International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 4, Issue 5, Sep. 2016, pp.1006-1009, ISSN 2278 -1412

A Review of Secret Share Design for Color Image Using Visual Cryptography Scheme and Halftone

Surabhi Tiwari[1], Neetu Sharma[2], Paresh Rawat[3]
[1]*MTech Scholar, DC (ECE), TIEIT Bhopal (RGPV), tiwari.surabhi177@gmail.com, India;*
[2,] *AP, ECE, TIEIT Bhopal (RGPV), neetusharma85@gmail.com, India;*
[3,] *HOD, ECE, TIEIT Bhopal (RGPV), parrawat@gmail.com, India;*

Abstract *–A Review of the Secret Share Design for Color Image Using Visual Cryptography Scheme and Halftone technique are proposed. In this paper visual cryptography method are used for the encoding a secret binary image (SI) into shares of random binary sample. Visual cryptography (VC) may be a secret sharing scheme of decomposing a secret image into n transparencies, and the stacking of several t out of n transparencies reveals the secret content. The binary patterns of the N shares, however, don't have any visual which means and hinder the objectives of visual cryptography.*

Keywords*: Visual cryptography, Gray image,*

I. Introduction

VISUAL cryptography (VC) could be a branch of secret sharing information. Within the VC scheme, a secret image is encoded into transparencies, and therefore the content of every transparency is noise-like so the secret info can't be retrieved from anyone transparency by means of human being optical examination or signal examination procedure. In general, a -threshold VC scheme has the subsequent properties: The stack of any out of which VC generated transparencies will reveal the secret by visual perception, however the stacking of any or fewer number of transparencies cannot retrieve any information other than the size of the secret image. Naor and Shamir [1] projected a –threshold VC scheme based on basis matrices, and therefore the model had been additional studied and extended. The connected works embody the VC schemes supported probabilistic models [2]–[4], general access structures [5], [6], VC over halftone images [7], [8], VC for color images [9], cheating in VC [10], [11], the general formula of VC schemes [12], and region incrementing VC [13]. Contrast is one amongst the vital performance metrics for VC schemes. Generally, the stacking revelation of the secret with higher contrast represents the higher visual quality, and thus the stacking secret with high contrast is that the goal of pursuit in VC styles. Naor and Shamir [1] outline a contrast formula that has been wide employed in several studies. Supported the definition of contrast, there are studies attempting to achieve the contrast bound of VC scheme [4].

The probabilistic model of the VC scheme was first begin by Ito et al. [2], where the design is based on the basis matrix, however only one column of the matrix is elected to set a binary secret pixel, rather than the conventional VC scheme make use of the complete basis matrices. The size of the generated transparencies is identical to the secret image. Yangs also proposed a probabilistic model of VC scheme, and therefore the 2 cases and are explicitly created to realize the optimal contrast. Based on yang, Cimatoet al. projected a generalized VC scheme within which the pixel expansion is between the probabilistic model of VC scheme and therefore the traditional VC scheme. Encrypting a picture by random grids (RGs) was 1st introduced by Kafri and Keren in 1987. A binary secret image is encoded into 2 noise-like transparencies with a similar size of the initial secret image, and stacking of the 2 transparencies reveals the content of the secret. Comparison RGs with basis matrices, one among the most important benefits is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme isn't based on the basis matrices. The recent studies include the RG for color image RG, and RG schemes

II. Literature Survey

Sian-Jheng Lin et. al [1] "1) A Probabilistic Model Of Visual Cryptography Scheme With Dynamic Group", In this paper proposed a VC scheme with flexible value of. From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which

reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of VC with unlimited. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic model is adopted in the scheme. As the results listed in Table I, the proposed scheme also provides the alternate verification for the lower bound proved by Krause and Simon [20]. For , the contrast is very low so that the secret is visually insignificant. Therefore, in practical applications, the values of 2 or 3 for are empirically suggested for the proposed scheme.

Haibo Zhang et. al [2] "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Blocks Size", Multi-pixel encoding is an emerging method in visual cryptography for that it can encode more than one pixel for each run. However, in fact its encoding efficiency is still low. This paper presents a novel multi-pixel encoding which can encode variable number of pixels for each run. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image. The proposed scheme can work well for general access structure and chromatic images without pixel expansion. The experimental results also show that it can achieve high efficiency for encoding and good quality for overlapped images.

Zhi Zhou et. al [3] "Halftone Visual Cryptography", Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography [1] was proposed recently to construct meaningful binary images as shares using hyper graph colourings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via half toning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm [2] to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual qualities of the obtained halftone shares are observably better than that attained by any available visual cryptography method known to date.

Wei-Qi Yan et. al [4] "Visual Cryptography For Print And Scan Applications", Visual cryptography is not much in use in spite of possessing several advantages. One of the reasons for this is the difficulty of use in practice. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to print shares on paper in which case scanning of the share is necessary. The print and scan process can introduce noise as well which can make the alignment difficult. In this paper, we consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the vulnerabilities in the spatial domain, we have developed a frequency domain alignment scheme. We employ the Walsh transform to embed marks in both of the shares so as to find the alignment position of these shares. Our experimental results show that our technique can be useful in print and scan applications.

Ming Sun Fu et. al [5] "Joint Visual Cryptography And Watermarking", In this paper, we discuss how to use watermarking technique for visual cryptography. Both halftone watermarking and visual cryptography involve a hidden secret image. However, their concepts are different. For visual cryptography, a set of share binary images is used to protect the content of the hidden image. The hidden image can only be revealed when enough share images are obtained. For watermarking, the hidden image is usually embedded in asingle halftone image while preserving the quality of the watermarked halftone image. Inthis paper, we proposed a joint Visual-cryptography and watermarking (JVW) algorithm that has the merits of both visual cryptography and watermarking.

R.Youmaran et. al [6] "An Improved Visual Cryptography Scheme For Secret Hiding", Visual Cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

III. Method

The work is basically on Visual cryptography Scheme in which half tone is applied .The main aims to encode transparencies and the content of each transparency is noise like so that secret information cannot be retrieved from any one transparency via human visual observation or signal analysis.

III .1. Visual Cryptography Schemes

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to been crypted in such a way that the decryption can be performed by the human visual system, without the aid

of computers. Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares disclosed no info about the original image. every share was printed on a separate transparency, and decryption was performed by overlaying the shares. once all n shares were overlaid, the initial image would appear. Using a similar idea, transparencies can be used to implemental one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence.

III .2. Halftone Visual Cryptography

The main idea of halftoning is to 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 is; on the contrary, the sparser the dots are, the lighter the image is. For example, if the black dot densities of two areas with same size are 90% and 50% respectively, the human visual system can perceive the difference between them: the former is darker than the latter and the latter lighter than the former. Therefore, we can learn that the black dotdensity can simulate the gray-scale value of an area. Just by dominating the black dot density of an area, halfoning transforms a continuous-tone image into a binary one.

The meaningful shares generated in extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI [5] was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. 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. Also maintains contrast and security.

III .3. GRAY Images

The development of an algorithm to encrypt binary images, they were also aware of the eventual need to encrypt gray and color images. In the last section of their paper, they proposed a technique which involved printing each of the pixels in an image as half black - half white circles. This allowed the rotation angle of the corresponding circles to vary and which would reveal a range of gray tones throughout the overlapped shares. If the rotation angle of the first share pixel is chosen at random, then the relative change in rotation of the corresponding share pixels would result in uniformly gray shares with no information about the original image being revealed.

IV. Conclusion

This paper has reviewed the mainly latest research trends and proposed the Visual Cryptography Scheme and Halftone scheme. In this paper a design of secret shares for color images. In this paper we have presented Secret Share Design for Color Image Using Visual Cryptography Scheme and Halftone technique. In this paper a review of the proposed work is on extended visual cryptography scheme which can encrypt the secret image into meaningful cover images.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in Proc. Advances in Cryptography (EUROCRYPT’94), 1995, vol. 950, LNCS, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, “Image size invariant visual cryptography,” IEICE Trans. Fundam.Electron.,Commun., Comput. Sci., vol. 82, pp. 2172–2177, Oct. 1999.

[3] C. N. Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognit. Lett., vol. 25, pp. 481–494, Mar. 2004.

[4] S. J. Lin, S. K. Chen, and J. C. Lin, “Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion,” J. Vis. Commun. Image Represent., vol. 21, pp. 900–916, Nov. 2010.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[7] Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[8] Z. Wang, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[9] F. Liu, C. K.Wu, and X. J. Lin, “Colour visual cryptography schemes,” IET Inf. Security, vol. 2, no. 4, pp. 151–165, Dec. 2008.

[10] G. Horng, T. Chen, and D. S. Tsai, “Cheating in visual cryptography,” Designs, Codes, Cryptography, vol. 38, no. 2, pp. 219–236, Feb. 2006.

[11] C. M. Hu and W. G. Tzeng, “Cheating prevention in visual cryptography,” IEEE Trans. Image Process., vol. 16, no. 1, pp. 36–45, Jan. 2007.

[12] H. Koga, “A general formula of the -threshold visual secret sharing scheme,” in Proc. 8th Int. Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, Dec. 2002, pp. 328–345.

[13] R. Z. Wang, “Region incrementing visual cryptography,” IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009.

[14] M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes for general ," Designs, Codes, Cryptography, vol. 55, no. 1, pp. 19–35, Apr. 2010.

[15] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. DiscreteMath., vol. 16, no. 2, pp. 224–261, Feb. 2003.

[16] M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes," Designs, Codes, Cryptography, vol. 40, no. 3, pp. 255–267, Sep. 2006.

[17] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptology, vol. 12, no. 4, pp. 261–289, 1999.

[18] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," Designs, Codes, Cryptography, vol. 35, no. 3, pp. 311–335, Jun. 2005.

[19] T.Hofmeister,M. Krause, andH. U. Simon, "Contrast-optimal out of secret sharing schemes in visual cryptography," Theoretical Comput. Sci., vol. 240, no. 2, pp. 471–485, Jun. 2000.

[20] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," Combinatorics, Probability, Comput., vol. 12, no. 3, pp. 285–299, May 2003.