International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey on Visual Cryptography Schemes

Prajakta Nikam[1], Dr. Kishor Kinage[2]

[1]Department of Information Technology, MIT college of Engineering, University of Pune, India

[2]Professor, Department of Information Technology, MIT college of Engineering, University of Pune, India

Abstract: ***Visual cryptography (VC) is a encryption scheme used to share secret image. It encodes image into n shares. These shares are either printed on transparencies or are encoded and stored in a digital form. The shares can look as noise-like pixels or as meaningful images. Decoding does not require all n shares .These shares are printed on transparencies and stacking them top to each other reveal the secret image. In this survey paper, we present the readers a overview of visual cryptography scheme and different approaches of visual cryptography.***

Keywords: Visual secret sharing scheme, extended visual cryptography scheme , transmission risk

1. Introduction

Visual Cryptography is a secret-sharing method that encrypts a secret image into several shares but requires neither computer nor calculations to decrypt the secret image. The secret image is reconstructed visually simply by overlaying the encrypted shares the secret image becomes clearly visible. One of the best-known techniques has been credited to Moni Nair and Adi Shamir. They demonstrated a visual secret sharing scheme, where an image is split into *n* shares so that only someone with all *n* shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by superimposing the shares[4]. When all *n* shares were superimpose, the original image would appear .

Secret images can be of various types: photographs, images, handwritten documents, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. This scheme suffer from drawback: These random looking noise like shares are suspicious thus are vulnerable to attack by attacker in middle so there is high transmission risk . Another drawback is if number of share increase, it become more difficult to manage the shares. Problem of management of shares solved by extended visual cryptography scheme (EVCS) scheme. EVCS adds meaningful cover images in the share. But while recovering secret image from cover images it produce extra noise and degrade the quality of hidden image.

Using steganography techniques, secret images can be hidden in cover images that are halftone gray images and true-color images However, the stego-images still can be revealed by steganography analysis methods. Therefore the existing VSS schemes still must be investigated for reducing the transmission risk problem for carriers and shares. A method for reducing the transmission risk is an important issue in VSS schemes.

2. Related Work

Visual Cryptography (VC) is a technique for sharing secret image. This technique was proposed by Naor and shamir VC scheme spilt the secret image into share images shown in Fig 1 and Fig2.

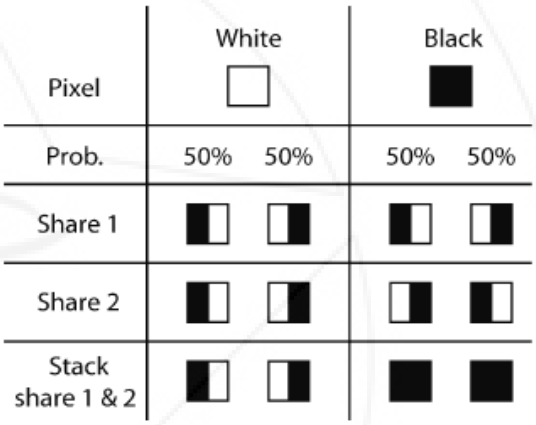

Figure 1: Construction of a two-out-of-two VC scheme [3].

The share images are appear as noise like images as shown in fig 2. The shares are printed on transparencies which are then distributed to participant. By overlapping transparencies directly, the secret images can be revealed and visually recognized by humans without any computational devices and cryptographic knowledge. Any one share cannot revealed information about secret image.

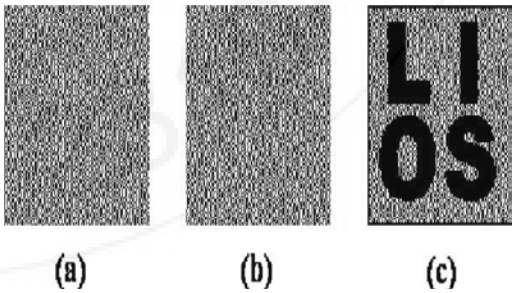

Figure 2: Example of traditional (2,2)-VCS

VC is a very good solution for sharing secrets when computers cannot be employed for the decryption process. This scheme suffers from drawback: These random looking noise like shares are suspicious thus are vulnerable to attack by attacker in middle so there is high transmission risk.

Another drawback is if number of share increase, it becomes more difficult to manage the shares.

Extended visual cryptography scheme (EVCS) is kind of visual cryptography scheme first introduced by Naor in [2].EVCS consist of meaningful shares and VCS consist of random shares. Input to EVCS is secret image and n original shares images. It outputs n shares which are meaningful images. Only qualified subset of shares can recover the secret image. Any forbidden subset of share cannot obtain any information of secret image. EVCS overcome the drawback of VCS as all shares of EVCS are meaningful images hence these shares are less suspicious. Limitation of EVCS is bad visual quality of the shares and recovered secret image. Another limitation is that pixel expansion is large and requires complementary share images.

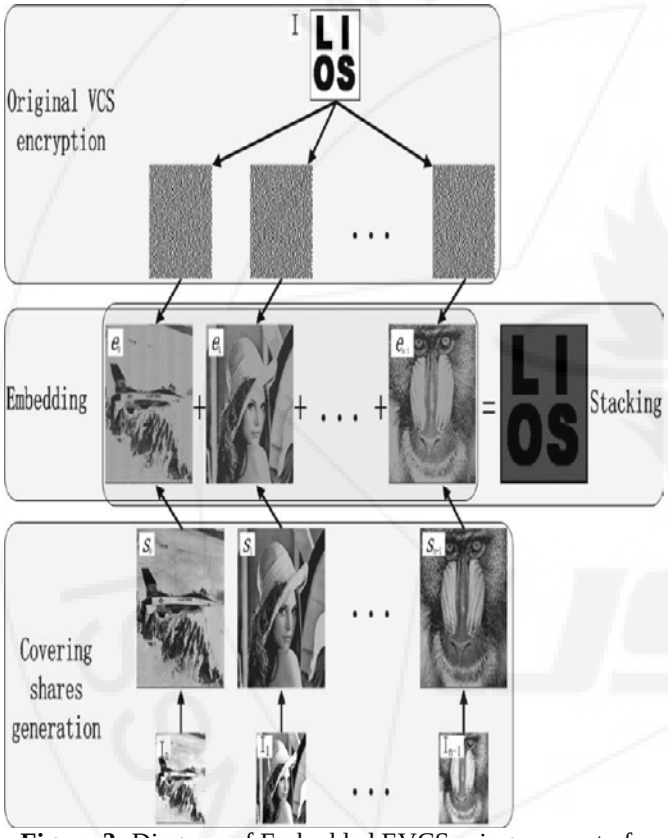

Figure 3: Diagram of Embedded EVCS using concept of Dithering matrix.

Embedded EVCS is a visual cryptography scheme proposed by Feng Liu and Chuankun Wu[2]. To encode secret image take n gray scale image as input and convert them into n covering share. Covering shares are divided into blocks of s sub pixels. *Mo* and *M1* are matrices of a traditional VCS. Embedding the rows of *Mo* and *M1* into the blocks of covering share. Finally outputs n shares. Covering shares are generated.

As compared with EVCS the embedded EVCS has many advantages such as it deals with gray scale input image, has smaller pixel expansion, does not require complementary share images. Halftone visual cryptography is a another technique for visual cryptography proposed by Zhi Zhou [3].In this method a halftone image*(HI)* obtained by applying any halftoning method such as the error diffusion on a grey level image .This image is given to first participant. Reverse all black/white pixels of *HI* to white/black pixels and get complementary image ($\overline{HI}$) assigned to second participant. In each of share secret pixel is encoded into halftone cell. Select only two pixel from each of share .Pixel position is same in each share These selected pixels are secret information pixels are need to modify. Rule for modification are given below

1) If pixel is white, a matrix is randomly selected from the collection of matrices Co of conventional VC.
2) If pixel is black, matrix is randomly selected from C1.

The secret information pixels in the i th share are replaced with the two subpixels in the i th row of matrix. Halftone share quality is better than conventional VC share. Fig 4 shows construction of a two-out-of-two scheme for halftone VC Scheme (n,n) NVSS scheme is a approach for sharing image using diverse image media. This approach is proposed by kai-Hui Lee and Pei-Ling Chiu[4]. It can share one digital secret image over n-1 arbitrary selected natural images. Natural images are also called as natural shares. Instead of altering content of natural share this approach extract features from natural shares. These natural shares are unaltered thus greatly reducing transmission risk problem. Secret image and all n-1 natural shares are encrypted by using encryption algorithm. (n,n) NVSS scheme finally outputs one noise like share. Noise like share is hidden by using data hiding technique to reduce a transmission risk problem. It is the first attempt to share image via heterogeneous carriers in VSS scheme. Compared with VSS scheme, NVSS scheme greatly reducing transmission risk problem.

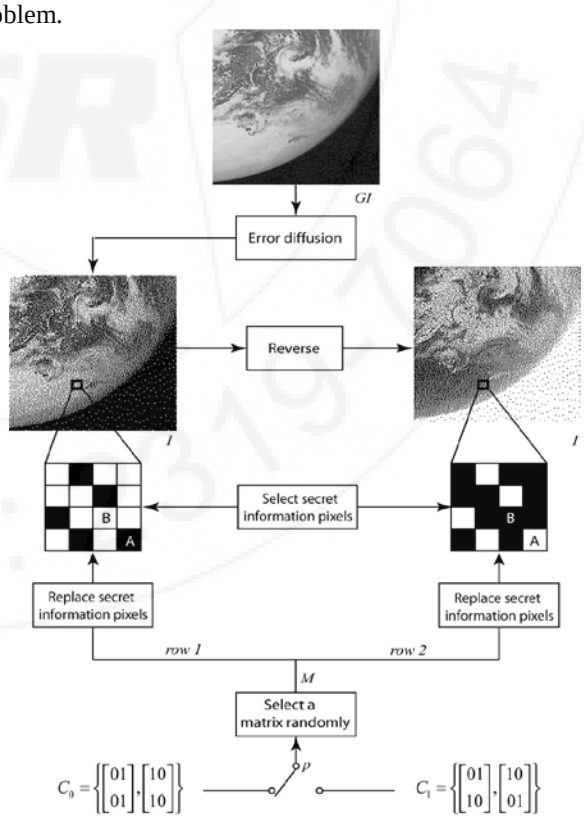

Figure 4: Construction of a two-out-of-two scheme for halftone VC Scheme.

3. Conclusion

In this paper, we briefly reviewed the literature of visual cryptography schemes This paper provides a review on various visual cryptography techniques. The visual cryptography (VC) scheme techniques can decode concealed images without cryptography techniques. EVCS scheme [2] which was realized by embedding the random shares into the meaningful covering shares. The shares of EVCS scheme are meaningful images and the stacking of qualified subset of shares will recover the secret images visually.

Applying the rich theory of halftoning into the construction mechanism of conventional VC, the proposed method generates visually pleasing halftone shares carrying significant visual information. The obtained visual quality is better than that attained by any other available VC method. The (*n*, *n*)-NVSS scheme[4], that can share a digital image using diverse image media. The shares are totally innocuous. NVSS scheme uses only one noise share for sharing the secret image. Compared with VSS schemes, the proposed NVSS scheme can effectively minimize transmission risk and provide the highest level of user friendliness, both for shares and for participants.

References

[1] M. Naor and A. Shamir, "Visual cryptography," *in Advances in Cryptology vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12*.
[2] F. Liu and C. Wu, "Embedded extended visual cryptography schemes" , *IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun.2011.*
[3] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453 Aug. 2006.
[4] K. H. Lee and P. L. Chiu, "Digital Image Sharing by Diverse Image Media" *IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, Jan. 2014.*
[5] Subba Rao Y.V , Brahmananda Rao S.S , Rukma Rekha N ," Secure Image Steganography based on Randomized Sequence of Cipher Bits", *Eighth International Conference on Information Technology,2011*
[6] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219–229, Feb. 2012.
[7] Z. Wang, G.R.Arce, and G.D.Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.
[8] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132–145, Jan. 2011.
[9] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1693–1703, Nov. 2011.
[10] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 992–1001, Sep. 2011.