



Image Security Using Visual Cryptography

H C Suchethana

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

January 5, 2022

Image security using visual cryptography

Suchethana H C

Assistant Professor, Dept of ISE JNNCE, Shimoga

Suchethanahc@jnnce.ac.in

Abstract

Visual cryptography is a secret sharing scheme as it breaks an original image into image shares such that, when the shares are stacked on one another, a hidden secret image is revealed. The Visual Cryptography Scheme is a secure method that encrypts a secret document or image by breaking it into image shares. A unique property of Visual Cryptography Scheme is that one can visually decode the secret image by superimposing shares without computation. Even to make the visual cryptography image shares more secure, public key encryption scheme is applied. Public key encryption technique makes image shares so secure that it becomes very hard for a third party to decode the secret image information without having required data that is a private key.

Keywords-Halftone visual cryptography, Encryption, Decrypted image.

I. Introduction

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in specific a way that decryption becomes a mechanical operation that does not require a computer. The idea was about producing image shares of a given secret image in a way that the image shares appear meaningless. Recovery of the image can be done by superimposing specified number of share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is a little more advantageous for implementation, while compared to conventional cryptography schemes, since the decryption process does not need any computation. Further, the image based information becomes more secure, since only the intended recipient can reveal the true meaning of the decrypted image. Suppose the data (image) D is divided into n shares. D can be constructed from any k shares out of n shares. Complete knowledge of $(k-1)$ shares reveals no information about D . So, k out of n shares is necessary to reveal secret data. For example: let 6 thieves share a bank account but they do not trust each other. The thieves split up the password for the account in such a way that any 3 or more thieves working together can have access to account, but not less than 3.

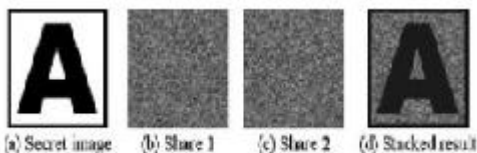


Fig. 1: illustration of visual cryptography

II. Visual Cryptographic Schemes

A. k out of k visual cryptography scheme

A common example of k out of k visual cryptography scheme is 2 out of 2 visual cryptography schemes. In (2, 2) Visual Cryptography Scheme, the original image is broken into 2 image shares. In original image, every pixel is represented by non-overlapping block of 2 or 4 sub-pixels in each share. If anyone is having only one share, will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image. There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the first two rows in Figure given below is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in figure given below. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the result will be white pixel and if a black pixel in one share overlaps with either a white or black pixel in another share, the result will be black pixel. This implies that the superimposition of the shares represents the Boolean OR function.

B. k out of n visual cryptography scheme

In $(2, 2)$ visual cryptography, both the shares are required to reveal secret information. Due to some problem if one share gets lost then the secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal the secret information and user can not afford to lose a single share. Naor and Shamir generalized basic model of visual cryptography into a visual variant of k out of n visual cryptography scheme to give some flexibility to user. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares superimposed, where value of k is between 2 to n . If less than k shares stacked together, secret original image cannot be revealed. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained. It also ensures the security as to know the secret information you have to have more than k shares out of n secret shares.











pixel		share #1	share #2	superposition of the two shares
□	$p = .5$			
	$p = .5$			
■	$p = .5$			
	$p = .5$			

Fig 2: Illustration of a $(2, 2)$ VC Scheme with 2 Subpixels

C. Visual Cryptography Scheme for General Access Structure

In (k, n) visual cryptography scheme, all n shares have equal importance. The secret information can be revealed if any k out of n shares are available. The security of system might get compromised due to this. To beat this issue, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure. In general access structure scheme, given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but fewer than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can not reveal secret information. So, Visual cryptography for general access structure improves the security of system.

D. Recursive Threshold Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, a secret of b bits is distributed among n shares of size at least b bits each. Since only k out of n shares is needed to reveal secret, every bit of any share conveys at most $1/k$ bits of secret. It results in inefficiency in terms of number of bits of secret conveyed per bit of shares. To overcome this limitation Abhishek Parakh and Subhash Kak proposed Recursive threshold visual cryptography [1]. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to $(n-1)/n$ bit of secret which is nearly 100

E. Halftone Visual Cryptography Scheme

Halftone visual cryptography uses half toning technique to create shares. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. Zhi Zhou et al. proposed halftone visual cryptography. In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the n shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It maintains good contrast and security and increases quality of the shares [2].

F. Visual Cryptography Scheme for Grey images

All previous visual cryptography schemes were only limited to binary images. These procedures were fit for doing operations on just highly contrasting black and white pixels. It is not sufficient for real life applications. Chang-Chou Lin, Wen Hsiang Tsai proposed visual cryptography for gray level images. In this scheme a dithering technique is used

to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares.

III. Proposed method

A. Basis matrices

Any black-and-white visual cryptography scheme can be described using two n Boolean matrices S_0 and S_1 , called basis matrices, to describe the sub pixels in the shares. The basis matrix S_0 is used if the pixel in the original image is white, and the basis matrix S_1 is used if the pixel in the original image is black. The use of the basis matrices S_0 and S_1 can have small memory requirements (it keeps only the basis matrices S_0 and S_1), and it is efficient (to choose a matrix in C_0 or C_1) because it only generates a permutation of the columns of S_0 or S_1 .

Basically, the two basis matrices S_0 and S_1 should satisfy the following.

Definition: 1. A k -out-of- n visual cryptography scheme with parameters $1 \leq d \leq m$ and $t \geq 0$ can be constructed from two $n \times m$ Boolean matrices S_0 and S_1 if the following three conditions are met:

1. The OR m -vector V of any k of the n rows in S_0 satisfies $H(V) \geq d$.
2. The OR m -vector V of any k of the n rows in S_1 satisfies $H(V) \leq d - t$.
3. For any set r_1, r_2, \dots, r_t , $1 \leq r_i \leq n$ with $t \leq k$, the $t \times m$ matrices obtained by restricting S_0 and S_1 to rows r_1, r_2, \dots, r_t , are equal up to a column permutation. where $H(V)$ is the hamming weight (the number of ones) of the m -vector V of any k of the n rows, m is the pixel expansion and t is the relative difference. The conditions (1) and (2) related to contrast in a reconstructed image and condition (3) related to security.

Relative-Difference: Let $H(S_0)$ and $H(S_1)$ be the hamming weight corresponding to the basis matrices S_0 and S_1 .

Then relative difference (α) is defined as:

$$\alpha = (H(S_1)H(S_0))/m$$

Contrast:

Let β be the relative difference and m be the pixel expansion. The formula to compute contrast in different VCS

is:

$$\beta = \alpha \cdot m, \beta \geq 1$$

The basic idea of visual cryptography can be best described by considering a 2-out-of-2 VCS.

B. Construction of 2 out of 2 VCS

Let us consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S_1 and S_2 , consisting of exactly two pixels for each pixel in the secret image. If the pixel in S is white, the dealer randomly chooses one row from the first two rows of the figure 3 given below. Similarly, if the pixel in S is black, the dealer randomly chooses one row from the last two rows of figure 3.

Original Pixel	Pixel Value	Share1	Share2	Share1 + Share2
	0			
	0			
	1			
	1			

Fig 3: Illustration of a (2, 2) VC Scheme with 2 Subpixels

To analyse the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table for the shares S_1 and S_2 . Randomly the pixels are selected so that the shares S_1 and S_2 consist of equal number of black and white pixels. Therefore, by reviewing a single share, one cannot distinguish the secret pixel as black or white. This technique gives flawless security. By superimposing the two shared sub pixels, the two participants can recover the secret pixel. The original pixel was black, If the superimposition results in two black sub pixels and if the superimposition creates one black and one white sub pixel, it indicates that the original pixel was white[1]. In visual cryptography, the white pixel is represented by 0 and the black pixel by 1. For the 2-out-of-2 VCS, the basis matrices, S_0 and S_1 are designed as follows:

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Figure 4: S0 and S1 matrices

The relative difference and contrast, for the above basis matrices can be computed as:

$$\alpha = 1/2$$

$$\beta = 1$$

There are two collections of matrices, C0 for encoding white pixels and C1 for encoding black pixels. Let C0 and C1 be the following two collections of matrices:

$$C_0 = \pi(S_0) \quad C_1 = \pi(S_1)$$

where $\pi(S_0)$ and $\pi(S_1)$ represents the collection of all matrices obtained by permuting the columns of matrices S0 and S1 respectively.

That is,

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \quad \text{and} \quad C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

To share a white pixel, the dealer randomly selects one of the matrices in C0, and to share a black pixel, the dealer randomly selects one of the matrices in C1. The first row of the chosen matrix is used for share 1 (S1) and the second row for share 2 (S2). The two shares individually do not reveal the secret message. When we merge the two shares one upon another we can reveal the secret.

C. construction of k out of n VCS

In this type of VCS, we are given a secret message. We would like to generate n transparencies so that the original secret message is visible if any k (or more) of them are stacked together but totally invisible if fewer than k transparencies are stacked together. A solution to the k out of n VCS consists of two collection of n*m Boolean matrices C0 and C1. To share a white pixel, the dealer randomly chosen one of the matrices in C1. The chosen matrix defines the color of the m sub pixels in each one of the n transparencies and likewise for black pixels. We apply 2 out of 2 VCS for every share images to create more shares[5].

IV. Conclusion

Visual cryptography is the current area of research where lot of scope exists. In this thesis, we have demonstrated the construction of basis matrices for 2-out-of-n, n-out-of-n, k-out-of-n VCS is demonstrated with examples. Also, using public key encryption, secret shares are made more secure which make secret image shares impossible to be altered by any third through a channel.

References

- [1] Feng Liu, Chuankun Wu, Xijun Lin. "Step Construction Of Visual Cryptography Schemes". IEEE transactions on information forensics and security, vol. 5, no. 1, march 2010.
- [2] N. Askari, H.M. Heys, and C.R. Moloney. "an extended visual cryptography scheme without pixel expansion for halftone images". 26th annual IEEE Canadian conference on electrical and computer engineering year 2013.
- [3] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo "Halftone Visual Cryptography". IEEE transactions on image processing, vol. 15, no.8, august 2006.
- [4] Gyan Singh Yadav and Aparajita Ojha "A Novel Visual Scheme Based on Substitution Cipher". Proceedings of the IEEE Second International Conference on Image Information Processing (ICIIP-2013).
- [5] Archana B. Dhole and Prof. Nitin J. Janwe "An Implementation Algorithms in Visual Cryptography in Images". International Journal Scientific and Research Publications, Volume 3, Issue 3, March 2013 1 ISSN 2250-3153.
- [6] Kaur and Vineeta Khemchandani. "Securing Visual Cryptographic Shares using Public Key Encryption". 2013 3rd IEEE International Advance Computing Conference (IACC).
- [7] Parakh and S. Kak. "A Recursive Threshold Visual

Cryptography Scheme ". Department of Computer Science,
Oklahoma State University Stillwater, OK 74078.

- [8] D. Jena and S. Jena . "A Novel Visual Cryptography Scheme".
978- 07695-3516-6/08 2008 IEEE DOI 0.1109/ICACC.2009.109.
- [9] P. S. Revenkar, Anisa Anjum and W. Z. Gandhare.
"*Survey of Visual Cryptographic Schemes*". International Journal of
Security and Its Applications Vol. 4, No. 2, April, 2010.
- [10] Chakraborty et al. "Design and Implementation of a (2, 2)
and a (2,3) Visual Cryptographic Scheme". International Conference
[ACCTA-2010], Vol.1 Issue 2, 3, 4, PP 128-134.