Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

A (n, n) Extended Visual Cryptography Technique to Share Grayscale Image

Akshay Gajanan Bhosale[1], Pritam Baburao Nikam[2]
[1,2] *Assistant Professor, Sanjay Ghodawat University, Kolhapur, Maharashtra, India*

Abstract:- Visual Cryptography (VC) is used for sharing secret images among various participants. Different VC techniques are available to share binary, grayscale and colour images. Basic advantage of VC is that the secret image can be revealed without any computation. Now-a-days due to evolution of digital world the internet and computing devices are available everywhere. So, for revealing the secret image, computing devices can be used instead of printing the share on transparencies. Also, it is easy to maintain the transparencies in digital form rather than printed transparencies. In this paper, we have developed a (n, n) visual cryptography technique, where $n \leq 8$, to share grayscale images. Shares generated are meaningful and hence it avoids suspicion. The recovered secret image is totally lossless. Each pixel of grayscale secret image is decomposed into 8 binary bits and these bits are encrypted in the shares. Every pixel of secret image is converted into a block of 3×3 pixels, hence the dimensions of cover image are increased by three times. There is no pixel expansion in this technique, it means the dimensions of original secret image and recovered secret image are same.

Keywords*: Grayscale Visual Cryptography, Secret Image Sharing, Extended Visual Cryptography, Perfect Reconstruction.*

1. Introduction

The concept of Visual Cryptography (VC) was introduced by Naor and Shamir [1]. VC is used to share binary, grayscale or colour images among a set of participants. The secret image is divided into 'n' pieces called shares and when the required number of shares are overlapped, the ORing operation takes place between the pixels of shares and the secret image is revealed. The traditional VC has drawbacks of pixel expansion and loss of contrast of recovered images. The dimensions of recovered secret image are large as compared to the original secret image and the contrast is also poor. In addition to this, the shares are random noise-like images which creates suspicion in mind of the eavesdropper. A lot of research was done to improve the contrast of recovered secret image. Some techniques were developed to minimize the pixel expansion. Ateniese et al. developed an extended VC scheme in which the shares were having meaningful images on it to avoid suspicion about encrypted secret image [2], [3]. Some techniques use Generalized Access Structures (GAS) to share the secret. These GAS have two sets viz. qualified access structure and forbidden access structure [4] – [6]. Random grid VC was developed to have size-invariant recovered secret image [7], [8]. XOR-based VC was introduced to eliminate the problem of pixel expansion and to have perfect reconstruction of the secret image [9], [10]. The main advantage of VC is that it does not require any computation for recovering the secret image. When the shares are overlapped, the Human Visual System (HVS) identifies the contrast difference and recognizes the secret image.

There are some practical disadvantages of VC. The shares have to be printed on transparent sheets of paper or plastic. As the number of participants go on increasing, it becomes tedious task to handle these shares. For revealing the secret image, all the shares must be properly aligned. If one of the shares is misaligned, then the secret will not get revealed. Also, if the number of shares are more, then the contrast of recovered secret image is very low. All these practical problems associated with VC make it less useful for real world applications. But today in the world of digital evolution, almost everywhere we have Internet and computing devices. So instead of printing the shares on transparencies, the shares can be digitally superimposed using some computing device and the secret can be revealed. This can avoid the problem of handling the printed transparencies and also the problems related to alignment of these shares after superimposing. In this paper, we have introduced a (n, n) VC technique

to share grayscale images. For this technique the maximum value of 'n' can be 8. It means this technique can have minimum 2 to a maximum of 8 participants. This technique generates meaningful shares using cover images. A single pixel of secret image is represented using a 3×3 block in the shares; hence the dimensions of shares are increased by 3 times as compared to original secret image. However, the dimensions of recovered secret image and original secret image are exactly same i.e., there is no pixel expansion. Also, the recovered secret image is totally lossless. As the number of participants increase from 2 to 8, the quality of cover images on shares also improves.

The contributions of this paper are as follows. We have developed a (n, n) visual cryptography technique to share true grayscale image with a constraint on maximum participants involved ($n \leq 8$). The shares generated by the proposed technique are meaningful grayscale shares. The reconstruction of the secret image is totally lossless and size-invariant.

The remaining sections in this paper are as follows. In the second section, some works related to the proposed technique are discussed. Section 3 describes the proposed (n, n) VC technique to share grayscale image. The results obtained by the proposed technique are showcased in section 4. Finally, some concluding remarks are given in section 5.

2. Related Work

The traditional VC shares only binary secret images and the shares generated by these techniques are random noise-like images. These techniques have drawback of pixel expansion and loss of contrast. The sharing of binary images is relatively easy as it has only two bits 0 and 1, but each pixel in grayscale and colour image must be represented using 8 and 24 bits respectively. For sharing grayscale images, most of the researchers used a technique called halftoning. Using halftoning a continuous tone grayscale image is converted into binary image. Some other techniques like dithering, error diffusion etc. are used for the same purpose. Yung-Fu Chen et al. developed a technique that maps a block from secret image into the share without pixel expansion. They have developed two techniques based on width and depth of histogram to generate blocks having multiple levels based on the density of black pixels. The quality of recovered secret image is much better than the previous techniques [11]. Cheng-Chi Lee et al. developed a technique without pixel expansion to share grayscale images having different distribution of gray pixel values. The reconstructed images were having high contrast and were free from artefact and contours [12]. Bin Yan et al. developed a framework to combine halftoning and VC encoding process. In this framework, the shares from encoder are used for reconstructing the pixel and the difference between the reconstructed pixel and original pixel is fed back to the system. This technique generates good quality recovered secret images [13]. Longdan Tan et al. proposed a technique which uses Chinese Remainder Theorem (CRT) to share grayscale images. In this technique, weights are assigned to shares and when the weights cross a certain level threshold of then the secret image is revealed. For this technique, as the number of shares increase, the quality of recovered secret image also improves and lossless recovery is possible if all the shares are involved [14]. Yogesh K. Meghrajani et al. proposed a binary arithmetic-based technique to share multiple secrets. Using this technique grayscale images can be shared but the shares generated are not meaningful [15]. Xuehu Yan et al. developed a General Access Structure (GAS) in which each qualified share can be assigned probability. This technique uses CRT and the shares generated are not meaningful [6]. Xuan Zhou et al. developed a polynomial based technique to share secret images. The size of shares is also reduced and the recovered secret image is lossless [16]. Shravani Mahesh Patil et al. developed a technique based on pixel value co-ordinate sharing for sharing multiple secrets. The shares generate are of fixed size irrespective of the size of original secret image also the recovered secret image is completely lossless [17]. Maroti Deshmukh et al. developed a technique to share multiple colour secret images combining multi-secret sharing scheme and Chinese Remainder Theorem [18]. Priyanka Singh et al. proposed a XOR-based technique having different algorithms to generate basis matrices, random shares and to convert random shares to meaningful shares [19]. Kirti Dhiman et al. proposed two techniques to share true colour images having meaningful shares. The first technique is a (3, 3) extended visual cryptography technique (EVCT) and the second is (2, 3) EVCT [20]. Saeideh Kabirirad et al. investigated the existing (n, n) multi-secret sharing schemes and claimed that even if less than 'n' participants are involved still some information about secret image can be revealed by some computations. They proposed a technique to remove

this drawback and to share grayscale and colour images [21]. Rui Sun et al. developed a size-invariant technique to share grayscale images using direct binary search and multi pixel encryption [22]. This algorithm is applied on halftone images. XuehuYan et al. developed a random grid-based VC technique with meaningful shares and no pixel expansion [23]. The quality of recovered secret image is adaptive in nature. It can be changed at the cost of quality of meaningful shares. Dao-Shun Wang et al. proposed a reversing based VC technique to minimize pixel expansion and have optimal contrast for grayscale images [24]. A VC technique with optimal contrast and with minimum number of shares to be held by each participant was designed. Peng Li et al. developed a (2, 3) VC technique which has 3 shares and can be used to share 1 or 2 secret images [25]. The secret can be revealed by performing OR operation and the contrast of recovered secret images can be further improved by performing XOR operation. The shares have 1.5 times the dimensions of secret images. Shivendra Shivani et al. developed a (2, 2) verifiable multi-tone VC technique in which the secret image is shared using meaningful shares of same size and each share is having a dedicated bit for providing the authenticity of shares [26]. The recovered secret image is lossless and size-invarient. The paper introduces a (2, 2) Visual Cryptography (VC) technique for sharing two secrets with only two shares. Unlike traditional methods with cumbersome rotations, the technique in [27] allows revealing the secrets by overlapping the shares and flipping the second share horizontally. Additionally, it accommodates secrets of different dimensions, and its performance is evaluated on various binary images using different metrics. The paper [28] presents an authentication system utilizing Visual Cryptography (VC) to encrypt passwords for accessing question papers. Two transparencies, each containing part of the password, are sent to internal and external supervisors. The passwords can be revealed by overlapping these transparencies using a simple software or by physically printing and overlapping them, offering a secure method for accessing exam materials.

3. The proposed (n, n) extended VC technique to share grayscale image

The proposed (n, n) VC technique allows a maximum of 8 participants. So, we can share the grayscale image with up to 8 people. In this technique, every pixel of grayscale secret image is converted in 8-bit binary number and shared using a 3×3 pixel block. The position of every binary bit in the 3×3 pixel block is fixed as shown in table 1. The number of 3×3 blocks that will be present in the share will depend on the number of pixels present in the secret image. The shares that are generated using this technique will have 3 times the dimensions of secret image. However, when the secret image is extracted and reconstructed, it is lossless and having same dimensions as original secret image. Hence, this technique is also size-invariant technique. The process for the proposed encryption and decryption is shown in figure 1.

Encryption Process

Step 1: Select the grayscale secret image and grayscale cover images equal to the number of participants. The dimensions of the cover images should be same as the dimensions of secret image.

Step 2: The grayscale secret pixel is decomposed in 8 binary bits. These bits are placed in a 3×3 block at specific positions and these blocks are placed in different shares. The position of these bits for specific number of participants is as shown in table 1.

Step 3: Repeat step 2 for every grayscale secret pixel. Intermediate shares are generated after placing 3×3 blocks in all the shares for every secret pixel.

Step 4: The final shares are generated by embedding the cover image pixels at vacant positions in intermediate shares. Cover image 1 is used for share 1, cover image 2 is used for share 2 and so on. The (i, j) th pixel of cover image is embedded in (i, j) th 3×3 block of intermediate share.

Step 5: The meaningful shares are ready to be shared among ‘n’ participants.

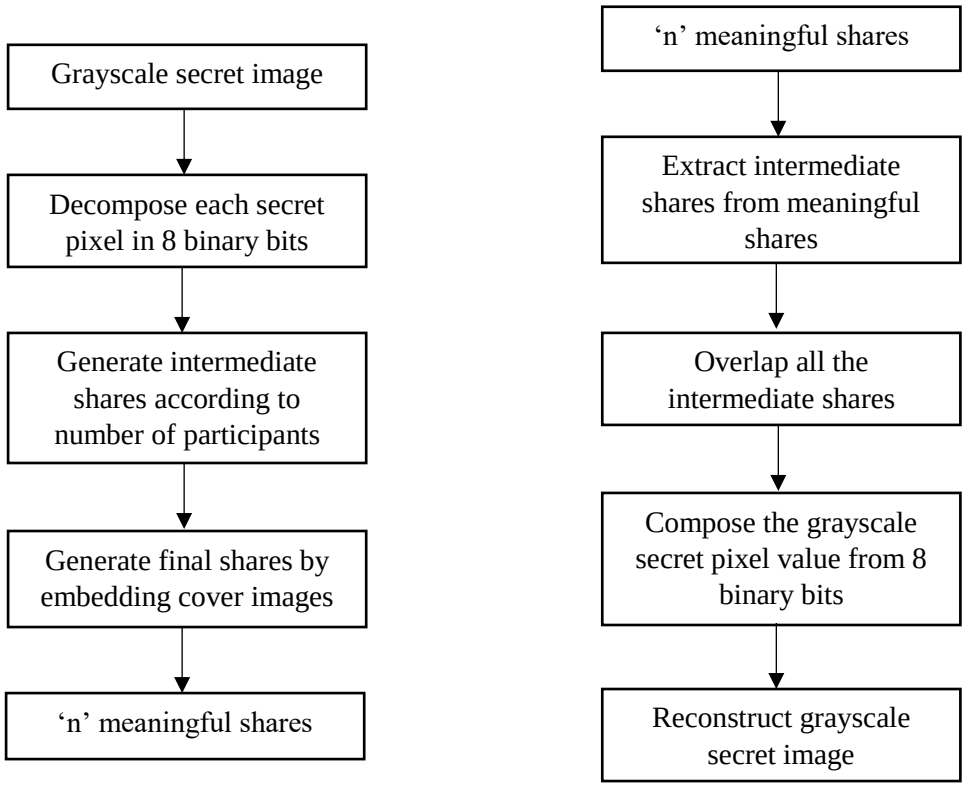
Decryption Process

Step 1: Get the ‘n’ meaningful shares from ‘n’ participants.

Step 2: For every 3×3 block in each share, make the values greater than 1, equal to zero.

Step 3: Superimpose all the shares using OR operation. The resultant share generated will be a matrix in which each 3×3 block has 8 binary bits related to grayscale secret pixel value as shown in figure 2.

Step 4: The 8 binary bits in each 3×3 block are recomposed to form a value between 0 to 255 and the matrix generated is a grayscale secret image.



a. Encryption Process b. Decryption Process

Fig. 1. Process of the proposed VC technique

D_1	D_2	D_3
D_4	0	D_5
D_6	D_7	D_8

Fig. 2. 3×3 blocks formed in resultant matrix after ORing 'n' shares

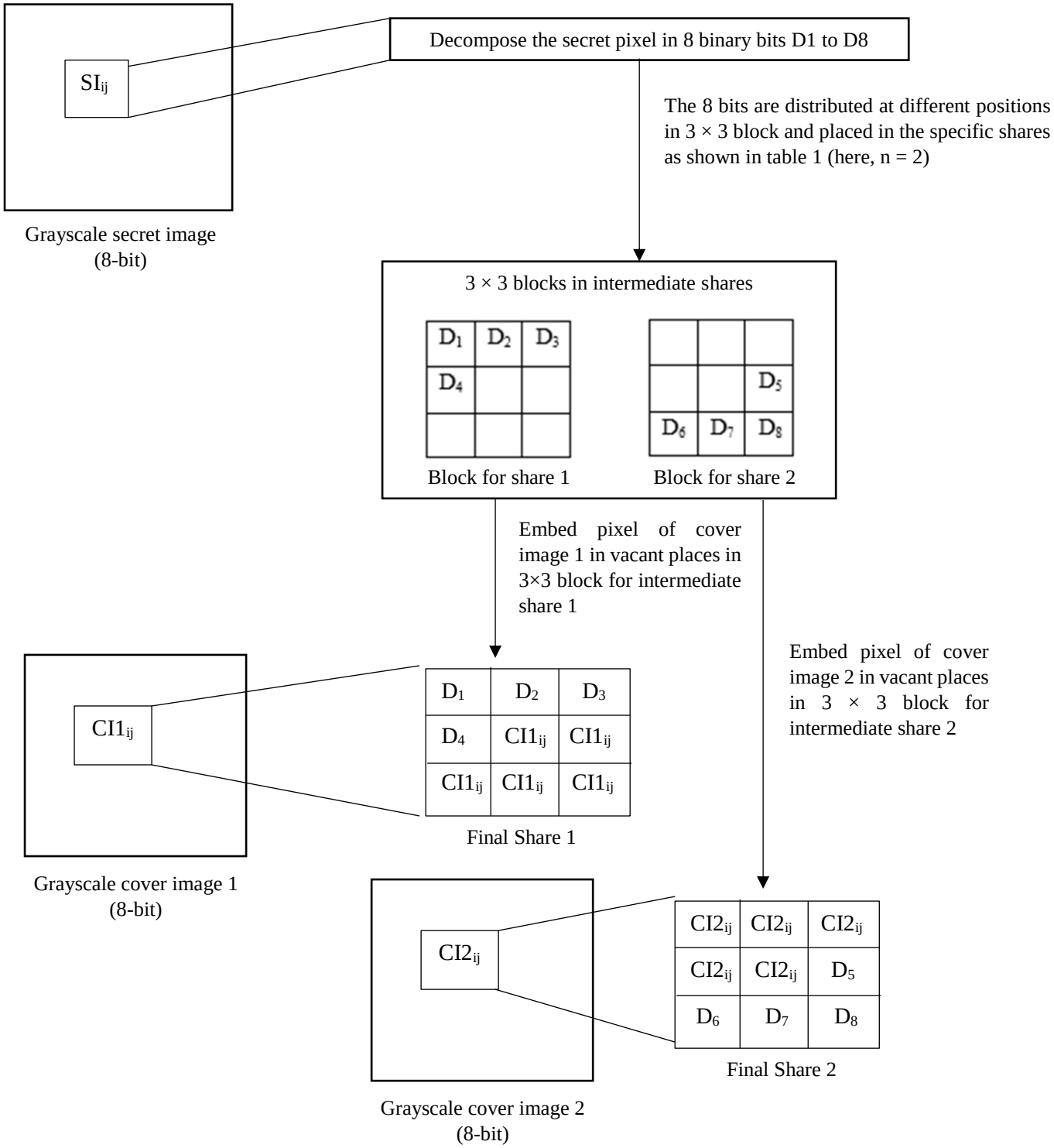


Fig. 3. Detailed encryption process for the proposed technique

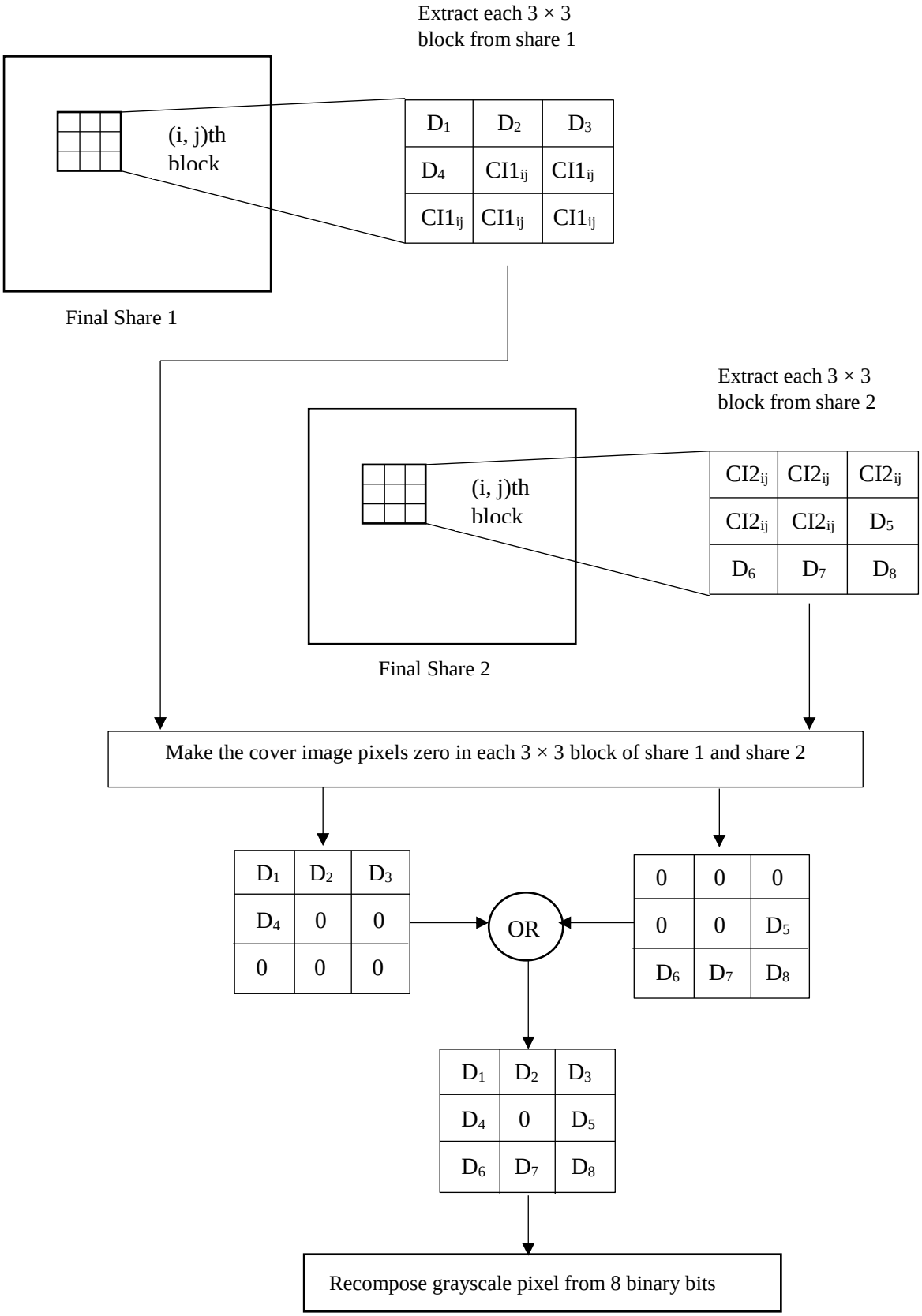
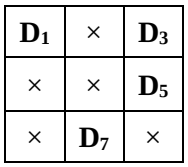
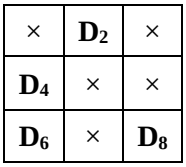
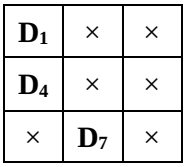
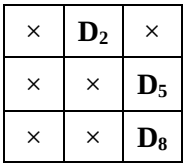
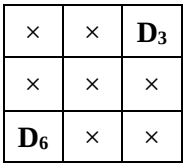
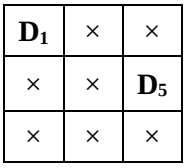
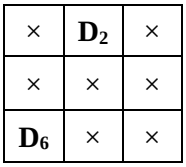
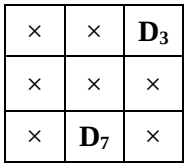
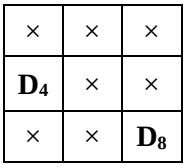
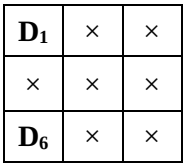
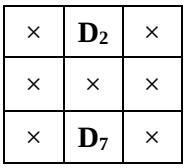
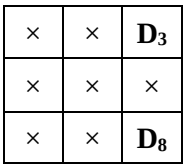
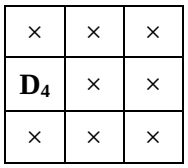
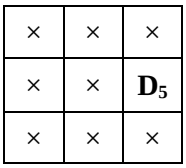
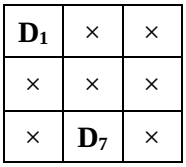
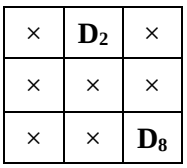
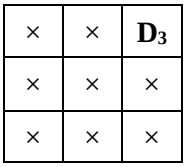
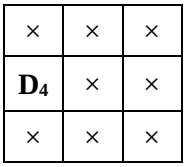
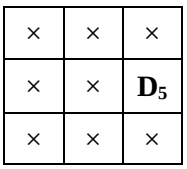
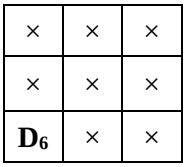


Fig. 4. Detailed decryption process for the proposed technique

Table 1. 3×3 block templates for distributing binary bits for different shares according to number of participants

Number of participants (n)	Distribution of 8 binary bits in 3 × 3 block for different shares according to number of participants
2	 Share 1  Share 2
3	 Share 1  Share 2  Share 3
4	 Share 1  Share 2  Share 3  Share 4
5	 Share 1  Share 2  Share 3  Share 4  Share 5
6	 Share 1  Share 2  Share 3  Share 4  Share 5  Share 6

Number of participants (n)	Distribution of 8 binary bits in 3 × 3 block for different shares according to number of participants			
7	**D1** × × / × × × / × × **D8** — Share 1	× **D2** × / × × × / × × × — Share 2	× × **D3** / × × × / × × × — Share 3	× × × / **D4** × × / × × × — Share 4
	× × × / × × **D5** / × × × — Share 5	× × × / × × × / **D6** × × — Share 6	× × × / × × × / × **D7** × — Share 7	
8	**D1** × × / × × × / × × × — Share 1	× **D2** × / × × × / × × × — Share 2	× × **D3** / × × × / × × × — Share 3	× × × / **D4** × × / × × × — Share 4
	× × × / × × **D5** / × × × — Share 5	× × × / × × × / **D6** × × — Share 6	× × × / × × × / × **D7** × — Share 7	× × × / × × × / × × **D8** — Share 8

The 8 binary bits are distributed in different shares in such a way that even if any unauthorised participant gets access to any of the share, he will not be able to get any information of the secret image. This happens because the bits are distributed sequentially among all the shares. For example, for n = 2, the bits from D_1 to D_8 are distributed alternately between share 1 and share 2. Hence share 1 contains 50% of information about the secret pixel value and remaining 50% information is present in share 2. As the number of participants increase, the information about the secret pixel gets distributed among all those shares. For n = 8, each share has only one bit information about the secret pixel.

The entire process of encryption and decryption is explained using a specific case of (2, 2) VC technique. Consider a grayscale secret image is to be shared among 2 participants. Let the grayscale secret image has a matrix SI, cover image 1 has matrix CI1 and cover image 2 has matrix CI2 as shown below.

$$SI = \begin{bmatrix} 123 & 80 & 200 \\ 48 & 154 & 125 \\ 66 & 44 & 89 \end{bmatrix} \quad CI1 = \begin{bmatrix} 45 & 112 & 145 \\ 211 & 134 & 90 \\ 26 & 144 & 189 \end{bmatrix} \quad CI2 = \begin{bmatrix} 13 & 43 & 20 \\ 148 & 54 & 25 \\ 166 & 94 & 91 \end{bmatrix}$$

Now we have to decompose the grayscale secret image pixels into 8 binary bits and we have to place these binary bits in 3×3 blocks for share 1 and share 2 as shown in figure 5.

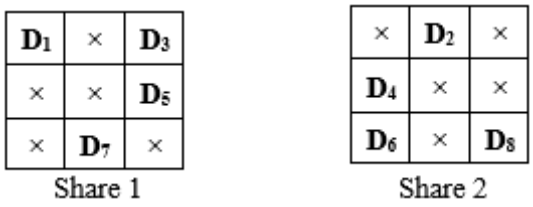


Fig. 5. 3×3 blocks for share 1 and share 2 for 2 participants

Here, bit D_1 is Least Significant Bit (LSB) and D_8 is Most Significant Bit (MSB). The first pixel in SI has value $(123)_{10}$ which is represented in binary as $(01111011)_2$. These bits are placed in 3×3 blocks as shown in figure 6. These 3×3 blocks are placed in the intermediate shares as shown in figure 7. Once all the secret pixels in SI are converted in 8 binary bits and placed in 3×3 blocks in the intermediate shares, we have to embed the cover image pixels in the intermediate shares. Cover Image 1 (CI1) is used for share 1 and Cover Image 2 (CI2) is used for share 2.

a. 3×3 block for share 1 b. 3×3 block for share 2

Fig. 6. 3×3 blocks for secret pixel value of $(123)_{10}$

a. 3×3 block placed in intermediate share 1 b. 3×3 block placed in intermediate share 2

Fig. 7. Intermediate Shares

The first pixel of CI1 is placed in the vacant places of first 3×3 block of intermediate share 1. Similarly, the first pixel of CI2 is placed in the vacant places of first 3×3 block of intermediate share 2. This process is repeated for the entire secret image and final meaningful share matrices are generated as shown in figure 8.

1	45	0	0	112	0	0	145	0
45	45	1	112	112	1	145	145	0
45	1	45	112	1	112	145	1	145
0	211	0	0	134	0	1	90	1
211	211	1	134	134	1	90	90	1
211	0	211	134	0	134	90	1	90
0	26	0	0	144	1	1	189	0
26	26	0	144	144	0	189	189	1
26	1	26	144	0	144	189	1	189

a. Share 1 matrix

13	1	13	43	0	43	20	0	20
1	13	13	0	43	43	1	20	20
1	13	0	0	43	0	0	20	1
148	0	148	54	1	54	25	0	25
0	148	148	1	54	54	1	25	25
1	148	0	0	54	1	1	25	0
166	1	166	94	0	94	91	0	91
0	166	166	1	94	94	1	91	91
0	166	0	1	94	0	0	91	0

b. Share 2 matrix

Fig. 8. Meaningful share matrices

For decryption of the secret image, the values in meaningful shares that are greater than 1 are made 0. After that both the shares are ORed together and a single matrix is formed as shown in figure 9. From this matrix 3×3 non-overlapping blocks are formed as shown in figure 10 and grayscale value is calculated. The first 3×3 block has the values as shown in figure 10. After comparing it with figure 2, we get the binary value as $(01111011)_2$ which is equivalent to $(123)_{10}$.

1	1	0	0	0	0	0	0	0
1	0	1	0	0	1	1	0	0
1	1	0	0	1	0	0	1	1
0	0	0	0	1	0	1	0	1
0	0	1	1	0	1	1	0	1
1	0	0	0	0	1	1	1	0
0	1	0	0	0	1	1	0	0
0	0	0	1	0	0	1	0	1
0	1	0	1	0	0	0	1	0

Fig. 9. Matrix formed after making the values in share 1 and share 2 matrices equal to zero and ORing them together

1	1	0
1	0	1
1	1	0

Fig. 10. First 3×3 non-overlapping block from matrix in Fig. 9

4. Results and Discussions

The results shown here are for a specific case of proposed (n, n) VC technique with number of participants n = 2. The grayscale secret image is shown in figure 11.


a. Secret image (128×128)


b. Cover image 1 (128×128)


c. Cover image 2 (128×128)

Fig. 11. Images used for proposed (2, 2) VC technique

The meaningful shares that are generated are shown in figure 12. These shares have dimensions, three times that of the secret image. During step 3 of decryption process, the two shares are ORed and a single matrix is formed. The image of that matrix is as shown in figure 13. The recovered secret image is shown in figure 14.


a. Share 1 (384×384)


b. Share 2 (384×384)

Fig. 12. Meaningful shares generated from proposed VC technique

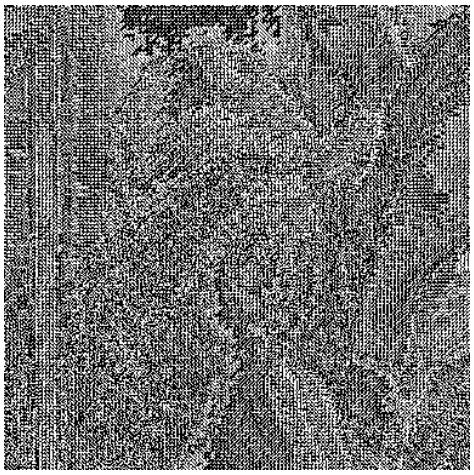
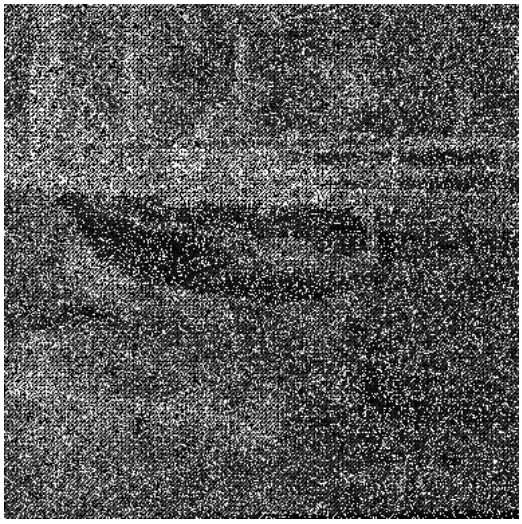


Fig. 13. Image generated during step 3 of decryption process

Fig. 14. Recovered secret image (128×128)

The proposed technique is also tested on share images corrupted by noise. The share images were made noisy by adding salt and pepper noise with the density of 0.3. Approximately, 0.3×M×N pixels will get affected by the noise, where M and N are the number of rows and columns in the share image. After adding noise, the binary bits that are embedded in the shares may get corrupted and the secret image may not get recovered properly. The noisy share images are shown in figure 15. The recovered secret image from noisy shares is shown in figure 16.

a. Share 1 (384×384)



b. Share 2 (384×384)

Fig. 15. Meaningful shares corrupted with salt and pepper noise of density 0.3

Fig. 16. Recovered secret image (128×128) from shares in Fig. 14

The effect of noise on the recovered secret image will go on reducing as the number of participants increase from 2 to 8. The number of binary bits of secret image that are embedded in each share decreases as the number of shares increase, hence the probability that the binary bits are corrupted also decreases. The quality of recovered secret images and the quality of shares is computed using Peak Signal to Noise Ratio and Structural Similarity Index [29]. Some other objective evaluation metrics are used in [30], but most of these are suitable for binary images. The results of the quality metrics are as shown in table 2.

Table 2. Image quality metrics

Parameter	Share 1		Share 2		Recovered secret image	
	Without noise	With noise	Without noise	With noise	Without noise	With noise
PSNR	6.5528	6.2840	6.5484	6.2487	39.1339	13.5169
SSI	0.9906	0.9896	0.9904	0.9895	1	0.9988

The PSNR indicates the quality of image, higher the value of PSNR, better is the quality of image. The PSNR value for share 1 and share 2 for both noise and without noise is very close to each other. However, the visual quality of the share images with noise is very poor. There is significant difference in the value of PSNR for recovered secret images in both cases but still the secret image is recognizable. The SSI finds the visual impact of structure, contrast and luminance of the image. The value of SSI close to 1 indicates that the image is similar to the reference (original) image. The values obtained for noisy shares and normal shares is nearly equal to 0.98 and 0.99 respectively.

Some of the VC parameters are considered for comparison of some of the existing VC techniques. These parameters are described as follows:

1. Type of secret image: Using VC, binary, grayscale and colour images can be shared. The proposed technique can share a grayscale image.
2. Type of shares: The shares generated can be either random or meaningful. The random shares have noise-like structure on it while the meaningful shares have some valid image embedded on it. The proposed technique has meaningful shares.
3. Type of scheme: The VC technique can have different number of participants involved in it. The secret image gets revealed when the desired number of participants are present. The proposed technique requires ‘n’ participants and all ‘n’ participants should be present to reveal the secret image.
4. Recovered secret image: The recovered secret image can be lossy or lossless. The lossy image has loss in contrast while the lossless image is same as secret image. The proposed technique has lossless reconstruction of secret image.
5. Pixel expansion: For many VC techniques, the dimensions of recovered secret image are larger than the original secret image. For the proposed technique, there is no pixel expansion.

Table 3. Comparison of some VC techniques

Authors	Type of secret image	Type of shares	Type of scheme	Recovered secret image	Pixel expansion
Kirti Dhiman et al. [20]	Colour	Meaningful	(2, 3) and (3, 3)	Lossless	No
Maroti Deshmukh et al. [18]	Grayscale, Colour	Random	(n, n)	Lossless	No
Priyanka Singh et al. [19]	Grayscale	Meaningful	(n, n)	Lossless	No
Rui Sun et al. [22]	Grayscale	Random	(2, 2)	Lossy	No
Longdan Tan et al. [14]	Grayscale	Random	(k, n)	Lossy / Lossless	No
XuehuYan et al. [23]	Grayscale	Meaningful	(2, 3)	Lossy	No
Shivendra Shivani [26]	Grayscale	Meaningful	(2, 2)	Lossless	No
Proposed technique	Grayscale	Meaningful	(n, n) $n \leq 8$	Lossless	No

5. Conclusion

In this paper, we have developed a (n, n) VC technique to share true 8-bit grayscale image. The minimum and maximum number of participants for the proposed technique are 2 and 8 respectively. The shares generated in the proposed technique are meaningful and the visual quality of shares increases as the number of participants involved in the technique increase. The dimensions of the shares generated are three times the dimensions of secret image, however, the dimensions of recovered secret image and original secret image are same. For revealing the secret, small computation power is required but the recovered secret image is totally lossless. We have made intentional attacks of 'salt and pepper' noise with a density of 0.3, on the shares and still were able to recover the secret image with slight degradation. The effect of such noise attacks will be minimum as the number of participants increase. Finally, we have used image quality metrics to evaluate the quality of the shares and recovered secret image and also compared some of the existing VC techniques with our proposed technique using some parameters related to VC.

References

[1] M. Naor and A. Shamir, "Visual Cryptography Scheme," *Proc. Adv. Cryptol.*, vol. 9, no. 12, pp. 1–6, 1994.

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, 2001, doi: 10.1016/S0304-3975(99)00127-9.

[3] M. Nakajima and Y. Yasushi, "Extended Visual Cryptography for Natural Images," *Dep. Comput. Sci. Univ. Toronto*, vol. 2, 2002.

[4] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 219–229, 2012, doi: 10.1109/TIFS.2011.2167611.

[5] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Contrast-Improved Visual Cryptography for General Access Structure," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp. 578–583, 2017, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.129.

[6] X. Yan and Y. Lu, "Generalized general access structure in secret image sharing," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 89–101, 2019, doi: 10.1016/j.jvcir.2018.11.031.

[7] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Opt. Lett.*, vol. 12, no. 6, p. 377, 1987, doi: 10.1364/ol.12.000377.

[8] S. J. Shyu, "Image encryption by multiple random grids," *Pattern Recognit.*, vol. 42, no. 7, pp. 1582–1596, 2009, doi: 10.1016/j.patcog.2008.08.023.

[9] P. Tuyls, H. D. L. Hollmann, J. H. Van Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes," *Des. Codes, Cryptogr.*, 2005, doi: 10.1007/s10623-004-3816-4.

[10] P. Tuyls, H. D. L. Hollmann, J. H. v. Lint, and L. Tolhuizen, "A polarisation based Visual Crypto System and its Secret Sharing Schemes," *IACR Cryptol. ePrint Arch.*, vol. 2002, p. 194, 2002.

[11] Y. Chen, Y. Chan, C. Huang, M. Tsai, and Y. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," vol. 177, pp. 4696–4710, 2007, doi: 10.1016/j.ins.2007.05.011.

[12] C. C. Lee, H. H. Chen, H. T. Liu, G. W. Chen, and C. S. Tsai, "A new visual cryptography with multi-level encoding," *J. Vis. Lang. Comput.*, vol. 25, no. 3, pp. 243–250, 2014, doi: 10.1016/j.jvlc.2013.11.001.

[13] B. Yan, Y. Xiang, and G. Hua, "Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach," *IEEE Trans. Image Process.*, vol. 28, no. 2, pp. 896–911, 2019, doi: 10.1109/TIP.2018.2874378.

[14] L. Tan, Y. Lu, X. Yan, L. Liu, and L. Li, "Weighted Secret Image Sharing for a (k , n) Threshold Based on the Chinese Remainder Theorem," vol. 7, 2019, doi: 10.1109/ACCESS.2019.2914515.

[15] Y. K. Meghrajani, L. S. Desai, and H. S. Mazumdar, "Secure and efficient arithmetic-based multi-secret image sharing scheme using universal share,", *Journal of Information Security and Applications*, vol. 47, pp. 267–274, 2019, doi: 10.1016/j.jisa.2019.05.010.

[16] E. P. S. Image, "Lossless and Efficient Polynomial-Based Secret Image Sharing with Reduced Shadow Size," *Symmetry* 2018, 10, 249, doi: 10.3390/sym10070249.

[17] S. M. Patil and B. R. Purushothama, "Pixel co-ordinate-based secret image sharing scheme with constant size shadow images," *Comput. Electr. Eng.*, vol. 89, no. November 2020, p. 106937, 2021, doi: 10.1016/j.compeleceng.2020.106937.

[18] M. Deshmukh, N. Nain, and M. Ahmed, "A novel approach for sharing multiple color images by employing Chinese Remainder Theorem," *J. Vis. Commun. Image Represent.*, vol. 49, no. October, pp. 291–302, 2017, doi: 10.1016/j.jvcir.2017.09.013.

[19] P. Singh, B. Raman, and M. Misra, "A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares," *Signal Processing*, 2017, doi: 10.1016/j.sigpro.2017.06.015.

[20] K. Dhiman and S. S. Kasana, "Extended visual cryptography techniques for true color images R," *Comput. Electr. Eng.*, vol. 70, pp. 647–658, 2018, doi: 10.1016/j.compeleceng.2017.09.017.

[21] S. Kabirirad and Z. Eslami, "Improvement of (n, n) -multi-secret image sharing schemes based on Boolean operations,", *Journal of Information Security and Applications*, vol. 47, pp. 16–27, 2019, doi: 10.1016/j.jisa.2019.03.018.

[22] R. U. I. Sun, Z. Fu, and B. I. N. Yu, "Size-Invariant Visual Cryptography with Improved Perceptual Quality for Grayscale Image," *IEEE Access*, vol. 8, pp. 163394-163404, 2020, doi: 10.1109/ACCESS.2020.3021522.

[23] X. Yan, S. Wang, X. Niu, and C. Yang, "Generalized random grids-based threshold visual cryptography with meaningful shares," *Signal Processing*, vol. 109, pp. 317–333, 2015, doi: 10.1016/j.sigpro.2014.12.002.

[24] D. S. Wang, T. Song, L. Dong, and C. N. Yang, "Optimal contrast grayscale visual cryptography schemes with reversing," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 2059–2072, 2013, doi: 10.1109/TIFS.2013.2281108.

[25] P. Li, J. Ma, L. Yin, and Q. Ma, "A Construction Method of (2, 3) Visual Cryptography Scheme," *IEEE Access*, vol. 8, pp. 32840–32849, 2020, doi: 10.1109/access.2020.2973659.

[26] S. Shivani, "VMVC: Verifiable multi-tone visual cryptography," *Multimed. Tools Appl.*, vol. 77, no. 5, pp. 5169–5188, 2018, doi: 10.1007/s11042-017-4422-6.

[27] A. G. Bhosale and V. S. Patil, "A (2, 2) Visual Cryptography Technique to Share Two Secrets," *2020 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 2020, pp. 563-569, doi: 10.1109/ICICT48043.2020.9112420.

[28] A. G. Bhosale, V. S. Patil and P. S. Bidkar, "An Authentication System for Online Question Paper Delivery using Visual Cryptography," *2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, Trichy, India, 2022, pp. 1-5, doi: 10.1109/ICEEICT53079.2022.9768442.

[29] N. C. Mhala, R. Jamal, and A. R. Pais, "Randomised visual secret sharing scheme for grey-scale and colour images," *IET Image Process.*, vol. 12, no. 3, pp. 422–431, 2018, doi: 10.1049/iet-ipr.2017.0759.

[30] A. G. Bhosale and V. S. Patil, "A (2, 2) Visual Cryptography Technique with Improved Contrast," *Inf. Secur. J. A Glob. Perspect.*, vol. 29, no. 04, pp. 199–208, 2020, doi: 10.1080/19393555.2020.1740840.