Analysis of the HalfTone Visual Cryptography and proposing a model for illustrating the related schemes

Dr. Amit Chaturvedi[#1], Imtiyaz Rehman[*2]

[#]1Assistant Prof.MCA Deptt., Govt. Engineering College, Ajmer

*2 M.Phil. Scholar

Ajmer, India

Abstract : Halftone visual cryptography (HVC) enlarges the area of Visual cryptography (VC) by using halftoning techniques. Halftoning technique is a reprographic technique.

The main applications of visual cryptography which includes Moire patterns, Watermarking and many others implies more research work to be done on various schemes regarding visual cryptography especially halftone VC which works in a different and better manner than others.

In HVC scheme, a secret image is embedded into halftone shares with meaningful information of the cover images. Meaningful shares are required so as to increase the efficiency of shares management and decrease the suspicion of secret image encryption, thus providing a good image quality as the error diffusion is known to have low complexity. In this paper, we presents an analysis of various construction methods using error diffusion and is guaranteed by the properties of visual cryptography.

Keywords **:** halftone, SIPs, ABPs, cryptography, security, HVCS, EVCS.

I. Introduction

Modern technological age empowers the concept of information sharing which in turn demands the secured sharing methodology to be inhibited so that our important information won't be lost and most importantly won't be misused.

Dealing with the visual information the security related encryption technique is referred to as the visual cryptography. In 1979 Adi shamir published an article "How to share a secret" in which the secret sharing scheme is based on the Lagrange interpolation polynomial [97]. Given a set of points (x_i, y_i) , i =0, 1, 2, 3, ...,k-1, the Lagrange interpolation polynomial can be constructed using :

$$P(x)=\sum_{i=0}^{k-1} y_i \prod_{i\neq} \frac{x-x_i}{x_j-x_i}$$

Later the basic model of the visual cryptography concept was again proposed by Adi Shamir and Moni Naor in 1994 [1].the main concept of visual cryptography scheme is to encrypt a secret image into divided shares, so that that the important information can't be revealed with only a few shares. For a miscreant to misuse the information, all shares are necessarily to be combined. This simple, secure and effective cryptographic scheme involves two transparent images in which one image consists of the random pixels and the second image consists of the secret information. Separately these both are of no use but when superimposed or stacked together reveal the secret image back. It is presented in the figure 1.

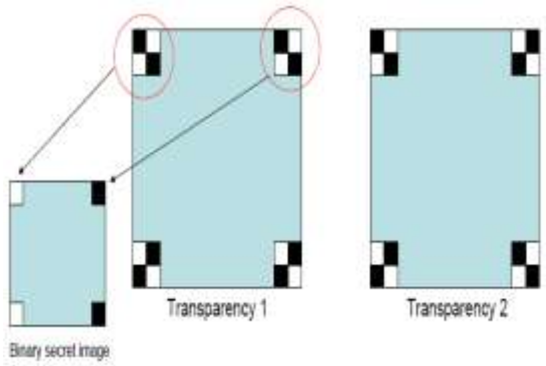

Fig 1: Visual Cryptography

For security reasons, it also ensures that hackers cannot perceive any clues about the secret image from the individual cover images. Initially, visual cryptographic technique was developed for binary images but later on it was advanced later for the color images also. Starting from the basic model, many visual cryptographic techniques have been evolved day by day listed as below:

- (2, 2) Visual Cryptography Scheme
- (k, n) Visual Cryptography Scheme
- Visual Cryptography Scheme for General Access Structure
- Recursive Threshold Visual Cryptography Scheme
- Visual Cryptography Scheme for Grey images
- Visual Cryptography Scheme for Color images
- Multiple Secret Sharing Scheme
- Extended Visual Cryptography Scheme
- Progressive Visual Cryptography Scheme
- Region Incrementing Visual Cryptography Scheme
- Segment based Visual Cryptography Scheme

II. Related work

The Halfotone visual cryptography method of secret sharing expands on Naor and Shamir's original findings in the two-out-of-two secret sharing scheme. This halftone visual cryptography(HVC) takes extended visual cryptography a step further. Halftone is the reprographic technique. The halftoning technique that is used can also be applied to colour and grayscale images. Halftoning simulates a continuous tone through the use of dots, varying either in size or in spacing [26]. Based on the idea of extended visual cryptography, Zhou et al. [21] set about improving these techniques by proposing halftone grayscale images which carry significant visual information.

Traditional VC produces random patterns of dots with no visual meaning until the shares are stacked. This raises the suspicion of data encryption. Halftoning attempts to overcome this suspicion by having visually pleasing attributes. This means creating halftone shares that carry one piece of information, such as another image, while having the secret hidden until both shares are superimposed. This gives no indication that any encryption has been performed on both shares. This way we get a very different and drastic security model for visual cryptography. Along with Zhou, Emi Myodo, Satoshi Miyaji, Z Wang [22, 23, 24] present novel techniques by which halftone images can be shared with significant visual meaning which have a higher quality than those presented by Thomas Hofmeister, Matthias Krause, and Hans-Ulrich Simon within [26] by employing error diffusion techniques [27].

These error diffusion techniques improve the overall quality by spreading the pixels as homogeneously as possible. A halftone scheme [28] was proposed by Mizuho Nakajima and Yasushi Yamaguchi, in which the quality of the shares is improved by using contrast enhancement techniques. However there arose a problem of perfect security with this scheme. By using a space-filling curve ordered dithering technique [29], grayscale images can be converted into an approximate binary image and so allows encryption and decryption of the gray-level images using traditional visual cryptography methods [30]. Further improvements were made in this area by using better error diffusion techniques, the technique proposed in [31] satisfies the following 3 requirements:

I. a secret image should be a natural image
II. Images that carry a secret image should be a high quality natural images and
III. Computational cost should be low.

This technique based on [38] satisfies both (ii) and (iii) and in order to satisfy (i) introduces an additional feedback mechanism into the secret image embedding process in order to improve the quality of the visually decoded secret image. In contrast to this methods described in [28, 35] only satisfy part of the three requirements.

A method was proposed by Myodo et al. [23] which allows natural embedding of grayscale images. Here the quality of the superimposed image highly depends on its dynamic range and pixel density. The possible pixel density of the superimposed image can be defined as: $\max(0, g'_1 + g'_2 - 1) < ds < \min(g'_1, g'_2)$, where g'_1 and g'_2 are pixel values of the dynamic-range-controlled input images and ds is the pixel density of the superposed image that is estimated with the surrounding pixels. The equation indicates that $g'_1 = g'_2 = 0.5$ gives the widest dynamic range of the superimposed image. Therefore, pixel values of input images should be modified around 0.5 by reducing their dynamic range. Each pixel value of a secret image should be restricted between 0 and 0.5 accordingly. This way it provides the mechanism for allowing any grayscale natural image to be used as an input.

The next stage which follows is to embed the grayscale secret image. Along with the conventional method of enhancing the images using a feedback mechanism, another feedback mechanism is proposed to the secret image embedding process to enhance the quality of the superimposed image, which works as follows. Here the typical error diffusion data hiding process is extended and another new system is also added. The extension involves ANDing the temporary shares within the system. The pixel values of the second share are determined one by one during the embedding process. Therefore, this superimposing operation can only be performed on the processed area of the share and therefore, then the proposed method needs to estimate the density of the temporary superimposed image. A low-pass filter such as a Gaussian fillter [31] is used during this density calculation. In order to make the superimposed result closer to the secret image, the new component is introduced. This new process decides how the current density should be controlled, either made darker or brighter. This is controlled by the distance between the pixel values in the secret and the density. If the density is much lower than the pixel value, then the density becomes brighter in order to achieve the desired embedding of the secret. Overall, this improves the quality of the original grayscale secret image. furthermore the most advantageous part of the new mechanism is that no iteration is required in the same way as the method described in [32].The conventional method described in [32] uses an error diffusion halftoning technique which uses two grayscale images as input along with a secret image. Typically, the secret image cannot be used as an input image therefore a ternary image is used as input instead of it. The output images (that carry the secret) are binary images. Firstly, image 1 is taken and an error diffusion process is applied to it (giving share 1), then an image hiding error diffusion process is applied on Image 2. During this image hiding error diffusion process, pixels from image 2 are modulated by corresponding pixels of share 1 and the secret image in order to embed the secret into the resultant share of image 2 (giving share 2). The secret is recovered by superimposing (stacking) share 1 and share 2.

All VC schemes we discussed, suffer from pixel expansion, as in that the shares are larger than the original secret image. Chen et al. [33] present a secret sharing scheme that maps a block in a secret image onto a corresponding equal-sized block in the share image without this pixel expansion. Two techniques which are discussed include histogram width-equalization and histogram depth-equalization. This scheme improves the quality of the reconstructed secret when compared with alternative techniques. Another scheme proposed by Wang et al. [34] uses only Boolean operations. The contrast is also higher than other probabilistic visual cryptography sharing schemes. The area of contrast within halftone and grayscale VC is an interesting one. It is the contrast that determines exactly how clear the recovered visual secret is.

Cimato et al. [35] developed a visual cryptography scheme in 2004 with ideal contrast by using a technique known as reversing, which was originally discussed by [36]. By Reversing technique we can change black pixels to white pixels and vice-versa. Viet and Kurosawa's scheme allows for perfect restoration of the black pixels but only almost perfect restoration of the white pixels. Cimato et al. provide their results for perfect restoration of both black and white pixels. Each share also contained a smaller amount of information than Viet and Kurosawa's which makes it a more desirable and secure scheme. Yang et al. [37] also looked at reversing and the shortcomings of Viet and Kurosawa's scheme. Their work presented a scheme that allowed perfect contrast reconstruction based on any traditional visual cryptography sharing scheme.

III. HALFTONE VISUAL CRYPTOGRAPHY

The journey of development from Visual Cryptography to Halftone Visual Cryptography is presented below in the form of a flowchart.

Basic VC scheme by Naor and Shamir.[1]

⬇

Study of VC problems like contrast, different formats and pixel expansion

⬇

Optical threshold VC with perfect black pixel reconstruction Blundo et al. [3].

⬇

General VC Access structure Ateniese et al.[4]

⬇

Color images scheme Liu et al. [5], Hou et al. [6], Luo et al. [7] and Krishna et al. [8]

⬇

Multiple secrets sharing Shyu et al. [9]

⬇

Threshold VC for different whiteness levels Eisen[10]

⬇

Step construction to improve the visual quality Liu et al. [11]

⬇

Probabilistic VC Ito, et al. [12]

⬇

Probabilistic VC for different thresholds, Yang[13]

⬇

Extended generalisation of probabilistic VCs, Cimato et al. [14].

⬇

Extended visual cryptograpy (EVC), Ateniese et al. [15],

⬇

Two-out of-two EVCs for grayscale images, Nakajima et al. [16].

⬇

EVCs proposed by modifying basic matrices and substituting the subpixels, Tsai et al. [17]and Wang et al. [18]

⬇

Enhanced image quality of traditional EVCs using range distribution instead of the fixed pattern, Yang and Yang [19]

⬇

Embedded EVCs by embedding the SIPs ino meaningful shares,(Design of dithering matrix) Liu et al.[20]

⬇

Halftone visual cryptography HVC (to embed secret into the shares), Zhou et al. [21]

⬇

Three HVCs based on error diffusion, Wang et al. [2]

Fig 2 : Half Tone Visual Cryptography developments

Liu et al.[20] proposed an embedded Extended Visual Cryptography Scheme (EVCS) by embedding the Secret Information Pixels(SIPs) into meaningful shares based on the special design of the dithering matrix, Liu et al.'s EVCS [24] paper proposed that, in order to satisfy the contrast condition, the cover images are darkened before halftoning which may affect the visual quality of the shares. In addition, patterning dithering enables slight grid patterns in the shares .

Later, halftone visual cryptography scheme (HVCS) was introduced by Zhou et al. [21] based on dithering in order to embed secret into the shares. However, in there may be a drop in the visual quality of the re-covered secret image in Zhou et al.'s HVCS, as the embedding scatter of secret information pixels (SIPs) relies on the content of the cover images. Moreover, a pair of complementary images is used and some participants may save more than one shares, which may increase the suspicion of secret image encryption and the bandwidth.

Furthermore, three HVCSs were developed by Wang et al. [2] based on error diffusion.

a. Error Diffusion

Error diffusion technology diffuses the error to the neighbouring pixels. The error means the difference between the original greyscale pixel value and its final halftone pixel value.

Let C denote a normalized image with size of M×N.

For the current pixel position (i, j), 1 ≤i ≤M, 1 ≤j ≤N, Q(i, j)denotes the threshold value, and SC(i, j)is the halftone value. H indicates the error diffusion matrix and E(i, j) denotes the quantization error. Here in Floyd–Steinberg error diffusion matrix [28] shown in Eq.(3) and output-dependent threshold modulation shown in Eq.(4) are adopted in this paper.

$$H=\begin{pmatrix} 0 & (i,j) & \frac{7}{16} \\ \frac{3}{16} & \frac{5}{16} & 1/16 \end{pmatrix} \quad (3)$$

$$Q(i, j) = 0.25 + 0.33 \times 0.25 \times [c(i, j-1) + c(i, j-2) + c(i, j-3)] \quad (4)$$

The flowchart of error diffusion halftoning process is shown in Fig.1, where the output SC(i,j)is computed by Eq.(3):

$$SC(i, j) = \begin{cases} \text{white} & \text{if } d(i,j) \geq Q(i,j) \\ \text{black} & \text{if } d(i,j) < Q(i,j) \end{cases} \quad (5)$$

where $d(i,j) = C(i,j) - \sum_{k,l} H(k,l)E(i-k, j-l)$ and $E(i, j) = SC(i, j) - d(i, j)$.

Since the color representation method of normal digital images is different that of VCS, so the reversing operation is actually applied in Eq.(5).Here the threshold d(i, j)can be position dependent. Error diffusion is simple, but an efficient algorithm to halftone a grayscale image.

$\frac{1}{16} \times$

	•	7
3	5	1

Fig. 3. Floyd–Steinberg error filter. • indicates the current pixel. The weights are given by: h(0, 1) = =7/16, h(1, -1) = 3/16, h(1, 0) = 5/16, and h(1,1) = 1/16

b. Complementary share pair

Given a secret halftone image and multiple grayscale images, halftone shares are generated such that the resultant halftone shares are no longer random patterns, but take meaningful visual images. Without loss of generality, the k -out-of-n scheme is described as follows . firstly a secret image pixel is encoded into □ pixels in each share.□ is the VC pixel expansion and only a function of (k, n).

In halftone VSS, a share image is divided into non-overlapping halftone cells of size q=v1 x v2, where q > □. A secret image pixel is encoded into one halftone cell in each share.

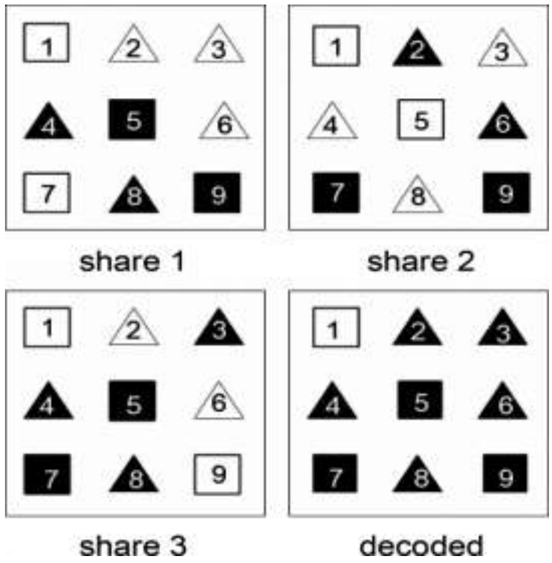

Fig. 4. Example of halftone cells with size q=9 in a 3-out-of-3 scheme using complementary share pair method . Pixels indicated by □ or ■ are SIPs. Pixels indicated by △ or ▲ arenon-SIPs. Shares 2 and 3 are complementary pair.

The locations of the SIPs do not depend on the share images or the secret image, but only on the HVC expansion and q and the underlying VSS scheme. Thus, the distribution of SIPs can be generated prior to the generation of halftone shares.

It is suggested to distribute randomly the SIPs in order to enhance the security purpose it is also desirable to distribute the SIPs homogeneously so that one SIP is maximally separated from its neighboring SIPs in order to achieve good image quality. Upto now the SIPs are maximally separated, the quantization error caused by an SIP will be diffused away before the next SIP is encountered leading to visually pleasing halftone shares.

The process of generating halftone shares via error diffusion is shown in Fig. 5, where the values of the SIPs are preset. To produce the halftone share i, a grayscale image is provided. Let fi(m, n) be the (m, n) th pixel of the grayscale image, then the input to the threshold block is

$$D_i(m, n) = f_i(m, n) - \sum_{k,l} h(k,l)ei(m-k, n-l)$$

Where h(k, l) ∈ H and H is a two dimendional error filter.ei(m, n) is the quantization error at point (m, n).

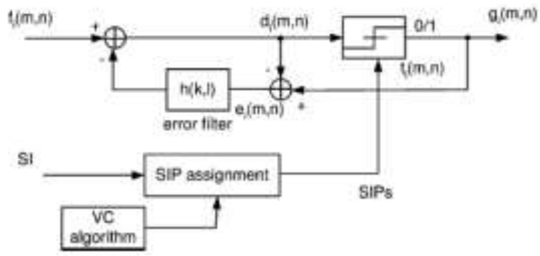

Fig 5 Block diagram of HVC using error diffusion. Depending on the secret image and VC scheme chosen, the SIP assignment block outputs the SIPs. If gi(m, n) is an SIP, its value is prefixed. Otherwise, gi(m, n) is determined by the output of the thresholding block.

c. Using Auxiliary Black Pixels

Use of auxiliary black pixels (ABPs) has the advantage that complementary image shares are not needed. In fact a share is also divided into non-overlapping halftone cells of size q. Over the q pixels,□ pixels are SIPs that carry the secret visual information. There are also □ black pixels that are forced to be black (value 1). These □ black pixels are called auxiliary black pixels (ABPs). ABPs are deliberately introduced into the shares so that some ABPs on one share block the visual information of the other shares. Thus, when qualified shares are stacked together, only the secret visual information is revealed.

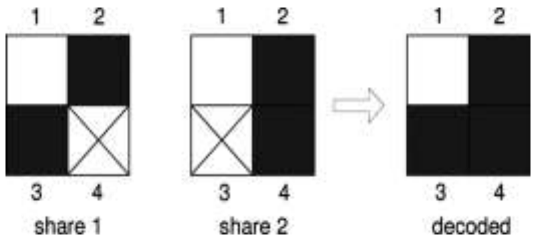

Fig. 6. Example of halftone cells in a 2-out-of-2 scheme using Auxillary Black Pixels. The first and the second pixels in both shares are SIPs. The third pixel in share 1 and the fourth pixel in share 2 are ABPs. Others (“X”) are assigned to carry visual information.

An example of the halftone cells in a 2-out-of-2 scheme using auxiliary black pixels is shown in Fig. 6 where the first and second pixels in each cell are SIPs. The third pixel in share 1 and the fourth pixel in share 2 are ABPs. When stacking two shares together, the result is a white pixel with contrast . The fourth pixel in share 1 and the third pixel in share 2 are assigned values to carry visual information of the shares. They can take value of 0 or 1, which will not affect the decoded image.

Once the assignments for the SIPs and ABPs are determined, a halftoning algorithm can be employed to produce the halftone shares from grayscale images. The process of generating halftone shares via error diffusion is similar to that shown in Fig. 6 except that when is an SIP or ABP, instead of simple thresholding, the value of the output pixel gi(m, n) is predetermined and set as the value of corresponding SIP or ABP. However, we still compute di(m, n) by (4) and the “quantization error” ei(m, n) by (5) for SIPs and ABPs. The error caused by the existence of the SIPs or ABPs is diffused away to the neighboring grayscale pixels. Thus, the SIPs and ABPs are embedded into the halftone shares naturally. Furthermore, the above procedure can be extended to an arbitrary access structure (TQual, Tforb).

d. Using Parallel Error Diffusion.

in this method, the shares are also divided into non-overlapping halftone cells of size q=v1 x v2. □ pixels within the halftone cell are SIPs carrying the secret visual information. But neither complementary shares nor uniformly distributed ABPs are used to satisfy the contrast condition of image decoding. Again, the distribution and the assignment of SIPs are predetermined using the same approach as in complementary share method. After that, the current method halftones the grayscale images in parallel to produce the halftone shares. Within the error diffusion process, all the shares are checked at each non-SIP position to see if a sufficient number of black pixels have been produced. If a sufficient number of black pixels have not yet been generated, black pixels are deliberately inserted at that position. The SIPs are again preserved and not changed.

IV. Conclusion

Comparing with other VCs like EVC and previous HVC methods using the different techniques described in this paper, the HVC using complementary share pair achieves better quality concerning the contrast as main, as the SIPs inserted into the shares are not done by modifying halftone images but are naturally embedded into shares via error diffusion when the halftone shares are generated. Unlike other VCS, halftone has a better strategy as it reduces the suspicion of encryption. It is not easy to predict that some important information is embedded as it is kind of an illusion for a miscreant, all he is seeing a different image beneath which the secret information is encrypted. This gives no indication that any encryption has been performed on both shares. In this paper error diffusion is mainly discussed as it is because of the various methods using error diffusion that a better quality image is decoded unlike all other VC schemes, thereby making HVC scheme a preferred one. Concerning the applications of the HVC and the improvements made in context of quality and contrast, more efforts are required to decrease the share's cross inference from other shares in the future.

ACKNOWLEDGMENT

We feel grateful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript.

REFERENCES

[1] M. Naor, A. Shamir, Visual cryptography, in: Proc. of Advances in Cryptology–EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May, 1994, in: Lecture Notes in Comput. Sci., vol.950, Springer, Berlin, 1995, pp.1–12.
[2] Z. Wang, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography via error dif-fusion, IEEE Trans. Inf. Forensics Secur. 4(3) (2009) 383–396.
[3] C. Blundo, A. De Bonis, A. De Santis, Improved schemes for visual cryptography, Des. Codes Cryptogr. 24(3) (2001) 255–278.
[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for gen-eral access structures, Inf. Comput. 129(2) (1996) 86–106.
[5] F. Liu, C.K. Wu, X.J. Lin, Colour visual cryptography schemes, IET Inf. Secur. 2(4) (2008) 151–165.
[6] Y.-C. Hou, Visual cryptography for color images, Pattern Recognit. 36(7) (2003) 1619–1629.
[7] H. Luo, F. Yu, J.-S. Pan, Z.-M. Lu, Robust and progressive color image visual secret sharing cooperated with data hiding, in: Eighth International Confer-ence on Intelligent Systems Design and Applications, ISDA'08, vol.3, IEEE, 2008, pp.431–436.
[8] N. Krishna Prakash, S. Govindaraju, Visual secret sharing schemes for color images using halftoning, in: International Conference on Computational Intelli-gence and Multimedia Applications, vol.3, IEEE, 2007, pp.174–178.
[9] S.J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, K. Chen, Sharing multiple secrets in visual cryptography, Pattern Recognit. 40(12) (2007) 3633–3651.
[10] P.A. Eisen, D.R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des. Codes Cryptogr. 25(1) (2002) 15–61.
[11] F. Liu, C. Wu, X. Lin, Step construction of visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 5(1) (2010) 27–38.
[12] H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 82(10) (1999) 2172–2177.
[13] C.-N. Yang, New visual secret sharing schemes using probabilistic method, Pat-tern Recognit. Lett. 25(4) (2004) 481–494.
[14] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, Comput. J. 49(1) (2006) 97–107.
[15] G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theor. Comput. Sci. 250(1) (2001) 143–161.
[16] M. Nakajima, Y. Yamaguchi, Extended visual cryptography for natural images, J. WSCG 10 (2002) 303–310.
[17] D. Tsai, T. Chen, G. Horng, On generating meaningful shares in visual secret sharing scheme, J. Imaging Sci. 56(1) (2008) 49–55.
[18] D. Wang, F. Yi, X. Li, On general construction for extended visual cryptography schemes, Pattern Recognit. 42(11) (2009) 3071–3082.
[19] C.-N. Yang, Y.-Y. Yang, New extended visual cryptography schemes with clearer shadow images, Inf. Sci. 271 (2014) 246–263.
[20]F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 6(2) (2011) 307–322.
[21] Z. Zhou, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography, IEEE Trans. Image Process. 15(8) (2006) 2441–2453.
[22] Emi Myodo, Shigeyuki Sakazawa, and Yasuhiro Takishima. Visual cryptography based on void-and-cluster halftoning technique. In ICIP, pages 97–100,2006.
[23] Emi Myodo, Koichi Takagi, Satoshi Miyaji, and Yasuhiro Takishima. Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In ICME, pages 2114–2117, 2007.
[24] Zhongmin Wang and Gonzalo R. Arce. Halftone visual cryptography through error diffusion. In ICIP, pages 109–112, 2006.
[25] Wen-Guey Tzeng and Chi-Ming Hu. A new approach for visual cryptography. Designs, Codes and Cryptography, 27(3):207–227, 2002.
[26] Thomas Hofmeister, Matthias Krause, and Hans-Ulrich Simon. Contrastoptimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science, 240(2):471–485, 2000.
[27] D. L. Lau and G. R. Arce. Modern Digital Halftoning. Marcel Dekker, 2000.
[28] Mizuho Nakajima and Yasushi Yamaguchi. Extended visual cryptography for natural images. In WSCG, pages 303–310, 2002.
[29] Yuefeng Zhang. Space-filling curve ordered dither. Computers & Graphics, 22(4):559–563, 1998.
[30] Chang-Chou Lin and Wen-Hsiang Tsai. Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1-3):349–358, 2003.
[31] Rafael C. Gonzalez and Richard E.Woods. Digital Image Processing. AddisonWesley Longman Publishing Co., Inc., Boston, MA, USA, 2001.
[32] C.N. Yang and C.S. Laih. Some new types of visual secret sharing schemes. volume III, pages 260–268, December 1999.
[33] Ching-Nung Yang and Tse-Shih Chen. New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE Transactions, 89-A(2):620–625, 2006.
[34] Daoshun Wang, Lei Zhang, Ning Ma, and Xiaobo Li. Two secret sharing schemes based on boolean operations. Pattern Recognition, 40(10):2776–2785, 2007.
[35] Chai W. Wu, Gerhard R. Thompson, and Mikel J. Stanich. Digital watermarking and steganography via overlays of halftone images. Volume 5561, pages 152-163. SPIE,2004
[36] Emi Myodo, Koichi Takagi, Satoshi Miyaji, and Yasuhiro Takishima. Halftone visual cryptography embedding a natural grayscale image based on error diusion technique. In ICME, pages 2114–2117, 2007.
[37] Y.J. Song and T.N. Tan. Comparison of four dierent digital watermarking techniques. In Signal Processing Proceedings, 2000. WCCC-ICSP 2000. 5th International Conference on, volume 2, pages 946–950 vol.2, 2000.
[38]Ching-Nung Yang, Chung-Chun Wang, and Tse-Shih Chen. Real perfect contrast visual secret sharing schemes with reversing. In Jianying Zhou, Moti Yung, and Feng Bao, editors, ACNS, volume 3989 of Lecture Notes in Computer Science, pages 433–447, 2006.