ISSN 2250-3153

An Implementation of Algorithms in Visual Cryptography in Images

Archana B. Dhole[*], Prof. Nitin J. Janwe[**]

[*] IIIrd Sem. M.Tech (C.S.E.)
[**] Department of Computer Science & Engg

***Abstract*-** Visual Cryptography is a new Cryptography technique which is used to secure the images. In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the bi-level or binary images or monochrome images. Later it was advanced to suit for the Colour Images means Gray Images and RGB/CMY Images. For the RGB/CMY Images different methods are developed based on the colour decomposition techniques.

I. INTRODUCTION

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want . To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography is introduced by first in 1994 Noar and Shamir.[1]
Visual cryptography is a cryptographic technique which allows visual information(e.g. printed text, handwritten notes 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. Naor and Shamir [1], in 1994 proposed a new security technique named visual cryptography scheme. In this technique, a secret image of type binary is encoded in a cryptographical manner into random binary patterns which contains n shares in a k-out-of-n scheme. The n shares are distributed among n participants in such a way the each participant‟s share is not known to another participant. The secret image can be visually revealed by k or more participants by joining all the shares available. Even if computational power decoding is available, cannot be done on the secret image by k-1 or fewer participants.

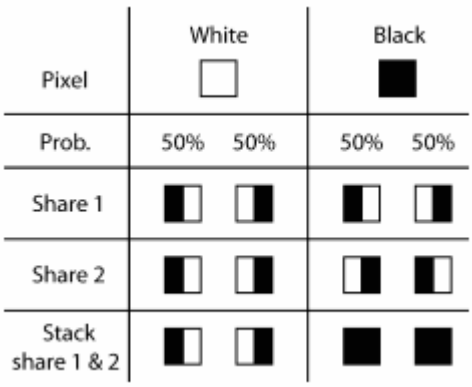


Fig. 1- Construction of (2, 2) VC Scheme

In fig. 1 If each pixel p of the SI is encoded into a pair of subpixels in each of the two shares.pixel. If a pixel p is white , the superposition of the two shares always outputs one black and one white subpixel. If p is black, it yields two black subpixels. There is a contrast loss in the reconstruction, however the decoded pixel is readily visible.

As the shares in the layers occur as random noise, the attackers cannot identify any useful information about the individual shares. Even with the availability of computer, it is not possible to decrypt the message or information with the limited availability of the share. The limitation of the above method is its randomness without any visual information. Extended Visual Cryptography have been suggested which also suffers from the same drawbacks of randomness. This paper is well thought-out as follows, Section II deals with the review of literature. Section III described image encryption technique. Section IV offers comparision. Finally the conclusion of this paper in Section V.

II. LITERATURE SURVEY

Recently in the literature, many new methods have been implemented for visual cryptography. In 1994 Naor and Shamir [1], have developed *the Visual Secret Sharing Scheme(VSSS)* to implement this model[Naor95]. In *k* out of *n* VSSS(which is also called (*k*, *n*) scheme), an binary image(picture or text) is transformed into *n* sheets of transparencies of random images. The original image becomes visible when any *k* sheets of the *n* transparencies are put together, but any combination of less than *k* sheets cannot reveal the original binary image. In the scheme, one pixel of the original image is reproduced by *m* subpixels on the sheets. The pixel is considered “on”(transparent) if the

number of transparent subpixels is more than a constant threshold, and "off" if the transparent subpixels is less than a constant lower threshhold, when the sheets are stacked together. The contrast α is the difference between the on and off threshhold number of transparent pixels. Which predicted an optimal dissimilarity in k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed image. A visual cryptography scheme is a broad spectrum method which is based upon general access structure. In k-out-of-n secret sharing scheme, any k shares will decode the secret image, which reduce the security level.

Rijimen presented a new 2-out-of-2 VC scheme by applying the idea of colour mixture. The stacking two transparencies with different colours leads to raises a third mixed colour.

A new method of Extended Visual Cryptograpy for natural images is used to produce meaningful binary shares which is predicted by Nakajima[2] in the year 2002 presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. Generally, visual cryptography suffers from the deterioration of the image quality. In this also describes the method to improve the quality of the output image.

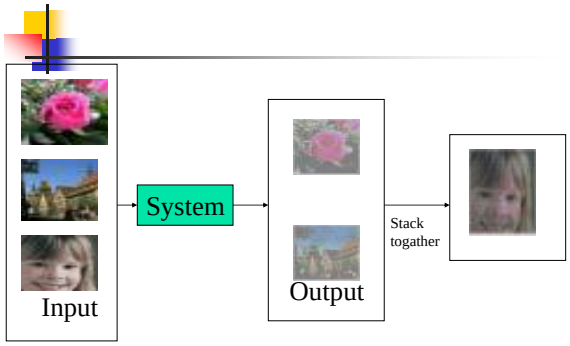


Figure- 2 The basic idea of the proposed system.

Hou[3] has proposed the binary visual cryptography scheme which is applied to gray level images, that a gray level image is converted into halftone images in the year 2004. The method that uses the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before processing.

According to this first transformed the gray level image into a halftone image and then generated two transparencies of visual cryptography. Obviously we indeed cannot detect any information about the secret image from the two sharing transperencies individually, but when stacking them together, the result clearly shows a picture.

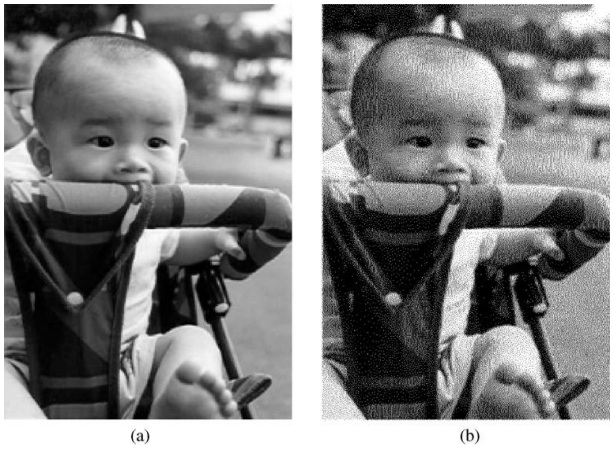
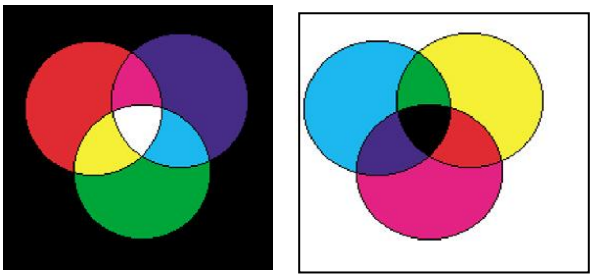


Fig. 4. (a) Continuous tone, and (b) Halftone

Hou[3] shares generated by applying halftone methods and colour decomposition. He decomposed the colour image into three (yellow, magenta and cyan) halftone images and then improvised three coloured 2-out-of-2 VC schemes which follow the subtractive model. Thus in the (C,M,Y) representation (0,0,0) represents full white and (255,255,255) represents full black.
R



Additive Model (R,G,B) **Substractive Model (C,Y,M)**

The earlier methods in VC, however, the colour schemes for 2-out-of-2 secret sharing where the reconstructed colours are interpreted by some mixing rules of colours. For colour shares the general construction of a k-out-of-n VC scheme was first introduced by Verheul All of these VC schemes for colour images generate random pattern shares. Even though the decrypted messages show messages with distinct colours, it is more desirable to produce meaningful shares which are less suspicious of encryption. Some other approaches to colour VC aiming to generate meaningful colour shares.

In 2006 the Zhi Zhou, Gonzalo, R.Arce and Giovanni Dicrescenzo [4] have proposed halftone visual cryptography which produce good high quality and meaningful halftone shares, the generated halftone shares contain the visual information. In halftone visual cryptography a secret binary pixel „P" is encoded into an array of Q1 x Q2 („m" in basic model) sub pixels, referred to as halftone cell in each of the „n" shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained and also maintained contrast and security. Based on the blue noise dithering principles the proposed method utilizes the void and cluster algorithm. Abhishek parakh and Subhash Kak have proposed recursive threshold visual

cryptography which is used in network applications and also reduce the network load.

In 2009 the Inkoo Kang,, Gonzo R. Arce,, and Heung-Kyu Lee [5]have proposed the Visual Cryptography for color image using visual information pixel (VIP) synchronization with error diffusion technique. They are introduced a color Visual Cryptography encryption method which leads to significant shares and is free of the previously mentioned limitations. This method is used to filtering the error in an image and produces the meaningful shares. The error filtering schemes for color images is very simple and efficient method.

In 2010 Chandramathi [6]proposed an overview of Visual Cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. In this paper we provide an overview of the emerging Visual Cryptography (VC) and related security research work done in this area.

1. Visual cryptography for general access structures.
2. Visual cryptography for gray level images.
3. Recursive Threshold visual cryptography.
4. Extended visual cryptography for natural images.
5. Halftone visual cryptography.
6. Visual cryptography for color images. .
7. Progressive color visual cryptography.
8. Regional incrementing visual cryptography (RIVC).
9. Segment based visual cryptography.

In 2010 Anantha Kumar Kondra, Smt. U.V. Ratna Kumari proposes " An Improved (8,8) Colour Visual Cryptography Scheme using Floyd Error Diffusion[7]. Which introduce a new solution helps to identify the error in the shares and to verify the authentication.

In 2011 S. Kandar, Maithi and Dhara [8]proposes a visual cryptographyic scheme for color images where the divided shares are envolped in other images using invisible digital watermarking. The shares are generated using random number.
Like other multimedia components, image is sensed by human. Pixel is the smallest unit constructing a digital image. Each pixel of a 32 bit digital color image are divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency.

A 32 bit sample pixel is represented in the following Figure.

11100111 11011001 11111101 00111110

Alpha Red Green Blue

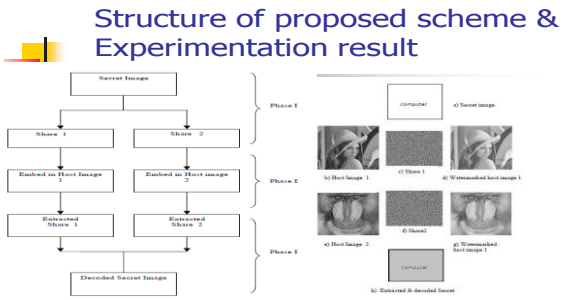
Fig3: Structure of a 32 bit pixel

To add more security to this scheme a technique called digital enveloping is used. This is nothing but an extended invisible digital watermarking technique.

In 2011 Mrs. Bhandare Shital, Mr. Jhade Manoj & Mrs. Jadhav Angarika [10] introduces An improved approach for Extended Visual Cryptography Scheme for Colour Images.

Visual Cryptography is an image encryption technique used to hide the secure information in images. It allows the encryption of secret image into *n* number of shares and distributed into *n* number of participants. For example in (k, n) secret sharing problem the secret image can be visually recover by stacking together any k or more transparencies of the shares. But cannot reveal any secrete information by stacking less thank transparencies together. The Embedded EVCS is constructed by adding random shares of secret image into meaningful covering images.

A visual cryptographic technique to secure Image shares by Jagdeep Verma in 2012[9] proposes an approach for embedding visual cryptographically generated image shares in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images.



In 2012 Tripta Deendayal & Ch.Sunitha [11] introduces Enhanced Visual Cryptography Using color Error diffusion and Digital Watermarking.

A new visual cryptography scheme is proposed for hiding information in images which divide secret images into multiple shares. In order to provide more security to existing schemes a new Technique called Digital Watermarking is used,and to improve the quality and size of images obtained color error diffusion technique is used .secret information can be retrieved by stacking any k number of decrypted shares. which reduces the color sets that renders the halftone image and chooses the color whose brightness variation is minimal.

In 2012 Dr.D.Vasumathi1 M.Surya Prakash Rao, M.Upendra Kumar3 Dr.Y.Ramadevi4 Dr.R.Rajeswapra Rao[12] introduces Novel Approach for Color Extended Visual Cryptography Using Error Diffusion. Error-diffusion scheme that produces higher quality results. The error filter employed in the error diffusion also affects the share quality. An error filter with longer weight leads to high contrast of encryption shares. The algorithm is faster than the universally used Floyd-Steinberg algorithm, while maintaining its original simplicity.

III. Performance Analysis of Visual Cryptography Schemes

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [1] suggested two main parameters: pixel expansion m and contrast α. Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast α is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

Accuracy is considered to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR) measure. Computational complexity concerns the total number of operators required both to generate the set of n shares and to restructure the original secret image C.

The meaningful shares generated in Extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. Also maintains contrast and security.

Colour constrast is improved in VIP synchronization. The watermarked images possess good Peak Signal to Noise Ratio (PSNR) and good visual quality.

From above literature some of them advised security, pixel expansion, accuracy and computational complexity as a performance measures. Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected. Visual cryptography scheme should support wide image format like color and gray scale. Author also argued that random looking shares appear to be suspicious and thus are vulnerable to attacks by attackers in the middle, to fill in this security gap, meaningful shares should be produced. VCS should support multiple secret to work efficiently. If scheme support only one secret to share at a time to share multiple secret images numerous share have to be generated, transmitted and maintained.

Table 1. Comparison of visual cryptography schemes on the basis of number of secret images, pixel expansion, image format, type of share generated.

Sr. No.	Authors	Year	Number of Secret images	Expansion	Image Format	Type of Share generated
1.	Naor and Shamir	1995	1	4	Binary	Random
2.	Nakajima	2002	1		Binary	Meaningful
3.	Young-Chang Hou	2003	1	4	Color	Meaningful
4.	Z. Zhou	2006	1	4	Binary	Meaningful
5.	Inkoo Kang,	2009	1	4	Color	Meaningful
6.	Jagdeep Verma, Dr.Vineeta	2012	1	4	Color	Meaningful
7.	Dr.D.Vasumathi1 M.Surya Prakash Rao2 Rao5	2012	1	4	Color	Meaningful

m indicate pixel expansion of corresponding visual cryptography schemes, c number of colors in visual cryptography schemes, n is the number of shares. As shown in the Table 1 shows visual cryptography schemes with pixel expansion. If m>1 large storage space required to store and transmit the shares. Schemes with m=1 are good candidate for secure transmission over limited bandwidth communication networks. Meaningful shares can be helpful to avoid attacks by hacker. Scheme supporting color images are useful in the multimedia environment. Less overhead for storage and transmission is required to share multiple secrets while using the scheme. In order to hide secrecy we go for expansion and increasing of the number of shares, but this affect the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in VC is towards maintaining the contrast at the same time maintaining the security.

IV. Conclusions

Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. The decoded secret image quality is improved. Yet many possible enhancements and extensions can be made to improve further.

References

[1] M. Noar and A. Shamir, "Visual cryptography," Advances in Cryptology - EUROCRYPT'94, pp. 1-12, 1995.

[2] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography for Natural Images"

[3] Young-Chang Hou, "Visual cryptography for color images," Pattern Recognition, Vol. 36, No. 7, pp. 1619-1629, 2003.

[4] Z. Zhou, G.R. Arce and G. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, No. 8, pp. 2441-2453, 2006.

[5] Inkoo kang, G.R. Arce, and H.K. Lee, "Color Extended Visual Cryptography using Error Diffusion," 2009.

[6] Chandramati S., Ramesh Kumar R. , Suresh R. and Harish S., " An overview of visual cryptography" issue 2010.

[7] Anantha Kumar Kondra, Smt. U.V. Ratna Kumari , " An Improved (8,8) Colour Visual Cryptography Scheme using Floyd Error Diffusion. Vol.2 2010.

[8] S. Kandar, Maithi and Dhara , "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking,"2011.

[9] Jagdeep Varma, Dr. Vineeta Khemchandani, "A Visual Cryptographic Technique to Secure Image shares" Feb. 2012.

[10] Sagar Kumar Nerella, Kamalendra Varma Gadi, Raja Skhar Chaganti , " Securing Images Using Colour Visual Cryptography and Wavelets", volume 2, March 2012.

[11] Dr. S. Vasumathi, M. Surya Prakash Rao, M. Upendra Kumar, ''Novel Approach for color Extended Visual Cryptography Using Error Diffusion" volume 3, 2012.

[12] Tripta Deendayal, Ch. Sunita, "Enhanced Visual Cryptography using Color Error Diffusion and Digital Watermarking", Vol.3, 2012.

[13]

AUTHORS

First Author – Archana B. Dhole, IIIrd Sem. M.Tech (C.S.E.), Email: archana_ajmire@rediffmail.com

Second Author – Prof. Nitin J. Janwe, Department of Computer Science & Engg. , Email: nitinj_janwe@yahoo.com