

## Visual Cryptography Based on Halftoning

<sup>1</sup>Pratiksha P.Patil, <sup>2</sup>Y.M. Patil

<sup>1</sup>(Department of Electronics, K.I.Ts College of Engineering, Kolhapur, India)

<sup>2</sup>(Department of Electronics, K.I.Ts College of Engineering, Kolhapur India)

**ABSTRACT:** Visual cryptography is a type of cryptography which allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. It encodes a secret binary image into shares of different binary patterns. When the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a set of transparencies. But the shares of the decoded image have no meaning. Extended visual cryptography [1] was proposed to construct meaningful binary images as shares, but the visual quality is poor. In this paper, a technique named halftone visual cryptography is implemented to achieve visual cryptography via halftoning. This method utilizes the void and cluster algorithm [2] to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method.

**Keywords -** Digital halftoning, digital watermarking, error diffusion, secret sharing, visual cryptography.

### I. Introduction

The two out-of-two visual threshold scheme where each pixel  $p$  of the secret image is encoded into a pair of sub pixels in each of the two shares is considered. If  $p$  is white, one of the two columns under the white pixel in Fig. 1 is selected. If  $p$  is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly, such that each column has equal probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, is encoded into a black–white or white–black pair of sub pixels with equal probabilities, independent of whether is black or white, an individual share gives no clue as to the value of  $p$ . No secret information can be gained by looking at groups of pixels in each share. If a pixel is white, the superposition of the two shares always outputs one black and one white sub pixel, no matter which column of sub pixel pair is chosen during encoding. If  $p$  is black, it results into two black sub pixels. This is shown in fig. 1. Encoding the secret image shown in Fig.2 (a) leads to the two shares shown in Fig. 2(b) and (c), respectively. Superimposing these two shares leads to the output secret as shown in Fig. 2(d). The decoded image is clearly identified, although some contrast loss is observed. The width of the decoded image is twice that of the original secret image since each pixel is expanded to two sub pixels in each share as shown in Fig. 1. This is called as *pixel expansion*. The two-out-of-two visual threshold scheme demonstrates a special case of t-out-of-n schemes [3], [7]–[9]. All qualified and forbidden subsets of the participants are defined in a more general model for visual sharing schemes based on general access structures in [10]. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The properties of t-out-of-n scheme including the conditions needed for optimal contrast and the minimum pixel expansion that can be attained can be found in [7]–[9]. The concepts of VC have been recently extended such that the secret image is allowed to be a grey-level image rather than a binary image in [12]. Although the secret image is grey scale, shares are still constructed by random binary patterns. The limitation of above methods is that all shares are random patterns carrying no visual information, raising the suspicion of data encryption. Very recently, the method referred to as extended VC has been implemented in [1], where hypergraphcolourings are used aimed at constructing meaningful binary images as shares. Extended VC, however, provides very low quality visual information in the shares, as illustrated later in this paper. Since hypergraphcolourings are constructed by random distributed pixels, the resultant binary shares contain strong white noise consequently leading to inadequate results. The shares also suffer from low contrast between hypergraph black and hypergraph white pixels. This paper focuses on implementing a general halftone visual cryptography framework, where a secret binary image is encrypted into high-quality halftone shares. It applies the rich theory of blue noise halftoning to the construction mechanism used in conventional VC to generate halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image.















	White Pixel	Black Pixel
Share 1		
Share 2	 	 
Stack share1 & share 2	 	 
	 	 

Fig1. A pixel can be encoded into two subpixels in each of the two shares

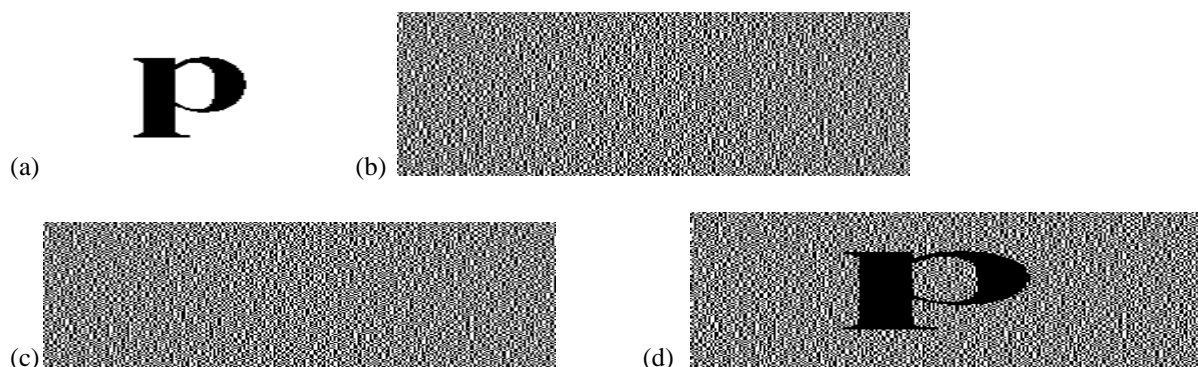


Fig.2 Example of (2,2) visual cryptography.

The halftone shares carry significant visual information to the viewers. The visual quality obtained by the new method is significantly better than that attained by extended VC.

## II. Two-out-of-two halftone visual cryptography method:

Two out- of-two halftone visual threshold scheme is shown in Fig. 3. In this method, a halftone image  $I$ , obtained by applying any halftoning method such as the error diffusion algorithm on a grey level image  $GI$ , is given to participant 1, and its complementary image  $\hat{I}$ , obtained by reversing all black/white pixels of to white/black pixels, is given to participant 2. To encode a secret pixel into a  $Q1 \times Q2$  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. 3. If  $p$  is white,  $M$  a matrix is randomly selected from the matrices  $C0$  of conventional VC. If  $p$  is black,  $M$  is randomly selected from  $C1$ . The secret information pixels in the  $i^{th}$  share are replaced with the two subpixels in the  $i^{th}$  row of  $M$ , as shown in Fig.3. Since  $C0$  and  $C1$  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 pixels in the reconstructed halftone cell, obtained by superimposing the two encoded halftone cells, is white while all other pixels are black as shown in Fig. 4(a) and (b). If  $p$  is black, all pixels in the reconstructed halftone cell are black, as shown in Fig. 4(c) and (d). Thus, the contrast condition is satisfied. The secret pixel can be visually decoded with contrast  $(1/ Q1 \times Q2)$ . In the above procedure, the selection of the secret information pixels in a halftone cell is important as it affects the visual quality of the resultant halftone shares. The simplest method to select the locations of the secret information pixels is random selection. The corresponding pixel replacements, however, are equivalent to adding white noise, which leads to poor visual quality. To obtain better visual results, the void and cluster algorithm [2] is applied to choose these pixel locations. The void and cluster algorithm, performed on a binary dither pattern of the halftone cell, first applies a low-pass finite-impulse response (FIR) filter to obtain a measure of minority pixel density (m.p.d.) at each minority pixel location. The minority pixel is white/black and the majority pixel is black/white, if the halftone cell contains more black/white pixels. The minority pixel with the highest density, denoted as pixel A, is replaced with a majority pixel. The dither pattern is then filtered again by the same low-pass FIR filter to obtain a measure of m.p.d. at each majority pixel location. The majority pixel (different from pixel A) with the lowest density, denoted as pixel B, is then replaced with a minority pixel. Since the complementary pair has the same distribution of the minority and majority pixels, the located pixels A and B are at the same positions in the two shares. The void and cluster algorithm, identifies the minority pixel A with the highest

m.p.d. and the majority pixel B with the lowest m.p.d., and switches their locations. This, in effect, spreads the minority pixels as homogeneously as possible leading to an improved blue noise halftone cell in each share.

The locations of the secret information pixels are then chosen as that of the pixels A and B. Once the matrix M is randomly selected, the  $j^{\text{th}}$  located secret information pixel in the  $i^{\text{th}}$  share is replaced with the  $j^{\text{th}}$  subpixel in the  $i^{\text{th}}$  row of M. The replacement in each share either keeps their original values or switches them with equal probabilities. If the values are kept original, the blue noise halftone cell, generated by the error diffusion algorithm, is used, e.g., the first halftone cell in Fig. 4(a) and (c), and the second halftone cell in Fig. 4(b) and (c). On the other hand, if the values are switched, the new blue noise halftone cell, generated by the void and cluster algorithm, is used, e.g., the first halftone cell in Fig. 4(b) and (d), and the second halftone cell in Fig. 4(a) and (d). Visually pleasing halftone shares are thus obtained. In the void and cluster algorithm, generally, the filter window covers multiple neighboring halftone cells besides the one currently being processed. If a white secret pixel  $p=0$  was encoded into one of the neighboring halftone cells, there is inconsistency in the distribution of the minority/majority pixels between two shares, such as Fig. 4(a) and (b). If the conventional void and cluster algorithm [2] is performed on each share, it may result in different locations of the secret information pixels in the two shares, which is highly undesirable in the halftone VC scheme.

To address this problem, a slightly modified void- and cluster-finding filter, is used to find the m.p.d:

$$DA(x, y) = \sum_{p=-W/2}^{W/2} \sum_{q=-W/2}^{W/2} f(p, q) \cdot P(x + p, y + q) \quad (1)$$

where,  $DA(x, y)$  is the m.p.d. of the pixel with coordinate is the filter, also called weighting function,  $W$  is the filter's window width, and  $P(x+p, y+q)$  is the pixel value at defined as follows:

$$P(x + p, y + q) = \begin{cases} 0.5 & \text{if } P(x + p, y + q) \text{ is a} \\ & \text{secret information pixel} \\ 1 & \text{if } P(x + p, y + q) \text{ is a} \\ & \text{minority pixel} \\ 0 & \text{if } P(x + p, y + q) \text{ is a} \\ & \text{majority pixel} \end{cases} \quad (2)$$

The Gaussian filter is used in [2] as:

$$f(p, q) = e^{\left(-\frac{(p^2+q^2)}{2\sigma^2}\right)} \quad (3)$$

where  $\sigma$  is a scalar constant, offering best results at  $\sigma = 1.5$  in the void and cluster algorithm based on Ulichney's simulations. Unlike the conventional void- and cluster-finding filter, each secret information pixel in the previously processed neighboring cells always takes the value 0.5 in this method, regardless if it is a minority or majority pixel. The value 0.5 is the statistical mean of each secret information pixel, because it has equal probability to be a minority or majority pixel. The above modification of the void and cluster algorithm guarantees that the selection of the secret information pixels A and B is independent of the value of any secret information pixel in the previous halftone cells. Thus, no secret can be inferred from the locations of the secret information pixels which can be detected by comparing the original halftone image and the corresponding halftone share. In addition, since the values of secret information pixels come from the basis matrices of conventional VC, no secret can be obtained by looking at the values of secret information pixels of one share either. Thus, this halftone visual threshold scheme is fully secure. The above proposed construction implements a two out- of-two halftone VC scheme with a pixel expansion  $m^h = Q1Q2$  and relative difference  $a^h = (Q1, Q2)$ , where the superscript "h" indicates that the parameters are for halftone VC. Visually pleasing halftone shares are generated by the blue noise halftoning techniques and the secret image can be reconstructed by superimposing the two shares. The peak signal-to-noise ratio (PSNR) of each halftone share, compared to its original halftone image, can be estimated as,

$$PSNR = 10 \log \frac{255^2}{|0-255|^2 \cdot \frac{2}{Q1Q2} \cdot 50\%} \quad (4)$$

$$= 10 \log Q1Q2$$

where, the item  $|0 - 255|$  denotes the value difference of switching a secret information pixel, the item  $\frac{2}{Q1Q2}$  indicates that two out of  $Q1Q2$  pixels are secret information pixels, and the item 50% indicates that each

secret information pixel is either unmodified or switched with equal probabilities. Thus, the larger the halftone cell size, the higher the PSNR. Also, better performance of the void and cluster algorithm can be obtained in larger halftone cells, leading to higher visual quality halftone shares. On the other hand, the relative difference  $\alpha^h = (Q1, Q2)$  is proportional to the reciprocal of the cell size. Smaller halftone cell sizes lead to higher contrast of the decoded secret image. Therefore, a tradeoff exists between the visual quality of the halftone shares and the contrast of the reconstructed secret image. Also, the share size is usually limited. If the number of sub pixels is increased, the size of sub pixels becomes smaller; this leads to difficulty of superimposing the transparencies onto one another.

### III. Simulation results:

Simulation results for the halftone visual threshold method are illustrated in this section, including the comparison of the proposed method with the method of extended VC. The relationship between the visual quality of the halftone shares and the contrast of the decoded secret image is also exposed.

To compare the result of halftone VC with that of extended VC, a  $128 \times 128$  secret binary image is encoded into two  $512 \times 512$  halftone images using the two methods, respectively. The pixel expansion (halftone cell size) and the relative difference of both methods are the same. The original halftone images, obtained by the error diffusion algorithm and pixel reversal are shown in Fig. 5. The extended VC method [1] results in two shares with poor visual quality and low contrast as shown in Fig. 6(a) and (b). The halftone VC method results in the two visually pleasing halftone shares shown in Fig. 6(c) and (d). The PSNR of these two halftone shares is greater than extended VC. Having the same relative difference in both methods indicates that the same contrast of the reconstructed secret images can be obtained by both methods. This is precisely the case, as shown in Fig. 6(e) and (f). The advantage of the error diffusion is that halftone shares with much better visual quality can be generated, reducing the suspicion of encrypted secret. Note that the positions of secret information pixels in halftone shares are content-based, selected by the void and cluster algorithm. It causes the appearance of some content information in reconstructed secret images, such as the shape of the star in Fig. 6(f).

### IV. Conclusion:

In this paper, a general framework of halftone visual cryptography is implemented. Applying the theory of blue noise halftoning into the construction mechanism of conventional VC, the proposed method generates visually pleasing halftone shares carrying significant visual information. The obtained visual quality is better than that attained by any other available VC method known to date. The new method can be broadly used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, etc.

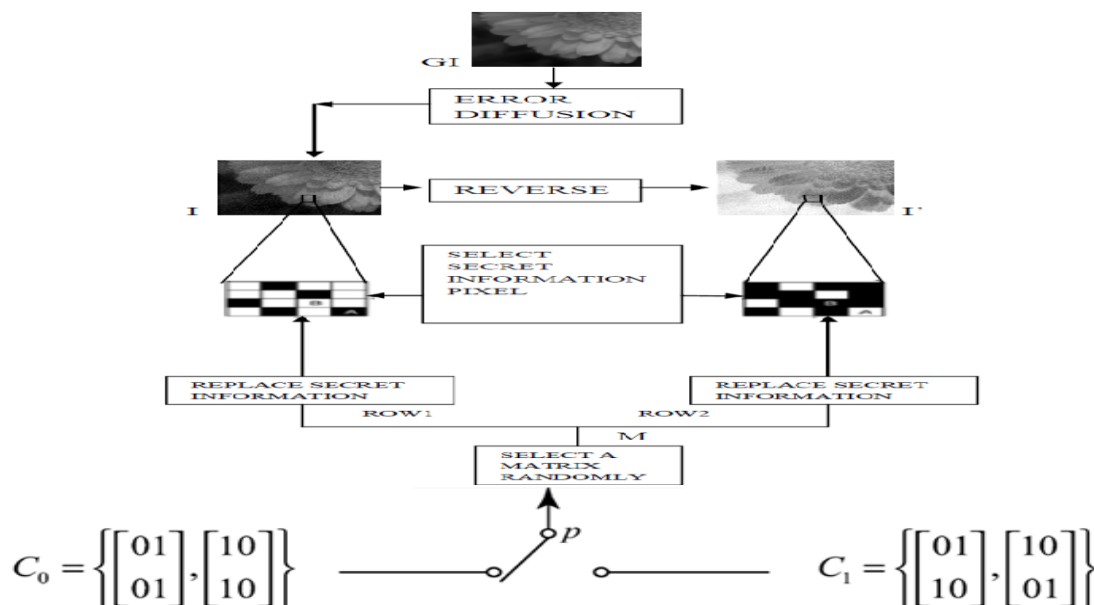


Fig 3.Construction of a two-out-of-two method.

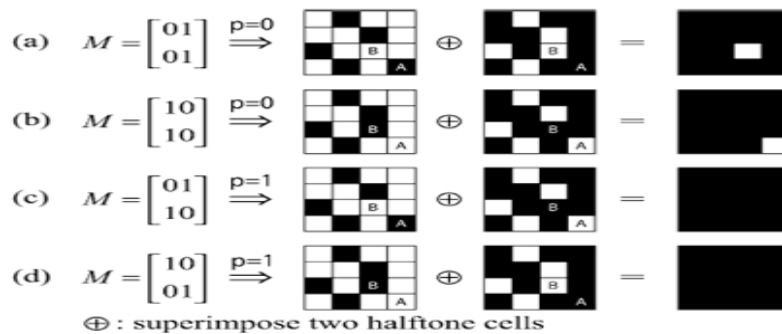


Fig. 4 Matrix M is randomly selected (a),(b) from C0 if p=0, (c), (d) from C1 if p=1 and SIPs are replace



with corresponding sub pixels in

Fig. 5. Original complementary half-tone images generated by error diffusion algorithm and pixel reversal, respectively.

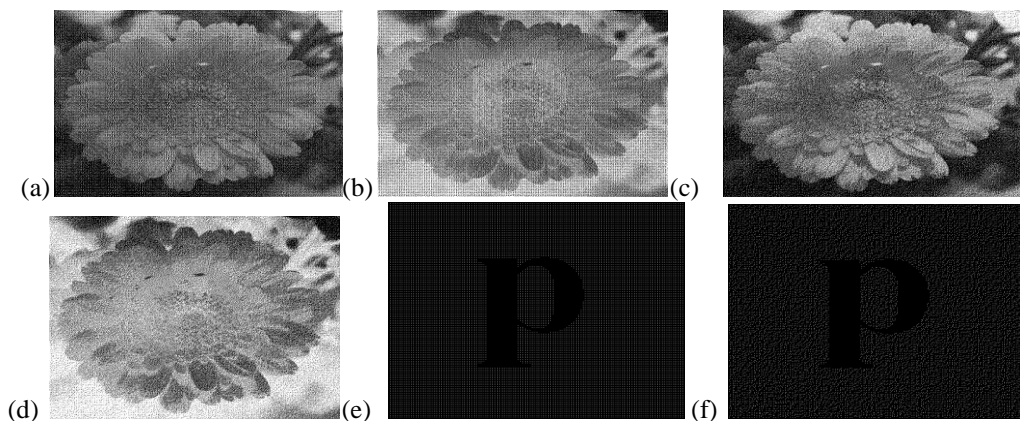


Fig.6. Comparison between extended VC and halftone (a), (b) Two shares of extended VC. (c), (d) Two shares of halftone VC. (e) Decoded Image of extended VC. (f) Decoded image of halftone VC.

**References:**

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoret. Computer Science*, vol. 250, no. 1–2, pp. 134–161, 2001.

[2] R. A. Ulichney, "The void-and-cluster method for dither array generation," in *Proc. SPIE, Human Vision, Visual Processing, Digital Displays IV*, Sep. 1996, vol. 1913, pp. 332–343.

[3] M. Naor and A. Shamir, "Visual cryptography," *Adv. Cryptol.: EUROCRYPT, Lecture Notes Comput. Sci.*, vol. 950, pp. 1–12, 1995.

[4] M. Naor and B. Pinkas, "Visual authentication and identification," *Crypto, Lecture Notes Comput. Sci.*, vol. 1294, pp. 322–340, 1997.

[5] C. Chang and H. Wu, "A copyright protection scheme of images based on visual cryptography," *Imag. Sci. J.*, vol. 49, no. 3, pp. 141–150, 2001.

[6] C. Wang, S. Tai, and C. Yu, "Repeating image watermarking technique by the visual cryptography," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E83A, no. 8, pp. 1589–1598, Aug. 2000.

[7] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptol.: J. Int. Assoc. Cryptol. Res.*, vol. 12, no. 4, pp. 261–289, 1999.

[8] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, 2003.

[9] 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.

[10] 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.

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

[12] L. A. MacPherson, "Grey Level Visual Cryptography for General Access Structures," M.S. thesis, Univ. Waterloo, Waterloo, ON, Canada,