Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of Halftone Visual Cryptography Schemes

Dr. Amit Chaturvedi
MCA Deptt. Govt. Engg. College,
Ajmer, India

Imtiyaz Rehman
M.Phil Scholar,
Ajmer, India

Abstract— In visual secret sharing (VSS) schemes, a secret image can be visually revealed from overlapping shadow images without additional computations. Originally proposed by Naor and Shamir various other visual cryptographic schemes were proposed, so as to make the concept better compact and to get a better image quality concerning contrast, quality , pixel expansion and various other issues. In this paper various modes and methodologies are described in order to understand a special type of visual cryptography known as Halftone visual cryptography. Furthermore, the various techniques and types included in halftone visual cryptography are described in brief. More efforts are required to decrease the share's cross inference from other shares in the future. So, that the quality of recovered image does not degrades.

Keywords— halftone visual cryptography (HVC), visual secret sharing (VSS),error diffusion.

I. INTRODUCTION

Appropriate techniques are required to prevent illicit usage of information. Such techniques are called as Secret Sharing Schemes. G.R. Blakley and Adi Shamir, independently invented secret sharing scheme in 1979 [1,2].Visual cryptography and in general secret image sharing techniques enable distributing sensitive visual materials to involved participants through public communication channels, as the generated secure images do not reveal any information if they are not combined in the prescribed way. In visual cryptography, the decoding process is performed directly by the human eyes; while in general, the shared images need some processing to reconstruct the secret image. Visual cryptography (VC), is a paradigm for cryptographic schemes that allows the decoding of concealed images without any cryptographic computation. Particularly in a k-out-of-n visual secret sharing scheme (VSS), a secret image is cryptographically encoded into n shares. Each share resembles a random binary pattern. The n shares are then Xeroxed onto transparencies respectively and distributed among n participants. The secret images can be visually revealed by stacking together any k or more transparencies of the shares and no cryptographic computation is needed. However, by inspecting less than k shares, one cannot gain any information about the secret image, even if infinite computational power is available. Apart from the obvious applications to information hiding, the VC techniques can be applied to access control, copyright protection, watermarking, visual authentication, and identification.

II. HALFTONING VISUAL CRYPTOGRAPHY

Halftone visual cryptography uses halftoning technique to create shares. Halftone is the reprographic technique. It works as simulation of continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography [6].In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the "n" shares. If halftone cells with an appropriate size are used, visually pleasing halftone shares can be obtained. It results in good contrast and security and increases quality of the shares.

A. Random Share Creation

The encrypted message consists of black and white pixels in which each pixel appears in *n* shares, one for each transparency. The share is a collection of m black and white sub pixels. The resulting structure can be described by an [n x m] Boolean matrix S = $[s_{ij}]$ where $s_{ij}=1$ iff the j^{th} subpixel in the i^{th} transparency is black or $s_{ij}=0$ iff the j^{th} subpixel in the i^{th} transparency is white. Therefore the grey level of the combined share is obtained by stacking the transparencies in a participant subset X= $\{i_1,...,i_s\}$, is proportional to the Hamming weight w(V) of the m-vector,V=OR($r_{i1},\ldots,r_{is}$) where r_{i1} , ..., r_{is} are the rows of matrix S associated with the transparencies that are stacked. This grey level is interpreted by the visual system of the users as black or as white.

1. Halftoning Grayscale Image

Halftoning process includes conversion of a continuous-tone image (grayscale image) into a binary valued image using algorithms like Error diffusion. Using the secret image and multiple grayscale images, halftone shares are generated such that the resultant halftone shares are no longer random patterns, but only taking meaningful visual images. A secret binary pixel p is applied with visual secret sharing pixel expansion to generate γ subpixels which are generated on random basis from matrix collections C0 and C1. Then the γ subpixels are encoded into a block of the halftoned image of size q=v1*v2, referred to as a halftone cell, in each of the n shares. Error diffusion diffuses quantization error over the neighbouring continuous tone pixels using error filter.

2. Generating Halftone Shares

The technique purposed by Zhou & Arce in halftone visual cryptography [5] is used. Few main steps of the technique are:

1. Select a secret image.
2. Select a grayscale image to be halftoned.
3. Apply error diffusion using appropriate error filter and generate the halftoned image.
4. From halftoned image generate the corresponding complemented image by reversing white/black pixels.
5. The halftone image and the complemented halftone image are distributed to Participant1 and Participant2.
6. Encode the pixel *p* to v1*v2 halftone cell where only two pixels are secret information pixels and other pixels carry visual information called as *ordinary pixels.*
7. Selection of subpixels is randomly done from C0, C1 matrix where row i of a matrix is distributed to halftoned image and row j to complemented halftoned image.
8. Secret pixels are encoded to the random position in halftoned image and complemented halftoned image.

The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. The higher the PSNR the better is the visual quality of the image. The PSNR of each share, compared to original grayscale image can be estimated as

$$\boldsymbol{PSNR = 10\ loglog_{10}\left\{\frac{R^2}{MSE}\right\}}$$

where *R* is the maximum fluctuation in the input image. .MSE is Mean Squared Error with *M* and *N* are the number of rows and columns in the input images.

3. Stacking

Shares are supposed to be copied on transparencies and decoding of the secret image involves stacking the shares physically. However, both the distribution of the shares and decoding of the secret image can be performed in a digital way where the decoding rule remains the same (OR operation)

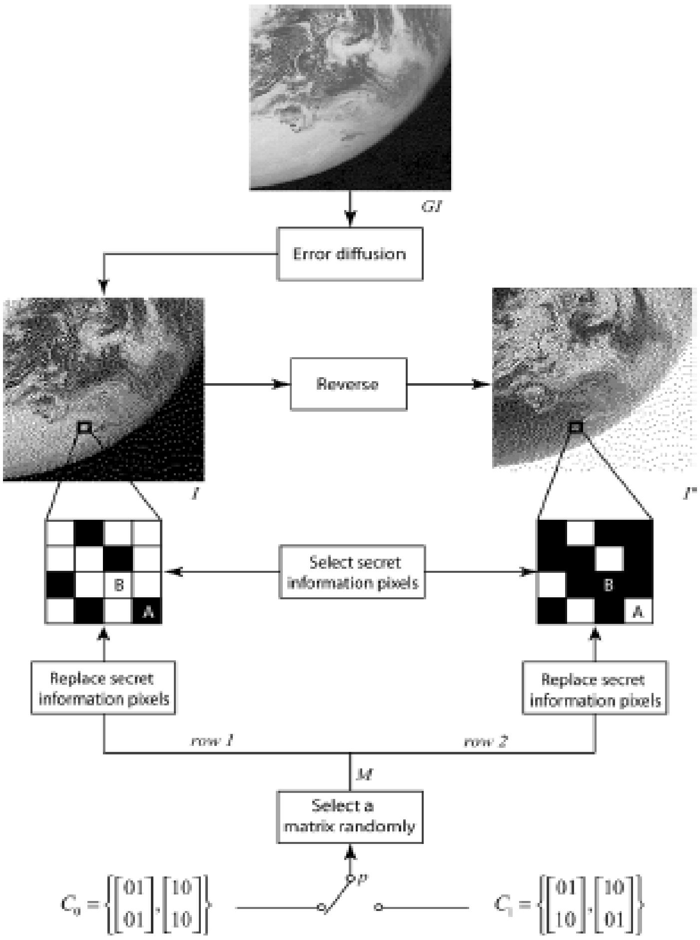

Figure 1: Construction of a two-out-of-two method. Cell size 4

B. Two-out-of-Two Halftone Visual Cryptography Method

To describe the principles of halftone VC, the simplest two out-of-two halftone visual threshold scheme is shown in Fig. 1 above. In the proposed method, a halftone image I, obtained by applying any halftoning method such as the error diffusion algorithm on a grey level image GI, is assigned to participant 1, and its complementary image I, obtained by reversing all black/white pixels of I to white/black pixels, is assigned to participant 2. To encode a secret pixel P into a Q_1 x Q_2 halftone cell in each of the two shares, only two pixels, referred to as secret information pixels, in each halftone cell need to be modified. The two secret information pixels should be at the same positions in the two shares, such as pixels and in Fig. 1. If P is white, a matrix M is randomly selected from the collection of matrices C_0 of conventional VC.

If P is black, M is randomly selected from C_1. The secret information pixels in the i-th (i=1,2) share are replaced with the two subpixels in the i-th row of M , as shown in Fig. 1. Since C_0 and C_1 are the collections of conventional VC, these modified pixels carry the encoded secret. The other pixels in the halftone cell which were not modified are referred to as ordinary pixels, maintaining halftone information. It can also be found that if P is white, one out of Q_1 x Q_2 pixels in the reconstructed halftone cell, obtained by superimposing the two encoded halftone cells, is white while all other pixels are black [see Fig. 2(a) and (b)]. If P is black, all pixels in the reconstructed halftone cell are black, as shown in Fig. 2(c) and (d). Thus, the contrast condition is satisfied. The secret pixel can be visually decoded with contrast $(1/Q_1Q_2)$

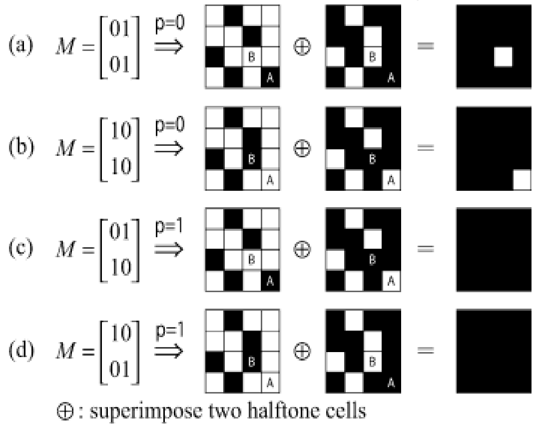

Fig. 2: Matrix M is randomly selected (a),(b) from C0 if p=0, (c), (d) from C1 if p=1 and SIPs are replace

C. Classical Halftoning:

In classical halftoning the images are represented with the following conditions:

- Use dots of varying size to represent intensities
- Area of dots proportional to intensity in image

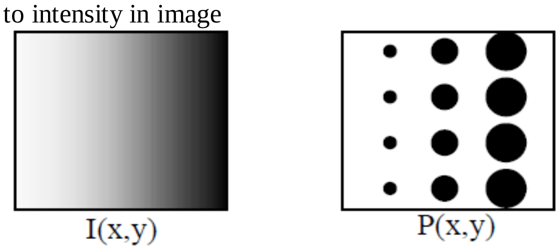

Fig. 3: classical halftoning

D. Dithering:

In dithering technique following majors are taken to represent an image:

- Distribute errors among pixels
- Exploit spatial integration in our eye
- Display greater range of perceptible intensities

Riginal(8 bits) Quantization(1 bit) Floyd-Steinberg Dither(1bit)

E. Types of Halftone Texture

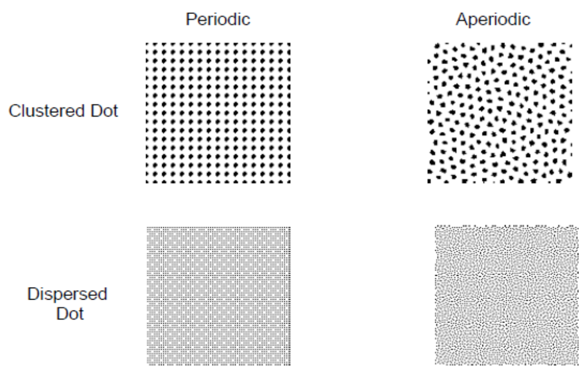

Figure 4: Halftoning types

III. RELATED WORKS

Here the model of VSS is described as a preliminary knowledge in brief. Based on this model, some schemes with reversing have been presented. They usually repeat the distribution in the VSS model for more runs and employ reversing operation during the reconstruction. Next, we review those well-known schemes with such facilities and show some simple remarks on them.

A. The Model of VSS

It is usually assumed that the secret image is composed of a collection of black and white pixels. The model of VSS consists of two phases as follows.

• ***Distribution***

At this phase, the secret image is encoded pixel by pixel into *n* shadows and then distributed to *n* participants. Generally, a pixel of the original image is encoded into *m* black and white sub pixels of each shadow. Those sub pixels are printed in close proximity to each other, so that the human visual system averages their individual black/white contributions and a gray level forms. Usually two basis matrices, *M*0 and *M*1, are required to encode the secret image. They are both $n \times m$ Boolean matrix $M = [a_{ij}]$ where $a_{ij} = 1$ if and only if the *j*-th sub pixel in the *i*th shadow is black, otherwise $a_{ij} = 0$. When encoding a white (resp. black) pixel in the secret image, the dealer randomly permutes all the columns of M_0 (resp. M_1), and then chooses the *i*-th row of the permuted matrix to fill into the corresponding positions of the *i*-th shadow. After all pixels in the secret image are encoded, *n* shadows are formed. Obviously, each shadow has the size *m* times as that of the original image. Therefore, we call the parameter m pixel expansion.

• *Reconstruction*

At this phase, any k ($\leq n$) or shadows more than *k* are stacked, and then a secret image with gray level is reconstructed. The gray level is proportional to the Hamming weight of the ORed m-vector V, which is usually denoted as H(V). This gray level is interpreted by the visual system of the users as black or as white according to certain rule of contrast. Generally, in the reconstructed image, if $H(V) \geq (m - l)$, the gray level is interpreted by our visual system as black, and $H(V) \leq (m - h)$ as white, where $m > h > l \geq 0$ [5] and *l* is the number of the whole-white columns in M_1 and means the whiteness of the black secret pixel in the reconstructed image. Especially, if $l = 0$ in a VSS scheme, a black secret pixel is totally reconstructed by *m* black sub pixels, so we call such scheme perfect black VSS (PBVSS) scheme; otherwise we call it non-perfect black VSS (NPBVSS) scheme. Here, two notations p_0 and p_1 denoting the whiteness rate of the white and black secret pixel in the reconstructed image, respectively. Therefore, there are $p_0 = h / m$ and $p_1 = l / m$; it is easily to know that there is $p_1 = 0$ in the PBVSS scheme. From the model of VSS, we know without difficulty that there is a very poor contrast in the reconstructed image. The essential reason is that a pixel in the original image becomes m pixels with a gray level in the reconstructed image

B. Viet-Kurosawa Scheme

Viet and Kurosawa proposed a new scheme based on a traditional (k, n) VSS scheme to achieve an almost ideal contrast [6]. At the distribution of this scheme, a (k, n)- PBVSS scheme is independently performed for r times. Each participant gets a shadow at each run and finally each participant gets r shadows. At reconstruction, for each run any k or shadows more than k are stacked, and then a secret image T_i ($1 \leq i \leq r$) with gray level is reconstructed from the foundational (k, n)-PBVSS scheme. Subsequently, reverse each T_i, stack them, and then reverse the stacked image too. Finally, the last rebuilt image is $\overline{\overline{T_1} + \overline{T_2} + \overline{T_3}}$. After the reversing-stacking- reversing process, namely NOT-OR-NOT operations, the contrast is improved largely [6]. Let P0 and P1 denote the average whiteness rate of the white and black secret pixel after reconstruction, respectively. If $P_0 = 1$ and $P_1 = 0$ for a VSS scheme, we call it an ideal contrast VSS Scheme. Obviously there is $P_1 = 0$ for Viet-Kurosawa scheme because this scheme is based on a PBVSS scheme. The value of P_0 after finishing r runs in Viet-Kurosawa scheme can be deduced as follows: T_1

$$P_0 = 1- (1- p_0)r$$
$$=1- (1 - h/m)^r$$

Because there are $0 < p_0 < 1$ in the foundational PBVSS scheme for each run, to achieve an ideal contrast (i.e., also $p_0 = 1$), the value of *r* needs to be infinite. It is evident that for Viet-Kurosawa scheme, the more the runs are, the more the contrast is improved. So each participant needs to hold more shadows to achieve higher resolution of the reconstructed image. As a result, Viet-Kurosawa Scheme is only an almost ideal contrast VSS scheme in practice. At the same time, it inherits the pixel expansion m and the pixel by pixel encoding method from the traditional VSS scheme.

C. Rendering Systems

The goal (destination) of an image rendering system, of which halftoning is a part, is to take device independent image date and tailor it to a target display. Figure 5 illustrates the major phases of an image rendering system: (1) filter and scale, (2) color adjust, (3) dither, and (4) color space convert.

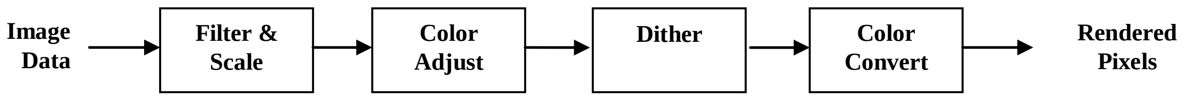

Fig. 5: Stages of an image rendering system

In the first stage, the original image data must be resample to match the target window or page size. Scaling should be independent in each dimension to allow for asymmetric pixel aspect ratios in either the source data or the target display.

A band-limiting filter should be used for reductions and an interpolating filter should be used for enlargements. Sharpening can also occur in this stage. A typical sharpening scheme can be expressed by the following equation:

$$I_{sharp}[x,y] = I[x,y] - \Psi\beta[x,y] * I[x,y]$$

where $I[x,y]$ is the input image, $\Psi[x,y]$ is a digital Laplacian filter, and "*" is the convolution operator. The nonnegative parameter β controls the degree of sharpness, with β =0 indicating no change in sharpness. When enlarging, sharpening should occur before scaling, and when reducing, sharpening should take place after scaling.

The second stage of rendering is color adjust, most easily achieved with a look-up table (LUT). In the case of color images, each color component can use a separate adjust LUT. In the case of luminance-chrominance color, an adjust LUT for the luminance component controls contrast and brightness, and LUTs for the chrominance components control saturation.

- ***Multilevel dithering***

While hard copy display products are capable of marking the color component of a pixel as either on or off, video products generate many levels. When an ordered dither array is used, such as that generated by the method of recursive tessellation, void-and-cluster, or other methods, multilevel dithering can be implemented very efficiently.

- ***Color conversion***

In the case of video rendering, a frame buffer that is expecting RGB data will not need / required to convert the color space if the source data is already represented in RGB, as is the case of graphics generation systems. However, uncompressed motion video is essentially transmitted and stored in a luminance-chrominance space. Although the chromaticity of the RGB primaries of the major video standards varies slightly, the luminance-chrominance space is always YUV. Y represents the achromatic component / part that is loosely called luminance. U and V are the chrominance components.

IV. CONCLUSIONS

The ideal contrast schemes are very significant in practice by reason of that a VSS scheme with ideal contrast is very suitable for sharing secrete images including useful information of only white, only black or both. A reversing based on a PBVSS scheme achieves really ideal contrast within only (m/h) runs where *m* and *h* are the number of the total columns and the number of the whole white columns in the basis matrix to encode white pixels respectively**,** and encodes the secret image block by block without pixel expansion. It is suitable for any access structure and also can be applied to encrypt gray-scale and chromatic images. How to design a really ideal contrast VSS scheme based on NPBVSS scheme within the runs as less as possible is a challenge future. Furthermore, more efforts are required to decrease the share's cross inference from other shares in the future.

Future researchers may work for proposing the solutions to decrease the cross interference of one share on another. So, the quality of the recovered image will be improved.

ACKNOWLEDGMENT

We are very thankful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript and whose valuable suggestions made this paper better in quality and presentation.

REFERENCES

[1] M. Naor, A. Shamir, Visual cryptography, in: Proc. of Advances in Cryptology–EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May, 1994, in: Lecture Notes in Comput. Sci., vol.950, Springer, Berlin, 1995, pp.1–12.

[2] Z. Wang, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography via error dif-fusion, IEEE Trans. Inf. Forensics Secur. 4(3) (2009) 383–396.

[3] C. Blundo, A. De Bonis, A. De Santis, Improved schemes for visual cryptography, Des. Codes Cryptogr. 24(3) (2001) 255–278.

[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for gen-eral access structures, Inf. Comput. 129(2) (1996) 86–106.

[5] F. Liu, C.K. Wu, X.J. Lin, Colour visual cryptography schemes, IET Inf. Secur. 2(4) (2008) 151–165.

[6] Y.-C. Hou, Visual cryptography for color images, Pattern Recognit. 36(7) (2003) 1619–1629.

[7] H. Luo, F. Yu, J.-S. Pan, Z.-M. Lu, Robust and progressive color image visual secret sharing cooperated with data hiding, in: Eighth International Confer-ence on Intelligent Systems Design and Applications, ISDA'08, vol.3, IEEE, 2008, pp.431–436.

[8] N. Krishna Prakash, S. Govindaraju, Visual secret sharing schemes for color images using halftoning, in: International Conference on Computational Intelli-gence and Multimedia Applications, vol.3, IEEE, 2007, pp.174–178.

[9] S.J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, K. Chen, Sharing multiple secrets in visual cryptography, Pattern Recognit. 40(12) (2007) 3633–3651.

[10] P.A. Eisen, D.R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des. Codes Cryptogr. 25(1) (2002) 15–61. H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 82(10) (1999) 2172–2177.

[11] C.-N. Yang, New visual secret sharing schemes using probabilistic method, Pat-tern Recognit. Lett. 25(4) (2004) 481–494.

[12] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, Comput. J. 49(1) (2006) 97–107.

[13] G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theor. Comput. Sci. 250(1) (2001) 143–161.

[14] M. Nakajima, Y. Yamaguchi, Extended visual cryptography for natural images, J. WSCG 10 (2002) 303–310.

[15] D. Tsai, T. Chen, G. Horng, On generating meaningful shares in visual secret sharing scheme, J. Imaging Sci. 56(1) (2008) 49–55.

[16] D. Wang, F. Yi, X. Li, On general construction for extended visual cryptography schemes, Pattern Recognit. 42(11) (2009) 3071–3082.

[17] C.-N. Yang, Y.-Y. Yang, New extended visual cryptography schemes with clearer shadow images, Inf. Sci. 271 (2014) 246–263.

[18] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 6(2) (2011) 307–322.

[19] Z. Zhou, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography, IEEE Trans. Image Process. 15(8) (2006) 2441–2453.

[20] Emi Myodo, Shigeyuki Sakazawa, and Yasuhiro Takishima. Visual cryptography based on void-and-cluster halftoning technique. In ICIP, pages 97–100,2006.

[21] Emi Myodo, Koichi Takagi, Satoshi Miyaji, and Yasuhiro Takishima. Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In ICME, pages 2114–2117, 2007.

[22] Zhongmin Wang and Gonzalo R. Arce. Halftone visual cryptography through error diffusion. In ICIP, pages 109–112, 2006.

[23] Wen-Guey Tzeng and Chi-Ming Hu. A new approach for visual cryptography. Designs, Codes and Cryptography, 27(3):207–227, 2002.

