Various Visual Cryptography Schemes for Database Security

Mamta Rani[1], Raj Kumar[2]

[1]M.Tech. Scholar, Department of CSE, Jind Institute of Engineering & Technology, Jind Haryana, India
[2]Assistant Professor, Department of CSE, Jind Institute of Engineering & Technology, Jind, Haryana, India

ABSTRACT

Security and Confidentiality is one of the most common aspects of information technology. The secure and effective protection of sensitive information is a primary concerns in any scientific, military, medical and commercial systems. This is achieved using different techniques for different types of information. Visual cryptography is one such technique that secures visual information, which is a very secure and unique way to protect secrets. Visual cryptography is an encryption technique which is used to hide and encrypt information present in an image encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. In this, images are distributed as shares that need to be superimposed to retrieve the hidden secret image. The intent of this paper is to study various visual cryptography schemes and research works done on the basis of pixel expansion, number of secret images and the merits and demerits of each.

Keywords: **Cryptography, secret image sharing, contrast, pixel expansion, Shares**

I. INTRODUCTION

Various confidential data such as commercial identifications, military and defence secrets and scientific findings are transmitted over the Internet. While using such secret images, security and confidentiality issues should be taken in to consideration as any unauthorized person may utilize weak links over the communication network to tamper or even steal information. Secret sharing is a very hot area of research in the field of computer Science in the recent past. To deal with these security concerns of sharing secret images, various image secret sharing schemes have been developed.

Visual cryptography is a cryptographic technique which allows visual information such as printed text and pictures to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

II. BASIC VISUAL CRYPTOGRAPHY

Visual cryptography scheme was first developed by Naor and Shamir [1] in 1994. In this, two transparent images called shares are generated of which one is made of random pixels in which black and white pixels are of equal number. The second share is made according to the first share. The information is revealed when these two shares are superimposed. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. The process of visual cryptography is shown in below figure 1.

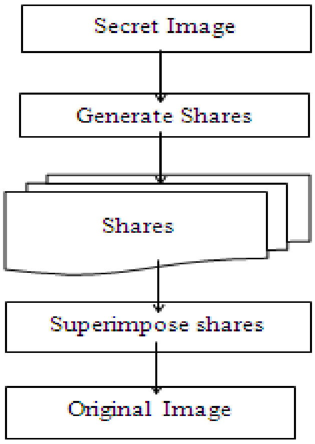
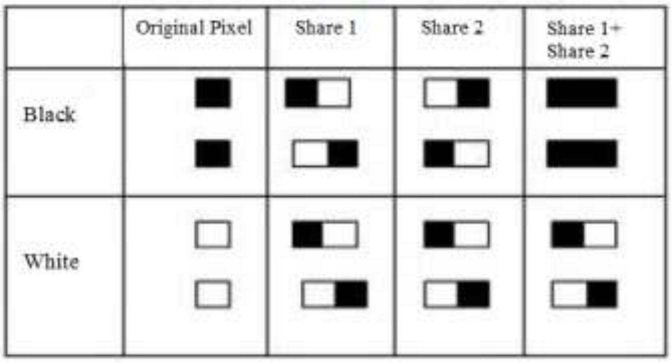


Fig. 1 Flow of visual cryptography

As shown in the above figure, the secret image is used for encryption process which generates shares of images. Then this share images are shared and are ready to be decrypted at the receiver side by just superimposing the share images. A (2, 2) visual cryptography scheme can be used to discuss fundamental visual cryptography. Senders create two layers. Basically pixel expansion may be 2 4, 8 etc. we have taken pixel expansion 2. That means one pixel of our original image is replaced by 2 pixels in share image. If the pixel is white the sender takes any row from the last two rows of Figure 2 randomly and if the pixel is black, the sender takes any row from the first two rows of Figure 2 randomly. By overlapping the two shares as shown in the last row of figure 2 randomly.

Visual cryptography is a method for fulfilling secret sharing activities in the environments with insufficient computing power. Secure image sharing techniques overcome the traditional cryptographic approach, providing new solution for the development of new and secure imaging applications.



	Original Pixel	Share 1	Share 2	Share 1+ Share 2
Black	■	■□	□■	■■
	■	□■	■□	■■
White	□	■□	■□	■□
	□	□■	□■	□■

Fig. 2Construction of a (2, 2) Visual Cryptography Scheme

III.VISUAL CRYPTOGRAPHY TECHNIQUES

A. Multple Secret Sharing Visual Cryptography Technique

Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu presented multiple secret sharing visual cryptography technique. Here, two binary secret images are shared in two share image A and B both of which are binary image and is random. Shares are made such that the first secret can reveal the information as shown in basic model, that is, by superimposing two share images, and the second share can be obtained by rotating the first share i.e. share A by anti-clockwise direction. A rotating angle 90◦ was taken. Wu and Chang refined the idea by programming share to be circles so that the restriction to the rotating angle can be removed. [2]

B. The Progressive Visual Cryptography

It was proposed by Young-Chang Hou and Zen-Yu Quan[3]. In this technique reconstruction of secret image is probabilistic and the share images have the same size as the secret image size. The output of the secret image pixel is constructed using 'OR' operation applied on the corresponding pixel in share images. As the name probabilistic visual cryptography suggests, there is no absolute guarantee on the correct reconstruction of the original pixel. It is different from a traditional visual cryptography in that a wrong reconstruction of pixel is possible. 'Approximation' of secret pixel is guaranteed in the traditional technique. Here, approximation means that a white (black) pixel can be, in some cases, replaced in the reconstructed image by a set of sub pixels having a given set of whiteness (blackness). Since in probabilistic models the secret pixel is correctly reconstructed with some probability, the quality of the reconstructed images depends on how big is the probability of correctly reconstructing the secret pixels.

C. Random grid based visual cryptography technique

It was presented by Kafri and Keren [4]. In this method size of pixel is same as original image pixel size. This means that retrieved secret image size and original image size is same so it reduces the problem of pixel expansion. In this method random grid R is defined as a two dimensional array of pixels. Each pixel is either transparent (white) or opaque (black) by a coin-flip procedure. The numbers of transparent pixels and opaque pixels are probabilistically same and the average opacity of a random grid is 50% [8].

D. Region Incrementing Visual Cryptography

It is used to hide multiple secrecy levels in a single image. In n level region incrementing visual cryptography scheme, image is divided in n regions. Each region consists of one level of information [5]. For implementing visual cryptography in n levels we need to encode (n+1) shares in such a way so that any single share is not able to show the information and by combining any two shares, first level information would be visible. Similarly by super imposing any three shares, information upto second level could be seen. In similar way, for revealing whole information all the (n+1) shares are superimposed. These n levels are created according to user specification. In the proposed scheme, user does not need to address the area of different levels manually and levels are created automatically. Only a particular level information with a particular size of text is needed.

E. THE TAGGED VISUAL CRYPTOGRAPHY TECHNIQUE

It was proposed by Ran-Zan Wang and Shuo-Fang Hsu [6].It is an innovative type of visual cryptography in which additional tags is obscured into each generated share. By folding up each single share, the related tagged pattern is visually discovered. Such supplementary tag patterns significantly supplement extra abilities of VC, such as improved message carried in a single share, user-friendly interface to manage the shares. However, reported (k, n) tagged visual cryptography proposed by Wang and Hsu still suffers from the defects such as pixel expansion.

F. THE HALFTONE VISUAL CRYPTOGRAPHY

It was presented by Zhongmin Wang, Gonzalo R. Arce, Giovanni Di Crescenzo [7] uses error diffusion method. A gray scale image is taken and converted into binary image by applying halftone technique. In this binary share images, secret image pixel is put in to each share image by applying void and cluster algorithm. The reconstructed image is obtained by superimposing two share images. Though it is a very good method, there is still a tradeoff between pixel expansion and contrast loss of original image.

IV. COMPARISON OF DIFFERENT VISUAL CRYPTOGRAPHY TECHNIQUES

Table I: Comparison Of Various Visual Cryptography Schemes

Author	Technique Used	No. of Secret Image	Pixel Expansion	Merits	Demerits
Naor and Shamir	Traditional VC	1	1:2	Provide Security for binary image	Does not generate meaningful share image
M Nakajima and Yamaguchi	Extended VC	1	1:2	Generates meaningful shares	Contrast loss occurs
Kafri and Keren	Random grid VC	1	1:1	No pixel expansion	Lower visual quality
Wu and Chen	Multiple secret sharing VC	2	1:4	Image can encrypt two secret images between two shares. Rotating angle is 90◦	Size of the shares is 4 times the size of the main secret image.
Young-Chang Hou and Zen-Yu Quan	Progressive VC	1	1:1	No pixel expansion	No absolute guarantee on the correct reconstruction of the original pixel
Wu and Chang	Multiple secret sharing VC	2	1:4	Rotating angle is invariant.	Pixel expansion is more
Zhongmin Wang, Gonzalo R. Arce	Halftone VC	1	1:4	Provide meaning full share images	Tradeoff between pixel expansion and contras of original image

CONCLUSIONS

In this paper, several visual cryptography schemes are briefly analysed along with a comparative study. It is observed that the existing visual cryptography schemes have their own set of advantages accompanied by a set of limitation. In order to achieve encryption of the secret information, expansion and increasing of the number of shares are performed, which in turn this affects the resolution. Hence, continuous research and advancement in visual cryptography is pretty much necessary to achieve best and optimum balance of security and quality.

ACKNOWLEDGEMENTS

I would like extend my thanks and gratitude to all the referenced authors.

REFERENCES

[1]. MoniNaor and Adi Shamir, “Visual Cryptography”, advances in cryptology– Euro crypt, pp 1-12, 1995.

[2]. J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu. “Visualsecret sharing for multiple secrets” Pattern Recognition, 41:3572{3581, 2008

[3]. Young-Chang Hou and Zen-Yu Quan“Progressive Visual Cryptography with Unexpanded Shares” IEEE Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 11, November 2011

[4]. O. Kafri and E. Keren. “Image encryption by multiple random grids”Optics Letters, 12(6):377{379, 1987.

[5]. Wang, R.Z.[Ran-Zan], “RegionIncrementing VisualCryptography”,SPLetters(16), No. 8, August 2009,pp. 659-662.

[6]. Ran-Zan Wang and Shuo-Fang Hsu,” Tagged Visual Cryptography:, IEEE Signal Processing Letters, Vol. 18, No. 11, November 2011 627

[7]. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol. 4 pp 383–396, Sep.

[8]. S. J. Shyu, “Image encryption by random grids,” Patt. Recognitions, vol. 40, no. 3, pp. 1014– 1031, 2007

[9]. Xiao-qing Tan, “Two Kinds of Ideal Contrast Visual Cryptography Schemes”, International Conference onSignal Processing Systems, pp. 450-453, 2009.

[10]. Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, “Sharing A Secret Two-Tone Image in Two Gray-LevelImages”, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.