extended to (k, n) threshold cryptography where any ‘k’ or more shares will reveal the secret image. The construction of ‘k’ out of ‘n’ visual secret sharing is similar to the basic model with one difference. That is in basic model the threshold value is n where as here it is k which is the subset of n.

2. Visual Cryptography schemes
2.1. Visual cryptography for gray level images

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang-ChouLin, Wen-Hsiang Tsai [3] proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub-pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

2.2. Visual cryptography for general access structures

In (k,n) Basic model any ‘k’ shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [2], where an access structure is a specification of all qualified and forbidden subsets of ‘n’ shares. Any subset of ‘k’ or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

2.3. Halftone Visual Cryptography

The meaningful shares generated in Extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI [5] was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel ‘P’ is encoded into an array of Q1 x Q2 (‘m’ in basic model) sub
pixels, referred to as halftone cell, in each of the ‘n’ shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

2. 4. Recursive Threshold visual cryptography
The (k,n) visual cryptography explained in section I needs ‘k’ shares to reconstruct the secret image. Each share consists at most \( \lceil 1/k \rceil \) bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and SubhasKak [4] eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

2.5. Visual cryptography for color images
The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of color image .F.Liu,C.K. Wu X.J. Lin proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows:
1. The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded color image.
2. The second approach converts a color image into black and white images on the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.
3. The third approach utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level. This results in better quality but requires devices for decryption.

2.6. Regional incrementing Visual Cryptography
VC schemes mentioned above usually process the content of an image as a single secret i.e all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang [7] proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The ‘n’ level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features:
(a) Each share cannot obtain any of the secrets in S,
(b) Any \( t(2 < t < n + 1) \) shares can be used to reveal \( (t-1) \) levels of secrets,
(c) the number and locations of not-yet-revealed secrets are unknown to users,
(d) all secrets in S can be disclosed when all of the \( (n+1) \) shares are available, 2.9.

Segment based visual cryptography
The VC Methods mentioned above is based on pixels in the input image. The disadvantage of pixel based visual cryptography is loss in contrast of the reconstructed image which is directly proportional to pixel expansion ‘m’. A New approach proposed by Bernd Borchert [8] was based on segments which takes pixels as the smallest unit to be encrypted. The advantage of segment based over pixel is that it may be easier for the human eye to recognize the symbols, The messages consists of numbers can be encoded by segment based visual cryptography using seven segment display.
2.7. Extended visual cryptography for natural images

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI [5] proposed Extended visual cryptography for natural images constructs meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, [5] establishes the extended visual cryptography scheme suitable for natural images.

2.8. Progressive visual cryptography

In traditional Color Visual Cryptography, loss of contrast makes VCS practical only when An overview of visual cryptography International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–0474 Volume 1, Issue 1, 2010 35 quality is not an issue, which is quite rare. The application of digital halftoning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. Duo Jin Wei-Qi Ya n, Mohan S, Kankanhalli[6] proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image.

3. Related Work

Naor et al proposed method in which pixel is divided into sub pixel. Sub-pixel contains one half white and remaining half black [1]. There is four possible way, they are white, black, white-black, black-white, here author assign the values for black and white is ‘0’ and ‘1’. This calculation is based on permutation and combination of black-white images or grayscale images [2]. In this method, encryption of image takes more complexity in its computation time. It is based on the principle of blue noise dithering and void cluster algorithm[3]. Figure 1 explains the actual image and output image, which uses above two principles. The output image looks like double the width of image because it uses sub pixel principle using grayscale image. With these colors, combination and permutation method is applied in the Figure 2. Then it uses the concept of probability for each pixel.
Fig. 1 Visual cryptography representation

Fig. 2 shows the basic working principle of visual cryptography. Here each pixel is divided into two sub pixels and uses 50% probability.

Zhou et al proposed the following mathematical method. They are considering a group set is $\rho$, having the number of participants is $\eta$, one share is called $\tau$ as qualified set and other share is called $\tau$ forb as Forbidden set. Here it should satisfy the condition that $\tau$ qual $\Pi \tau$ forb $= \emptyset$. The maximum chances for retrieving secret share of image should be less than one participates, the combination of $\tau$ qual and $\tau$ forb is called access structure [2][3][6].

They also proposed the method called Halftone visual cryptography. In this method, secret pixels are hidden using the matrices. Here, they are considering $Q_1$ is the original secret information pixels of the image, $Q_2$ is the reverse of secret information pixels both shares are equal. If the number of black pixel is less than the original image, some of the pixels are added to that black pixel. Same condition have been applied for white pixel using the concept of matrices [3].

4. Analysis of different types of visual cryptography

1. Blue noise dithering: This method used to improve the quality of image during reconstruction of the image [5].

Void cluster algorithm: This method is used to find the secret pixel in the halftone cell [6].

Halftone: It is a production of graphic through mechanical or electrical such as photography or xerography techniques that simulates images where each color can be reproduced as single tone in monochromatic print. In proposed method, the secret image can be decoded without showing any interaction with share image [3].

Z. Zhou and et al explained Visual cryptography secret schemes. In these images shares can be done on the basis of mathematical calculation $\tau$ qual have information of share of image, while $\tau$ forb
have no information of Image. Here author says about number of participates and dividing shares. [1][2][3][11].

Z. Zhou and et al explained Halftone visual cryptography and says that some of disadvantage in basic visual cryptography. The some important things are:

- The position of secret information pixel.
- The secret information pixels depend upon on black and white distribution to halftone images.
- The changing of pixels position during the operation, chances of loss maximum shape of the image.[9][10]

Z. Zhou and et al explained direct binary search for visual cryptography and explain about pixels distribution, The selection of secret pixel should be randomly or homogeneously distributed [2][3][4].

**Advantage:** If one of share of image is losses during the operation, the maximum possibility of retrieving the image is 30-40% only.

**Disadvantage:** The decoded image only gain or getting ≈ 09.877% only.

**Error diffusion:** This method is used to improve the quality of image. It is two types of error diffusion are

- **One dimensional error diffusion:** In this method, any pixel (black pixel) can be considered, while doing error diffusion method the some of the properties of a black pixel will be assigned or distribution to neighbour pixel.

- **Two dimensional error diffusion:** The pixel have to donate the half property to neighbour pixel and one quarter of diffusion is added to below the next line, another quarter of diffusion is added to pixel on next line below and one pixel forward.

2.M. Naor et al. explain the method of basic Visual cryptography scheme reconstructs image in which losses its contrasts and the width of image will be double after the operation completed. It happens because pixel is divided into sub-pixel and based on the following two principles [1][3].

3. **Disadvantage:** Selecting the random pixel as secret information and secret information can be obtained by the intruder.

Z. Zhou and et al explained Complementary halftone image pair and distributed secret information pixels. Primary shares contain secret information and complementary share contains reverse of non secret Information pixel. The reconstructed of image will be performed on bases of OR- XOR operation. The quality of image based on the condition of δ ≥20 [11].

After that deliberately introduce homogeneously and distributed black pixel into each share. Z. Zhou and et al explained that no need uses complementary image share, instead of that using auxiliary black pixel. Here no need of complementary function and easy to reliable the image without any calculation of black pixels in shares [11].

4.**The quality of halftone share represented as**

\[
S = \begin{cases} 
\text{Complementary halftone image pair} \\
\text{Auxiliary black pair}
\end{cases}
\]

In equation (1) the upper equation represents complementary halftone image pair. Where,

- δ = secret information pixel
- θ = halftone cell size

Lower equation represents auxiliary black pair. Where,

- δ = secret information pixel
- \(μ = \text{number of auxiliary black pixels}\)
5. Disadvantage of Basic Watermarking

- Selection of pixels is random, when restored watermark pattern from image.
- An image with some similarities with the original image M, watermark pattern p should be restored the image.

Hwang proposed method to overcome basic technique for selecting specific pixels from the original image instead of random selection of pixels. The user will select watermark pattern p which specify image, user can characterize an image M using the watermark pattern and the expanded key S. pk represents the length of the watermark pattern P, Mk represents the length of the image M and M'k represents the length of the image M'.

The method uses different steps to assign the length key and verification of ownership of image.

\[ S[i] = (S[i-8] \oplus S[i-4] \oplus S[i-3] \oplus S[i-1]) \] (2)

Where \( \oplus \) represents exclusive-or.

Fig. 3 Original Image

Fig. 4 Disturbed Images

Fig. 5 Unidentified Images

Fig. 3 represents the original image send by the sender to receiver using the technique of watermarking. Fig. 4 shows the disturbed image which is identified by the receiver by using the key length. Fig. 5 shows unknown image can be claim by using length key and verification code generated by the owner.

The watermark pattern is restored successfully if there is no change on the image, because this is embed and verification process will be followed as same, the only difference is the final step in which author or user using the XOR operation.

\[ X \oplus Y \oplus Y = X \] (3)

The change in image which represents a changes occur in it, then this change will be reflected on the regain watermark pattern p', image M having some minor
changes to become image, the watermark pattern can be recognized but it having some noise or distribution of image.[9]

6. Conclusion:

This paper discusses the introduction of different types of Visual Cryptography schemes. It compares the image quality and security using various visual cryptography schemes. In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore, an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography (VC) is towards maintaining the contrast at the same time maintaining the security.

References


