A COMPARATIVELY STUDY ON VISUAL CRYPTOGRAPHY

Prashant B Swadas[1], Samip Patel[2],Dhruti Darji[3]

[1]Professor, [3]Student, Computer department Birla vishwakarma Mahavidhylaya, Vallabh vidhyanagar,India
[2]Professor, IT department Birla vishwakarma Mahavidhylaya, Vallabh vidhyanagar,India

Abstract

The effective and secure protections of sensitive information are primary concerns in commercial, medical and military systems. To address the reliability problems for secret images, a visual cryptography scheme is a good alternative to remedy the vulnerabilities. Visual cryptography is a very secure and unique way to protect secrets. Visual cryptography is an encryption technique which is used to hide information which is present in an image. Unliketraditional cryptographic schemes, it uses human eyes to recover the secret without any complex decryption algorithms and the facilitate of computers. It is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed.In this paper we represent various cryptography technique and research work done in this field.

Keywords: *Secret image sharing, cryptography, visual quality of image, pixel expansion*

----------***----------

1. INTRODUCTION

Managing secret has been aproblem of importance from the timehuman beings started to live together. Important things and messages have been always there to be sealed and confined from promising misuse or loss. Military and defense secrets have been the subject matter for secret sharing in the past as well as in the modern days. Secretsharing is a very hot area of research in Computer Science in the recent past. Digital media has replaced almost all forms ofcommunication and information preservation and processing. Security in digital media has been a matter of serious concern. Thishas resulted in the development of encryption and cryptography. Secret Sharing is an important tool in Security and Cryptography.

1.1 Basic Model

Visual cryptography scheme was developed by Naor and Shamir [1] in 1994. In this scheme two transparent images called shares are developed. One of the shares is made of random pixels in which black and white pixels are of equal number. Second share is made according to first share. When these two shares are superimposed, information is revealed. 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.

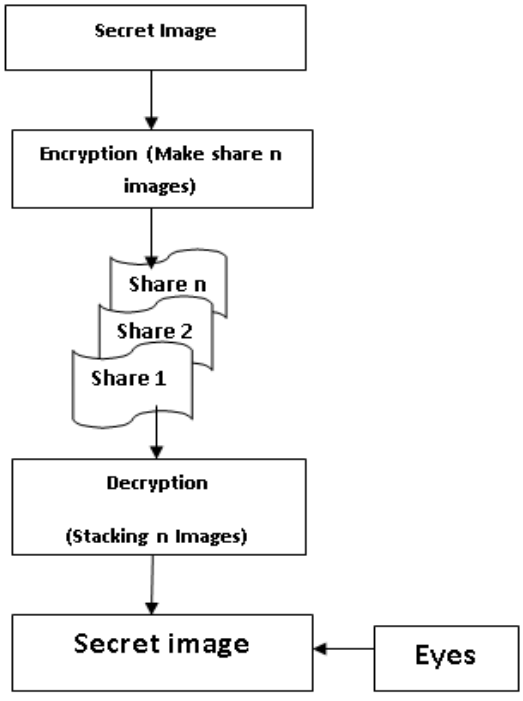

Fig 1 Flow of visual cryptography

As shown in above figure,we tack secret image.Then make encryption process which is nothing but a share of images.Then this share images mail or fax and at the receiver side decryption process is made using just superimposing images.which can be visualy visible by human vision system.
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.

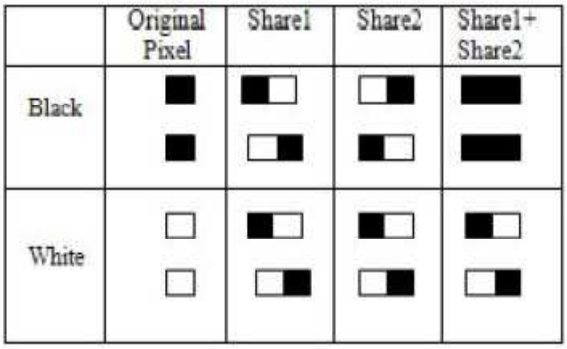

Fig. 2- Construction of (2, 2) VC Scheme [3]

For example, in below figure3 for encryption bvm.bmp as taken as input secret image Instead of sending secret image we send two encrypted images and for decryption we just superimpose two images, we will get result. All thought we will not get clear image but we can visually visualize the content.

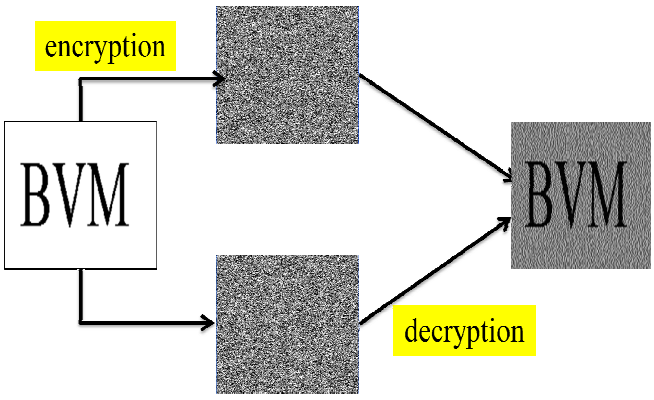

Fig 3 two out of two VC scheme

The (2,2) visual cryptography extended to (k,n) and (k,k) visual cryptography. In (k, n) visualcryptography scheme allows dividing a secret into K number of shares. Then the secret can be revealed from any N number of Shares among K.and in (k, k) visual cryptography scheme secret is divided into K number of shares and for reconstruction of the secret, all K shares are necessary. This scheme is not so popular because managing k number of shares is difficult task and it also increases time complexity to compute shares.

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 solutions for the development of new and secure imaging applications.

2. VISUAL CRYPTOGRAPHY TECHNIQUES:

B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu [2] presentedmultiple secret sharing visual cryptography technique. Here they shared twobinary secretimages in a two share image .They made two share names A and B.Both share are binary image which is random .They make share such that first secret can be revilethe information as shown in basic model that is superimpose two share image and for the second share can be obtained by rotating first share i.e. A share by anti-clockwise direction.They take the rotating angle 90◦.Again new researcher Wu and Chang refined the idea by programming share to be circles so that the restriction to the rotating angle can be removed.

Kafri and Keren [3]presented a random grid based visual cryptography technique. In this method size of pixel is same as original image pixel size .that means relieved 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]:

Young-Chang Hou and Zen-Yu Quan[4] present a new visual cryptography technique i e. progressive visual cryptography. In this technique reconstruction of secret image is probabilistic and the share images have the same size as the secret image size.Here, output of our secret image pixel is constructed using ‘OR’ing operation appliedn the corresponding pixel in share images. As the technique name is probabilistic visual cryptography, they give no absolute guarantee on the correct reconstruction of the original pixel. It might be possible reconstruction pixel is wrong so this is different from traditional visual cryptography in which ‘approximation’ of secret pixel is guaranteed. Here the 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.

Region incrementing visual cryptography 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 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 proposed scheme, user does not need to address the area ofdifferent levels manually and levels are created automatically. User needs only to usea particular level information with a particular size of text.

Ran-Zan Wang and Shuo-Fang Hsu [6]proposed a new technique which is called tagged visual cryptography.Tagged visual cryptography (TVC) is an innovative type of visual cryptography (VC) 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 significantlysupplement extra abilities of VC, such as improved message carried in a single share, user-friendly interface to manage the shares. However, reported (*k, n*) TVC proposed by Wang and Hsu still suffers from the defects such as pixel expansion.

Zhongmin Wang, Gonzalo R. Arce, Giovanni Di Crescenzo[7]presented a halftone visual cryptography. In this technique they used error diffusion method. They take one gray scale image and convert it into binary image by applying halftone techniuue.In this binary shareimages, they put secret image pixel in to each share image by applying void and cluster algorithm. The reconstructed image is obtained by superimposing two share images. It is a very good method but still there is a tradeoff between pixel expansion and contrast loss of original image.

3. COMPARISONS OF DIFFERENT VISUAL CRYPTOGRAPHY TECHNIQUE

Author	Technique used	Number of secret image	Pixel expansion	Merits	Demerits
Naor and Shamir	Traditional VC	1	1:2	Provide security for binary image	Not generate meaningful share image
M. Nakajima and Yamaguchi	Extended VC	1	1:2	Generate meaningful share	Contrast loss occur
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 imagesbetween two shares. Rotating angleis 90◦	Size of theshares 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 introduction of visual cryptography is provided. This paper does analysis of different visual cryptography scheme and a comparative study has been done. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveal secret image.Every existing method having own advantages even though it has set of limitation to achieve the good encryption method via Visual cryptography. In order to hide the secret information we go for expansion and increasing of the number of shares, but this affects the resolution. Hence research in visual cryptography (VC) is going on to achieve better visual quality.

ACKNOWLEDGEMENTS

We would like to thank reference authors and also like to thank the anonymous reviewers,whose comments and suggestions have helped them to improve the quality of the originalmanuscript.

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]. O. Kafri and E. Keren. "Image encryption by multiple random grids"Optics Letters, 12(6):377{379, 1987.
[4].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
[5].Wang, R.Z.[Ran-Zan], "RegionIncrementing Visual Cryptography",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.