A NOVEL CRYPTOGRAPHIC TECHNIQUE THAT EMPHASIS VISUAL QUALITY AND EFFICIENY BY FLOYD STEINBERG ERROR DIFFUSION METHOD

Jainthi.K[1], Prabhu.P[2]

[1]*Student, Department of ECE, Christ College of Engineering and Technology, Pondicherry, India*
[2]*Assistant Professor, Department of ECE, Christ College of Engineering and Technology, Pondicherry, India*

Abstract

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. The original image can be split into shares, where unauthorized person cannot get the data which we hide within that share images. By stacking the two shares, the secret data can be revealed. The highlighted issue in VC is, the size and quality of the reconstructed image should be same as the original image. In this paper, a novel k out of k extended visual cryptography scheme (EVCS) is used, to improve security and to produce meaningful shares. Halftone visual cryptography (VC) encodes a secret image into k halftone meaningful image shares through Floyd Steinberg error diffusion algorithm. The algorithm achieves dithering using error diffusion, meaning it pushes (adds) the residual quantization error of a pixel onto its neighboring pixels, to be dealt with later. This algorithm takes a substantial time for encryption and decryption in a considerably calmer manner. Comparisons with previous approaches show the superior performance of the new method.

Keywords: *k out of k, extended visual cryptography, halftone visual cryptography, Floyd Steinberg error diffusion algorithm.*

---***---

1. INTRODUCTION

As technology progresses and as more and more personal data is digitized, there is still more of an importance required on data security today than there has ever been. Guarding this data in a harmless and protected way which does not impede the access of an authorized authority is an immensely difficult and very remarkable problem. Many efforts have been made to solve this problem within the cryptographic community. One of these data security methods has been credited to Moni Naor and Adi Shamir known as visual cryptography (VC) is presented. Specially, visual cryptography allows effective and efficient secret sharing between a numbers of favorite parties. Visual cryptography provides a very dominant technique by which one secret can be distributed into two or more shares. In visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with some *k* shares could decrypt the image, while any $k - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by superimposing the shares. When all *k* shares were overlapped, the original image would appear, where n≥k.

Then by [1] the original share can be broken into n shares, with all k shares only the original secret can be revealed, k-1 shares does't give any information. For example, a secret image can be split into 5 shares (n=5) the value of k=3, then by joining the three share image can only be the way to recover the secret. To further improve the security of this secret sharing scheme, the secret can only be revealed by combining all the share images, that is by stacking all the 5 shares. this method is called k out of k secret sharing scheme.

In traditional techniques the codebook is used to generate share images where a secret image can be encoded as four times larger than the original size of the secret image. A single pixel in the secret image can be encrypted as four pixels in all the share images, by stacking all the share images the reconstructed image will be larger than the secret.

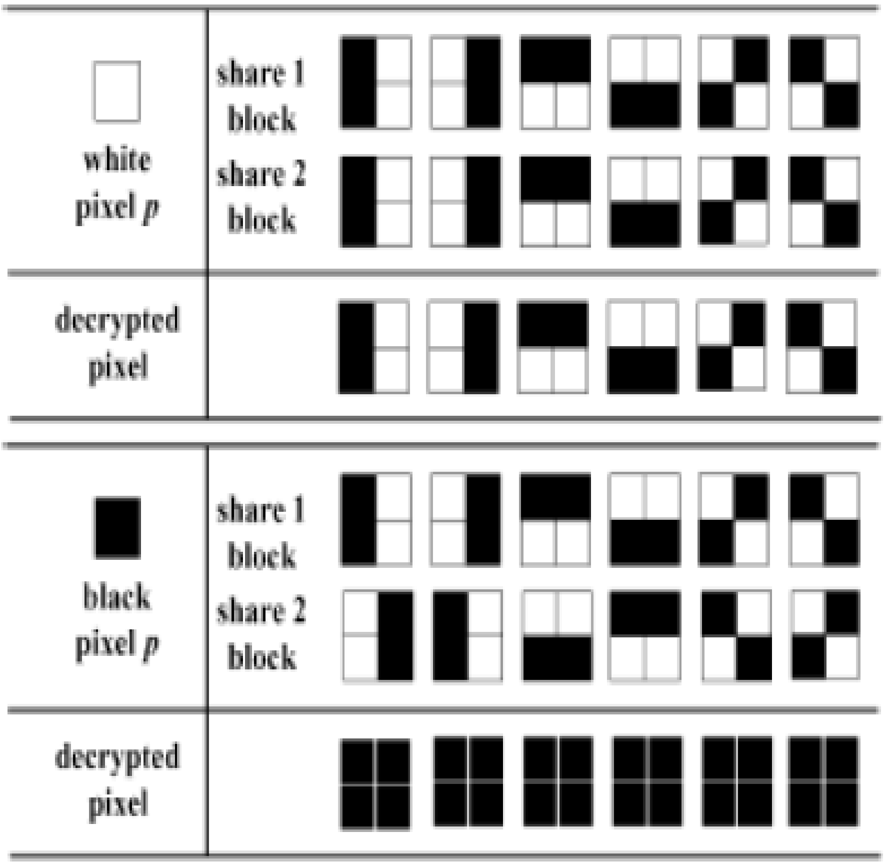


Fig-1: Basic share pattern for VC

To illustrate the basic principles of VC scheme, consider a simple (2, 2) VC scheme as shown in figure. Each pixel from a binary secret image is embedded as white and black pixel p in the share image. If a white pixel p is to be encoded then the one of the row can be selected randomly with equal probability. Based on the pixel in the secret image, it is replaced by a set of four subpixels, two of them black and two white.

Thus, the subpixel set gives no clue as to the original value of. When two subpixels originating from two white are superimposed, the decrypted subpixels have two white and two black pixels. On the other hand, a decrypted subpixel having four black pixels indicates that the subpixel came from two black pixels.

Fig. 2 shows an example of a simple (2, 2)-VC scheme with a set of subpixels shown in Fig.1 Superimposing these two shares leads to the output secret message as shown in Fig.2. The decoded image is clearly identified, although some contrast loss is observed. Several new methods for VC have been introduced recently in the literature.

Moni and Shamir introduces a cryptographic concept where the secret can be only be split as two share images and proposed k out of n scheme and k out of k scheme. Tzung-Her Chen and Tsao proposed a threshold sharing scheme which improves the contrast of share and decoded image.

0. Kafri and E. Keren introduce a technique which reduces the size expansion of the decoded result by random grids technique. Tzung-Her Chen and Kai-Hsiang Tsao uses user friendly random grids technique instead of using code book design (traditional visual sharing scheme).

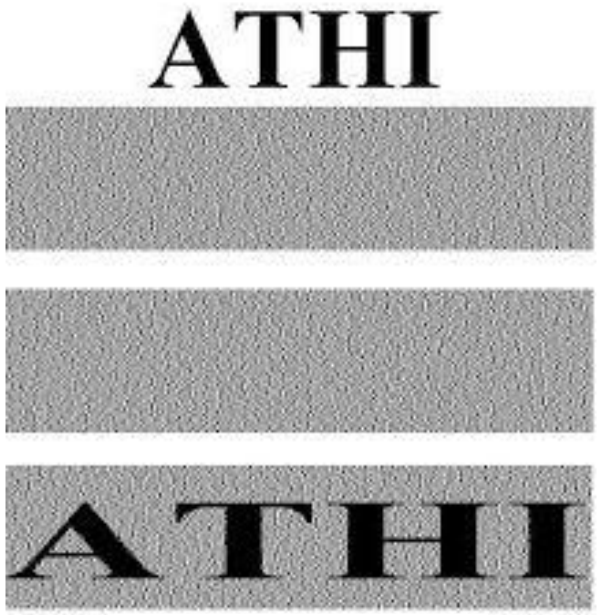


Fig-2: Basic 2 out of 2 VC scheme

Ateniese and Blundo proposed a VC scheme based upon general access structure. The shares are look like noise like structure and the management of the shares is complex. The access structure is specified as qualified and forbidden subsets of share images. Participants have the qualified subset can recover the original image and the forbidden subset cannot recover the secret, this method is applied to binary and gray scale images.

Ateniese developed [3] an extended visual cryptography (EVC) method in which shares contain secret information as well as different information that is used to hide the secret information on the shares, simply as meaningful shares. Hypergraph colorings are used in constructing meaningful binary shares. Since hypergraph colorings are constructed by random distributed pixels, the resultant binary shares contain strong white noise leading to inadequate results.

Chen and Tsao [5] proposed a modification to kafri and keren scheme. That method proposes random grid technique for 2 out of 2 visual secret sharing schemes. But Chen introduces a novel n out of n and 2 out of n secret sharing based on random grids without pixel expansion to encrypt the secret into n cipher grids but not user friendly. Chen and Tsao [6] also introduce the user friendly random grids based on visual secret sharing which produces meaningful shares.

Zhi zhou [12] proposed halftone visual cryptography, which increases the visual quality based on blue noise dithering principles by void and cluster algorithm encode a secret into n shares having meaningful information.

Wang, Z. [13] introduce a halftoning technique via error diffusion algorithm , while the secret images are embed on a binary valued shares can be halftoned through error diffusion where the quantization error can be spread to different pixel location around the processing pixel.

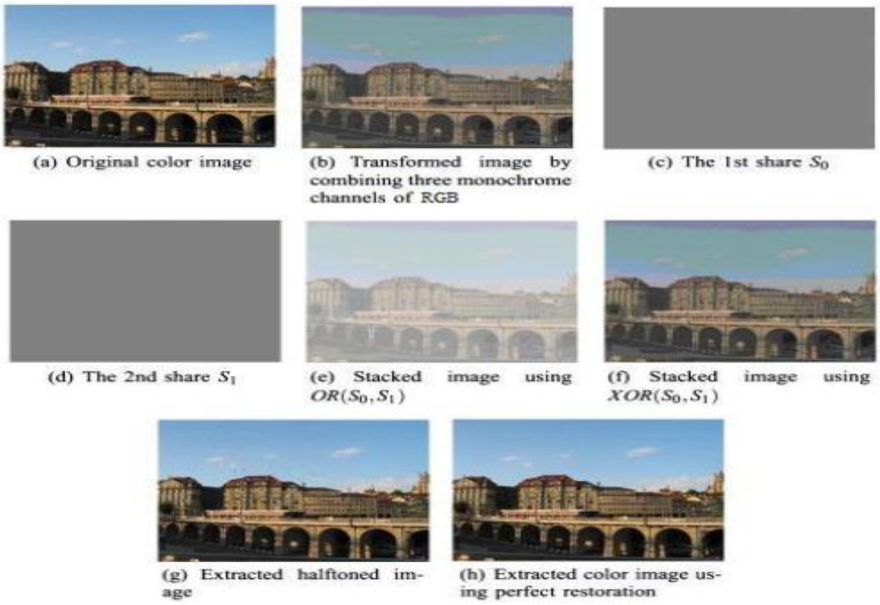
Error diffusion [16] is a simple but efficient algorithm for image halftone generation. The quantization error at each pixel is filtered and fed to future inputs. The error filter is designed in a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision.

Robert W. Floyd and Louis Steinberg [17] proposed halftoning technique via error diffusion which diffuses the error to four pixel around the current location. J. F. Jarvis, C. N. Judice and W. H. Ninke [18] introduce the error diffusion algorithm to 12 surrounding pixels. P. Stucki, Mecca [19] proposes a diffusion algorithm which diffuses the low amount of error to 12 surrounding pixels.

The rest of the paper is organized as, section 2 discuss about the k out of k extended visual cryptography scheme and random grids method. Section 3 explains the fundamentals of halftoning, error diffusion algorithm, different error diffusion filters and encryption procedure. Section 4 analyzed detailed about the previous method result and proposed halftoning via error diffusion method results.

2. EXTENDED VISUAL CRYPTOGRAPHY:

Ateniese and Blundo and Stinson proposed extended visual cryptography scheme which can encrypt the secret image into meaningful cover images. Usually the shares do not carry any useful information and looks like noise. In this scheme the shares have some useful data on it but not the secret which is to be hiding shows in fig-3. All the share images have different cover images, while transmission an unauthenticated person may indulge and get any of the shares; he thinks that is the secret data but actually it is not. By stacking all the covered share images only the secret can be revealed otherwise don’t. This can be an efficient way to improve the security.



(a) Original color image

(b) Transformed image by combining three monochrome channels of RGB

(c) The 1st share S_0

(d) The 2nd share S_1

(e) Stacked image using $OR(S_0, S_1)$

(f) Stacked image using $XOR(S_0, S_1)$

(g) Extracted halftoned image

(h) Extracted color image using perfect restoration

Fig-3: Extended visual cryptography

For example, a mobile number is going to transmitted via a wireless channel that numbered image can be split as shares, then by extended visual cryptography scheme all these shares are watermarked by some other numbers. The original secret can be revealed only by combining all the covered shares

2.1 Random Grids:

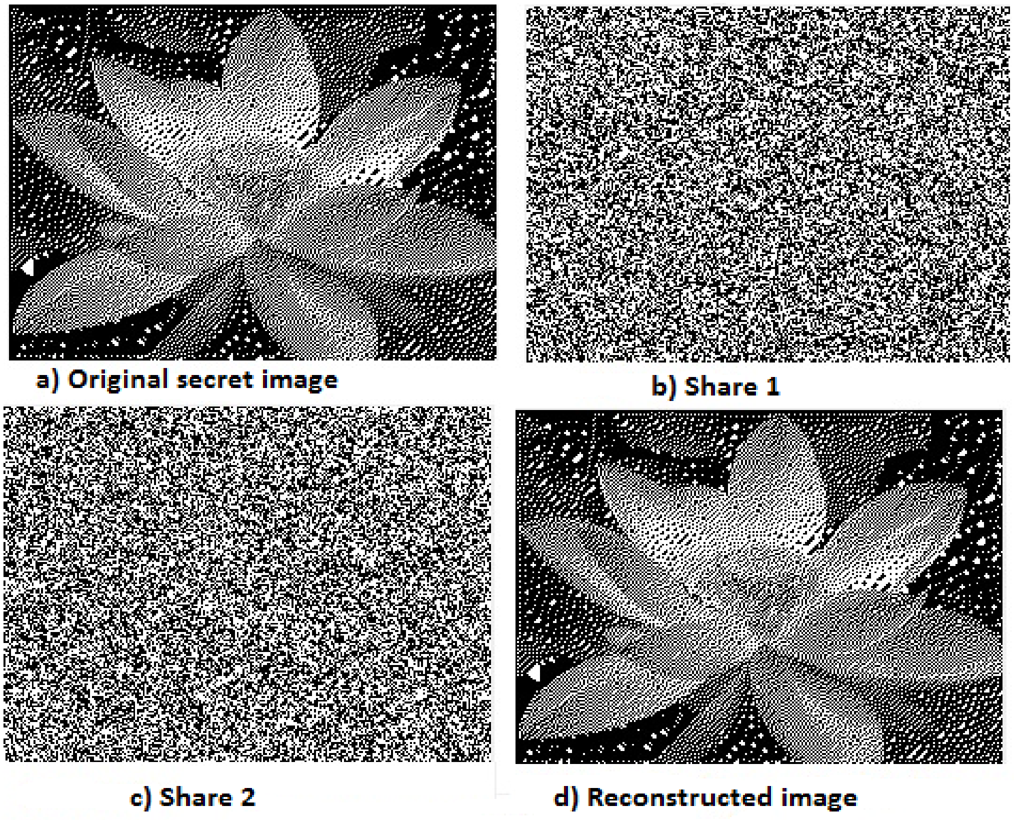
O. Kafri and E. Keren introduce a technique called random grids which is mainly useful to reduce the pixel expansion problem of the reconstructed images. In general VC scheme, a pixel can be encoded as four subset of pixels with the use of codebook, the output of VC is larger than the original size of the secret. [3] Introduces the k out of n random grids method.

Table-1: Random Grids Technique

For white pixel	White pixel	White pixel	white pixel
	White pixel	Black pixel	Black pixel
For black pixel	Black pixel	White pixel	Black pixel
	Black pixel	Black pixel	Black pixel

For (2, 2) RG based VC scheme, first share is generated randomly of 0 and 1 representing transparent and opaque pixels. Second share is to hide the original image. If the secret is transparent pixel, the pixels in the second share as same as the first share otherwise the flipping operation can be done (i.e. inversion of 0's to 1's and vice versa). Output can be obtained by XOR operation between those two shares.

For (k, n) visual cryptographic scheme, the input can be a single share and output should be n shares, by combining k shares can recreate the original. Use the (2, 2) scheme for the secret pixel so that two shares are generated, and encode the second share as in the same way of the previous scheme so that k number of shares are generated. And generate n-k random bits based on uniform distribution and these shares are arranged randomly in the shares.


a) Original secret image

b) Share 1

c) Share 2

d) Reconstructed image

Fig-4: Example for Random Grids

2.2 Existing Work:

K out of k extended visual cryptography scheme by random grids method can have the advantage of improving contrast compared with the other works. In which, the encryption is based on probability of the biased bit. If the biased bit d is equal to one then then encryption of the shares can be done as previously discussed method, (2, 2) and (k, n) VC scheme. Suppose that biased bit d is not equal to zero or one then embedding the cover images to the share images can be done. That is if the cover pixel is white then generating either transparent or opaque pixel for secret, else that cover pixel is black then construct black pixel for the secret image. Certainly all the generated k pixels are white then randomly choose a number, and set that pixel to be black. Finally the generated cover images and the share images are to be filled correspondingly.

By this technique, the security can be improved thus by combining all the shares only can reveal the secret image and the pixel expansion problem are reduced. The issue in this work is the visual quality is tradeoff between the quality of the share images and the quality of the reconstructed image. If the visual quality of the share image is high then the contrast of the reconstructed image is low else if the contrast of the reconstructed image is high then the visual quality of the share images is low and the share images looks like noise structure. This method can be applied to gray scale images, further moving to colour images it is processed RGB and CYMGY separately.

3. PROPOSED WORK:

Halftoning is a method to represent an image in discrete tone rather than continuous tone, images printed in the newspaper. Error diffusion is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Unlike many other halftoning methods, error diffusion is specified as a current area operation; because the algorithm creates some changes at one pixel location influences create the same changes at other pixel locations. This requires buffering and complicates parallel processing. Error diffusion has the tendency to enhance edges in an image, so that text can also be easily readable.

The error filter filters the quantization error at each pixel and distributes that error to further processing pixels not to previous processed pixels. It removes the frequency difference among all the locations and produces more visual pleasing shares. There are different types of error filter are used in visual cryptography further we will discuss about it.

Where *P (i, j)* represents the pixel point at *(i, j)* position of the input image. *S (i, j)* is the sum of the input pixel value and the diffused errors, *O (i, j)* is the output quantized pixel value. Error diffusion mainly consists of two components.

The first component is the thresholding block, is to set the threshold level to the further pixels, where the output, *O (i, j)* is given by

$$O(i,j) = \begin{cases} 1, & \text{if } S(i,j) \geq T(i,j) \\ 0, & \text{otherwise} \end{cases} \qquad (1)$$

The threshold *T (i, j)* can be dependent to the position of the pixels. The second main component is the error filter *h (m, n)* where the input error *e (i, j)* is the difference between *S (i, j)* and *O(i, j).*

Finally, we compute *S (i, j)* as

$$S(i,j) = P(i,j) - \sum_{m,n} h(m,n)\, e(i-m, j-n) \qquad (2)$$

Where *h (m, n)* is the impulse value of the 2-D error filter.

$$\begin{matrix} \bullet & 2 & 5 \end{matrix}$$

$$h(m,n) = 1/16 * \begin{bmatrix} 7 & 5 & 6 \end{bmatrix} \qquad (3)$$

where ● is the current processing pixel. The error filter, is in such a way that the low frequency difference between the input and output image is minimized.

The quantization error that is diffused away by the error filter are high frequency or “blue noise”. These structures of error diffusion produce halftone images that are pleasant to human eyes with high visual quality.

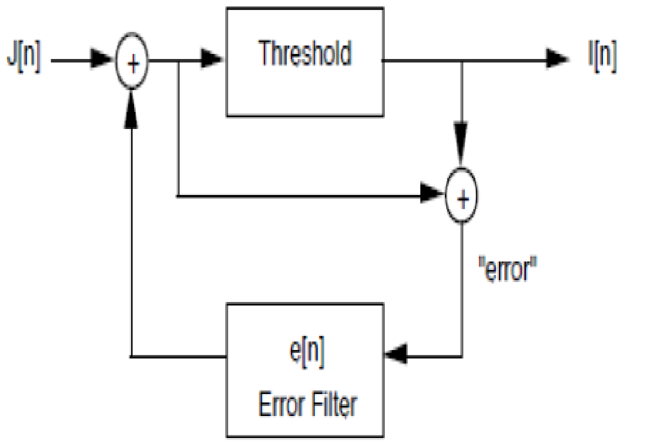


Fig-5: Error Diffusion Filter

For gray scale images ranges from 0 to 255, every input pixel value J(i, j) is compared to the threshold value of the error diffusion filter. Suppose if the threshold value is 154, which is greater than the threshold value, I(i, j) is assigned as black pixel else the current value of the pixel is smaller than the threshold, I(n) is as white pixel. The difference between the threshold values is the quantization error among pixels. The error can be distributed in the scan line order, which is from upper left to the lower bottom.

The most common filter is **Floyd-Steinberg** error diffusion filter. The boundary conditions are ignored to get better results. In this filter, for (m, n) gray scale the quantization error can be distributed only to right, right diagonal, left diagonal and bottom. The amount of error which is spread to right and left side is 3/8, whereas 1/8 can be send to the right and left diagonal pixels gives good simulation results.

Halftoning algorithm

```
for i = 1 to m
    for j = 1 to n
        I[i,j] = (J[i,j] < 128);  0 : 1
        err = J[i,j] - I[i,j]*255
        J[i+1,j] = err*(3/8)
        J[i-1,j+1] = err*(1/8)
        J[i,j+1] = err*(1/8)
        J[i+1,j+1] = err*(3/8)
    end for
end for
```

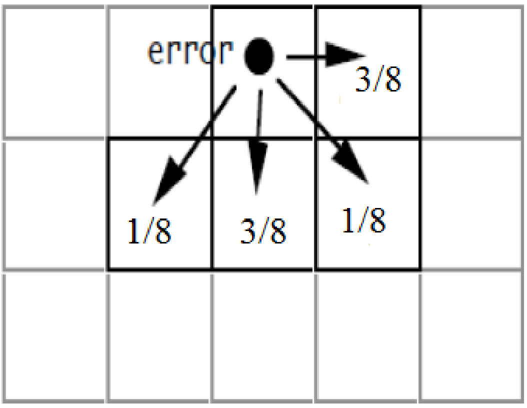


Fig-6: Floyd Steinberg Error Filter

The next error diffusion filter proposed by **Jarvis**, Judice and Ninke. Instead of four neighboring cells the error can be spread to 12 neighboring cells around the processing pixels, which can increase the encryption time. The error is going to spread is 1/48 with respect to pixel values.

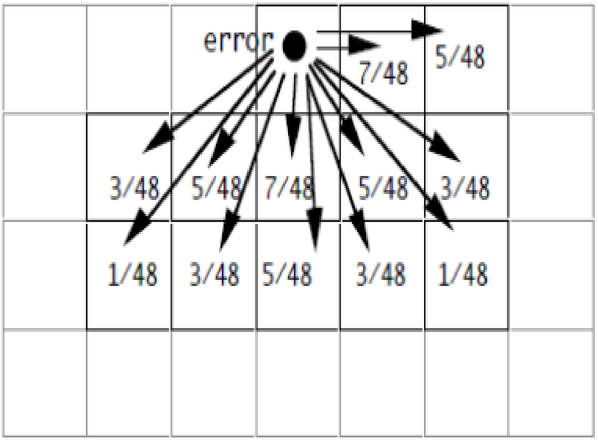


Fig-7: Jarvis Error Diffusion Filter

Another error diffusion algorithm proposed by **Stucki**, which is same as the Jarvis algorithm and spread the diffusion error to the 12 neighboring cells but the only difference is the fraction of error can be varied to the future inputs.

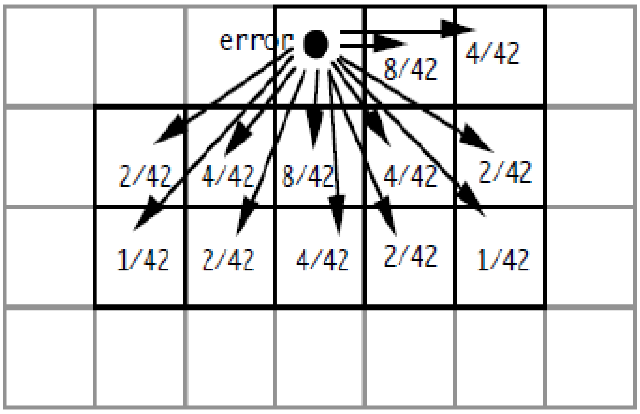


Fig-8: Stucki Error Diffusion Filter

We are going to use the Floyd-Steinberg error diffusion filter to perform the halftoning for the images and to produce the visual pleasing shares. Halftoning can be performed for both gray scale and colour images of any size. And can able to embed the secret image into four cover images and also for eight cover images in a secure way. For that the original secret image can be split into four shares, then hiding the four shares into those four cover image.

3.1 Encryption Procedure:

1. Read the input secret image it can be gray scale or colour image.
2. Execute halftoning of the input image.
3. Read the cover images.
4. Execute halftoning of the share images.
5. Split the original secret image into four segments as message shares.
6. Exclaim each message into size of the cover image.
7. Declare two random shares S0 and S1 of same size equal to 256×256.
8. For message 1,
9. for i = 1,………m
10. for j = 1………..n
11. If message m (i, j) is equal to zero then perform ex-or operation for S(I, j) with the random share S0.
12. Else ex-or S(I, j) to the random share S1.
13. end if
14. end for
15. end for
16. Repeat this procedure for all the message segments.
17. Retrieve the messages from encrypted share images, decimate the message images and concatenate all the message images.

4. SIMULATION RESULTS:

The implantation of the algorithm was done using MATLAB Version 7.12.0 (R2011a). The image sizes used were not fixed since the algorithm can work on all m x n image size. The algorithm was written in m-file and tested on a set of sample images. The images were encrypted and the results were analyzed below.

In previous work, the contrast improved with a probability of the biased bit. So based on the probability, the contrast can be varied between share images and reconstructed images. If the contrast of the share images are good i.e. the cover images are clearly visible then the quality of the reconstructed images are poor, it may be fully black or the original secret cannot be retrieved properly. Else the quality of the share images are poor, which are looks like a noise structure then the reconstructed images are more visual pleasing to eyes, gives better contrast gives in table-2. To overcome this variation problem a new technique is used in this method referred as halftoning to further improve contrast and to obtain good peak signal to noise ratio (PSNR).

Halftoning used four different error diffusion filters, to produce shares. First, Floyd-Steinberg error filter spreads the quantization error to right, left, right diagonal and left diagonal pixel only. A typical problem that is seen in this halftoning technique is spectral whitening where the variation in average separation distance between minority pixels becomes so great that the pattern starts to resemble the halftone pattern created by white noise. In order to reduce these artifacts the modifications to the original error diffusion algorithm has been introduced. Second, modified Floyd-Steinberg algorithms the fraction of error can be sent to surrounding pixels are high, so that contrast loss can be reduced. Third, Jarvis error diffusion filter will spread the quantization error to the 12 neighboring pixels fourth, Stucki error filter is also similar to Jarvis algorithm. In an effort to break up worm patterns in error diffusion, Jarvis and Stucki introduced 12-element error filters and it is apparent that both filters break up worms at extreme gray levels.

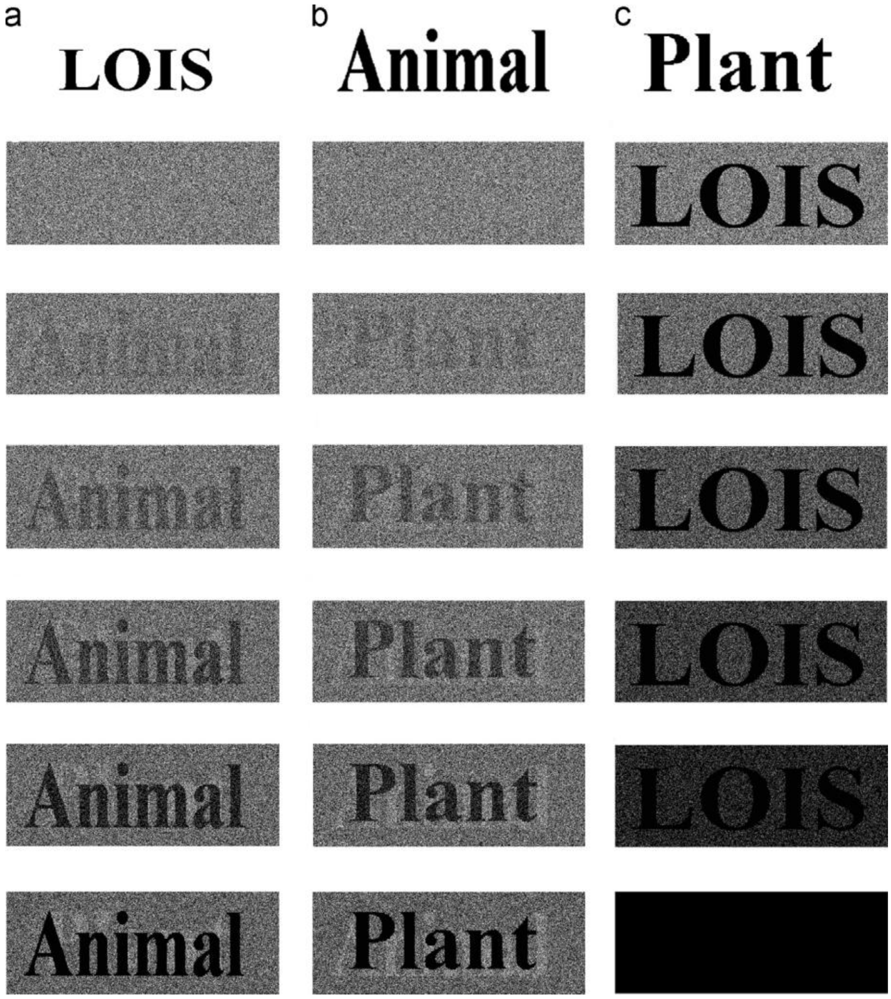
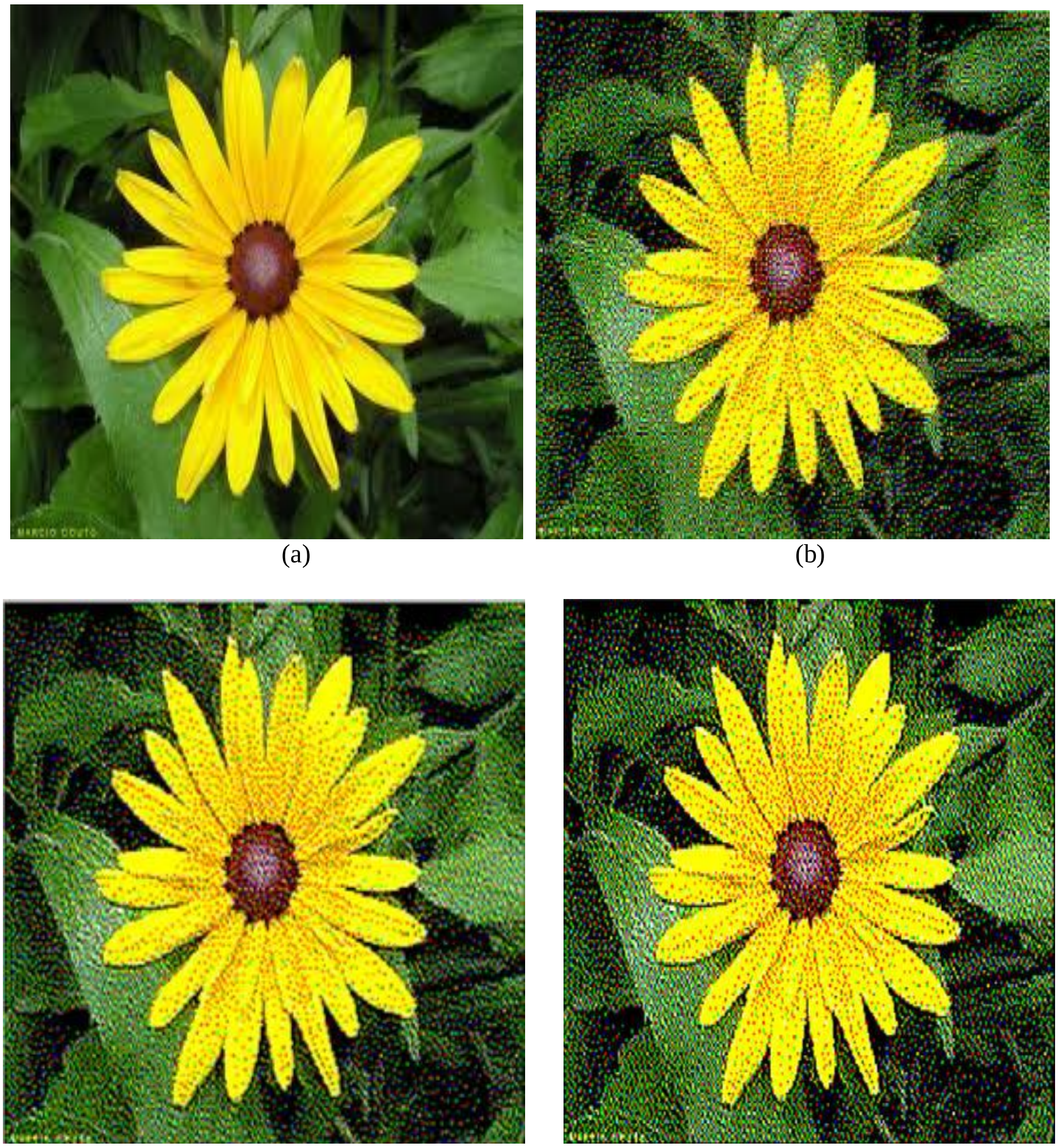


Fig-9: Contrast Variation of Existing Method

The results from the previous work are shown below; the contrast is varied by the parameter value, which is increased from 0 to 1 by o.2.

Table-2: output of previous work based on probabilistic parameter

Probabilistic parameter	**Contrast of the shares**			**Contrast of decoded image**
	Share 1	**Share 2**	**Share 3**	
0	0	0	0	0.25
0.2	0.07	0.07	0.07	0.2
0.4	0.1538	0.1538	0.1538	0.15
0.6	0.25	0.25	0.25	0.1
0.8	0.36	0.36	0.36	0.05
1	0.5	0.5	0.5	0



(a) (b)

(c) (d)

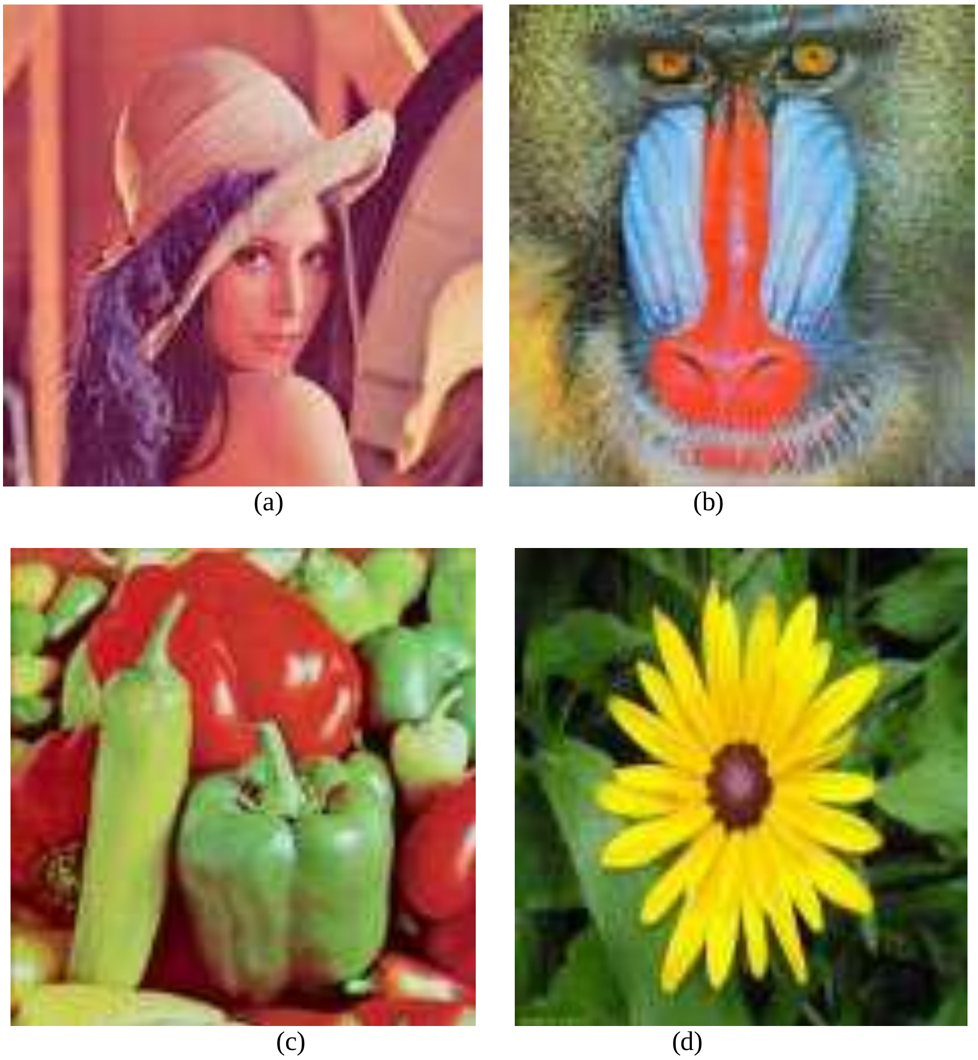
Fig-10: (a) Secret image; (b) Floyd Steinberg error filtering; (c) Jarvis error diffusion filter; (d) Stucki error diffusion filter

Table-3: Comparison of Various Error Filter

Error filtering method	**Test image – Flower**			
	PSNR in dB	**Perceived error ratio**	**Encryption time(s)**	**Mean square error**
Floyd Steinberg error filtering	20.618	4013225	1.688607	6.844e+07
Modified Floyd Steinberg error	20.619	421756	1.768488	6.844e+07
Jarvis error diffusion filter	20.6182	4206273	1.629220	6.8437e+07
Stucki error diffusion filter	20.6187	4.213e+006	1.7539	6.8429e+07

From the above results shown in table-3, Floyd Steinberg algorithm gives better PSNR compare to other error diffusion filter with that filter, encryption can be done by a set of four images, and the input image size is of 128 × 128 and all the cover images of size 256 256 as shown in fig-12 (a), (b), (c), (d).

Fig-11: Original Secret Image



(a)

(b)

(c)

(d)

Fig-12: cover images (a) Lena; (b) Baboon; (c) vegetables; (d) flower

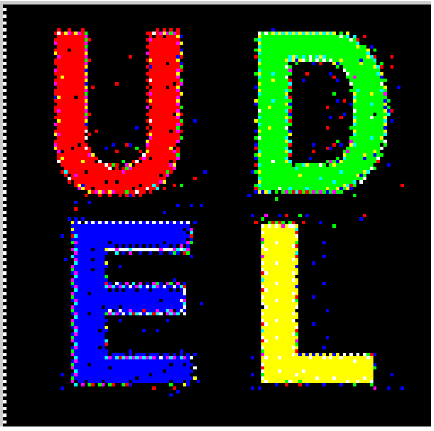
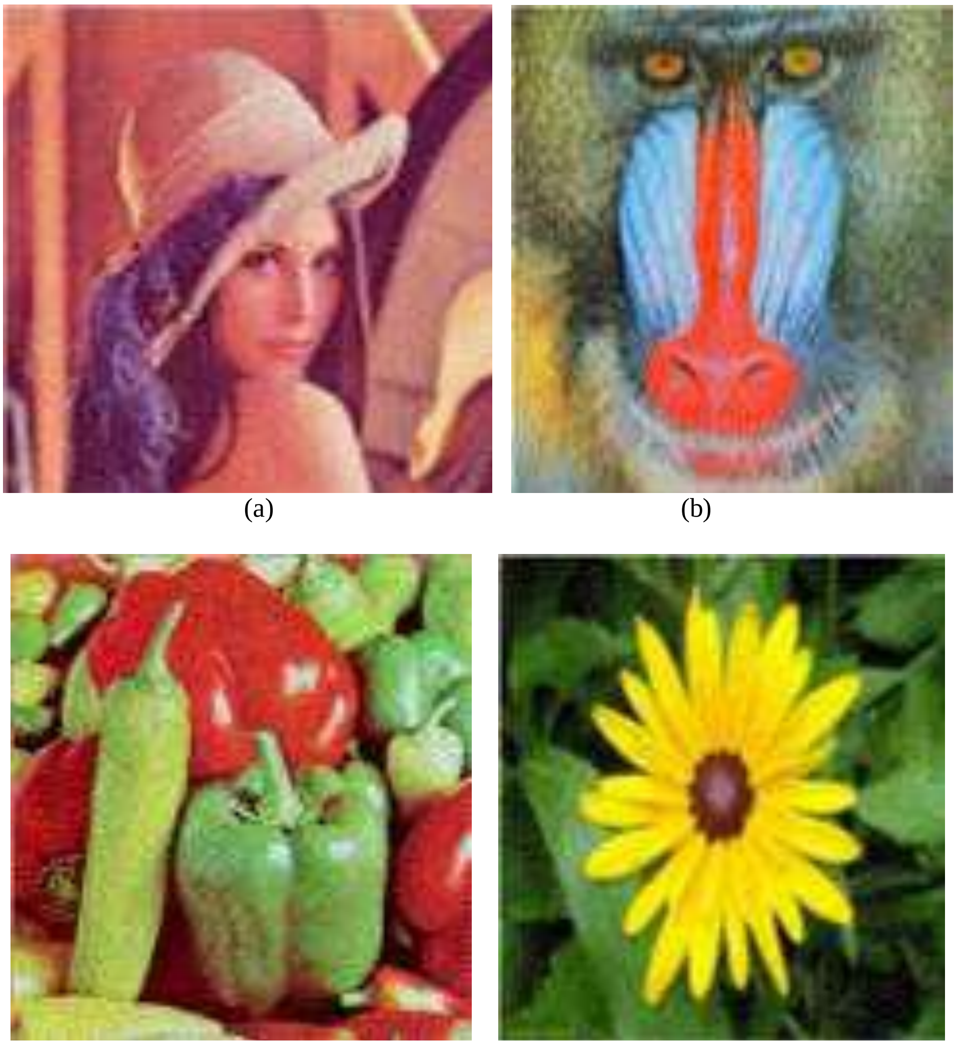


Fig-13: Halftoned Secret Image

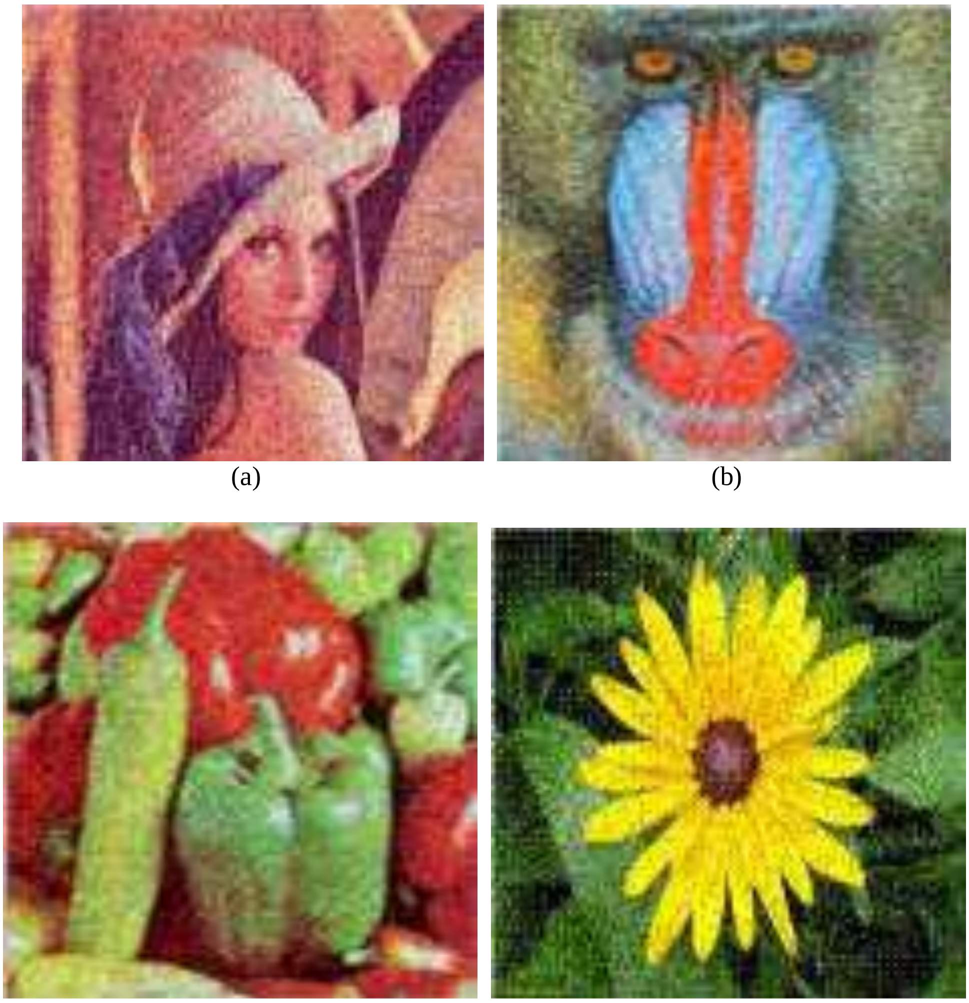

(a)

(b)

(c)

(d)

Fig-14: Halftoned image (a) Lena; (b) Baboon; (c) Vegetables; (d) Flower



(a) (b)

(c) (d)

Fig-15: Encrypted images (a) Lena; (b) Baboon; (c) Vegetables; (d) Flower

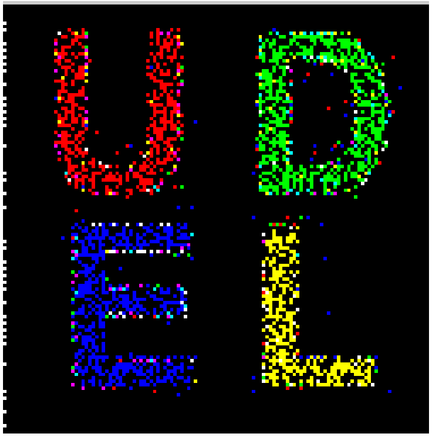


Fig-16: Reconstructed image

Table-4: Output obtained by Floyd error diffusion Halftoning Encryption Method

	PSNR	**Perceived error**
Secret image	23.104566	907187e+005
2 shares	12.3004	8.2697e+006
4 shares	13.52007	5.4748e+006
8 shares	15.71042	5.4740e+006

5. CONCLUSION

In this paper, different algorithms for error diffusion halftoning are compared. The comparison is done on the basis of contrast loss, perceived error between original and halftoned image and the PSNR values. From the implementation of all the algorithms, we detect that

1. If the error is diffused in larger region of pixels it gives sharper details and reduces some of the artifacts.
2. This minimizes the low-frequency artifacts and makes it invisible for the eyes.
3. As the number of elements of the error filters increases, the algorithm becomes slower.
4. Visual quality of halftoned image is higher when Jarvis algorithm is used.
5. Time required is least when Floyd-Steinberg algorithm is used.

By using Floyd Steinberg algorithm, the encryption time can be reduced and the PSNR, Perceived error for combination of 2 shares, four shares and eight shares can also be improved, as shown in table. K out of k extended visual cryptography by random grids technique's contrast can be improved by halftoning through error diffusion method.

REFERENCES:

[1]. M. Naor and A. Shamir, "Visual Cryptography," In Proc. Eurocrypt, 1994, Pp. 1–12.

[2]. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual Cryptography for General Access tructures," Inf. Comput., Vol. 129, No. 2, Pp. 86–106, 1996.

[3]. G.Ateniese, C.Blundo, A.D.Santis, D.Stinson, Extended capabilities for visual cryptography, ACM Theoretical Computer Science 250 (1–2) (2001)143–161.

[4]. C. Blundo, P.D'Arco, A.D.Santis, D.Stinson, Contrast optimal threshold visual cryptography schemes, SIAM Journal on Discrete Mathematics 16(2)(2003)224–261.

[5]. T.Chen, K.Tsao, Visual secret sharing by random grids revisited, PatternRecognition42(2009)2203–2217.

[6]. T.Chen, K.Tsao, Threshold visual secret sharing by random grids, Journal of Systems and Software 84(2011)1197–1208.

[7]. T.Chen, K.Tsao, User-friendly random-grid based visual secret sharing, IEEE Transactions on Circuits and Systems for Video Technology 21(11) (2011)1693–1703.

[8] Y.Chen, G.Horng, D.Tsai, Comment on "cheating prevention in visual cryptography", IEEE Transactions on Image Processing21(7) (2012)3319–3323.

[9]. O. Kafri, E.Keren, Encryption of pictures and shapes by random grids, Optics Letters12(6)(1987)377–379.

[10]. F.Liu, T.Guo, C.Wu, L.Qian, Improving the visual quality of size invariant visual cryptography scheme, Journal of Visual Communication and Image Representation 23(2012)331–342.

[11]. F.Liu, C.Wu, Embedded extended visual cryptography schemes, IEEE Transactions on Information Forensics & Security 6(2)(2011) 307–322

[12]. Z. Zhou, G.Arce, G.D.Crescenzo, Halftone visual cryptography, IEEE Transactions on Image Processing 15(8)(2006)2441–2453.

[13]. 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.

[14]. M. Naor And A. Shamir, "Visual Cryptography Ii: Improving The Contrast Via The Cover Base," Lect. Notes Comput. Sci., Vol. 1189, Pp. 197–202, 1997.

[15]. C. N. Yang and T. S. Chen, "Visual cryptography scheme based on additive color mixing," Pattern Recognit., vol. 41, pp. 3114–3129, 2008.

[16]. Gonzalo R. Arce, Color Extended Visual Cryptography Using Error Diffusion IEEE Transactions on Image Processing, Vol. 20, No. 1, January 201

[17]. Robert W. Floyd and Louis Steinberg, an Adaptive Algorithm for Spatial grayscale. Proceedings of the Society for Information Display 17 (2) 75-77, 1976.

[18]. J. F. Jarvis, 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, 5 13-40, 1976

[19]. P. Stucki, Mecca - A Multiple Error Correcting Computation Algorithm For Bi-Level Image Hard Copy Reproduction. Research Report Rz1060, Ibm Research Laboratory, Zurich, Switzerland, 1981.

[20] Panagiotis Takis Metaxas- Parallel Digital Halftoning By Error- Diffusion.

[21] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, "Visual Cryptography for General Access Structure Using Pixelblock Aware Encoding", Journal Of Computers, Vol. 3, No. 12, December 2008

[22]. S. H. Kim and J. P. Allebach, "Impact of HVS models on model based halftoning," IEEE Trans. Image Process., vol. 11, no. 3, pp. 258–269, Mar. 2002.

[23]. C. C. Lin and W. H. Tsai, "Visual Cryptography for Gray-Level Images by Dithering Techniques," Pattern Recognit. Lett., Vol. 24, Pp. 349–358, 2003.