

An overview of visual cryptography

Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S.

Abstract- Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin authentication, but it is not the only means of providing information security, rather one of the techniques. Visual cryptography is a new technique which provides information security which uses 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 a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. In this paper we provide an overview of the emerging Visual Cryptography (VC) and related security research work done in this area.

Keywords: Contrast, Shares, Pixels, Secret sharing, stacking

Introduction

Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Visual cryptography (VC), proposed by Naor and Shamir [1], is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption process is performed by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations. In the above basic VC scheme each pixel 'p' of the secret image is encrypted into a pair of sub pixels in each of the two shares. If 'p' is white, one of the two columns under the white pixel in Fig. 1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black-white or white-black

pair of sub pixels, an individual share gives no clue about the secret image. By stacking the two shares as shown in the last row of Fig. 1, if 'p' is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If 'p' is black, it outputs two black sub pixels.

















Pixel	White		Black	
				
Prob.	50%	50%	50%	50%
Share 1				
Share 2				
Stack share 1 & 2				

Fig. 1- Construction of (2, 2) VC Scheme

Hence there is a contrast loss in the reconstructed image. However the decrypted image is visible to naked eye since human visual system averages their individual black-white combinations.

The important parameters of this scheme are

a) Pixel expansion 'm', which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.

b) Contrast ' α ', which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image.

Generally, smaller the value of m will reduce the loss in resolution and greater the

value of 'a' will increase the quality of the reconstructed image.

As mentioned above if 'm' is decreased, the quality of the reconstructed image will be increased but security will be a problem. So research is focused on two paths

1. To have good quality reconstructed image
2. To increase security with minimum pixel expansion.

This paper provides an overview of this emerging technique in three sections. Section I gives details about the Basic model of visual cryptography. Section II summarizes the following research works in visual cryptography and its extensions.

1. Visual cryptography for general access structures..
2. Visual cryptography for gray level images.
3. Recursive Threshold visual cryptography.
4. Extended visual cryptography for natural images.
5. Halftone visual cryptography.
6. Visual cryptography for color images. .
7. Progressive color visual cryptography.
8. Regional incrementing visual cryptography (RIVC).
9. Segment based visual cryptography.

Section III provides details about research works regarding security issues in visual Cryptography.

1. Basic Model

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 $S=[S_{ij}]$ an $[n \times m]$ matrix

$S_{ij}=1$ if the jth sub pixel in the ith share is black

$S_{ij}=0$ if the jth sub pixel in the ith share is white

When the shares are stacked together 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 $n \times m$

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 $H(V) \leq n - \alpha m$.
2. For any 'S' in C_1 , the OR-ed 'V' of any 'n' rows satisfies $H(V) \geq n$.

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 $n=3$.

$C_0 = \{ \text{all the matrices obtained by permuting the columns complement of } [BI] \}$

$C_1 = \{ \text{all the matrices obtained by permuting the columns of } [BI] \}$

Where,

B is the matrix of order $n \times (n-2)$ which contains only ones

I is the identity matrix of order $n \times n$

$$\text{For } n=3 \text{ } B = \begin{bmatrix} 1 & & \\ 1 & & \\ 1 & & \end{bmatrix} \text{ and } I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{Hence } C_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \text{ and } C_0 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

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 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

k out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion than [1].

2.2 .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-HsiangTsai [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. 3. 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 Subhash Kak [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.

2.4. 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.

2.5. 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 $Q_1 \times Q_2$ ('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.

2.6. 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.

2.7. Progressive visual cryptography

In traditional Color Visual Cryptography, loss of contrast makes VCS practical only when

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 Yan, 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 gray-scale or color image.

2.8. 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.

3. Security issues

Hornig et al. proposed that cheating is possible in (k, n) VC when k is smaller than n. There are two types of cheaters in VC. One is a malicious participant (MP) who is also a legitimate participant, namely $MP \in P$ (Qualified participant) and the other is a malicious outsider(MO), where $MP \notin P$.

A cheating process against a VCS consists of the following two phases:

1. Fake share construction phase: the cheater generates the fake shares;
2. Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake shares.

In order to cheat successfully, honest participants who present their shares for recovering the secret image should not be able to distinguish fake shares from genuine shares. A reconstructed image is perfect black if the sub pixels associated to a black pixel of the secret image are all black. Most proposed VC schemes have the property of perfect blackness. An example of the cheating process is shown in fig.2

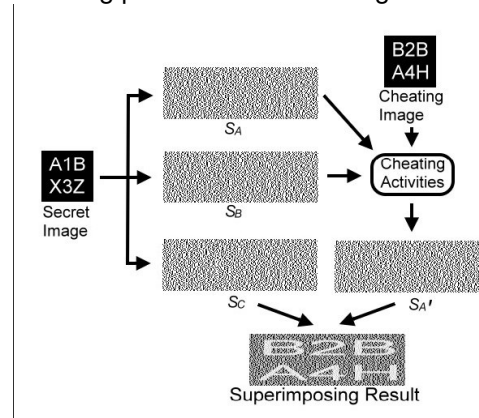


Fig. 2- The Cheating Process

Some of common ways how MO and MP cheats visual cryptography are

1. Cheating a VC by an MP
2. Cheating a VC by an MO
3. Cheating an EVCS by an MP.
4. Cheating Prevention Algorithm

3.1 Cheating a VC by an MP

A qualified participant can also be a cheater, where the participant uses his original share to create a fake share. By doing so, he will try to cheat the other

genuine participants because the fake share generated will be indistinguishable from the original shares and also the decoded output image will be different from the original secret image. The process of cheating is shown in the fig.3

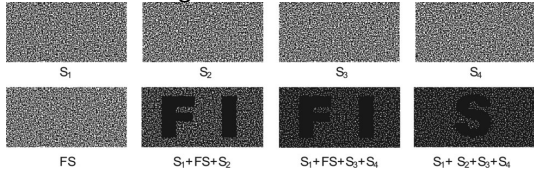


Fig. 3- Cheating a VC by an MP

3.2 Cheating a VC by an MO

A disqualified participant called as MO will create fake shares by using some random images as input and will try to decode the original image. The MO will try to create fake shares of different sizes because the size of the original share may vary. The process is shown below in fig 3.4

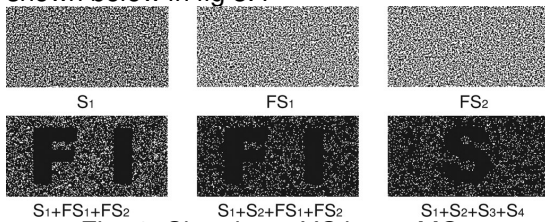


Fig. 4- Cheating a VC by an MO

3.3 Cheating an EVCS by an MP

The Qualified participant creates the fake share from the genuine share by interchanging the black pixels by the white pixels which leads to less contrast of the reconstructed image. The less contrast in reconstructed image will be hard to see the image. The fake image in the stacking of the fake shares has enough contrast against the background since the fake image is recovered in perfect blackness. The process is shown below in fig 3.5

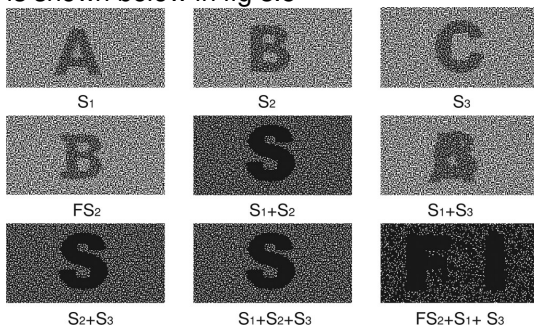


Fig. 5- Cheating an EVCS by an MP

3.4 Cheating Prevention Algorithm

The Cheating method explained in section 3.1 is prevented by Robust cheating prevention algorithm proposed by chih ming hu and wen guey tzeng [9].The cheating prevention method has following features

- 1) It does not rely on the help of an on-line TA. Since VC emphasizes on easy decryption with human eyes only, we should not have a TA to verify validity of shares.
- 2) The increase to pixel expansion should be as small as possible.
- 3) Each participant verifies the shares of other participants. This is somewhat necessary because each participant is a potential cheater.
- 4) The verification image of each participant is different and confidential. It spreads over the whole region of the share. We have shown that this is necessary for avoiding the described attacks.
- 5) The contrast of the secret image in the stacking of shares is not reduced significantly in order to keep the quality of VC.
- 6) A cheat-preventing method should be applicable to any VCS.

Conclusion

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 VC is towards maintaining the contrast at the same time maintaining the security.

References

- [1] Naor, M., and Shamir, A. (1995), Visual cryptography, in "Advances in Cryptology Eurocrypt '94" (A. De Santis, Ed.), Lecture Notes in Computer Science, Vol. 950, pp. 1-12, Springer-Verlag, Berlin.
- [2] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, Visual cryptography for general access structures, Proc. ICALP96, Springer, Berlin, 1996, pp. 416-428.
- [3] Chang-Chou Lin, Wen-Hsiang Tsai, Visual cryptography for gray-level images by dithering techniques,

- Pattern Recognition Letters, v.24
n.1-3.
- [4] Abhishek Parakh, Subhash Kak: A Recursive Threshold Visual Cryptography Scheme CoRR abs/0902.2487: (2009).
 - [5] Nakajima, M. and Yamaguchi, Y., Extended visual cryptography for natural images. Journal of WSCG. v10 i2. 303-310.
 - [6] Jin, D., Yan, W. and Kankanhalli, M.S., Progressive color visual cryptography. J. Electron. Imaging. v14 i3.
 - [7] Wang, R.Z.[Ran-Zan], Region Incrementing Visual Cryptography, SPLetters(16), No. 8, August 2009, pp. 659-662.
 - [8] Bernd Borchert, Klaus Reinhardt: Abh or- und manipulation ssichere Verschl usselung f ur Online Accounts. Patent application DE-10-2007-018802.3, 2007.
 - [9] HU Chih-Ming, TZENG Wen-Guey, "Cheating prevention in visual cryptography", IEEE transactions on image processing ISSN 1057-7149 ,2007, vol. 16, no1, pp. 36-45.