

PERFORMANCE OF ERROR FILTERS IN HALFTONE VISUAL CRYPTOGRAPHY

Anshul Sharma¹

Department of Electronic & Communication, Chandigarh University, Gharuan (S.A.S Nagar), India

¹ er.sharma.anshul@gmail.com

ABSTRACT

Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns. 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. 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. Halftone visual cryptography is extended technique in visual cryptography where the random shares are embedded in high quality grayscale images to give them meaning and thus reducing the doubt of eve's droppers that some secure data is hidden. Improved shares have been developed by changing the error filters that were earlier used in halftone visual cryptography via error diffusion and results were compared with the existing work for improvements on visual basis and on mathematical basis using mathematical parameters for index of quality of the image like PSNR and Universal quality index UQI.

KEYWORDS

Visual cryptography, error diffusion, halftone visual cryptography, secret sharing, universal image quality index.

1. INTRODUCTION

Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Secure digital imaging combines methods and techniques of cryptography and image processing. Visual cryptography enables distributing sensitive visual materials to authentic user 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], 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. The n shares are then xeroxed onto transparencies respectively and distributed among n participants and the secret images can be visually revealed by stacking together any k or more transparencies of the shares and no cryptographic computation is needed. Each of the n shares resembles a random binary pattern. However, by inspecting less than k shares, one cannot gain any information about the secret image, even if infinite computational power is available.

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.















Pixel	White 		Black 	
Probability	50%	50%	50%	50%
Share1				
Share2				
Stack Share 1&2				

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.

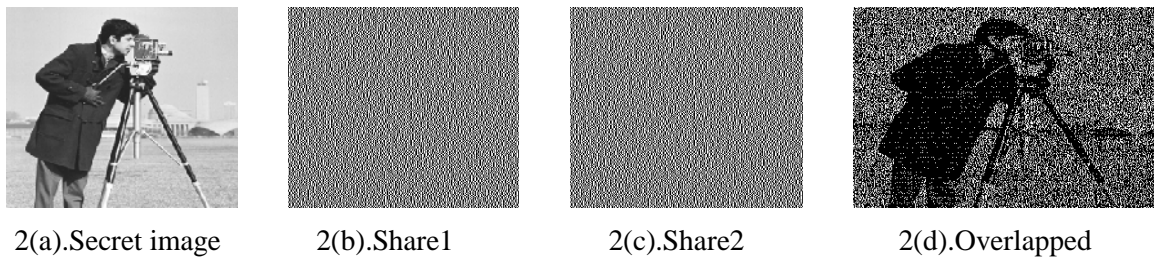


Figure 2. Example of 2-out-of-2 scheme.

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 $\mathcal{P} = \{1, \dots, n\}$ be a set of elements called participants. A VC scheme for a set \mathcal{P} of n participants is a method to encode a secret binary image SI into n shadow images called shares, where each participant in \mathcal{P} receives one share. Let $2^{\mathcal{P}}$ denote the set of all subsets of \mathcal{P} and let $\mathcal{Q} \subseteq 2^{\mathcal{P}}$ and $\mathcal{F} \subseteq 2^{\mathcal{P}}$, where $\mathcal{Q} \cap \mathcal{F} = \emptyset$. We refer to members of \mathcal{Q} as qualified sets and call members of \mathcal{F} forbidden sets. The pair $(\mathcal{Q}, \mathcal{F})$ is called the access structure of the scheme [3]. Any qualified set of participants $X \in \mathcal{Q}$ can visually decode SI, but a forbidden set of participants $Y \in \mathcal{F}$ has no information of SI [3]. A visual recovery for a set $X \in \mathcal{Q}$ 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 α , which is the number of subpixels on each share that each pixel of the secret image is encoded into, and the contrast β , 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, still 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], Stucki [10], Burkes [11], Sierra [12] and Stevenson’s-Arce [13] error diffusion filter.

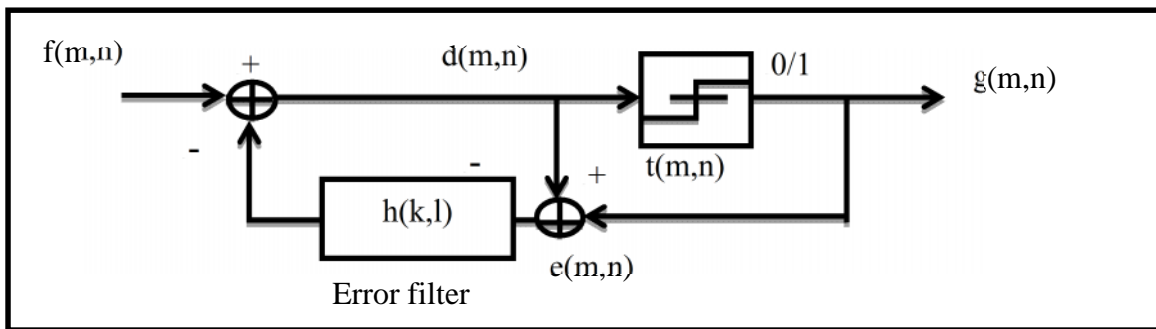


Figure 3. Error Diffusion

3. PROPOSED WORK

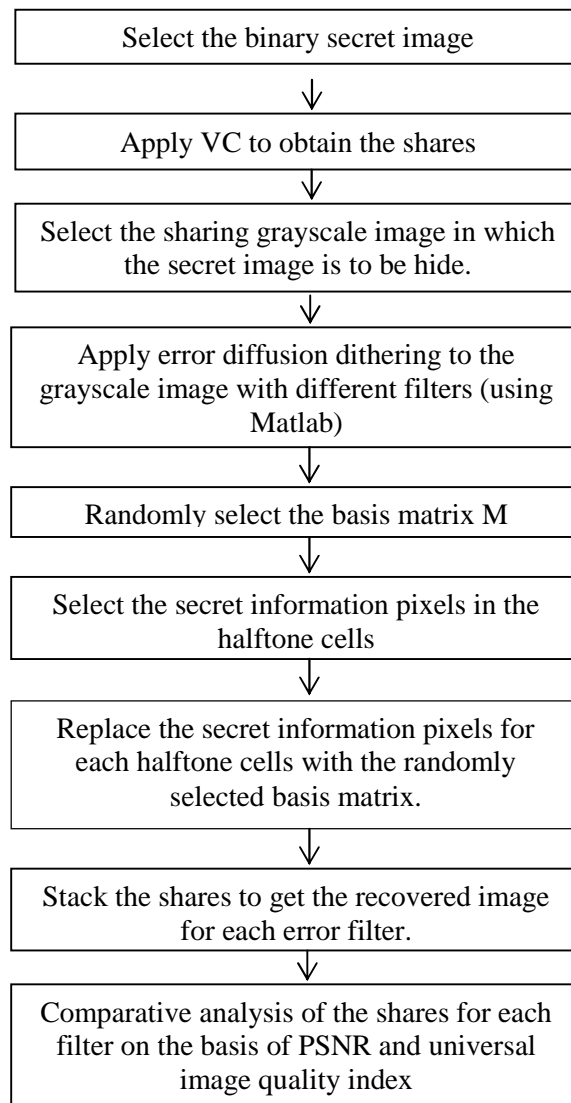


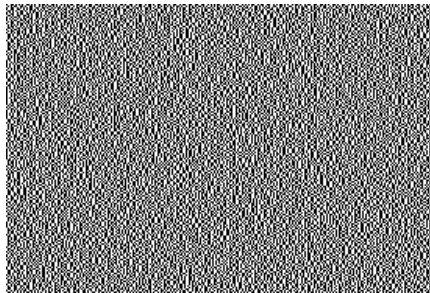
Figure 4: Methodology for effects of error filters if used for dithering of grayscale images

Step1:

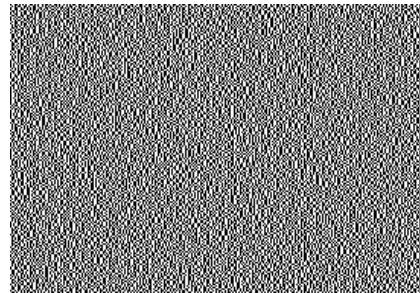
- The first step in constructing a halftone VSS scheme is to construct the *underlying k-out-of-n* VSS scheme where a secret image pixel as shown in 4.1(a) is encoded into $Q_1 \times Q_2$ pixels in each share given in 4.1(b) and 4.1(c). Q is the VC pixel expansion and only a function of (k, n) .



Figure 4.1 (a): Secret image



4.1 (b). Share1



4.1 (c). Share2

Figure 4.1: Secret image encoded into 2 shares

Step2:

- 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 \bar{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 $Q_1 \times Q_2$ halftone cell in each of the two shares, only two pixels, referred to as the 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 A and B in Fig. 4.2.

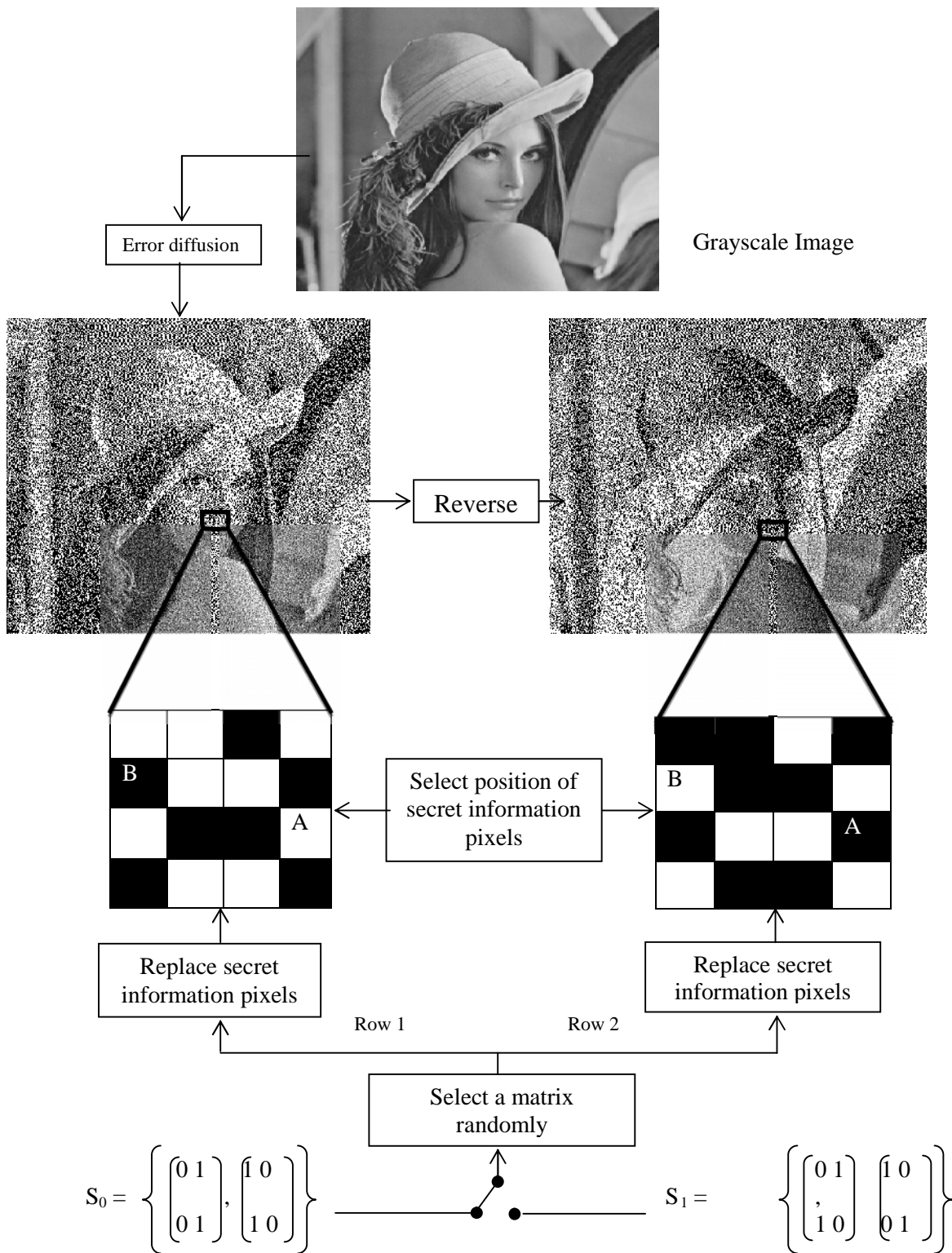


Figure 4.2: Procedure for replacing the secret image pixels in dithered images in halftone visual cryptography

- 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 .
- 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 $Q_1 Q_2$ pixels in the reconstructed halftone cell, obtained by superimposing the two encoded halftone cells, is white while all other pixels are black. If p is black, all pixels in the reconstructed halftone cell are black. Thus the contrast condition is satisfied. The secret pixel p can be visually decoded with contrast $(1/Q_1 Q_2)$. However, as long as their locations are independent of the secret information construction satisfies the security condition.

Step 3:

- When stacking together shares of a qualified subset, the pair of complementary halftone shares prevent the share visual information from appearing on the reconstructed image as a result of the OR operation.

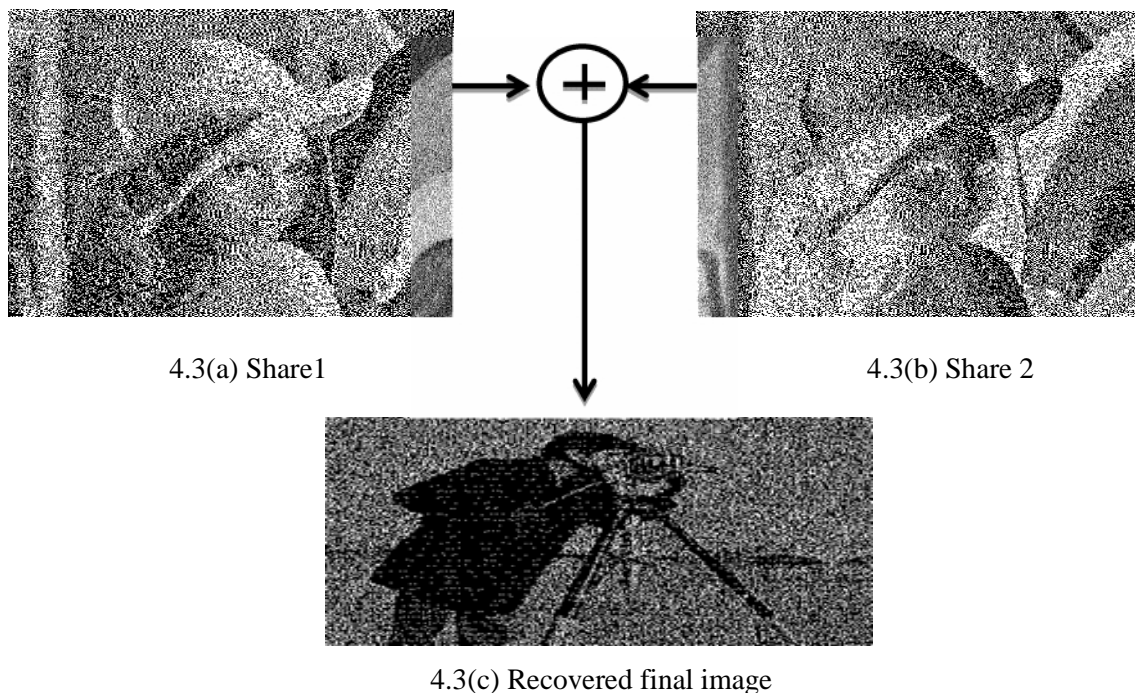


Figure 4.3: Halftone shares stacked together to get final recovered share

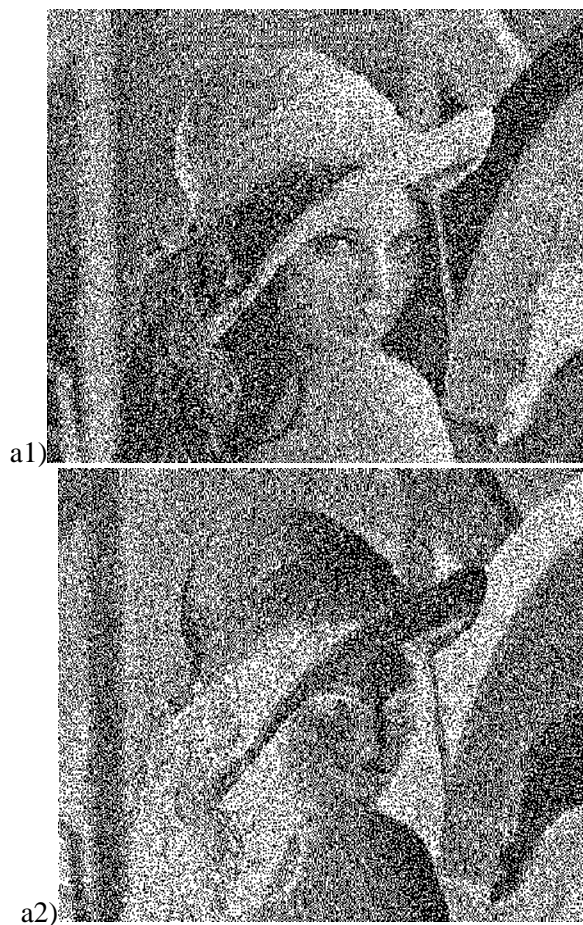
- Only the secret information carried by SIPs is shown.
- The secret image can be recovered visually by taking the shares given in figure 4.3 (a), 4.3 (b) onto transparencies and then stacking them together (figure 4.3(c)) or digitally they can be combined by using XOR operation.

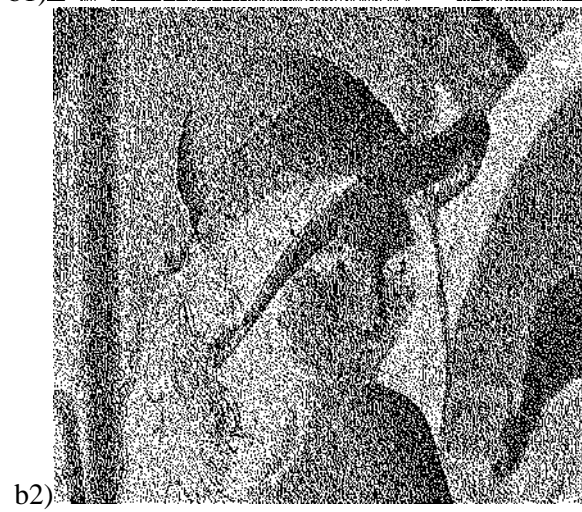
Step 4:

- For each of the filters primary halftone share i.e. of the grayscale image is calculated for PSNR and universal image quality index and a comparison based on the visual quality of The halftone shares along with mathematical parameter of universal image quality index and PSNR is made and for better understanding they are shown graphically also.

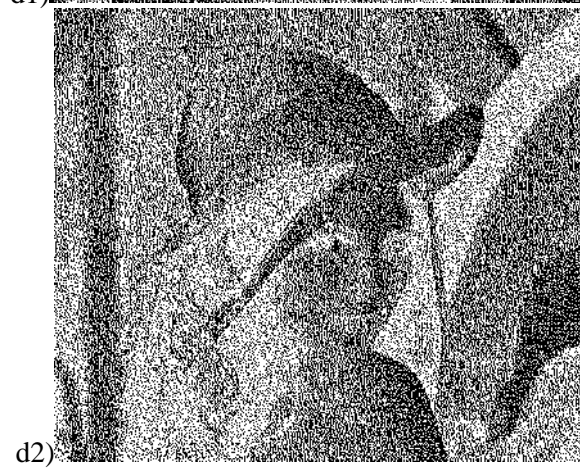
4. SIMULATION RESULTS

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. An 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. And finally any of the two shares can be stacked digitally to get the recovered secret image shown in Figure 8.









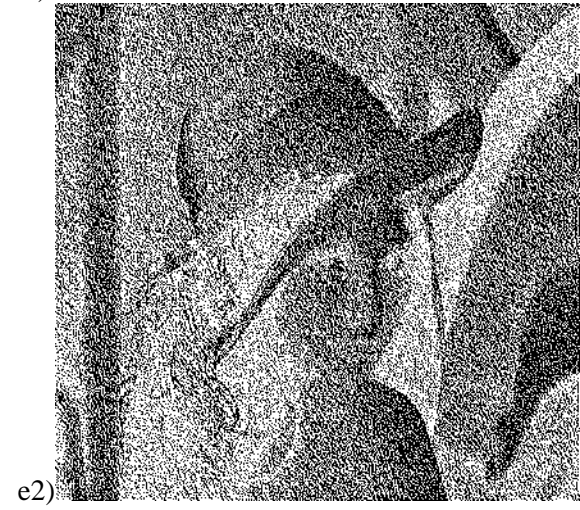
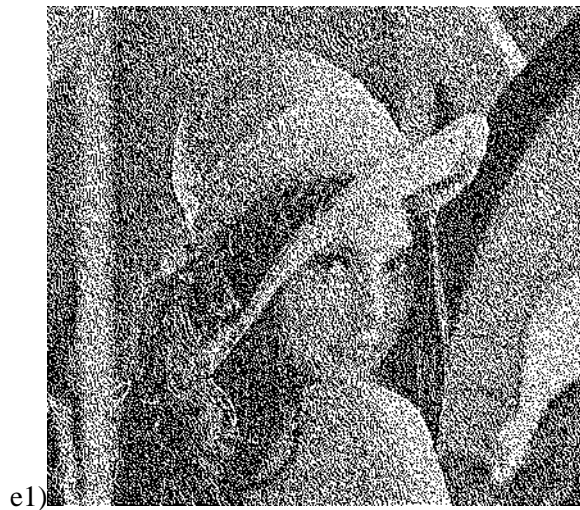




Figure 5. Impact on shares of halftone VC with different error diffusion filters .(a1), (a2),(b1),(b2),(c1),(c2),(d1),(d2),(e1),(e2),(f1),(f2) are two halftone shares of Floyd-Steinberg, Jarvis, Stucki, Sierra, Burkes and Stevenson-Arce error filters respectively.

On the basis of shares obtained by using different error filters it can be seen on examining the images that images gets sharper with the Stucki, Sierra and Stevenson-Arce filter as compared to that obtained by Floyd Steinberg filter. In Floyd Steinberg filter there is loss of contrast which is better in case of Stucki and Sierra filters but Stevenson Arce filter provides the best results as edges are best identified in its case.

But as the difference is very small we take the help of mathematical parameters to find out the filter which provides best results in terms of visual quality of the image. Hence we choose two parameters which are generally used in image processing to measure the quality of the image. UQI is better than PSNR in terms that UQI can be used under any conditions but PSNR varies with conditions and the viewer. But the previous results were made based on PSNR therefor PSNR is used for comparison purpose.

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

Table 2: UQI for primary halftone shares as compared to grayscale image as obtained by applying different error filters for dithering of the grayscale image before applying VC.

Error Filter	Floyd-Steinberg	Jarvis-Judice-Ninke	Stucki	Burkes	Seirra	Stevensons Arce
UQI	0.1954	0.2001	0.1937	0.1957	0.1995	0.2125

These values in table can be drawn into graph for better and easy comparison of the filters. As given in figure 6.

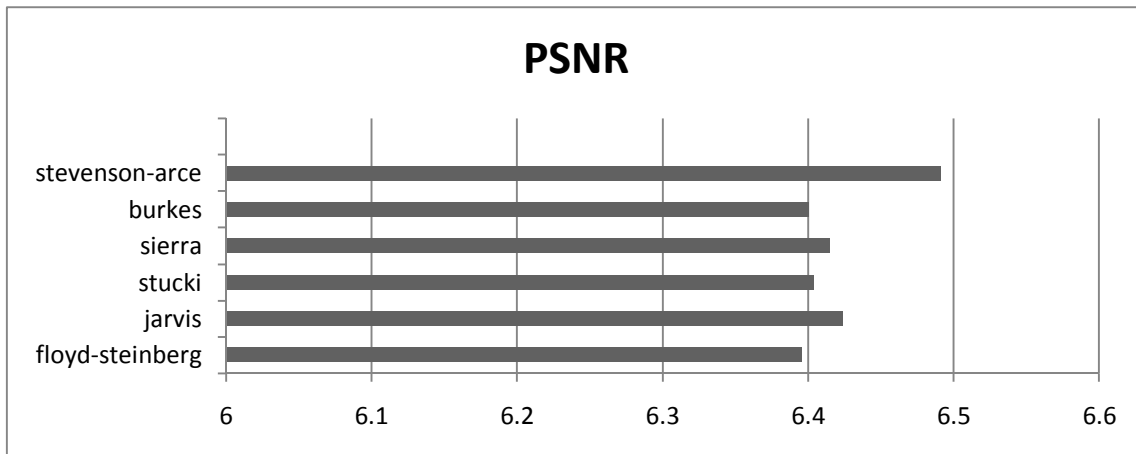


Figure 6: Graphical representation for PSNR values of the primary share in comparison to grayscale image as given by using different error filters for dithering of the grayscale image before applying VC.

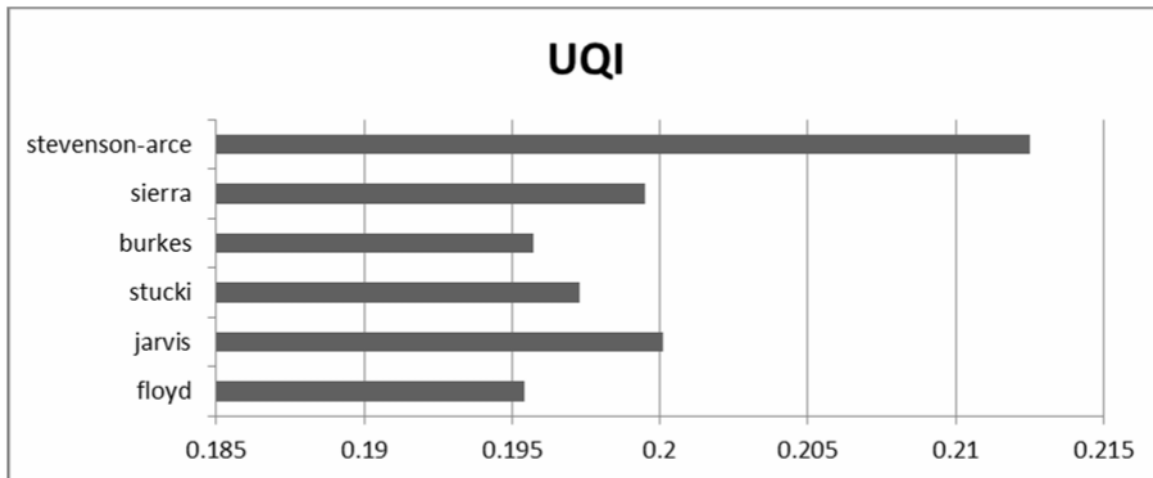


Figure 7: UQI measures for primary halftone shares as compared to grayscale image as obtained by applying different error filters for dithering of the grayscale image before applying VC.

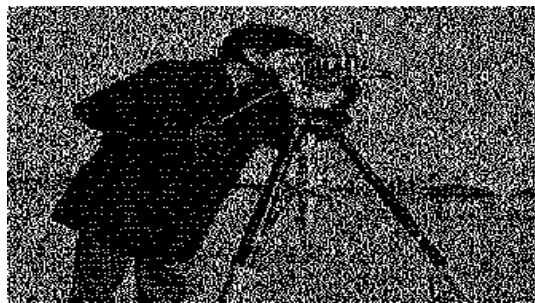


Figure 8. Stacked secret image

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.

From the results it is clear that visual quality of the halftone shares increases with the complexity of the error filters. Since the secret image pixels are added as white noise they produce quantization error at a particular location therefore degrading the quality of the halftone share.

A filter that diffuses the quantization error to more of the neighboring filters produces visually better images. Sierra, Stucki, and Stevenson's error filter produces more sharp images than Floyd Steinberg filter and the contrast is better. But Stevenson-Arce filter shows best results along the edges which can be clearly distinguished.

Also it can be derived that shares provided by using Stevenson's-Arce error filter provided the best results for PSNR and UQI as it diffuses the quantization error in a better way to more pixels.

REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptography: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* 2, pp. 1009{1013, July 1985}.

Author

Anshul Sharma received his B.tech degree in electronics and communication in 2009 and M.E. degree in electronics & communication from University Institute of Engineering & Technology in Panjab University Chandigarh, India in 2012. He is presently Assistant Professor at Chandigarh University, Gharuan (SAS Nagar), India. He has couple of research papers in international conferences and Journals. His research interests include image processing and automotive electronics.

