International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 03 | March -2019 e-ISSN: 2395-0126

Various Visual Secret Sharing Schemes- A Review

Mrunali T. Gedam
Department of Computer Science and Engineering
Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, India

Vinay S. Kapse
Department of Computer Science and Engineering
Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, India

***Abstract*— Visual cryptography is a new technique which provides information security by using simple algorithm instead of the complex algorithms. Aim to focuses on the encryption techniques that are used in each scheme. 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 lot of computational power. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image.**

Keywords- Contrast, Shares, Pixels, Secret sharing, stacking

I. INTRODUCTION

With the coming era of the internet more and more multimedia data are transmitted and exchanged on the network system with rapid speed. In electronic commerce there is a need to solve the problem of ensuring information safety in today‟s increasingly open network environment. The encryption is a very important field in the present era in which information security is an important issue in communication and storage of images, the encrypting technologies of traditional cryptography are used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images.

Visual Cryptography is a new Cryptography technique which is used to secure the images. this technique divided the image into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image.

The basic principles of Visual Cryptography, each pixel of secret binary image are cryptographically encoded into m black and white subpixel in each share. If secret image pixel is white, this white pixel encode with a set of four subpixel each subpixel has equal probability it contains two of them white and two of them black, thus, the subpixel set gives no clue as the original value of pixel. When a decrypted subpixel has two white and two black pixels indicate that the decoded pixel is a white. On the other hand a decrypted subpixel having four black pixels indicates that the decoded pixel is black.

RELATED WORK

Several new methods for VC have been introduced recently in the literature.

Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir [1] proposed a k-out-of-n scheme of visual cryptography, a secret binary image is encoded in to n shares and distributed amongst n participants, one for each participant. No participant knows the share given to another participant. By stacking the k shares decode the secret image. Less than k shares cannot be decoded by secret image

Ateniese [2] proposed a more general method for VC scheme based upon general access structure. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants of forbidden subset cannot recover secret image.

Chang-Chou Lin, Wen-Hsiang Tsai [3] proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub-pixels directly to constructed shares, a dithering technique is used to convert gray level images into binary images and a visual cryptography method for binary images is then applied to the resulting dither image. The advantages of this scheme reduce the size of image in ordinary situations. The decoded images can reveal most details of original images.

M. S. Fu and O. C. Au, [4] proposed Joint visual cryptography and watermarking (JVW) algorithm. In this paper use a watermarking technique for visual cryptography. Both halftone watermarking and visual cryptography involve a hidden secret image. For visual cryptography secret image encoded into shares, more shares are required to decode the secret image. For watermarking secret image embedded into watermark halftone image. The (JVW) algorithm has the merits of visual cryptography and watermarking. It embeds the hidden pattern in two high visual quality halftone share images to prevent from hackers. Both shares must be required to extract the secret image.

C. S. Hsu and Y. C. Hou [5] proposed a copyright protection scheme for digital images based on visual cryptography and sampling method. This method can register multiple secret images without altering the host image and can identify the rightful ownership without resorting to the original image.

Nakajima [6] proposed extended visual cryptography for natural images constructs meaningful binary images as shares. This will encode secrets image more securely in to a shares and also describes the contrast enhancement method to improve the quality of the output images.

Zhou et al. [7] used halftoning methods to produce good quality halftone shares in VC. In halftone visual cryptography a secret binary pixel is encoded into an array of Q1 x Q2 sub pixels, is called as halftone cell, in each of the „n" shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

E. Myodo [8] proposed a method to generate meaningful halftone images using threshold arrays.

Hou [9] proposed a new approach on visual cryptography for colored images. In this paper two techniques used halftone technology and color decomposition for both gray-level and color visual cryptography. In color decomposition, every color on a color image can be decomposed into three primary colors: C, M, and Y. With the halftone technology, we can transform a gray-level image into a binary image. This method expand every pixel of a color secret image into a 2×2 block in the sharing

images and keep two color and two transparent pixels in the block.

Wang et. al. [10] produced halftone share images by using error diffusion techniques. This scheme generates more pleasing halftone shares and diffused errors to neighbor pixels.

Jin, D., Yan, and Kankanhalli [11] proposed a new encoding method that transform gray-scale and color images into monochrome image without loss of any information. This new encoding scheme allows perfect recovery of the secret grayscale or color image.

V. Rijimen [12] presented a 2-out-of-2 VC scheme by applying the idea of color mixture. Stacking two shares with different colors rises a third mixed color.

Koga and Yamamoto [13] used a lattice structure to define the mixing result of arbitrary two colors. It is more desirable to generate meaningful shares which are less suspicious of encryption.

III. PRELIMINARIES

In this section, we give a brief description of VC, color models in VC and error diffusion.

A. Fundamentals of VC

Visual cryptography scheme encrypts a secret message into shares to be distributed to participants. By stacking the sufficient numbers of shares reveal the secret image. A black and white (k,n) VC scheme consists of two collections of binary matrices and, having elements 0 for a black pixel and 1 for a white pixel. To encrypt a white (black) pixel, a user randomly chooses one of the matrices and distributes its rows to the participants.

B. Color Models

The additive and subtractive color models are widely used to describe the constitutions of colors. In terms of RGB model, each color is mixed with red, green, and blue, which are the three primary colors of light. This model is commonly used for on-screen display. Therefore, RGB model is also called additive model. On the other hand, CMY model is called subtractive model. For CMY model, each color is mixed with cyan, magenta, and yellow, which are the three primary colors of pigments. This model is commonly used for color printing.

IV. ENCRYPTIONAND DECRYPTION PROCESS

1. Pre-Processing

In Preprocess scan the input image for increase intensity of image, image enhancement and avoid the illumination problems by using threshold method.

2. Halftone Conversion

The general printer, such as dot matrix Printers, laser printers, and jet printers, can only control single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the color tone of an image directly. As such, the way to represent the gray level of images is to use the density of printed dots; Transform the continuous-tone image into a binary image is called halftoning. The main idea of halftoning is utilize the density of Printed dots to simulate the grey scale of pixels. For human eyes, the denser the dots are, the darker the image and sparser dots are lighter the image.

3. Creation of Shares

Visual cryptography technique encrypts a secret image into shares; the shares are usually presented in transparencies. The basic matrices S0 and S1 are used for generate the shares.

4. Error diffusion

Error diffusion is a neighborhood operation that quantizes the current input pixel and

then transfers the quantization error onto future input pixels. The color error diffusion methods reduces the color sets that render the halftone image and chooses the color from sets by which the desires color may be rendered and whose brightness variation is minimal. The Error diffusion technique is a dispersed dot dither method. In this method for each point in the image find the closest color available and calculate the difference between the value in the image and the color.

5. Stacking of Shares

In the decryption process the color image channels are reconstructed by stacking the shares of channels. The stacking (OR) operation is performed between the shares, to recover the secret image.

6. Post-processing

The stacked shares results in an image where the some pixels will show the required information. But other pixels are randomly distributed. To avoid this noise, the technique of post-processing is applied on this image.

V. COMPARATIVE ANALYSIS

This Part compares the features of some of the visual secret sharing schemes that were analyzed and studied in the literature. The Table.1 depicts the comparison between some of the VSS schemes focusing mainly on their encryption technique and their advantages and limitation.

Technique	Characteristics	Advantages	Limitations
k-out-of-n scheme	A secret image is encoded into n shares and shares are distributed into n participants	provide security of binary images	secret cannot be decoded by any or fewer participants shares.
	shares are required to decode the image.		
General access Structure	Access structure is a specification of all qualified and forbidden subsets of „n" shares	general access structure is better for pixel expansion	only qualified shares decrypt the secret image not forbidden shares
Dither technique	This technique is used to convert gray level image into binary.	This technique increase in size& quality of o/p image	this scheme is not useful for color images
Extended VC for natural images	it construct meaningful binary images as shares	it suitable for natural images	It generate meaningful shares but its quality poor
void & cluster halftone technique	for halftone images threshold array use generated by void & cluster method.	The high quality share images & high speed of processing	It is not useful of color images
Color Decom-Position And Halftone Technique	Color image decompose into three primary color& the halftone technology transform gray-level image into binary	it decrease the pixel expansion & provide better quality due to binary representation of color of pixel	Contras loss on decrypted images loss the information due to halftone Process.

VI. CONCLUSION

This paper does analysis of different visual cryptography scheme and a comparative study has been done. In order to hide the secret information we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore, an optimum number of shares are required to hide the secret information. There are different kinds of visual secret sharing techniques are used. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveal secret image.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT*, 1994, pp. 1–12.

[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, pp. 86–106, 1996.

[3] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, pp. 349–358,2003.

[4] M. S. Fu and O. C. Au, "Joint visual cryptography and Watermarking," in *Proc. IEEE Int Conf. Multimedia Expo*, 2004, pp. 975–978.

[5] C. S. Hsu and Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Opt.Eng.*vol.44, p.077003, 2005.

[6] M. Nakajima and Yamaguchi, "Extended VC for natural images," *J. WSCG*, vol. 10, no. 2, 2002.

[7] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 18, no. 8, pp. 2441–2453,Aug. 2006.

[8] E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in *Proc. IEEE Int. Conf. Image Process.*, 2006, pp. 97–100.

[9] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, pp. 1619–1629, 2003

[10] 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. 2009.

[11] Jin, D., Yan and Kankanhalli, M.S.,Progressive color visual cryptography. J. Electron. Imaging. v14.

[12] V. Rijimen and B. Preneel, "Efficient color visual encryption for shared colors of benetton," presented at the Proc. Eurocrypto Rump Session, 1996 [Online].

[13] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fundamentals*, vol. E81-A, no. 6, pp. 1262–1269, Jun. 1998.

[14]] R. A. Ulichney, "Dithering with blue noise," *Proc. IEEE*, vol. 76, no. 1, pp. 56–79, Jan. 1988.

[15] R. Lukac and K. N. Plataniotis, "Colour image secret sharing," *Electron. Lett.*, vol. 40, no. 9, pp. 529–531, Apr. 2004.

[16] C. N. Yang and T. S. Chen, "Visual cryptography scheme based on additive color mixing," *Pattern Recognit.*, vol. 41, pp. 3114–3129, 2008.

[17] D. L. Lau and G. R. Arce, *Modern Digital Halftoning*. New York: Marcel Dekker, 2001

[18] D. L. Lau, G. R. Arce, and N. C. Gallagher, "Digital halftoning by means of green-noise masks," *J. Opt. Soc. Amer. A*, vol. 16, no. 7, pp. 1575–1586, Jul. 1999.

[19] D. L. Lau, G. R. Arce, and N. C. Gallagher, "Digital color halftoning with generalized error diffusion and multichannel green-noise masks," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 923–935, 2000.

[20] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognit.*, vol. 39, no. 5, pp. 866–880, May 2006.