ISSN: 2348 - 2117

Available Online at www.ijetcr.org

International Journal of Engineering Technology and Computer Research (IJETCR) 2 (2) 2014, 09-15

An Analysis of Extended Visual Cryptography Using with Error Diffusion Half Toning Method

Megha Sharma[1*], Aruna Bansal[2]

[1]M.Tech Scholar, Rajasthan College of Engineering for Women, Jaipur, India.

[2]Rsearch Supervisor, Rajasthan College of Engineering for Women, Jaipur, India.

Received 10 April 2014; Accepted 25 April 2014

ABSTRACT

Extended visual cryptography allows the printing of meaningful images on transparencies so that it can conceal the very existence of "secret" in the transparencies. There have been a lot of studies to incorporate photograph images into extended visual cryptography. This scheme Visual Secret Sharing Schemes, it generates ***n*** transparencies from an original secret image. The transparencies are usually shared by ***n*** participants so that each participant is expected to keep one transparency [8]. Half toning is the reprographic technique that simulating to continuous tone imagery from side to side, that use of dots, changeable moreover in the size, shape and space. Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Its main use is to convert a multi-level image into a binary image, though it has other applications.

Key Word: Cryptography, Image, Pixel, Visual, Halftoining, VSSS, EVCS, GAS.

1. INTRODUCTION:

Visual cryptography is a kind of cryptography that can be decoded directly by the human visual system without any computation for decryption. It usually prints certain images on transparencies and the secret image is reconstructed by simply stacking the transparencies together [12]. Extended visual cryptography allows the printing of meaningful images on transparencies so that it can conceal the very existence of "secret" in the transparencies. There have been a lot of studies to incorporate photograph images into extended visual cryptography.

Half toning is the reprographic technique that simulating to continuous tone imagery from side to side, that use of dots, changeable moreover in the size, shape and space. The transparencies are usually shared by ***n*** participants so that each participant is expected to keep one transparency. Each pixel of a shadow image is generated separately in the conventional VSSS. An original secret pixel will be transformed to ***n*** patterns of pixels for shadow images.

1. Visual Cryptography Schemes:

In order to determine basic terminology in this chapter, this section explains basic concepts of visual cryptography, namely, k out of n Visual Secret Sharing Scheme ((k, n) VSSS), an Extended Visual Cryptography Scheme (EVCS).

1.1 Visual Secret Sharing Schemes:

This scheme Visual Secret Sharing Schemes, it generates ***n*** transparencies from an original secret image. The transparencies are usually shared by ***n*** participants so that each participant is expected to keep one transparency. Thus, a secret image is sometimes called a shared image. The secret image can be observed if any ***k*** or more of them are stacked together. However, the secret image is totally invisible if fewer than k transparencies are stacked. The images on transparencies are called shadow images [7]. Each pixel of a shadow image is generated separately in the conventional VSSS. An original secret pixel will be transformed to ***n*** patterns of pixels for shadow images. These pixels on shadow images are called shares [9]. A share consists of ***m*** black and white sub pixels. The human visual system observes the average of sub pixels, because they exist in close proximity.

This structure is usually described by an ***n × m*** Boolean matrix $M = [m_{ij}]$. Here m_{ij} = 0 or 1 if the ***j*** th sub pixel in the ***i*** th shadow is white or black, respectively. If transparencies of ***r*** shadows $i_1, i_2, \ldots\ldots, i_r$ out of ***n*** are stacked in a way that properly aligns the sub pixels, each combined share can be represented by the boolean ***"OR"*** of the corresponding rows $i_1, i_2, \ldots\ldots, i_r$ in the boolean matrix ***M***.

*Corresponding author: Megha Sharma |

Figure1: Extended visual cryptography for images

In this ***Figure 1***: six possible pattern of sub pixel arrangement with 50% gray. Each pattern is represented as [0011], [1100], [0101], [1010], [0110], [1001] from left to right. Let M_r denote the ***m-D*** vector obtained by taking the boolean "***OR***" of ***r*** row vectors. They gray level of a pixel combined by ***r*** shares is obtained by the Hamming weight $H(M_r)$ of the ***"OR"*** ed ***m-D*** vector M_r. User interprets this gray level as black if $H(M_r) \geq t$ and as white if $H(M_r) < t - \alpha m$. Here $t \in \{1 \ldots m\}$ is called threshold, while the value $\alpha > 0$ and the number $\alpha m \geq 1$ are called relative viz difference and contrast.

Now here two parameter ***m*** and ***α*** are very important to this conversation, the parameters ***m*** indicate the number of sub pixel in a share, which is called pixel expansion. Each pixel of the original secret images is represented by ***m*** sub pixel so that the reconstructed images as well as the shadow image will be ***m*** large as the original image [15]. Researcher would like ***m*** to be as small as possible. The parameter ***α*** indicates the relative difference between combined shares of originally white pixel and an originally black pixel. Since it means the loss of contrast of the reconstructed images, researcher would like ***α*** to be as large as possible.

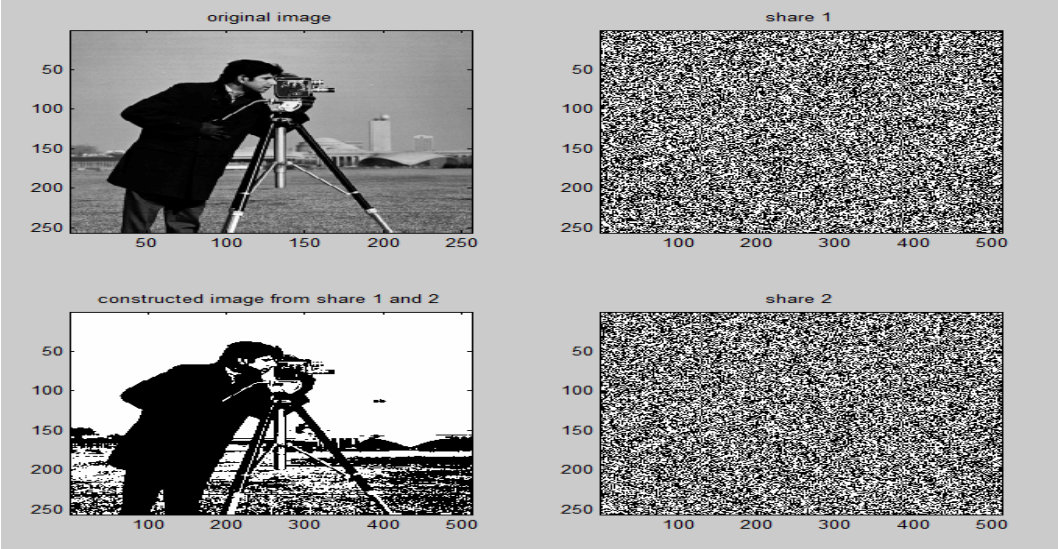

Figure 2: Reconstructed secret image from share 1 and 2

Let us consider a special case of (2, 2) VSSS. Each share consists of 4 sub pixels of a 2 × 2 array in a physical implementation, where two of them are white and the rest two are black. The Boolean matrix of this scheme is 2 × 4 where each row consisting of two 0's and two 1's represents an arrangement of sub pixels in a share [16]. For instance, six possible patterns of shares having 50% gray as shown in ***figure 2:*** are represented as [0011], [1100], [0101], [1010], [0110], [1001]. The scheme is accomplished by the following two collections:

C***w*** = {matrices obtained by permuting the columns of S***w***}

C***b*** = {matrices obtained by permuting the columns of S***b***}

Where S***w*** and S***b*** are given as below:

$$Sw = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad Sb = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

The above matrices Sw and Sb are called basis matrices. Because the collections are obtained by permutation of sub pixels, each share may have randomly arranged two white and two black sub pixels, which looks 50% gray [17]. A pair of shares from ***Cw*** has the same arrangement of sub pixels. The combined result is the same pattern, which looks 50% gray. A pair of shares from ***Cb*** has the complementary arrangement of sub pixels. The combined result consists of four black sub pixels, which looks completely black. ***Figure 2:*** shows an example of reconstructed secret image from share ***1 and 2***. The sizes of all images are 128 ×128 pixels, because the original secret image has 64 × 64 pixels.

The original scheme of visual cryptography is uniform, such that any combined shares from $q < k$ shadow images yield ***"OR"*** ed ***m-D*** vector ***Mq*** with ***H (Mq) = f (q)*** with uniform probability distribution, regardless of if the matrices were taken from ***Cw*** or ***Cb***. Suppose the case of ***q = 1***, the above-mentioned combined share is a single share of each shadow image. It means all the shadow images consist of uniformly random pattern of black and white sub pixels.

2.2 Extended Visual Cryptography Scheme:

An extended the VSSS in the sense of a General Access Structure (GAS) and extended capability. A General Access Structure controls the qualified set of transparencies with which one can recover the secret image, while any k or more transparencies can reconstruct the secret image in ***(k,n)***VSSS [19]. An extended capability is able to introduce a meaningful image as a shadow image. An innocent-looking image of a house, dog, or something else would be much less suspicious than a random-dotted image as a shadow image.

In the Extended Visual Cryptography Scheme (EVCS), for an access structure ($\Gamma_{Qual}, \Gamma_{Forb}$) on a set of n participants, the shared (secret) image can be recovered by any qualified set $X \in \Gamma_{Qual}$ with no trace of the shadow images, but any forbidden set $X \in \Gamma_{Forb}$ has no information on the secret image. Moreover, the shadow images are meaningful so that each participant can recognize the image on one's transparency. Similar to the ***(k, n)*** VSSS, an EVCS can be constructed in a pixel-wise manner. Since n participants share one secret image and have their own images in the n shadow images, we have to consider n+1 colors, ***c, c1,…… ,cn ∈ {w, b}*** where ***w*** and ***b*** stands for white and black, respectively [20].

The value ***c*** denotes the color of the secret image pixel and c_i denotes the color of the original image pixel for ***i-th*** participant's shadow image. In order to realize an EVCS that obtains a ***c*** pixel when transparencies associated to a set $X \in \Gamma_{Qual}$, we need 2^n pairs of collections of $n \times m$ Boolean matrices $(C_w^{c_1 \cdots c_n}, C_b^{c_1 \cdots c_n})$, one for each possible combination of white and black pixels in the ***n*** original images for the shadow images.

An EVCS for an access structure ***(ΓQual, ΓForb)*** for n participants is valid if it fulfills the following conditions.

1. For any $X \in \Gamma_{Qual}$ and for any $c_1 \ldots c_n \in \{b, w\}$, the threshold t_X and the relative difference α_R exist, which satisfy $H(M_X) \leq t_X - \alpha R^m$ for any $M \in C_w^{c1 \ldots cn}$ and $H(M_X) \geq t_X$ for any $M \in C_b^{c1 \ldots cn}$. Here M_X denotes the ***m-D*** vector obtained by taking Boolean ***"OR"*** of the row vectors of ***M*** corresponding to the participants in ***X*** and $H(M_X)$ denotes the Hamming weight of the vector M_X.
2. For any $X = \{i1; \ldots\ldots iq\} \in \Gamma Forb$ and for any $c_1, \ldots\ldots, c_n \in \{b,w\}$, the two collections of $q \times m$ matrices, $D_w^{c}{}_1 \ldots\ldots {}^{c}{}_n$ and $D_b^{c}{}_1 \ldots\ldots {}^{cn}$, obtained by extracting rows i1,……. iq from each n × m matrix in $C_w^{c1} \ldots\ldots {}^{c}{}_n$ and $C_b^{c1} \ldots\ldots {}^{c}{}_n$, respectively, are indistinguishable so that the collections contain the same matrices with the same frequencies.
3. For any i ∈ {1, 2…,n} and any c1……. ; ci+1,…….. $c_n \in$ {b,w}, it results that and $H(M_i)$ denotes the Hamming weight of the ***i-th*** row vector M_i of a matrix ***M.***

$$\min_{M \in \mathcal{M}_b} H(M_i) - \max_{M \in \mathcal{M}_w} H(M_i) \geq \alpha_S m$$

Where:

$$\mathcal{M}_b = C_b^{c_1 \cdots c_{i-1} b c_{i+1} \cdots c_n} \cup C_w^{c_1 \cdots c_{i-1} b c_{i+1} \cdots c_n}$$
$$\mathcal{M}_w = C_b^{c_1 \cdots c_{i-1} w c_{i+1} \cdots c_n} \cup C_w^{c_1 \cdots c_{i-1} w c_{i+1} \cdots c_n}$$

The values $\alpha_R > 0$ and $\alpha_s > 0$ are referred to as the relative difference of the reconstructed image and relative difference of shadow images, respectively. The number $\alpha R^m \geq 1$ and $\alpha S^m \geq 1$ are contrasts of the reconstructed image and the shadow images. People would like both α_R and α_S to be as large as possible [21]. Here we show how to accomplish a 2

out of 2 EVCS. Each share consists of 4 sub pixels like (2, 2) VSSS. However, it contains either two 1's or three1's depending on the colors of pixels of the corresponding original image, white or black, respectively.
The scheme is given by the 4 pairs of collections ***(Cw^{c1c2}, Cbc12)***, namely 8 collections ***Cc^{c1c2}*** , where ***c, c_1, c_2 ∈{b.w}***.
The collections are obtained by permuting the columns of the following 8 basic matrices, ***Sc^{c1c2}*** :

$$\mathcal{S}_w^{ww} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \mathcal{S}_b^{ww} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

$$\mathcal{S}_w^{wb} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \mathcal{S}_b^{wb} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\mathcal{S}_w^{bw} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \mathcal{S}_b^{bw} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

$$\mathcal{S}_w^{bb} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \mathcal{S}_b^{bb} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

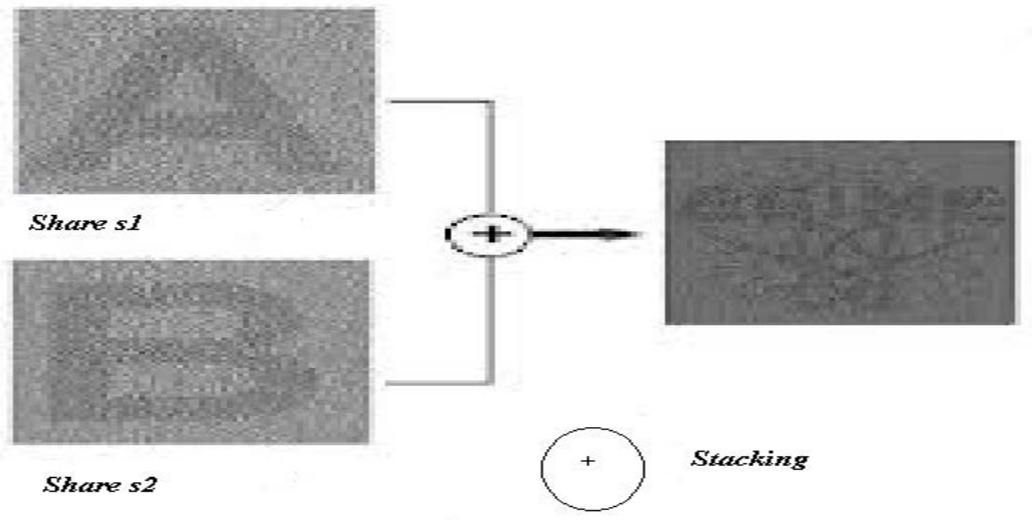

Figure 3: Two shadow images share (s1) share (s2) and reconstructed stacking image.

The reconstructed pixel has ***3 or 4*** black sub pixels if the original secret pixel is white or black, respectively. In this scheme, the relative contrasts are given as $\alpha_R = \alpha_S = 1/4$. ***Figure 3*****:** shows an example of two shadow images share ***(s1)*** share ***(s2)*** and reconstructed stacking image. The size of all images is 128 ***× 128*** pixels, because all the original shadow and secret images have 64***×*** 64 pixels. Pointed out some of the most important aspects of the extended capability [24]. One is related to the contrasts of images. A tradeoff between two relative differences exists, α_R and α_S, in any ***(k, k)*** EVCS as below:

$$2^{k-1}\alpha_R + \frac{k}{k-1}\alpha_S \leq 1$$

This means we cannot increase both contrasts of a reconstructed image and shadow images, α_R^m and α_S^m, simultaneously. They also specified the lower bound of the pixel expansion ***m*** in ***(k, k)*** EVCS as below:

$$m \geq 2^{k-1} + 2$$

This means we need more pixels to obtain EVCS. Although people would like contrasts to be as large as possible and pixel expansion as small as possible, there exist certain limits of them.

3. Half toning methods:

There exist a number of advanced half toning methods. The algorithms can be categorized into three categories, based on their computational complexity [3]. The first and simplest method is to operate on each pixel individually, without taking into account neighbors. The second is region-based method, which quantifies each pixel using a neighborhood operation instead of a simple point wise operation. The last one is an iterative method. Unlike the other two methods, the iterative methods normally operate over the entire original image and iteratively try to minimize the errors [5]. However, so far the last type of methods is times demanding even for images of small size. In this, we define Error diffusion half toning method half toning methods for analysis of extended visual cryptography.

4. Half toning Working Process:

The grayscale digital image consists of 256 gray levels, while the black and white printers only have one colored ink. So, there is a need to replace wide range of grayscale pixels for printers [9]. These 256 levels of gray should some- how be represented by placing black marks on white paper. Half toning is a representation technique to transform the original continuous tone digital image into a binary image only of ***1's and 0's*** consisting. The value "***1"*** means to fire a dot in the current position and **"0"** means to keep the corresponding position empty.

Since the human eyes have the low pass spatial-frequency prosperity, human eyes perceive patches of black and white marks as some kind of average grey when viewed from sufficiently far away. Our eyes cannot distinguish the dots patterns if they are small enough. Instead, our eyes integrate the black dots and the non-printed areas as varying shades of gray. ***Figure 4(b)***: shows a typical half toning image. Zooming in a part of the half toning image, we can see that the image is actually structured by a certain strategy of distributed black dots.

Figure 4: (a) The original image (b) The half toning image (c) An enlargement of (b)

5. Error diffusion half toning method:

Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed [10]. Its main use is to convert a multi-level image into a binary image, though it has other applications. Unlike many other half toning methods, error diffusion is classified as an area operation, because what the algorithm does at one location influences what happens at other locations. This means buffering is required, and complicates parallel processing. Point operations, such as ordered dither, do not have these complications. Error diffusion has the tendency to enhance edges in an image. This can make text in images more readable than in other half toning techniques.

Unlike the block replacement and ordered dithering methods, which treat each pixel individually, error diffusion quantifies each pixel using a neighborhood operation [12]. In this case, the value of each output point depends no longer only on the value of the corresponding input point. A schematic diagram of error diffusion method is given in ***Figure 5***.

In this ***figure***, "***H"*** and "***I"*** denote the final half toning image and the original image, respectively.

This method moves through the original image in raster order, normally starting from the pixel up to the left such as the first element of the matrix and then goes through all pixels from left to right until the end [16]. The value of each pixel in ***"I"*** is quantified by the constant threshold method.

One or zero is set at the corresponding position in ***"H".*** Since the pixel value in ***"I"*** is replaced by ***"0"*** or ***"1"*** in ***"H",*** there is a difference between the pixel value in "***I"*** and ***"H"*** at the position ***(i, j***).

After computing the difference, we obtain an error "***e"***. And then this error is pushed forward to a number of non-processed pixels, such as the neighborhoods [24]. To which neighborhoods and how this error is pushed is decided by an error diffusion weight matrix, such as an error filter ***"w".***

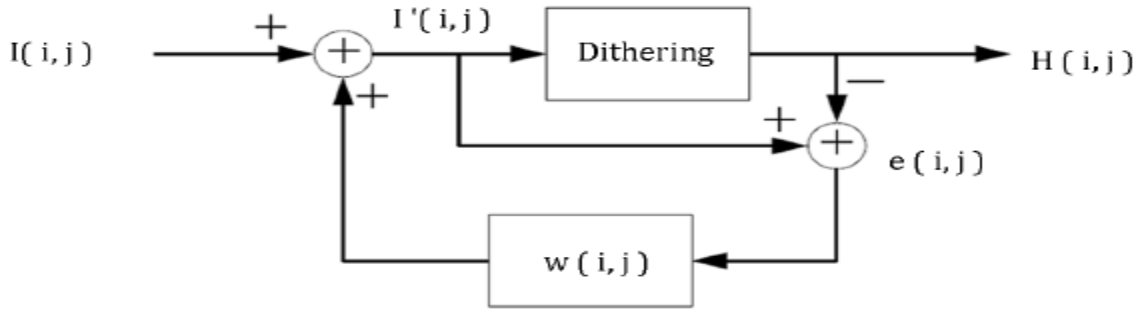

Figure 5: Error Diffusion half toning method

In ***Figure 6:*** two common different error diffusion weight matrices are shown. If using the Floyd and Steinberg matrix, the error occurred at the position ***(i, j)*** is weighted by ***7/16*** and added to the neighborhood pixel at ***(i+1, j).*** At the same time the error is also weighted by ***1/16*** and added to the neighborhood at ***(i+1, j+1)*** and so on. After the error has been diffused, we get the new input image ***"I"***. The same process moves to the pixel at the next position and performs the above described steps until all pixels have been proceeding.

			7/48	5/48
3/48	5/48	7/48	5/48	3/48
1/48	3/48	5/48	3/48	1/48

(a)

		7/16
3/16	5/16	1/16

(b)

Figure 6: Two error diffusion weight matrixes (a) Jarvis, Judice, and Ninke (b) Floyd and Steinberg.

Figure 7: shows two images being half toned by error diffusion with different error diffusion weight matrices. Using a larger weight matrix, the final half toning image has sharper details and reduces some of the artifacts [25]. In general, error diffusion shapes the error to make the most of the noise energy concentrated in the high frequencies, so that the low-frequency artifacts are minimized made not visible for the eyes. Such kind of high-pass filtering property produces the effect of edge enhancing ***[1, 6, 7]***. However, since error diffusion accomplishes good resolution by spreading the dots, the final half toning images are normally darker than the images using other methods presented so far. It is, thus, very sensitive to ink spreading.

(a) (b)

Figure 7: Half toning image by error diffusion. (a) The error diffusion weight matrix in Figure 6 (a) is used. (b) The error diffusion weight matrix in Figure 6 (b) is used.

5. CONCLUSION:

Visual cryptography is a kind of cryptography that can be decoded directly by the human visual system without any other computation for decryption. The transparencies are usually shared by ***n*** participants so that each participant is expected to keep one transparency. Each pixel of a shadow image is generated separately in the conventional VSSS. Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Error diffusion is classified as an area operation, because what the algorithm does at one location influences for what happen at other location.

6. REFERENCES:

1. Zhigang Fan, A simple modification of error-diffusion weights. SPIE'92.
2. M. Naor and A. Shamir. Visual cryptography. In Advances in Cryptology- EUROCRYPT94 LNCS 950, pages 1-12, 1994.
3. Yuefeng Zhang, Line Diffusion: A Parallel Error Diffusion Algorithm for Digital Halftoining, The Visual Computer, 12(1) 40-46, 1996.
4. T.N. Pappas; D.L. Neuho, Printer models and error discussion, Image Processing, IEEE Transactions, Jan. 1995.
5. H. R. Kang, Digital Color Halftoining, New York: IEEE Press, 1999.
6. K. T. Knox. Evolution of diffusion. JEI, 8(4):422–429, 1999.
7. J. P. Allebach, DBS: retrospective and future directions, Color Imaging: Device-Independent Color, Color Hardcopy, and Graphic Arts VI. Proc. SPIE vol. 3963, 2000.
8. M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," Journal of WSCG 10 (2), pp. 303–310, 2002.
9. Y. H. Chan and S. M. Cheung, "Feature-preserving multi scale error diffusion for digital half toning," Journal of Electronic Imaging, Vol. 13, No. 3, pp. 639-645, 2004.
10. Li, P. and Allebach, J. P., Block interlaced pinwheel error diffusion, "Journal of Electronic Imaging14(2),1{13 (2005).
11. S. Bhatt, J. Sabino, J. Harlim, J. Lepak, R. Ronkese and C. W. Wu, Comparative study of search strategies for the direct binary search image half toning algorithm, Proceedings of NIP 22: IST's International Conference on Digital Printing Technologies, Denver, CO, pp. 244-247, 2006.
12. Z. M. Wang and G. R. Arce "Halftone visual cryptography through error diffusion", IEEE Int. Conf. Image Processing, pp.109 -112, 2006.
13. C.N. Yang, K.H. Yu, and R. Lukac. User-friendly image sharing using polynomials with different primes. International Journal of Imaging Systems and Technology, 17:40-47, 2007.
14. C.C. Chang, Y.P. Hsieh, and C.H. Lin. Sharing secrets in stego images with authentication. Pattern Recognition, 41:3130{3137, 2008.
15. F. Liu, C.K. Wu, and X.J. Lin. Color visual cryptography schemes. IET Information Security, 2:151-165, 2009.
16. Z.M.Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009.
17. C.N. Yang and C.B. Ciou. Image secret sharing method with two decoding-options: lossless recovery and previewing capability. Image and Vision Computing, 28:1600-1610, 2010.
18. Z. Eslami, S.H. Razzaghi, and J.Z. Ahmadabadi. Secret image sharing based on cellular automata and steganography. Pattern Recognition,43:397-404, 2010.
19. Embedded Extended Visual Cryptography Schemes F. Liu. Forensics and Security, IEEE Transactions on, 2011 - ieeexplore.ieee.org.
20. Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes", IEEE Transactions on information forensics and security, Vol. 6, No.2, June 2011.
21. A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security , vol. 6, no. 1, pp. 70-81, 2011.
22. N. Askari, C. Moloney and H.M. Heys,"A Novel Visual Secret Sharing Scheme Without Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.
23. S. Gooran, Digital Halftoning, Thesis, Linkoping University, Linkoping, Sweden.
24. K. T. Knox, Error Image in Error Diffusion, Proc. Of SPIE, vol. 1657, 268-279.
25. J. F. Jarvis; C. N. Judice; W. H. Ninke, A survey of Techniques for the Display of Continuous-tone Pictures on Bilevel Displays, Computer Graphics and Image Processing, vol. 5, 13-40.

