THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Visual Cryptography:A Concern of Privacy

Balraj Kumar[1], Preeti[2], Prince Arora[3],
School of Computer Science & Engineering[1,3]
Lovely Professional University, Phagwara - 144411, Punjab, India[1,3]
Innocent Hearts Group of Institution, Punjab, India[2]
balraj_kr@yahoo.co.in[1],preeti.daviet@gmail.com[2],princearorabca@gmail.com[3]

Abstract:*Visual Cryptography is an exciting area of research and is widely being used in diverse applications such as online banking, internet voting, cloud computing, biometrics, etc. It is one of the powerful encryption tool that can be used to hide visual information and can be decrypted by the human-visual system without requiring the use of any decryption technique. This paper examines the vital aspects of visual cryptography and analyse the findingsafter going through an extensive literature review. The major emphasis of present study is to highlight the key visual cryptography schemes and recent advances in the area of visual cryptography.*

Keywords: Visual cryptography, shares,secret sharing, pixel expansion, error diffusion.

1. Introduction

Visual Cryptography(VC) is a magical technique whereinthe secret image ispartitioned into two/more shares, also known as transparencies and decryption is performedusing human-visual system. In other words, VCis an influential method that allows us to encrypt the original information in the form of multiple layers on which the exact data is scattered.This techniquewas introduced by thetwo mathematicians Moni Naor andAdiShamir in 1994[1].It is widely used in diverse applications areas such as online banking, internet voting, cloud computing, biometrics, etc. [2].In visual cryptography technique, the encrypted data is divided into two layers: cipher layer and transparency layer. Cipher layeris the one that containsciphertext. The secret key is written on another layer known as transparency layer. Each cipher layer is decrypted with distinct transparency layer. Decryption is purely dependent upon the criteria to blend the transparency layer on to the cipher layer that enables the human sight to visualize the original information. Due to its intelligibility any one can utilize this cryptography technique without any expertise in typical crypto computations.

In a secret sharing scheme [3], a dealer (a special person) encodes the enigmatic picture into '*n*'special transparencies and provides every member a share. Every share uncovers positively no data about the mystery picture. All things considered, a systematic arrangement of members can disentangle the picture by stacking their transparencies together with the goal that the darker mystery picture shows up and the members read it straightforwardly. Then, a taboo arrangement of members cannot get any data about the mystery picture from their transparencies even with interminable computing power.

The present study attempts to highlight the vital aspects of visual cryptography by going through an extensive literature review. Its main focus is on the key VC techniques and recent advances in the area of visual cryptography. Organization of this paper is as follows:

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Section-2 presents the background of visual cryptography. Section-3 describes the working of VC concept. Section-4 highlights the various VC schemes widely being used by researchers. The concluding remarks are presented along with further research pointers in section-5.

2. Background

This section throws light on the previous studies carried out on visual cryptography (VC) and attempts to establish a connect between the VC literature and the present article.

Naor and Shamir [1] introduced an interestingtechnique known as visual cryptography (VC) to decode concealed images without any computational effort. Implementation of this scheme is easy and secure. The authors extended the basic scheme to the k out of n secret sharing problem which was a visual variant. Secret sharing schemes are beneficial when secrecy of some confidential data has to be maintained. These schemes can also be used to construct shared control schemes [4] and fault tolerance schemes [5].Tzengand Hu [3] proposed a refineddefinitionofVCon the basisof their observations, wherein the discovered images are darker/lighter than the backgrounds. Based on this refined definition, they further proposed techniques to build VC schemes. Horng et al. [6] attempted to state the cheating problem by cheaters (dishonest participants) invisual cryptography.Apart from this, they also proposed two simple cheating avoidanceVC plans: one is authentication based while the other is based on *2*-out-of-(*n*+*l*) visual cryptography.Thomas and Gharge [2] examined the severalvisual cryptography techniques based on a number of factors. These factors include the number of secret, number of secret image, share type,pixel expansion, andimage format.Wang et al. [13] examined the features of both visual and cryptography of VC shares and integrated them into hash-code for VC authentication.

3. Working of Visual Cryptography

Visual Cryptography plays a major role when it comes to ensure the secure communication. VC aims to provide security and to distinguish between machine and human. VC uses human-visual system for decryption.The major steps involved in visual cryptography scheme are [2]:

(i) Secret image
(ii) Dividing the secret-image into '*n'* shares
(iii) Stacking of qualified shares
(iv) Recovered shares

The Boolean functions such as *or*, *xor* and *not*are used to perform visual cryptography scheme. Pixel expansion and the contrast are the parameters used to measure the performance of visual cryptography scheme. For example, if the pixel expansion is smaller, quality of visual cryptography schemeis better[2].

To implement visual cryptography, the first thing required is, a black and white picture of information that has to be encrypted. Divide each pixel of source image into smaller sub-pixels and shade these sub pixels accordingly to create cipher layers and transparency layers.A pixel can be divided into two parts or four parts. For example, if a pixel containing black colour:

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

(a) It can be divided into two parts.One part represents the white colourwhile the other part represents the black. This division is shown in Figure-1:

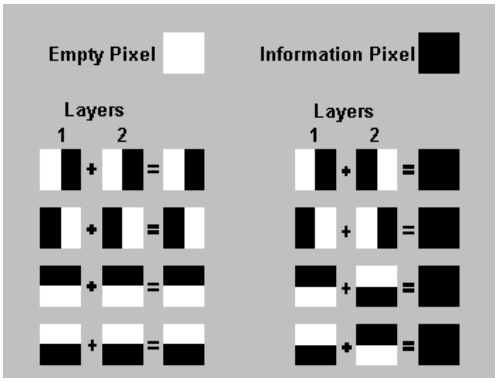

Figure-1: Pixel division in two parts

(b) If a pixel is divided into four parts, then two parts will represent black colour and other two parts signifythe white colour. It purely depends upon the requirement of the application in hand for creating cipher and transparency layers.

The distribution chart of pixels is given in Figure-2:

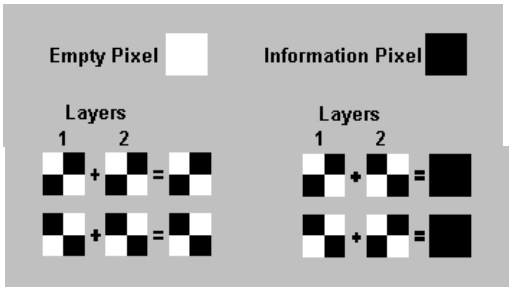

Figure-2: Pixel division in four parts

Colour Determination Method

A black-and-white VC scheme is generallyillustrated using two Boolean matrices i.e.M_1 and M_2 which are known as basis matrices. These matrices are used todescribe the subpixels in the shares [14].The colour of pixelsis represented using basis matrices.The basis matrix M_1 is used, if colour of the pixel in the original image is white, and if the colour is black, M_2 is used.

For white colour, the matrix entries will be:

$$M_1 = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \text{ or } \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

For black colour, the matrix entries will be:

$$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

M_2=0 1 or 1 0

To produce white colour, one can pick one of the matrix from M1 or M2 and to produce black colour one can pick matrix from M3 or M4.

For instance,suppose there is a need to send a message as shown in Figure-3:

Figure-3: Secret Image

Now continuing with above format,first create one transparent layer consisting of all the pixels at arbitrary positions from one of the above combination and also one cipher layer in which information pixels must be of black colour placed at arbitrary positions.Thus, when one layer is overlapped on another layer the identical region will produce grey shade and opposite region will produce black shade to represent original message. Both of these layers are presented in Figure-4.

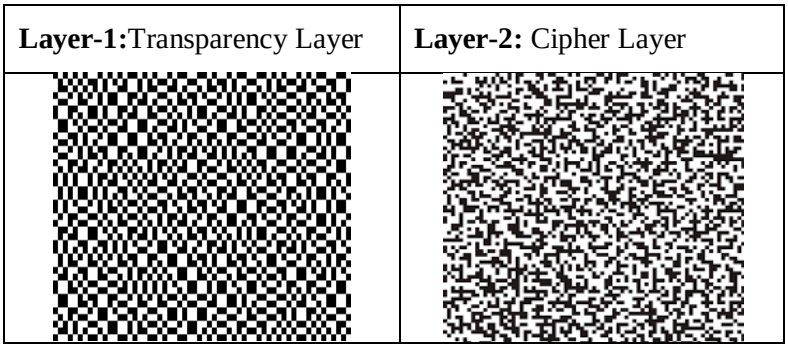

Figure-4: Transparency and Cipher Layers

After overlapping the resultant decrypted message is shown in Figure-5:

Figure-5: Decoded Image

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

For better proficiency, each sender can distribute one transparent layer to all the receivers and as and when required can create corresponding cipher layer and send it to respective receiver for decrypting the message.

4. Visual Cryptography Schemes

This section touches upon the diverse visual cryptography schemes being heavily used in VC research. These schemes include:

(a) **Monochrome Image VC:** Thisvisual cryptographytechnique is the one wherein the secret images are inmonochromatic format. There are many techniques used wherein the secret image is represented in monochrome layout.Weir and Yan [7] proposed to make a master key for all the secrets.Multiple secrets can be revealed by adjusting this master key. Fang [8] proposed a look-up table that is notessential for non-expansion reversible VCmethod. It uses 2 sharesto encode4 secrets and to recover the rebuilt image without anyalteration.Fu and Yu in [9] suggested a method on the basis of randomvariation and co-relation matrices set.

(b) **Halftone VC:** Halftone visual cryptography technique was introduced by Wang et al. [10]. In this type of cryptography, secret image is concealed using the halftone method. The halftone technique causes pixel expansion and the dimensions of the images gets expandedbecause of pixel expansion. In this technique,secret image pixelispre-computedprior to the generation of the halftone shares. Error diffusion is a simple and commonly usedhalftone technique thatprovides good quality images with less computational effort. This procedure disperses away the quantization mistake into the neighboring dark scale pixel with the goal that an outwardly satisfying halftone pictures is accomplished.this technique spreads the pixels homogeneously to achieve the refinements in the overall quality of shares.

(c) **Extended VC:**This scheme enables the creation of visual mystery sharing plan utilizing important offers and disregards the offers with irregular noise. Hence, this technique help improves the security. Meaningful shares disappear on superimposing and the secret image is recovered. Because the existence of concealed information can’t be discoveredeasily, thus the security has to be enhanced. So this method is more secure.Pixel expansion is the limitation of this scheme. According to Liu and Wu [11], this limitation can be overcome with a strategy by mixing arbitrary offers into important secured shares, that is called expanded VC method. The all-encompassing VC without pixel extension gives great offers, bringing about a recapturing picture near the first one. The all-encompassing VC method endeavors to keep up a superior harmony between white and the dark pixels.

(d) **Colour VC:**Colour visual cryptography method uses natural colour image to protect information. The features of a colour imageenhances the information securitywithoutdisclosing the information. Distinctive graylevels can be mimicked by adjusting the thickness. Shading deterioration strategies is utilized for shading pictures. A mystery picture can be separated into one of the three prime hues that are yellow, cyan, and maroon. Top notch shading VC offer will bring about a superior modified picture. During the encoding procedure the recuperated pictures become bigger because of pixel development. So as to improve pixel extension and the complexity, top notch halftoned shares are utilized. Kang [12] usedhalftone visual cryptography technique in colour images, wherein error diffusion and visual

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

information pixel synchronizationget a colour visual cryptography and that provides useful colour shares havinggreat visual quality.

5. Conclusion

Visual Cryptography is an exciting area of research and is one of the powerful encryption toolthat isused to hide visual information and then used to decrypt through human-visual system without requiring the use of any decryption technique.The present study highlights the vital aspects of visual cryptography. Its main focus is on the key VC techniques and recent advances in the area of visual cryptography. The only thing required is the knowledge of distributing pixels among different layers of secret message that can be easily implemented if one can only have basic knowledge of matrices. The layers allow to create different shapes, even every type of text can be created with change in the value of the matrix. The ciphertext can be created to implement the wide variety of images and data.

The future perspective ofvisual cryptography is to improve the pixel contrast for better quality. There is a possibility of usage of fake share to reveal the secret, hence requires more work to carry out. Multiple sharing may cause alignment problem which requires more attention. The topics such as VC content features and algorithms for VC authentication need to be analysedmore critically.

References

[1] M. Naor, and A. Shamir, “Visual cryptography”, In *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 1-12, May1994.

[2] S.A. Thomas, and S. Gharge, “Review on Various Visual Cryptography Schemes”, In proc: *International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC).* IEEE, pp. 1164-1167, Sep 2017.

[3] W.G. Tzeng, and C.M. Hu, “A new approach for visual cryptography”, *Designs, Codes and Cryptography*, *27*(3), pp.207-227, 2002.

[4] G. J. Simmons, “An introduction to shared secret and/or shared control schemes and their applications, Contemporary Cryptology”, IEEE Press, Piscataway, pp. 491–497, 1991.

[5] M.O. Rabin, “Efficient dispersal of information for security, load balancing, and fault tolerance”, *Journal of the ACM (JACM)*, *36*(2), pp. 335–348, 1989.

[6] G. Horng, T. Chen, and D.S. Tsai, “Cheating in visual cryptography”,*Designs, Codes and Cryptography*, *38*(2), pp.219-236, 2006.

[7] J. Weir and W.Q. Yan, "Sharing Multiple Secrets using Visual Cryptography," IEEE International Symposium on Information Engineering and Electronic Commerce, Taipei, pp. 509-512, 2009.

[8] W.P. Fang, "Non-Expansion Visual Secret Sharing in Reversible Style," International Journal of Computer Science and Network Security, Vol. 9, No. 2, pp. 204-208, 2009.

[9] Z. Fu and B. Yu, "Research on Rotation Visual Cryptography Scheme," IEEE International Symposium on Circuits and Systems, Ternopol, pp. 533-536, 2009.

[10] Z. Wang, G. R. Arce and G. D. Crescenzo, “Halftone Visual Cryptography via Error Diffusion,” IEEE Transactions on Information Forensics and Security, Vol. 4, No. 3, pp. 383-396, 2009.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

[11] F. Liu and C. Wu, "Embedded Extended Visual Cryptography Schemes," IEEE Transaction on Information Forensics and Security, vol. 6, No. 2, pp. 307-322, 2011.

[12] I. Kang, G. R. Arce and H.K. Lee, "Color Extended Visual Cryptography Using Error Diffusion," IEEE Transaction on Image Processing, vol. 20, No. 1, pp.132-145, 2011.

[13] G. Wang, W. Yan, and M. Kankanhalli, "Content based authentication of visual cryptography", *Multimedia Tools and Applications*, *76*(7), pp. 9427-9441, 2017.

[14] https://shodhganga.inflibnet.ac.in/bitstream/10603/6102/12/12_chapter%202.pdf.