Performance of Error Filters on Shares in Halftone Visual Cryptography via Error Diffusion

Anshul Sharma
Department of Electronic & Communication,
Panjab University, Chandigarh, India

Sunil Agrawal
Department of Electronic & Communication,
Panjab University, Chandigarh, India

ABSTRACT
Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns. The decoding process of a visual cryptography scheme, which differs from traditional secret sharing, does not need any cryptographic algorithms like symmetric and asymmetric algorithms.Visual cryptography is based on the images and is obtained by sending pixel information and stacking of pixels for recovery of the secret image. Instead of using binary patterns of the shares, which does not give any visual meaning and hinder the objectives of visual cryptography, halftone visual cryptography via error diffusion is used that 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. Error diffusion has low complexity and provides halftone shares with good image 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 and better shares can be obtained by using complex filters without affecting the objectives of visual cryptography.

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

1. INTRODUCTION
Cryptography and image processing combines to form an important research area of Secure digital imaging and in general secret image sharing techniques that enables 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. While in traditional cryptography, the shared images need some processing to reconstruct the secret image, in visual cryptography, the decoding process is performed directly by the human eyes just by overlapping the transparencies.

In visual cryptographythe image consistsof black and white, grayscale or color images. Visual cryptography uses participates to send secret information. Itconsists of multiple party or multi-party methods. It follows many different techniques like sub pixel, errordiffusion, Boolean operation are used to specify particular method. Different technique methods are halftonevisual cryptography,watermarking visual cryptography, extended visual cryptography using complementaryshares pair, auxiliary black pixels, parallel error diffusion are also used. In this method, higher bandwidth andstorage is not required. Hence complexity decreases.

As an example of Visual secret sharing (VSS), consider a simple 2-out-of-2 VSS scheme shown in Figure 1. The secret image is divided into a number of pixels and each pixel *p* 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 randomly with 50% probability for selection of either column. Then, the first two subpixels in that column are assigned to share 1 and the following two subpixels are assigned to share 2. Each pixel *p* is encoded into two subpixels of black-white or white-black with equal probabilities in both the shares, without caring whether *p* is black or white. 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.

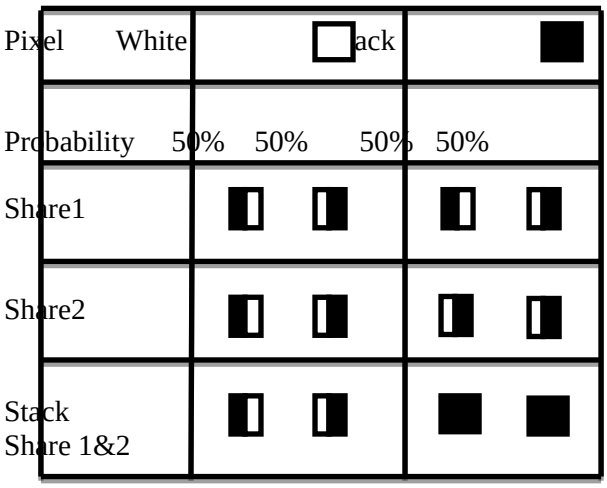
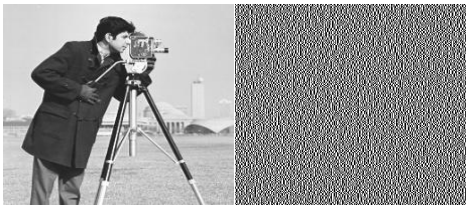
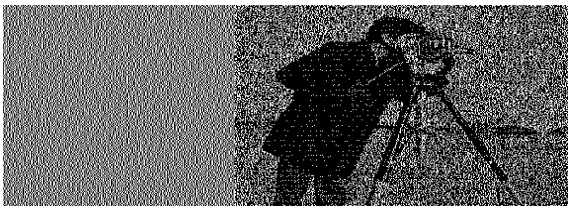


Figure 1. Construction of a two-out-of-two VC scheme: a secret pixel can be encoded into two subpixels in each of the two shares.

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 given 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]. Apart from binary image secret image in grayscale can also be used for VC [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. And later on improved the shares by applying error diffusion on halftone shares [6]. 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].on the basis of general access structuresAteniese et. al gave a more general model for VSS schemes[3]. All the qualified and forbidden subsets of sharesare specified into access structure such thatthe participants in qualified subsets can recover the secret image while the participants in a forbidden subset cannot.

According to the general access structure as given in [4], let the participants form a set of elementsp= {1, 2,…, n}. A VC scheme is a method to encode a secret binary image SI into n shadow images called shares, for a set p of n participants each participant in p receives one share from n shares. Let 2p denote the set of all subsets of p. Participant shares that can recover the secret image are called qualified shares and participant shares that cannot recover the secret image are called forbidden shares. Members of $\Gamma_{Qual} \subseteq 2p$ forms the qualified set and members of $\Gamma_{Forb} \subseteq 2p$ forms the forbidden set. Also, $\Gamma_{Qual} \cap \Gamma_{Forb} = \Phi$. And the pair($\Gamma_{Qual}$, Γ_{Forb}) is called the access structure of the scheme.A visual recovery for a set $X \in \Gamma_{Qual}$ consists of copying the qualified shares transparencies and then stacking them together to observe the secret image without performing any cryptographic computation. VSS have two characteristic 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 [7].

2.2. Halftone Visual Cryptography

In Traditional VC schemes the shares are random in nature. In the halftoning framework of VC, a secret binary image is encrypted into high quality halftone images, or halftone shares such that the shares have some visual meaning. This method applies blue noise halftoning to the construction mechanism used in conventional VSS schemes to generate halftone shares, maintaining the security and 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 also good. As a result, eves droppers, 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 [6] is used to achieve improved image quality in halftone shares.

2.3. Error Diffusion

Error diffusion is a simple, but 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 the more the number of future pixels to which the error is diffused the more is the clarity of the image. 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 [8]. 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[9], Jarvis [10], Stuki [11], Burkes [12], Sierra [13] and Stevenson's-Arce [14] error diffusion filter out of which all

filters except Stevenson-Arce filter have rectangular pattern, where Stevenson- Acre has hexagonal pattern to diffuse error to more neighboring pixels

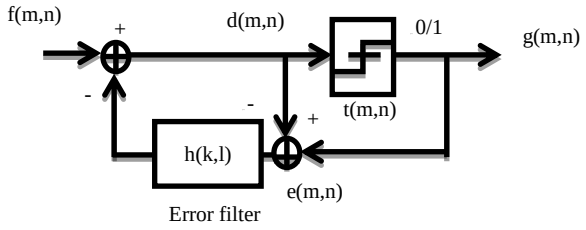


Figure 3. Error Diffusion

3. PROPOSED WORK

Few techniques that are being used here for halftone visual cryptography via error diffusion consist of some previously done work which forms the basis of the work done in this paper which can be described as below:

3.1. Random Share Creation

The encrypted message consists of black and white pixels. Each pixel appears in *n* shares, one for each transparency [1]. The share is a collection of m black and white subpixels. The resulting structure consists of a [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.This forms the basic VC technique that was purposed by Naor and Shamir[1].this technique encodes each secret image into random shares which are then transmitted over unsecured communication channel directly.

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 [5]. 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 grayscale imagecalled the halftone cell of size q=v1*v2 in each of the *n* shares.

3.3. Generating Halftone Shares

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

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.

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

The technique purposed by Zhou & Arce in halftone visual cryptography via error diffusion [6] is used.
Few main steps of the technique are:

1. Select a secret binary image.
2. Select a grayscale image to be used for sharing and embedding secret image pixels (figure 4).
3. Take complemented grayscale image as other shared image.
4. 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 C1as shown in figure1.

Figure 4. Grayscale image

Selection of subpixels is randomly done from C0, C1 matrix where row i of a matrix is distributed to grayscale image and row j to complemented grayscale image.

5. Then the **γ** subpixels from row i for each binary pixel *p*are encoded into a block of the grayscale image of size q=v1*v2.And similarly from row j into block of complemented grayscale image of same size.
6. Secret pixels from row i are encoded to the random position in grayscale image and at similar positions from row j in complemented grayscale image.
7. The grayscale image and the complemented grayscale image are distributed to Participant1 and Participant2.
8. The two shares are now halftoned using error diffusion such that the error at Non-SIP's is diffused but the SIP's remains unaltered. Error diffusion diffuses quantization error over the neighboring continuous tone pixels using error filter.
9. For error diffusion different error filters like Floyd's, Jarvis, Stucki, sierra, Stevenson Arce, Burkes have been applied and their impact on visual quality of the shares is noted.

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

Universal quality index in more advanced technique and require more mathematical complexity [15]. This measure is independent of individual visual system (or the person who is looking at the image) and viewing conditions. An expression can be derived for

UQI as follows;

Let's consider;

X= $xi|i$=1, 2, 3……N} as the original image;

X= $yi|i$=1, 2, 3……N} as the test image;

Then UQI=$\frac{4\sigma_{xy}\overline{x}\overline{y}}{(\sigma_x^2+\sigma_y^2)(\overline{x}^2+\overline{y}^2)}$

Where

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \ , \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

$$\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2$$

$$\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \bar{y})^2$$

$$\sigma_{xy}^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})$$

The universal quality index has a dynamic range from -1 to 1. QUI become +1 when the test image is equal to the original image. Consequently we can come to a conclusion about the image dithering algorithm used. If UQI value is nearer to 1 which means the algorithm is much better considering three factors; loss of correlation, luminance distortion and contrast distortion.

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. RESULTS AND DISCUSSION

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. An image of size 256 x 256 is used as a secret image. A Lena image of size 512 x 512 is used as grayscale image. This grayscale image is used for Share1 and a complement of grayscaleLena image is used for Share2. Halftone Shares as provided by using different error filters are shown (Figure5).

a1) 

a2) 

b1) 

b2) 

c1)  c2) 

d1)  d2) 

e1)  e2) 

f1)  f2) 

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.

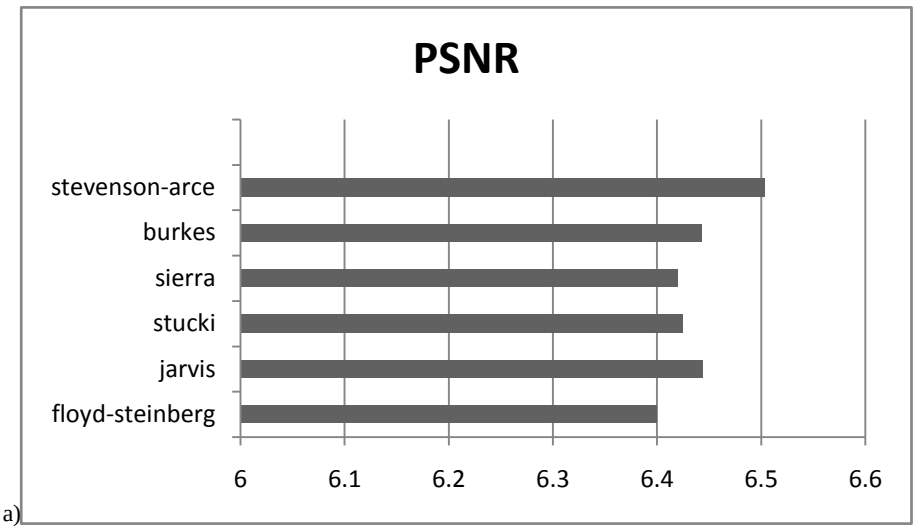
The pixel expansion of secret pixel is 9 times and the size of the grayscale cell is q=3. Different error filters are used to diffuse the error without affecting the secret pixels. It can be seen here that more complex filters or filters that diffuse the quantization error to more neighboring pixels produce more visually enhanced halftone shares, and Stevenson's-Arce filter has been able to produce most visually enhanced halftone shares. Stevenson-Arce uses a hexagonal grid pattern for diffusion of quantization error to neighboring pixels and also the divisor in in which the weights are distributed is largest among all the filters(1/200) therefore it takes more time to diffuse the error. But sierra and Stucki filter divides the weights in less term and are computationally efficient in terms of time and the amount of diffusion of quantization error. Sierra filters has 3 variants but even the simplest variant is able to produce better results than Floyd-Steinberg filter.

The results are quite close with not much of visual difference hence a comparison of the shares obtained by using different filters is made based on mathematical parameter for Quality of the images like PSNR and UQI measures as shown in the Table1.

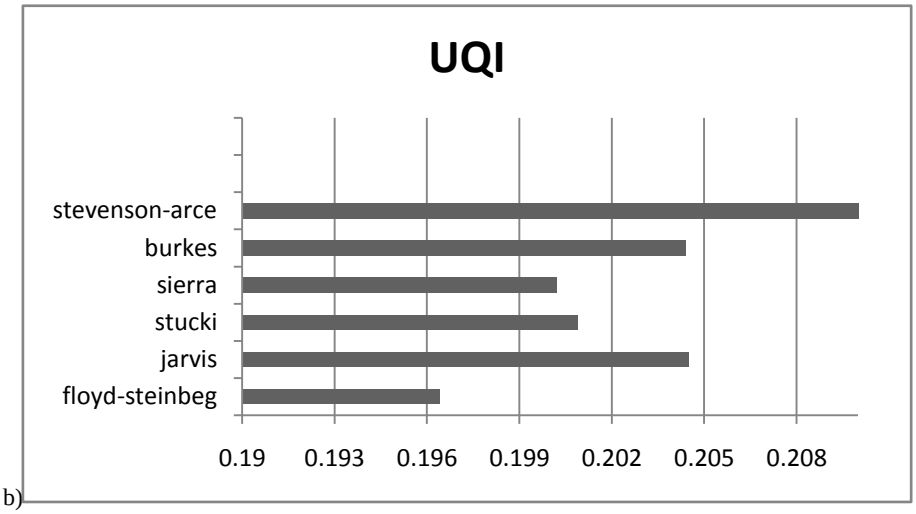
Table 1. PSNR and UQI measures for halftone shares

Error filter	**PSNR**	**UQI**
Floyd Steinberg	6.3997	0.1964
Jarvis-Judice-Ninke	6.4444	0.2045
Stucki	6.4244	0.2009
Burkes	6.4206	0.2002
Sierra	6.4436	0.2044
Stevenson-Arce	6.5036	0.2153

By the values of PSNR and UQI in the above table it can be seen that better shares can be obtained by using filters which distributes the error to more neighboring pixels. Stevenson-Arce produces the best results but it is heavy filter and it takes time. Stucki filter gives the good choice than Jarvis filter in terms of time taken as the division is by 42 rather than by 48 and after the initial 8/42 is calculated, some time can be saved by producing the remaining fractions by shifts. But sierra filter is the best choice as the sharpness of image is better and also the distribution of weights is by dividing into 32 parts .The difference can be shown more clearly if we look the results graphically (Figure 6).While calculatingthe PSNR it is found that, higher the PSNR better is the quality of the halftoned share.Also more the error is diffused, the better the visual quality of the image is. Also form universal image quality index it is very much clear that with higher UQI the share resemble more to the original image.



a)



b)

Figure 6(a), (b).Graphical representation of the PSNR and UQI as given by halftone shares provided by implementing different error diffusion filters in halftone visual cryptography via error diffusion.

And finally any of the two shares can be stacked digitally to get the recovered secret image which is expanded by 9 times (Figure 7). Therefore better halftone shares have been derived by using more complex error filters and without affecting the SIP's and hence the basic of VSS scheme. Hence it is established that more complex error filters can be used in visual cryptography to obtain better secrecy in shares and that too without affecting the final secret image.

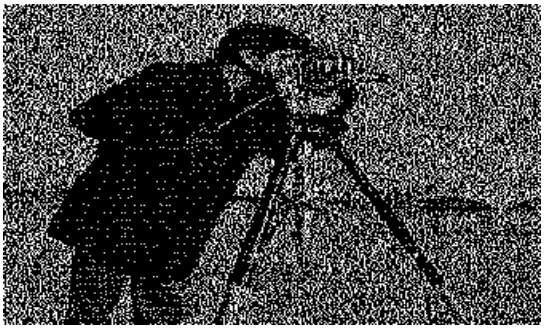


Figure 7. Stacked secret image

5. CONCLUSION

In this paper various error diffusion filters are applied to improve the image quality of the halftone shares. The halftone visual cryptography via error diffusion method inserts the secret information pixels into grayscale image. Visual cryptography is used along with the concept of halftoning where the continuoustone image is first embedded with visual sharing pixels and then halftoned using error diffusion and hence different error filters. 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. More complex error filter means better visual quality and better results.

A reconstructed secret image, obtained by stacking qualified shares together, does notsuffer from cross interference of share images and changed filters does not alter the stacked image and its quality and contrast is same as previous work [6]. Also the more the error is distributed among the neighboring pixels the better is the error filter.

6. 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] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visualcryptography via Error Diffusion," *IEEE Trans.* on InformationForensics And Security, Vol. 4, No. 3. , *Sep. 2009*

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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)

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

[14] 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}.

[15] Zhou Wang and Alan C. Bovik;"A Universal image quality index,"IEEE Signal processing letters, vol XX, no. Y, march 2002.