IMPACT OF ERROR FILTERS ON SHARES IN HALFTONE VISUAL CRYPTOGRAPHY

Sunil Agrawal[1] and Anshul Sharma[2]

Department of Electronic & Communication, Panjab University, Chandigarh, India
[1]s.agrawal@pu.ac.in
[2]er.sharma.anshul@gmail.com

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 shares, however, have no visual meaning and hinder the objectives of visual cryptography. Halftone visual cryptography encodes a secret binary image into n halftone shares (images) carrying significant visual information. When secrecy is important factor rather than the quality of recovered image the shares must be of better visual quality. Different filters such as Floyd-Steinberg, Jarvis, Stuki, Burkes, Sierra, and Stevenson's-Arce are used and their impact on visual quality of shares is seen. The simulation shows that error filters used in error diffusion lays a great impact on the visual quality of the shares.

KEYWORDS

Visual cryptography, error diffusion, halftone visual cryptography, secret sharing.

1. INTRODUCTION

Secure digital imaging is an important research area combining methods and techniques coming from cryptography and image processing. 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), proposed by Naor and Shamir in [1], 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

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 139–148, 2012.
© CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2215

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. Aside from the obvious applications to information hiding, VC can be applied to access control, copyright protection, watermarking, visual authentication, and identification.

To illustrate the principles of VSS, consider a simple 2-out-of-2 VSS scheme shown in Figure 1.Each pixel *p* taken from a secret binary image is encoded into a pair of black and white subpixels in each of the two shares. If *p* is white/black, one of the first/last two columns tabulated under the white/black pixel in Figure 1 is selected. The selection is random such that each column is selected with a 50% probability. Then, the first two subpixels in that column are assigned to share 1 and the following two subpixels are assigned to share 2. Independent of whether *p* is black or white, *p* is encoded into two subpixels of black-white or white-black with equal probabilities. Thus, an individual share gives no clue as to whether *p* is black or white [1]. Now consider the superposition of the two shares as shown in the last row of Figure 1. If the pixel *p* is black, the superposition of the two shares outputs two black subpixels corresponding to a gray level 1. If *p* is white, it results in one white and one black subpixel, corresponding to a gray level 1/2. Then by stacking two shares together, we can obtain the full information of the secret image.

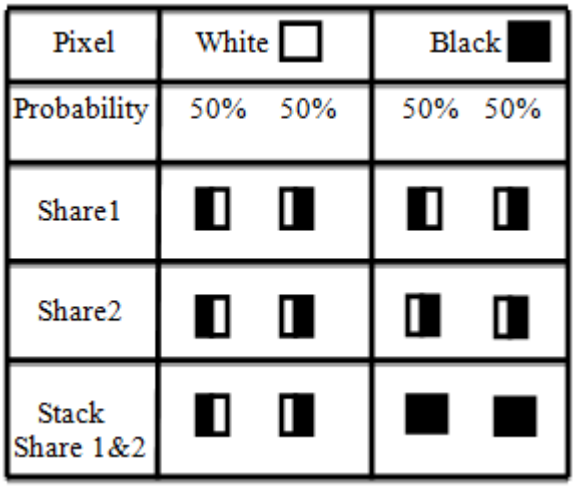
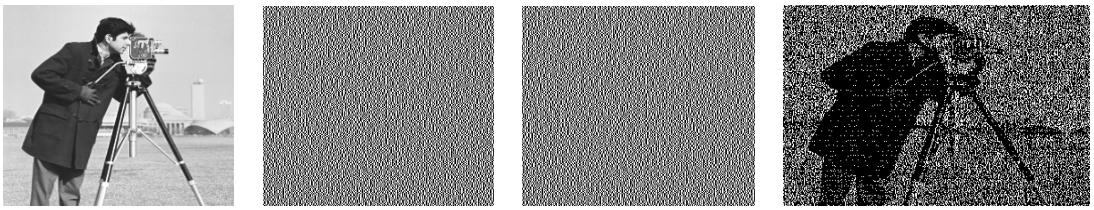


Figure 1. Construction of a two-out-of-two VC scheme: a secret pixel can be encoded into two subpixels in each of the two shares.

Figure 2 shows an example of the application of the 2-out-of-2 VSS scheme. Figure 2(a) shows a secret binary image SI to be encoded. According to the encoding rule shown in Figure 1, each pixel *p* of SI is split into two subpixels in each of the two shares, as shown in Figure 2(b) and Figure 2(c). Superimposing the two shares leads to the output secret image shown in figure 2(d).the decoded image is clearly identified, although some contrast loss occurs. The width of the reconstructed image is twice that of the original secret image since each pixel is expanded to two subpixels in each share.



2(a).Secret image 2(b).Share1 2(c).Share2 2(d).Overlapped

Figure 2 . Example of 2-out-of-2 scheme.

The two-out-of-two visual threshold scheme demonstrates a special case of *k*-out-of-*n* schemes [2]. Ateniese et al. [3] proposed *k*-out-of-*n* scheme to reduce the problem of contrast loss in the reconstructed images. The concept of access structure was developed which focused on the qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The properties of a *k*-out-of-*n* scheme including the conditions needed for optimal contrast and the minimum pixel expansion attainable can be found in [3]. The concepts of VC have been extended such that the secret image is allowed to be a grey-level image rather than a binary image [4]. Although the secret image is grey scale, shares are still constructed by random binary patterns. Zhou and Arce [5] proposed halftone visual cryptography to increase the quality of the meaningful shares based on the principle of void and cluster dithering. In this algorithm modifying the pixel in the original halftone image depends on the content of the pixel chosen and thus results in visible image residual features of the original halftone images.

Halftoning uses patterns of larger and smaller pixels in a monochrome images to give the illusion of gray i.e., process of converting a gray scale image into a binary image. Error diffusion is a method to produce higher quality images with less computation cost. Different error filters are available in error diffusion that can be used to enhance the visual quality of the shares.

2. RELATED WORK

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans without the aid of computers. The following sections provide an introduction to visual secret sharing scheme, halftone visual cryptography and error diffusion techniques.

2.1. Visual secret sharing scheme

Visual Secret Sharing is based on the access structure schemes specified as follows
k out of n Scheme:

The 2-out-of-2 VSS scheme demonstrated above is a special case of the k-out-of-n VSS scheme [1]. Ateniese et al. designed a more general model for VSS schemes based on general access structures [4]. An access structure is a specification of all the qualified and forbidden subsets of shares. The participants in qualified subsets can recover the secret image while the participants in a forbidden subset cannot.

Let p= {1,…..., n} be a set of elements called participants. A VC scheme for a set p of n participants is a method to encode a secret binary image SI into n shadow images called shares, where each participant in p receives one share. Let 2p denote the set of all subsets of p and let $\Gamma_{Qual} \subseteq 2p$ and $\Gamma_{Forb} \subseteq 2p$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \Phi$. We refer to members of Γ_{Qual} as qualified sets and call members of Γ_{Forb} forbidden sets. The pair (Γ_{Qual}, Γ_{Forb}) is called the access structure of the scheme [3]. Any qualified set of participants $X \in \Gamma_{Qual}$ can visually decode SI, but a forbidden set of participants $Y \in \Gamma_{Forb}$ has no information of SI [3]. A visual recovery for a set $X \in \Gamma_{Qual}$ consists of copying the shares given to the participants in X onto transparencies and then stacking them together. The participants in X are able to observe the secret image without performing any cryptographic computation. VSS is characterized by two parameters: the pixels expansion γ, which is the number of subpixels on each share that each pixel of the secret image is encoded into, and the contrast α, which, is the measurement of the difference of a black pixel and a white pixel in the reconstructed image [6].

2.2. HALFTONE VISUAL CRYPTOGRAPHY

Traditional VC constructions are exclusively based on combinational techniques. In the halftoning framework of VC, a secret binary image is encrypted into high quality halftone images, or halftone shares. In particular, this method applies the rich theory of blue noise halftoning to the construction mechanism used in conventional VSS schemes to generate halftone shares, while the security properties are still maintained, the decoded secret image has uniform contrast. The halftone shares carry significant visual information to the reviewers, such as landscapes, buildings, etc. the visual quality obtained by the new method is significantly better than that attained by any available VSS method known to date. As a result, adversaries, inspecting a halftone share, are less likely to suspect that cryptographic information is hidden. A higher security level is thus achieved [5]. Error diffusion algorithm [5] is used to achieve improved halftone image quality in each share.

2.3. ERROR DIFFUSION

Error diffusion is a simple, yet efficient algorithm to halftone a grayscale image. The quantization error at each pixel is filtered and fed back to a set of future input samples. Figure 3 shows a binary error diffusion diagram where *f(m,n)*represents the *(m,n)*th pixel of the input grayscale image, *d(m,n)* is the sum of the input pixel value and the "diffused" past errors, and *g(m,n)* is the output quantized pixel value [7]. Error diffusion consists of two main components. The first component is the thresholding block where the output *g (m, n)* is given by

$$g(m,n) = \begin{cases} 1, \text{ if } d(m,n) \geq t(m,n) \\ 0, \text{ otherwise} \end{cases}$$

The threshold *t (m, n)* can be position-dependent. The second component is the error filter *h(k,l)* whose input *e(m,n)* is the difference between *d(m,n)* and *g(m,n)* . Finally, we can compute *d (m, n)* as:

$$d(m, n) = f(m,n) - \sum_{k,l} h(k, l)\, e(m-k, n-l)$$

Different error filters that can be used are Floyd-Steinberg[8], Jarvis[9], Stuki[10], Burkes[11], Sierra[12] and Stevenson's-Arce[13] error diffusion filter.

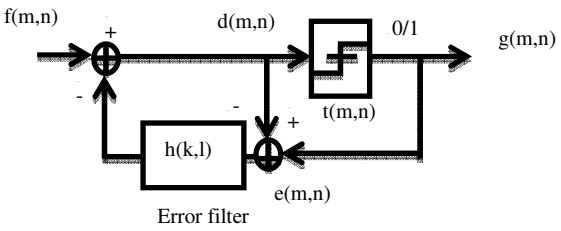


Figure 3. Error Diffusion

3. PROPOSED WORK

3.1. RANDOM SHARE CREATION

The encrypted message consists of black and white pixels. Each pixel appears in *n* shares, one for each transparency. The share is a collection of m black and white subpixels. 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},….,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.

3.2. HALFTONING GRAYSCALE IMAGE

Halftoning process converts a continuous-tone image (grayscale image)(Figure 4) 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 take 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 neighboring continuous tone pixels using error filter.

Figure 4. Grayscale image

3.3. 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 (Figure 5).

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

$$PSNR = 10\ log\log_{10}\left\{\frac{R^2}{MSE}\right\}$$

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 which is computed as follows.

$$MSE = \frac{\sum_{M,N}\{I_1(m,n) - I_2(m,n)\}^2}{M * N}$$

3.4. 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).

4. SIMULATION RESULTS

In this section examples are provided to illustrate the effectiveness of different error filters. A 2 out of 2 halftone visual cryptographic scheme is constructed. A image of size 256 x 256 is used as a secret image. A lena image of size 512 x 512 is halftoned with different error filters. This halftoned image is used as Share1 and a complement of halftoned lena image is used as Share2 (Figure 5). The pixel expansion of secret pixel is 9 times and the size of the halftoned cell is q=3. Different error filters are used to diffuse the error without affecting the secret pixels. While calculating the PSNR it is found that, higher the PSNR better the quality of the halftoned share

and more the error is diffused the better the visual quality of the image is. And finally any of the two shares can be stacked digitally to get the recovered secret image shown in Figure 6.

a1) 

a2) 

b1) 

b2) 

c1) 

c2) 

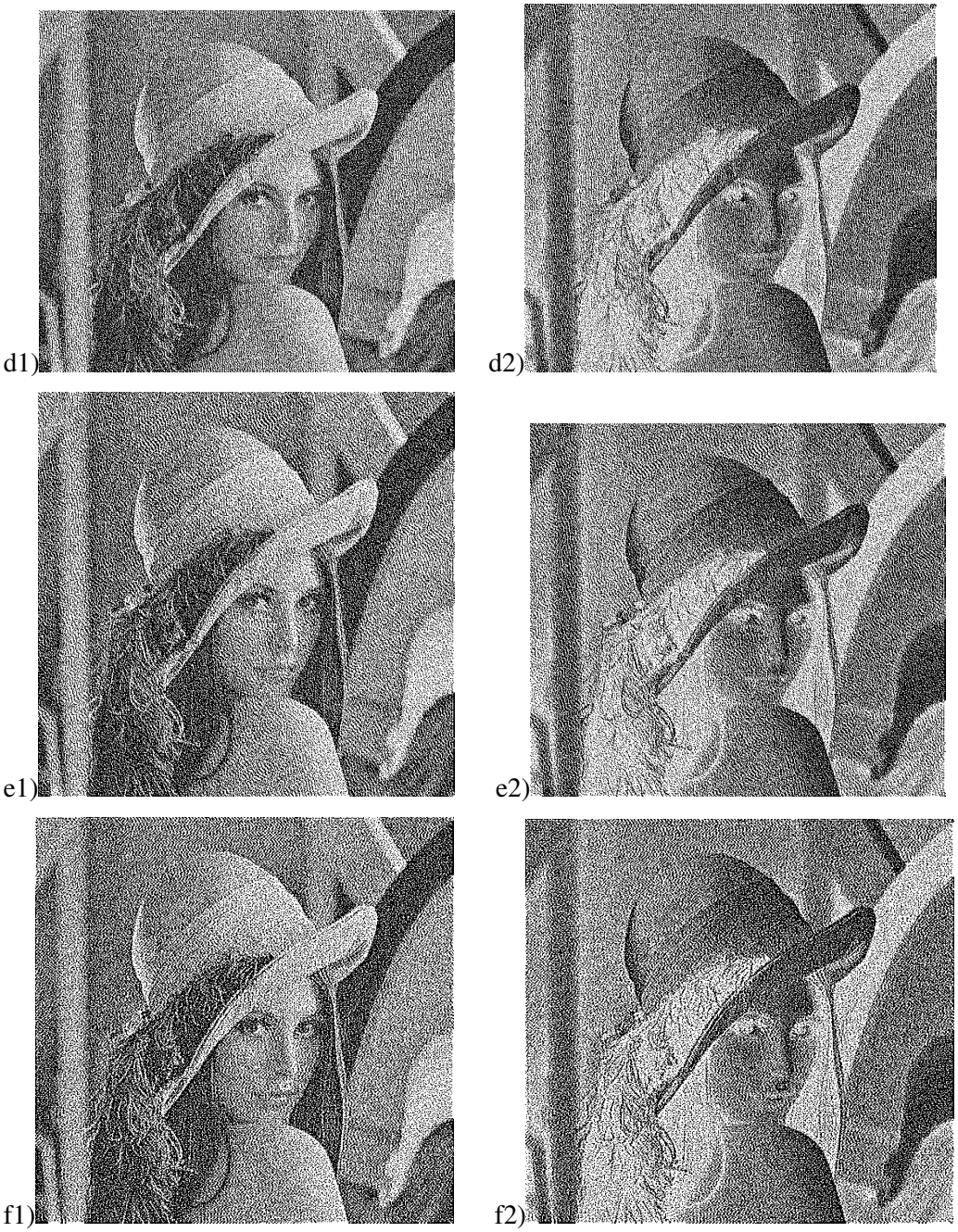


Figure 5. Impact on shares of halftone VC with different error diffusion filters .(a1), (a2),(b1),(b2),(c1),(c2),(d1),(d2),(e1),(e2),(f1),(f2) are two halftone shares of Floyd-Steinberg, Jarvis, Stuki, Sierra, Burkes and Stevenson-Arce error filters respectively.

Table 1. PSNR measures for halftone shares

Error Filter	Floyd-Steinberg	Jarvis-Judice-Ninke	Stucki	Burkes	Seirra	Stevensons Arce
PSNR	6.3957	6.4240	6.4040	6.4004	6.4147	6.4912

Figure 6. Stacked secret image

5. CONCLUSION

In this paper various error diffusion filters are applied to improve the image quality of the halftone shares. The halftoning visual cryptographic method inserts the secret information pixels into preexisting uncoded halftone shares. Visual cryptography is used along with the concept of halftoning where the continuous-tone image is first transformed into a binary image by using error diffusion and hence different error filters, and then the visual secret sharing is applied. Error diffusion has low complexity and provides halftone shares with good image quality. The recovered secret image is not so clear but the shares are of better quality means better secret hiding and hence the quality of the secret image can be traded off for better secrecy. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images. Also the more the error is distributed among the neighboring pixels the better is the error filter.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy:EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

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

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

[4] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett., vol. 75, pp. 255–259, 2000.

[5] 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.

[6] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson. Contrast optimal threshold visual cryptography schemes. SIAM J. Discrete Math.16 (2):224{261, 2003.

[7] D. L. Lau, R. Ulichney, and G. R. Arce, “Blue- and green-noise halftoning models—A review of the spatial and spectral characteristics of halftone textures,” IEEE Signal Process. Mag., vol. 10, no. 4, pp. 28–38, Jul. 2003.

[8] Floyd, R.W. and L. Steinberg, "An Adaptive Algorithm for Spatial Gray Scale." SID 1975, International Symposium Digest of Technical Papers, vol 1975m, pp. 36-37.

[9] Jarvis, J.F., C.N. Judice, and W.H. Ninke, "A Survey of Techniques for the Display of Continuous Tone Pictures on Bi-Level Displays," Computer Graphics and Image Processing, vol. 5, pp. 13-40, 1976.

[10] Stucki, P., "MECCA - a multiple-error correcting computation algorithm for bilevel image hardcopy reproduction." Research Report RZ1060, IBM Research Laboratory, Zurich, Switzerland, 1981.

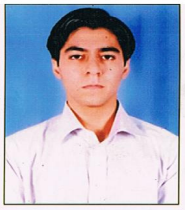
[11] Daniel Burkes, Presentation of the Burkes error filter for use in preparing continuous-tone images for presentation on bi-level devices, in LIB 15 (Publications), CIS Graphics Support Forum, September 15, 1988 (unpublished)

[12] Frankie Sierra, in LIB 17 (Developer’s Den), CIS Graphics Support Forum (unpublished)

[13] R. L. Stevenson and G. R. Arce,”Binary display of hexagonally sampled continuous-tone images,”Journal of the Optical Society of America a 2, pp. 1009{1013, July 1985}.

Authors

Sunil Agrawal received his B.E. degree in Electronics & Communication in 1990 from Jodhpur University in Rajasthan, India and M.E. degree in Electronics & Communication in 2001 from Thapar University in Patiala, India. He is Assistant Professor at the University Institute of Engineering & Technology in Panjab University, Chandigarh, India. He has 20 years of teaching experience (undergraduate and postgraduate classes of engineering) and has supervised several research works at masters level. He has 25 research papers to his credit in national and international conferences and journals. The author’s main interests include applications of artificial intelligence, QoS issues in Mobile IP.



Anshul Sharma after completing his b.tech degree in electronics and communication in 2009 is currently pursuing M.E. degree in electronics & communication from University Institute of Engineering & Technology in Panjab University, Chandigarh, India. His research interests include image processing and automotive electronics.