Analysis of Secret Share Design for Color Image using Visual Cryptography Scheme and Halftone

Surabhi Tiwari
MTech Scholar, DC (ECE),
TIEIT Bhopal (RGPV), India

Neetu Sharma
AP, ECE,
TIEIT Bhopal (RGPV), India

Neelesh Gupta
HOD, ECE, TIEIT Bhopal
(RGPV), India

ABSTRACT
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 N shares, however, have no visual meaning and hinder the objectives of visual cryptography. Visual cryptography (VC) is a secret sharing scheme of decomposing a secret image into n transparencies, and the stacking of any t out of n transparencies reveals the secret content. The perfect security condition of VC scheme requires the strict requirement where any t-1 or fewer transparencies cannot extract any information about the secret. A HVC construction method is proposed that can encode a secret halftone image into color halftone shares. The secret image is concurrently embedded into color halftone shares. In the present work CMY color model will be implemented with ((n-1), n) secret sharing scheme based on visual cryptography for the color image and compared and proved to be better that the black and white model and the RGB color model which is free from the issue of security, pixel expansion and accuracy issue as well. As the printer use the Cyan, Magenta, Yellow and Black color for printing that's why CMY color model is implemented in this work to prove that CMY color space is better than RGB color space.

Keywords
Visual cryptography, Gray image

1. INTRODUCTION
Visual cryptography (VC) may be a branch of secret sharing knowledge. in the VC scheme, a secret image is encoded into transparencies, and therefore the content of every transparency is noise-like so the key info can't be retrieved from anyone transparency via human visual observation or signal analysis techniques. In general, a -threshold VC scheme has the subsequent properties: The stacking of any out of these VC generated transparencies will reveal the secret by visual perception, but the stacking of any or fewer variety of transparencies cannot retrieve any info other than the dimensions of the secret image. Naor and Shamir [1] projected a –threshold VC scheme supported basis matrices, and therefore the model had been more studied and extended. The related works include 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 overall formula of VC schemes [12], and region incrementing VC [13]. contrast is one amongst the necessary performance metrics for VC schemes. Generally, the stacking revelation of the secret with higher contrast represents the better visual quality, and thus the stacking secret with high contrast is that the goal of pursuit in VC designs. Naor and Shamir [1] define a contrast formula that has been widely utilized in many studies. based on the definition of contrast, there are studies making an attempt to realize the contrast bound of VC scheme [4], [14]–[20]. for instance, Blundoet al. [17] provide the optimum contrast of VC schemes. Hofmeisteret al. [19] give a linear program which is able to calculate exactly the optimum contrast for VC schemes. Krause and Simon [20] provide the upper bound and edge of the optimum contrast for VC schemes. Moreover, there exist VC connected researches using differential definitions of contrast [21]–[23]. Another necessary metric is

the pixel expansion denoting the number of sub pixels in transparency used to encrypt a secret pixel. The minimization of pixel expansions has been investigated in previous studies [24], [25]. The probabilistic model of the VC scheme was 1st

introduced by Ito et al. [2], where the scheme is based on the basis matrices, however just one column of the matrices is chosen to write in code a binary secret pixel, instead of the traditional VC scheme utilizing the complete basis matrices. the dimensions of the generated transparencies is identical to the secret image. Yangs [31] also projected a probabilistic model of VC scheme, and therefore the 2 cases and are explicitly constructed to achieve the optimal contrast. based on yang [31], Cimatoet al. [32] planned a generalized VC scheme within which the pixel expansion is between the probabilistic model of VC scheme and therefore the traditional VC scheme. Encrypting an image by random grids (RGs) was initial introduced by Kafri and Keren [26] in 1987. A binary secret image is encoded into 2 noise-like transparencies with constant size of the initial secret image, and stacking of the 2 transparencies reveals the content of the key. scrutiny RGs with basis matrices, one among the main benefits is that the dimensions of generated transparencies is unexpanded. The RG scheme is comparable to the probabilistic model of the VC scheme, but the RG scheme isn't supported the basis matrices. The recent studies include the RG for color image [27], RG, and RG.

2. THEORY
Visual cryptography could be a cryptographically technique that permits visual info (pictures, text, etc.) to been crypted in such a way that the decryption are often performed by the human visual system, without the help of computers. Visual cryptography was pioneered by Moni Naorand Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares in order that only someone with all n shares could decrypt the image, whereas any n-1 shares revealed no info about the original image. every share was printed on a separate transparency, and decryption was performed by overlaying the shares. when all n shares were overlaid, the original image would appear. using a similar plan, transparencies are often used to implemental one-time pad encryption, where one transparency may be 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) so as to cipher or hide their existence.

2.1 Modules

1. Input Image modules.
2. Matrices (Black and White) Method.
3. Virtual Cryptography (VC) Method.
4. Encoding Algorithm (EA) Method.

2.1.1 Input Image Modules

Login or logon (also known as logging in or on and signing in or on) is that the process which individual access to a computing system is controlled by identification of the user using credentials provided by the user. A user will log in to a system and may then logout or logoff (perform a logout / logoff) when the access is not any longer required. logging out could also be done explicitly by the user performing some action, like as entering the appropriate command, or clicking a website link labeled as such. It also can be done by implicitly, such as by powering the machine off, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period. when logging in, in this module we have a tendency to design to take the input image for processing.

2.1.2 Matrices (Black And White) Method

The basis matrices of Virtual Cryptography scheme were 1st introduced, a white-and-black secret image or pixel is additionally represented as a binary image or pixel. In basis matrices, to encode a binary secret image, every secret pixel white black are going to be become blocks at the corresponding position of transparencies, respectively. Every block consists of sub pixels and every sub pixel is opaque or transparent. Throughout this paper, we tend to use zero to indicate a transparent sub pixel and one to point an opaque sub pixel. If any 2 sub pixels are stacked with matching positions, the illustration of a stacked pixel could also be transparent, when the 2 corresponding pixels are both transparent.

2.1.3 Virtual Cryptography Method

Proposed methodology relies on the premise matrices and therefore the idea of probabilistic model. For a (t, n) VC scheme, the "totally symmetric" type of (B0) and (B1) are both created and described as H0 and H1, respectively.

Virtual cryptography with flexible value of (n). From the sensible perspective, the projected scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, that reduces computation and communication resources needed in managing the dynamically changing user group.

2.1.4 Encoding Algorithm (EA) Method

For a given value of (t), the transparencies are often continuously generated with the Opt PrVC scheme. However, practical applications need the algorithmic rule to terminate inside finite steps. To satisfy the requirement, a finite number is used to specify the amount of transparencies within the algorithmic rule.

3. METHOD

The work is essentially on Visual cryptography scheme in which half tone is applied .The main aim is to encode transparencies and therefore the content of every transparency is noise like so secret info can't be retrieved from anyone transparency via human visual observation or signal analysis.

The original color image is taken and 3 basic colors (red, green, blue) is extracted out it. Pc creates the colors supported RGB model shown in fig.1. It produces spectrum of light. Monitor can produce many colors by combining completely different percentages of three primaries, red, green and blue. Whereas using the image process software system like Photoshop you'll see that these RGB colors are added with the help of numerical value, which is between 0 to 255. With RGB, mixing of red and green equally provides yellow, mixing of green and blue creates cyan and therefore the mixing of red and blue creates magenta. When all the 3 colors, red, green and blue are mixed equally they produces white light. Hence it's referred to as Additive color model. Another RGB model primarily based example is human eye itself and scanners. the fundamental advantage of RGB model is; it's useful for full color editing because it's wide range of colors. However at the same time this model is said to device dependent. It means that the approach colors showed on the screen depends on the hardware used to display it.

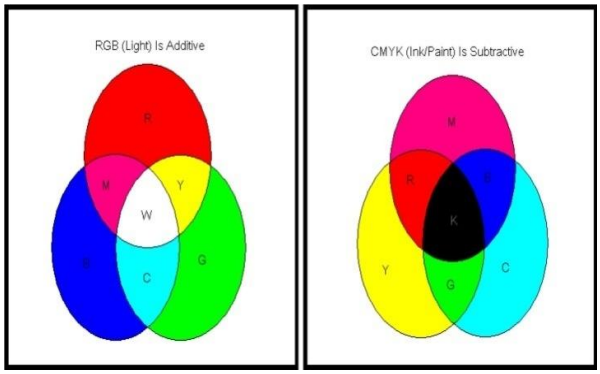


Figure 1: Van Diagram for Color Conversion

After extraction RGB is regenerate into CMY (cyan, magenta, yellow) that could be a opposite model of RGB. Printing inks are supported this model. With the complete presence of cyan, magenta and yellow we tend to get black. However practically in the printing business it's impossible to make black with these 3 colours. The result of the mixture of CMY is muddy brown due to the impurities of the printing inks. hence black ink is added to get solid black. the result of this method CMYK model and k stand for black color, that is also recognized as 'key' color. Since black could be a full presence of color, you will need to deduct the levels of cyan, magenta and yellow to supply the lighter colors. This could be explained in several means that. when light falls on the green surface or green ink. It absorbs (subtracts) all the colors from light except green. Therefore the model is termed subtractive model. Print production is based on this model.

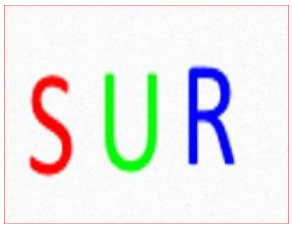
It is helpful to possess proper understanding of the color models. The monitors also as scanner works on RGB principle. Whereas scanning we'll modify the software to produce desired result. CMYK is for print business. It cannot produce the color vary of RGB thus after finishing the work on pc in RGB mode when you exchange it into CMYK for printing some tonal changes are going to be occurred. In spite of its limitation CMYK model is taken into account as best model obtainable for printing as a result of it will produce properly finished output. The projected methodology implemented is predicted to produce the enhanced quality of an image alongside the compression which is one among the limitations of existing techniques as several of them area unit

developed for compression however doesn't provide the desired quality. Within the projected work, completely different reference medical MRI image has taken that is subjected to compress the region of interest and therefore the non-region of interest by SPIHT algorithmic rule. The technique results in improved PSNR and good compression ratio in comparison to many existing methodologies. Also the compressed image by the projected algorithmic rule is more visually appealing than most of the existing ways.

4. RESULT

The proposed work is on visual cryptographic scheme. First take object (colored image) in figure 2 and extract as show in Figure 2(b). To get a red color image the existence of green and blue pixel are made null, similarly for green color image, red and blue color pixel are made null and so on. After extraction of RGB it is converted in to CMY. For CMY image segments subtracting other two colored pixel from the main image pixel (256) as show on figure 2(c).Individually halftone is applied into these segments. Through halftone, binary (grey) segments are generated since the paper [23] system is computable to binary (grey) image. Then get output as part of secret share. This share is result of VC scheme. After this choose share image for the result and append shares and get final result.

(a) Original sample image 1



(b) Gaussian noise module image

(c) Result Image

Figure2.Gaussian attack on Image 1

Table 1: Performance Analysis of Image 1

Performance	MSE			PSNR(in DB)		
	R	G	B	R	G	B
Speckle	217.24	218.17	218.54	14.7615	14.7429	14.7354
Salt & pepper	217.48	218.83	218.83	14.7560	14.7386	14.7297
Gaussian	219.34	220.32	220.46	14.7196	14.7003	14.6976

(a) Original Sample Image 2

(b) Gaussian Noise Module Image 2

(c) Result Image 2

Figure 3 Gaussian attacks on Image

It is observed from the above table 1 that sample image 1 has higher PSNR value for speckle noise module followed by salt and pepper. The PSNR value is least in Gaussian noise module.

PSNR values = Speckle noise module > salt and pepper module >Gaussian noise module

It is observed from performance analysis of input image1

Performance	**MSE**			**PSNR(in DB)**		
	R	**G**	**B**	**R**	**G**	**B**
0.02	180.84	182.94	182.26	15.5579	15.5077	15.5238
0.04	168.19	169.39	168.86	15.8729	15.8419	15.8555
0.06	160.81	162.25	161.91	16.0677	16.0289	16.0381
0.08	156.39	157.50	155.96	16.1887	16.1580	16.2005
0.10	192.01	193.43	193.08	15.2976	15.2656	15.2734

5. CONCLUSION

The proposed work is on extended visual cryptography scheme which can encrypt the secret image into meaningful cover images. Usually the shares do not carry any useful information and looks like noise. In this method the image is taken as an input and applied different type of noise on it. The noise applied on it like applied Gaussian noise, speckle noise and salt and peppers noise. For different type of noise analysis gives the different values of PSNR & MSE which is much better than previous techniques, like when speckle noise is considered then it provides MSE R (217.24) & PSNR for R (14.7615). As outcomes of the applied technique is better from the previous technique and more efficient. By stacking all the covered share images only the secret can be revealed otherwise don't. This can be an efficient way to with flexible value improve the security. This work develops a faster and easier encryption method to construct a color VC scheme with error diffusion half toning. Error diffusion half toning is used to construct the shares such that the noise introduced by the preset pixels is diffused away to the neighbors.

6. 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.