A COMPARATIVE ANALYSIS OF MEANINGLESS AND MEANINGFUL SHARES IN VISUAL CRYPTOGRAPHIC ALGORITHM

[1]K. Chitra, [2]Dr. V. Prasanna Venkatesan
[1]Research Scholar, [2]Professor
[1]Department of Banking Technology,
[1]Pondicherry University, Puducherry, India

Abstract: Visual cryptographic scheme was introduced mainly for security concern and the reduction of computation complexity. The working principles of various visual cryptographic schemes are discussed with security level. The PSNR value provides the security level of the information gained in the schemes. The comparative analysis of security features in visual cryptography are discussed as in the form of Meaningless and Meaningful shares in Visual Cryptography. For the security concern visual cryptography able to guaranteed that no one can access the content as well as they don't have any clue to get that information for fake user.

Index Terms **- Visual cryptography, Meaningful Shares, Meaningless Shares, Secret sharing, secret splitting.**

I. INTRODUCTION

Visual Cryptography is a new type of encrypting algorithm which allows the user for encryption and the decryption process is not needed for this algorithm. The beauty of this algorithm is, Human Vision system has to decrypt the encrypted data's. Initially visual cryptographic algorithm was designed by Naor and Shamir [2] based on pixels which are in matrix form. Later, Blakley, Asmuth etc. different people propose different concepts related to visual cryptography in that some of them provide better result and some of them take time to provide those results. For improving the shares quality, security and PSNR value for the image, a meaningful share has been used. The meaningful shares are embedded with other image like cover image using some techniques from that it seems like a different share to provide better security as compared to meaningless shares in visual cryptography.

The Meaningless shares are look like a noise like image that share does not reveal any secret to the user. The computation time is higher in meaningful share as compared to the meaningless share but it provides better security to the information. To maintain the security level higher the meaningful shares are used now a day with some of the security mechanism and also some well-known algorithms are additional used to provide better security to the secret information some of them are steganography, watermarking and some well-known cryptographic algorithms etc.

In this paper cover the full area of meaningful and meaningless shares of visual cryptography. In section 1 provides the slight introduction about the meaningful and meaningless shares of the visual cryptography and their importance. The section 2 provides the literature survey as in the form of generation growth of visual cryptography. The section 3 briefly describe about the working principles of meaningful and meaningless shares in various visual cryptographic schemes. Section 4 discuss the comparative analysis of meaningful and meaningless shares in visual cryptography. Section 5 discuss about the summary of this paper.

II. LITERATURE SURVEY ON MEANINGLESS AND MEANINGFUL SHARES IN VC

2.1 Meaningless shares in Visual Cryptography

Initially visual cryptography was introduced by Naor and Shamir et.al. [2] in 1994. They introduced this scheme for securing the image related data's. They carried out the encryption techniques in 2 out of 2 visual cryptographic schemes for binary images. Here they split the secret messages into n shares depending upon the user requirements. The decryption process has been carried out by the Human vision system. If all the generated shares are combined to retrieve the original secret message. Thomas Hofmeister et.al. [4] uses (k, n) secret sharing scheme for providing better contrast for secret image. The optimal usage of the contrast is done by the code book-based coding of the shares, this has been done by the division of pixels in shares with equal probability. The contrast and the division of sub pixels are made by the coding theory. Pei Fang Tsai et.al. [1] introduced another scheme as (3,3) visual cryptographic scheme. Here they are using 3 shares for encoding process, initially share1 and share 2 are combining to reveal the

secret message. In the same way share 3 and the anticlockwise rotation of the share 1 provides the same secret message. This type of revealing process has been done to providing high range of security features than the existing one.

The halftoning process in visual cryptography for binary image are carried out by Zhi Zhuo et. al. [11]. In this sharing scheme they are using blue noise halftoning process for proving better visual quality than the other scheme so for we discussed. Later the visual cryptographic scheme was migrated to color image by Bert W. Lenng et.al. [13]. This scheme maintains the two levels of security features for the secret message, initially this scheme works on the principle of color composition or decomposition of the primitive colors. For each and every pixel, the primary higher probability of two colors has been taken, from that color combination generates the composition and decomposition of the secret message has been created. This primitive color combination provides color code patterns to generate the black and white mask for the secret message. For the recovering process this scheme requires higher probability of color mask. Ching-Nung Yang et.al. [16] uses (2, n) secret sharing scheme for the concept of region incrementing visual cryptography. This scheme was invented for obtains perfect/correct color for all the regions in the given secret image. The main advantage of using this scheme is, which reduces the shares size and also it enhances the contrast of the particular image.

2.2 Meaningful shares in Visual Cryptography

The meaningful shares in visual cryptography was introduced to provide better security for the secret data's, for that the reviewer using so many techniques and methodology for the creation of meaningful shares some of them are given below as, Jerripothula Sandeep et.al. [8] created a new concept in visual cryptography called extended visual cryptographic scheme. In this scheme general procedure for (2, 2) secret sharing scheme has been used for the separation of shares. After the separation of those shares the cover image has been embedding with each and every share, as a resultant those shares are look like some other shares. Generally, this scheme was introduced for providing better security for communication. (k, n) Meaningful share creation of binary image was proposed by Manesh Kumar et.al. [20]. This scheme was used for getting lesser expansion of secret image and also it providing better image quality for the secret information. In this scheme k number of shares are required for obtaining the secret information, if the shares are lesser than the k number of shares then we can't reveal the secret information further.

Blue noise dithering principles for halftoning technique for meaningful shares was initially proposed by srinivasalu et.al. [19] in 2012. In this technique error dithering process is used to generate the halftone binary shares, this halftone share contains the secret information. That secret information is embedded with cover image using the same halftone dithering process. The advantage of using this scheme, provides better security features than the extended visual cryptography and also the regional incrementing visual cryptography. The migration of meaningful shares in color image was initially proposed by Anantha Kumar Kondra et.al. [18] in 2012. They are using CRC (cyclic Redundant check) algorithm and error diffusion technique for meaningful share generation. Here CRC is used for maintain the position and color composition of the image and the error diffusion is used for maintain the shadow image creation. The error diffusion technique helps to provide a best quality of shadow images. In this paper CRC not only used for above mention points but also used for visual information pixel synchronization, from that they make this method as so efficient and easy to generate the halftone process. CRC for VIPS provides best security features compared to other techniques in visual cryptographic scheme.

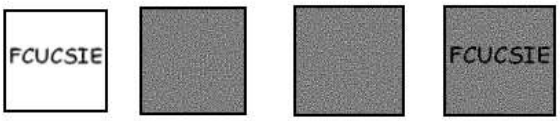
Anuprita Mande et.al. [21] using stucki Algorithm and error diffusion halftone, to produce a meaningful color image in visual cryptography. This algorithm makes the encryption and decryption of the secret message as much as easier from that they reduce the computation time for visual cryptography. The introduction of spectral model for color image was introduced by Jacques Machizaud et.al. [17] in 2012. The spectral model is used for color reproduction of the secret information. This approach generates a new method in visual cryptographic scheme as pixel color matching of the image. The spectral model describes the printed color as in the form of optical point of view.

III. WORKING PRINCIPLES OF VISUAL CRYPTOGRAPHY FOR MEANINGLESS AND MEANINGFUL SHARES:

These techniques focus on dealing with different types of shares needed to reveal a secret image and guarantee that the secret image can be transmitted on the Internet securely and it does not have any heavy computation or complex encoding/decoding process.

3.1 WORKING PRINCIPLES OF MEANINGLESS SHARES:

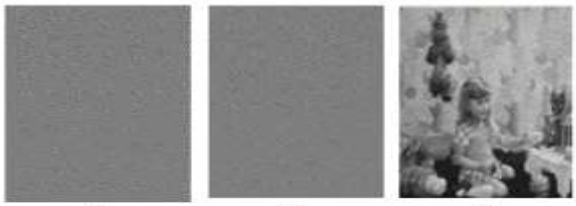
i) Meaningless Shares for Binary Images: The binary image [1, 22] format is the simplest form of image, which having two extreme levels of data as 0 and 255. We are taken that 0 as black pixel and 255 as white pixels. Nowadays, this type of image format occupies an important position in the image handling area. The original image is transformed into binary image which contain a group of two white and black pixels. The white pixel is called as transparency and black pixel is simply called as black. It is obvious that, to reveal the secret image, the two shares are stacked together to construct the original image. The following fig.6 shows the working process of meaningless shares for binary image in visual cryptography.



(a) (b) (c) (d)

Fig. 1. Visual cryptography in binary image domain: (a) original secret image, (b)First share image, (c) second share image, and (d) stacked result of (b) and (c).

ii) Meaningless Shares for Grayscale Images: Grayscale image [3, 6] is an image where the value of each pixel having independent pattern and this intensity carries information about the secret. This type of image composed exclusively to the shades of gray which varies weakest intensity value to the strongest intensity value i.e. from the black image to the white image. As a result, the measurement of the light intensity of each pixel having an electromagnetic spectrum of single band. The intensity of gray scale pixel image is expressed in the range from 0 to 255.



(a) (b) (c)

Fig. 2. An experimental result: a) and b) meaningless shares for grayscale image and c) Stacked image.

When dealing with the grayscale image, it initially transformed into halftone image. Mostly the transformed image should be in black and white format. This format of image can be easy to generate the meaningless shares which has to be shown in the fig.7. The shares are generated based on the code book of visual cryptography. If the selected pixel is black, then any one combination of the code book is selected for shares and the resultant will be black pixel. Similarly, the same process has to be taken for white pixel and the resultant will be white. According to this way, each pixel in the halftone image has been decomposed and overlapped at the receiver side. The overlapping must be in correct order to reveal the secret information.

iii)Meaningless Shares for Colorful Images: In the method [7], initially it carried out the halftoning process. In this halftoning process each and every pixel of the halftone image is expanded into n×m blocks of the two-share image. The shares having several blocks which has to be filled with primitive colors of RGB. The color intensity of RGB occupies a quarter space in that blocks. Besides, the particular color position of share 1 and share 2 are interchanged and the transparency is revealed by overlapping those two shares. For example, the share1 and share2 transparency shows the red color then the share pattern will be 1/2 of the blocks are in red color, 1/4 of the blocks must be in green and 1/4 of the blocks must be in blue color. These three-proposition combined to form a red like color. The construction of the color table has been clearly explained in this paper within the section visual graphic scheme for color image. To reconstruct the secret information is by stacking the share1 over the share 2 in correct order. From that the secret image can be gained, whose color intensity will range from (1/4, 1/4, 1/4) to (1/2, 1/2, 1/2). The result of this type of schemes has been shown in the fig.8. Furthermore, we are considering bout the security of the system. we are all know that 3! = 6. So, the combinations of each and every color distribution has 2 combinations of color, that has to be taken place within m×n blocks of share 1 and 2. The probability of 512×512 secret image is 1/220.585, this shows difficult the visual crypto system to crack the robustness of the secret image over the transmission taken place on the internet. Thus, the visual cryptographic system is guaranteed that it provides better security and robustness over the internet transmission.

(a) (b) (c)

Fig. 3. Experimental result: (a) and (b) meaningless colorful shares and (c) the stacked image.

iv)Meaningless Shares for Progressive Images: In progressive visual cryptography [8] the secret image can't be guess by any of the two or more shares. From the combination of two or more shares provides only the layout of the shares and we can't determine what it is? Most of the time it looks like a noise like image. In this method, we can reveal the secret progressively by one after the another by all combination of shares are put together, then only the secret image has to be clearly viewed by the human vision system. The progressive visual cryptography having percentage of shares i.e. if the first share looks like the noisy image from that we can't get any information about the secret. The second share having little bit of outlay with the combination of noise like image it also doesn't provide any information about the secret. Similarly, all the combination of shares having some layout along with the noise like image. At the last stacking of all the shares provides the secret image. The practical work of progressive visual cryptography has shown in the fig.9. From the given example initially, we took the halftoning process later share creation process has been taken place. In the share creation we set the threshold as 6 so we having only 6 no. of shares, by overlapping all the 6 shares only we can get the secret image.

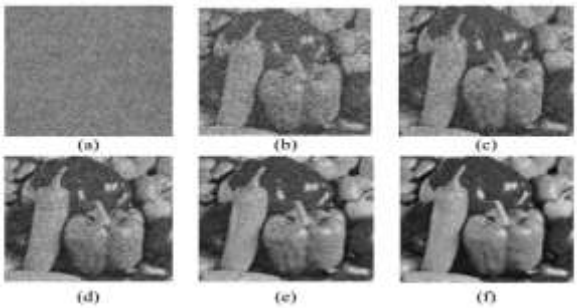


Fig. 4. Progressive mechanisms for viewing the secret image step by step on different levels: (a) Meaningless share, (b) two shares, (c) three shares, (d) Four shares, (e) five shares, and (f) six shares.

3.2 WORKING PRINCIPLES OF MEANINGFUL SHARES:

Visual cryptography provides various advantages to the researchers such as it provides less computation, it is free from the complex theories of cryptography and it generate results without any key generation mechanism. The meaningless shares are sometimes suspicious by the invaders. They can import malicious attacks to this technique from that they destroy the shares. So, to avoid this type of attacks, a meaningful share is proposed by the researchers on behalf of the noise like shares. Meaningful shares are providing better security over the transmission of an images in the internet. Visual cryptography provides an opportunity to the watermarking techniques, they can provide a way how the secret image has been securely transmitted over the internet. The meaningful shares are achieved by embedding the cover image to each and every share. After that it looks like a meaningful share called camouflage images.

i) Meaningful Shares for Binary Images: Meaningful shares for binary image [14, 15, 16] having 3 steps to construct the secret information. The first stage is the generation of shares (screen blocks), the second stage is the share block grouping and the final stage is the generation of secret images. The mechanism for the generation of those three stages is given as follows,

1. the shares has been generated based on the code book and rules of visual cryptography, those share values are kept in $m \times m$ sized arrays.

2. the generated shares are embedded with different cover images by using watermarking or steganography method.

3. stacking all the shares at the receiver end, it shows the required secret information that will be in the matrix size of $2m \times 2m$.

The meaningful shares for binary image are gained on the basis of traditional visual cryptographic schemes, and the experimental results are given in Fig. 10.

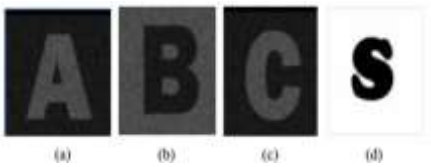


Fig. 5. Experimental results of the mechanism of Hsu *et al.*: (a), (b), and (c) meaningful binary shares and (d) stacked result image.

ii) Meaningful Shares for Grayscale Images: The grayscale visual cryptographic schemes [11, 16, 17] are widely used area. In the early years they were using meaningless share it provides prone to the attackers to get some information about the secret to avoid that meaningful share creation of gray scale image has been introduced. In that, cover image has been used for share protection that we call it as meaningful shares by combining all those shares then the original shares will be retrieved. As shown in Fig. 11, the secret information "FCUCSIE" can be viewed by stacking all the shares, which are meaningful that has to be embedded with cover image. According to the embedding rule, the process of overlapping images can vary with shares and characters of cover image. The embedding rules provides the meaningful shares which is shown in the Fig. 11, which is a small example for the generation of meaningful shares. Initially, the sub-blocks of the meaningless overlapped share are compared with their corresponding cover image. If the selected subpixel shows "1" in the meaningless overlapped share, then the corresponding block assigning the same value for the cover image. Otherwise, it will be "0" in the overlapped share block, then the corresponding block of the final share is still 0.

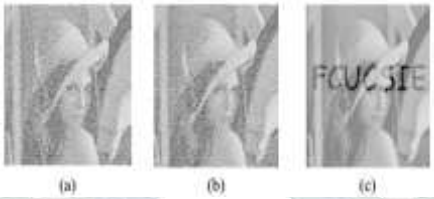


Fig. 6. Meaningful shares for a grayscale image.

iii) Meaningful shares for color image: the meaningful shares are produced to avoid arousing the attention of hackers. In the proposed scheme, halftone technique, [12, 13] cover coding table, and secret coding table are utilized to generate two meaningful shares. There are four main procedures in this scheme. The first one is color halftone transformation, where the color image is transformed into a colourful halftone image. The second procedure is the pixel extraction process, where the pixels are retrieved from the color halftone image. Following it, there come the encoding and decoding procedures, respectively. On the purpose of generating shares, two $N\times N$ cover images are employed to encode the $N\times N$ secret image and make two $2N\times 2N$ shares called share 1 and share 2. As it is concerned, share 1 is a meaningful share that appears just like the cover image 1, while share 2 is a meaningful share similar to the cover image 2. In the last, within the decoding procedure, the secret image can be easily figured out by stacking share 1 and share 2. Furthermore, in this scheme, there are two coding tables referred to in the encoding procedure, naming the cover coding table and the secret coding table. The cover coding table is responsible for the encoding process of the cover image; on the other hand, the secret coding table is used to encode the secret image. Moreover, the secret coding table works in a color recognition way. For example, if one pixel of the transferred halftone image is green, then the ratio of pixel color must be 100%, 0%, and 100% for C, M, and Y, respectively. By this way, each block in share 1 comes as the permutation of pixels: cyan, magenta, yellow, and white. Subsequently, the above rules are applied, and the coding table is used to produce a block of share 2, where the permutation of the pixels is yellow, magenta, cyan, and white. When all the pixels have been processed, two shares are produced faultlessly. Each block of the two shares consists of C, M, Y, and W. Therefore, the secret image can be rapidly recognized according to the human visual system when the two shares are stacked.

(a) (b) (c) (d)

Fig. 7. Secret image obtained by stacking the two color meaningful shares:(a), (b), and (c) the meaningful shares for color images; (d) the stacked image.

iv)Meaningful Shares on Progressive Visual Cryptography: Here the method with meaningful shares for progressive visual cryptography [24, 25] is introduced to simplify the management of the shares and enhance the security of the secret image. Fang proposed a mechanism of generating meaningful shares for progressive visual cryptography in 2007 based on the cover-image-embedding concept, which is illustrated in Fig. 12.

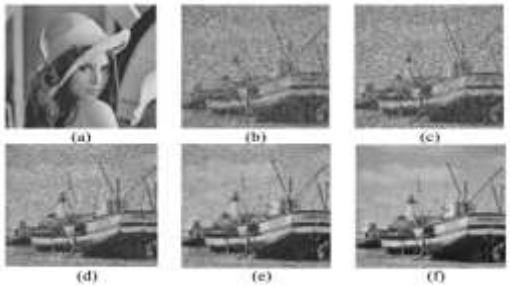
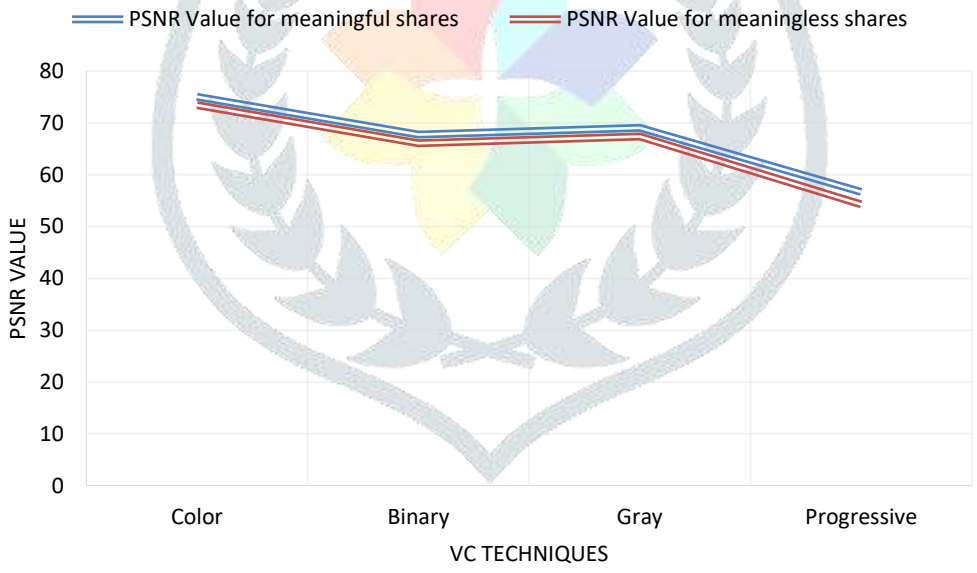


Fig.8. Experimental result comparison: (a) meaningful share and (b), (c), (d), (e), and (f) Progressive stacked images.

There are two phases, of which the first one expands the original image; thus, every pixel corresponds to a 2×2 block. That is to say, if the size of the original image is 256×256, then the size of the expanded one is 512×512. Referring to Table 2, if the pixel value is black, then all pixels of the corresponding block is black; on the contrary, if the pixel is white, the corresponding block contains two white and two black pixels. After finishing this, the second phase of creating shares is carried out. In this process, each block of shares is generated by checking the stego-image. Compared with the previous method for progressive visual cryptography with meaningless shares, this method employing the meaningful shares can withstand the malicious attacks coming from the suspicious invaders caused by the noise-like shares.

IV. RESULT EXAMINED BY VISUAL CRYPTOGRAPHYIC ALGORITHM:

In this section, we discuss about the PSNR Value variation in different schemes based on meaningful and meaningless shares in visual cryptography. From that survey we compared PSNR Values for meaningful shares and meaningless shares on various visual cryptographic techniques. From that it clearly shows that meaningful share provides more security compared to meaningless shares. In the meaningful shares, visual cryptographic technique for color image produce better security level among the other meaningful shares in VC techniques. The following graph clearly shows the comparison variation among the techniques and also the schemes.



Graph 1: security level comparison in meaningful and meaningless shares in visual cryptography

The following table discuss about the generation growth of the visual cryptographic schemes by various persons. Here the tabulation is based on various schemes used in meaningful and meaningless shares for visual cryptography. The results obtained by every author provides the security level what they obtained in that schemes not only that but also, they discussed about the various schemes security level approached by various cryptographic algorithms.

Table 1: summary of background study on meaningful and meaningless shares in visual cryptography

Author	No. of Secret image	Format	Type of Share	Pixel Expansion	Technique	Result

Naor and Shamir	1	Binary Image	Meaningless	4	VCS	**Fair**
Thomas hofmeister	1	Binary image	Meaningless	4	Contrast optimal k, n scheme	**Fair**
Pie-Fang Tsai	3	Binary image	Meaningless	2	3,3 visual secret sharing scheme	**Fair**
Bert W.Leung	1	Color image	Meaningless	2	Patten recognition	**Fair**
W. P Fang	1	Binary image	Meaningless	4	Patten recognition	**Fair**
Zhi Zhuo	N	Binary image	Meaningless	4	Novel encryption technique	**Fair**
Ching-Nung Yang	N	Color image	Meaningless	7	2, n regional incrementing technique	**Poor**
Srinivasulu	1	Binary image	Meaningful	4	Halftone technique	**Fair**
Anantha kumar	1	Color image	Meaningful	1	Error diffusion method	**Good**
Jerripothila Sandeep	1	Binary image	Meaningful	Pixel expansion small	General access structure	**Good**
JacquesMachi zaud	1	Color image	Meaningful	2	Classical clustered halftoning	**Fair**
Maneesh kumar	1	Binary image	Meaningful	1	k, n secret sharing scheme	**Good**
Anuprita Mande	1	Color image	Meaningful	1	Error diffusion method	**Good**

V. CONCLUSION

In this paper various visual cryptographic techniques are considered based on their security level. Here the security level is taken as the performance evaluation values of visual cryptography in meaningful and meaningless shares. The comparison between the meaningful and meaningless shares are discussed and the working principles of meaningful and meaningless shares are briefly explained here. The background study on meaningful and meaningless shares are obtained based on the result get by each and every author in different visual cryptographic schemes.

VI. REFERENCES

[1] P. Tsai and M. Wang, "An (3, 3) -Visual Secret Sharing Scheme for Hiding Three Secret Data," *Engineering*, pp. 1–4, 1994.

[2] M. Naor and A. Shamir, "Visual Cryptography," *Adv. Cryptogr.*, pp. 1–12, 1995.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, 1996.

[4] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal out of secret sharing schemes in visual cryptography," *Theor. Comput. Sci.*, vol. 240, no. 2, pp. 471–485, 2000.

[5] C. C. Thien and J. C. Lin, "An Image-Sharing Method with User-Friendly Shadow Images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 12, pp. 1161–1169, 2003.

[6] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, no. 1–3, pp. 349–358, 2003.

[7] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003.

[8] D. Jin, W. Yan, and M. Kankanhalli, "Progressive color visual cryptography," *J. ...*, vol. 14, no. 3, p. 033019, 2005.

[9] G. Xuan *et al.*, "Digital Watermarking," *Springer-Verlag Berlin Heidelb.*, vol. 4283, no. June 2014, pp. 323–332, 2006.

[10] W.-P. Fang and J.-C. Lin, "Progressive viewing and sharing of sensitive images," *Pattern Recognit. Image Anal.*, vol. 16, no. 4, pp. 632–636, 2006.

[11] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, 2006.

[12] H. C. Wu, H. C. Wang, and R. W. Yu, "Color visual cryptography scheme using meaningful shares," *Proc. - 8th Int. Conf. Intell. Syst. Des. Appl. ISDA 2008*, vol. 3, pp. 173–178, 2008.

[13] B. W. Leung, F. Y. Ng, and D. S. Wong, "On the security of a visual cryptography scheme for color images," *Pattern Recognit.*, vol. 42, no. 5, pp. 929–940, 2009.

[14] F. Liu and C. Wu, "Embedded Extended Visual Cryptography Schemes," *IOSR J. Comput. Eng.*, vol. 2, no. 1, pp. 30–37, 2010.

[15] X. Wu, D. S. Wong, and Q. Li, "Extended Visual Cryptography Scheme for color images with no pixel expansion," *2010 Int. Conf. Secur. Cryptogr.*, vol. 7, pp. 1–4, 2010.

[16] C. N. Yang, H. W. Shih, C. C. Wu, and L. Harn, "K out of n region incrementing scheme in visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 5, pp. 799–810, 2012.

[17] J. Machizaud and T. Fournel, "Two-out-of-two color matching based visual cryptography schemes," *Opt. Express*, vol. 20, no. 20, p. 22847, 2012.

[18] A. K. Kondra and S. U. V. R. Kumari, "An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion," *Int. J. Eng. Res. Appl.*, vol. 2, no. 5, pp. 1090–1096, 2012.

[19] M. V Srinivasulu and K. Ramanajaneyulu, "Visual Cryptography Scheme using Halftone Technique," *Int. J. Electron. Commun. Technol.*, vol. 7109, pp. 90–93, 2012.

[20] M. kumar and S. Mukhopadhyay, "Visual cryptography for black and white images," *Int. J. Inf. Comput. Technol.*, vol. 3, no. 11, pp. 1149–1154, 2013.

[21] A. Mande and M. Tibdewal, "A Fast Encryption Algorithm for Color Extended Visual Cryptography," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 4, pp. 364–371, 2013.

[22] X. Wang, Q. Yuan, H. Cai, and J. Fang, "A New Approach to Image Sharing with High-Security," *J. ACM*, vol. 61, no. 6, 2014.

[23] P. L. Chiu and K. H. Lee, "An XOR-based progressive visual cryptography with meaningful shares," *2016 1st IEEE Int. Conf. Comput. Commun. Internet, ICCCI 2016*, pp. 362–365, 2016.

[24] B. Sivakumar and K. Srilatha, "A novel method to segment blood vessels and optic disc in the fundus retinal images," *Res. J. Pharm. Biol. Chem. Sci.*, vol. 7, no. 3, pp. 365–373, 2016.

[25] C. Yang, C. Wu, and Y. Lin, "k out of n Region-Based Progressive Visual Cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8215, pp. 1–10, 2017.