An Optimal (2, 2) Visual Cryptography Schemes For Information Security

Datta R. Somwanshi[1](✉) and Vikas T. Humbe[2]

[1] Department of Computer Science, College of Computer Science and Information Technology (COCSIT), Latur, Maharashtra, India
somwanshi1234@gmail.com

[2] School of Technology, Swami Ramanand Teerth Marathwada University, Nanded, Latur, Maharashtra, India

Abstract. Visual information security is one of the important security aspects. Secret sharing based schemes of visual cryptography permits secret image encryption and provides a more secure method which allows access to more sensitive visual information. In modern k out of n secret sharing scheme secret image to be encrypted that is partitioned into n different parts or shares. Each part or share is then distributed among the n users are different, and then we can specify at least k out of n shares are needed to get the original secret image. Recently many Secrets Sharing Schemes of visual cryptography have been developed ranging from (2 out of 2 or 2, 2) Visual Cryptography Schemes to Segment based secret sharing schemes of visual cryptography. But most of the schemes are based on processing the binary image as secret, which is not suitable for many applications that are using color information images, and the security of the share is an important issue that is less discussed in previous work. Again there are many problems of secret sharing schemes such as pixel expansions, alignment problems, extensive requirement of the codebook design, flipping issues, distortion problem, and thin line problems are quite unresolved.

In this paper a new secure (2, 2) secret sharing scheme is suggested for securely transmitting the images over the network. The suggested approach can also provide more secured shares and overcome the problems such as pixel expansion, alignment problem, extensive codebook design, flipping Issues, and distortion problem. Finally the result is compared with previously known methods. The Results obtained and the analysis of the suggested method is used to predict the efficiency of the method.

Keywords: (2, 2) Visual Cryptography Scheme · Contrast Optimal Scheme · extensive codebook design · No Pixel Expansion · No flipping Issues

1 Introduction

Visual Cryptography (VC) allows us to encrypt the written material that is in the form of images, printed text, and handwritten notes, etc. in a perfectly secure way and that can be decoded directly by the visual systems of humans [1]. It is one of the most

R. Manza et al. (Eds.): ACVAIT 2022, AISR 176, pp. 164–177, 2023.
https://doi.org/10.2991/978-94-6463-196-8_15

powerful cryptography techniques and requires only encryption. Means there is no need for decryption and it does not require huge calculations for the decryption of the text. Because of this, everyone can use the system without acquiring the knowledge about encryption or decryption of cryptography and fail to carry out any computations.

This technique was first introduced by Naor et al. [1], in 1994. In this technique the message or image data to be protected or encrypted is divided into n different parts or shares. Each part or share is distributed among the n different users, and then we can specify at least k out of n shares are stacked together or required to get the original information. The k-1 shares cannot be used to generate the original message. For example, suppose there are six thieves who want to share a bank account, but the problem is they don't trust one another, and they split up the password that is required for transaction from an account and each part of the password is provided to individual thieves. While splitting up the password they implement such a mechanism that at least three or more than that have to come together, they have to provide their part of the password, then it will be combined together and will be provided to the system for performing transactions.

Each Pixel in the original binary image that is to be secured is divided into two or more blocks. There should be the same number of black and white pixel blocks. if any pixel is split up into two shares there will be one black and one white block. Similarly if any pixel is split up into four equal shares then there will be two black blocks and two white blocks [1, 2, 3]. The example Fig. 1 uses pixels that are divided into two parts.

The basic idea of (2, 2) Visual Cryptography is depicted in Fig. 1. The image that is to be secure is split up into 2 equal parts or shares. In each part 2, 4 or 8 sub-pixels blocks which are non-overlapping will be used to represent a single pixel from the original image. All the pixels in the original image are represented in this way and shares will be formed. A user having the single share cannot be able to reconstruct the original secret image. Both two shares are needed to reconstruct the original secret image [1].

For encrypting the pixels of an image, recently many methods have been developed. For one of the methods, every pixel in the image that is to be secured is split up into two pixels in every share. While reading and converting the original image into shares,

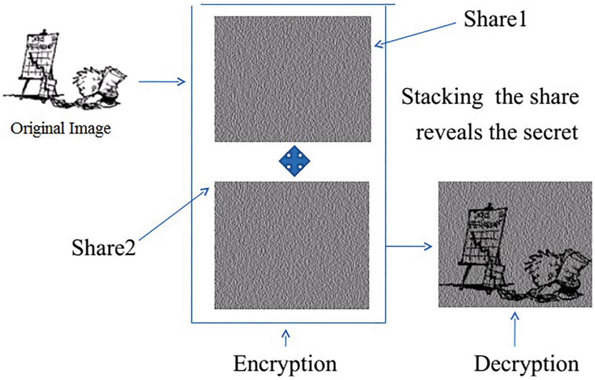


Fig. 1. Basic Idea of Visual Cryptography

Table 1. (2, 2) Secrete Sharing Scheme.

Original Image	Probability	Share1 Sub-Pixel	Share2 Sub-Pixel	Share1 || Share2
□	**0.5**	■□	■□	■□
□	**0.5**	□■	□■	□■
■	**0.5**	■□	□■	■■
■	**0.5**	□■	■□	■■

if the pixel value encountered is one it means the white pixel then one of the rows from the first two rows displayed in Table 1 is picked up. The probability of this is 0.5 and the 2 pixel blocks mentioned in the third and fourth column of Table 1 are selected and shares are assigned. Similarly, if the pixel value encountered is zero it means the black pixel, then one of the rows from the last two rows displayed in Table 1 is picked up. The probability of this is also 0.5 and the 2 pixel blocks mentioned in the third and fourth column of Table 1 are selected and shares are assigned, in this way shares are formed.

When reconstructing the original image from the two shared images, if the two pixels in two shares images are white, then the reconstructed pixel will white and if the one share image contains black pixels and the other share image contains either black or white then the reconstructed pixel will be black. So, this kind of operation can be achieved using Boolean OR operations. The result of this operation is depicted in the last column of Table 1 when the third and fourth columns are used in the reconstruction process [1].

Problems such as Improper alignment of pixels due to which image may look different, distortions of shares due to which original image may not be reconstructed properly, flipping issues due to which image may not be reconstructed in proper directions. These are some of the issues that may arise while reconstructing the original image from share images, Also for generating the shares there is need of a codebook using which the shares can be created; expansion of the pixels also needs to be taken care of, so that the size of share images will not increase. The Proposed novel (2, 2) methods eliminated all of the problems listed above except little bit pixel expansion.

2 Literature Review

Naor et al. [1] have generalized the scheme into (k, n), in which at least k shares are required from n different shares. In a generalized (k, n) scheme, ‘n’ shares of the original secret image are created and distributed to all n participants. For the reconstruction of the original image from the share images, at least k shares are necessary, less than k shares cannot be used to reconstruct the original image. This gives flexibility to the user.

if some of the shares are lost, still the secrete image can be formed from share images with only k shares or greater than equal to k and less than equal to n shares.

Ateniese et.al [6] further extended this (k, n) scheme and called it a general access structure. In this type shares generated are bifurcated into subsets of shares and which are called qualified subset and forbidden subset, this is as per the importance given to the subsets of shares. Any k numbers of shares from the subsets of qualified shares can be used to reconstruct the original image, but less than k numbers of shares cannot be used to reconstruct the original image. In case of shares from the forbidden subsets, any k, more than k cannot be used to reconstruct the original image. So the general access structure of visual cryptography can be used to enhance the security of the system. Abhishek p, et al. [7] presented the new scheme called "Recursive threshold Visual Cryptography", The major idea of this type of scheme is, its hides the small secrete information into the shares of the large secrete recursively, it means the secrete size doubled at every steps, and therefore it increases the secret information. Every single bit carries n-1/n bits and which is nearer to 100%. Zhi Zhou et al. [4, 5] have profound he new scheme called half-tone visual cryptography, In this scheme every pixel converts into coded form which are simply the array of sub-pixels and called half-tone cell. Using these half-tone cells of suitable size, shares of the image can be more pleasant. Means that there will be good contrast and quality of the image will be maintained and also it improves the security of the shares. Chang-Chou Lin et al. [8] worked on the gray scale image and proposed the scheme for gray level images. In the scheme proposed, a process called dithering technique is used that can be used to transform the gray level image into a binary image and binary image look similar to gray level image. The rest of the method works similar to other methods proposed earlier. In addition to the gray level images the F. Liu et al. [9] introduced the new approach for working on color images which is called color visual cryptography scheme. They proposed the approach of separating the three color channels: red, green and blue and working with each color channel for generating the shares. The approach introduced by them overcomes the pixel expansion problem, but because of the half-toning process the quality of the image gets reduced. To share the two secret information images in two different shares Wu and Chen [10] introduces the new scheme. In this proposed scheme two different binary secrete images are used to hide inside the two different random shares called A, and B. The secrete images are hidden in such a way that, the first secrete image can be reconstructed by superimposing the shares using XOR operation $A \otimes B$, and the second secrete image can be reconstructed by rotating share A anti-clockwise by 90 degree. In addition to this Shyu et al. [11, 12] proposed the scheme for sharing the multiple secrete image, through which two or more secrete information images can be hidden or secured at the same time in two different shares.

3 Methodology

The proposed research is focused on secure (2, 2) visual cryptography scheme for information security. There are many secrete sharing scheme are designed such as (k, n), Half toning, Multi-resolutions etc. [1, 2]. In k out of n shares scheme, consider the set p from n number of participants, the visual secrete image S, that is encrypted or divided in to "n" shadow images, these are called shares or parts where each participant gets a share to be used for getting the original message or visual image. The original message will be visible if only k or more than k is combined or superimposed together. Less than k cannot be used for getting the original message [2].

Consider the message that is to be encoded is composed of a set of white and black pixels and every pixel is processed separately. Each share of the participant is a set of m white and black sub-pixels. The derived image can be assumed as a [n × m] boolean matrix S = [s, i, j].

We can consider that s, i, j = 1 if the j^{th} sub-pixel in the i^{th} share is black and s i, j = 0 if the j^{th} sub-pixel in the i^{th} share is white.

The proposed methodology is as shown in Fig. 3. The information that is to be secure or the image that is to be protected is taken as input. Various applications such as biometric security, online voting system using biometric characteristics, secure banking transaction are the application of visual secrete sharing scheme. Pre-processing of input image is performed if there is a need of application. Then next step is to divide the input image into two or more share as per the need of application. Then next step is to divide the input image into two or more share as per the need of application. Each share is then provided to the participants (this can be provided via email or any other application) (Table 2).

Participants will now provide his share whenever needed. Finally shares are combined together and final image is formed. In this proposed study we have used 2, 2 secrete

Table 2. Relative review and study of different scheme of Visual cryptography

Name of Authors	Title of scheme and year of publication	Type of Image	Used techniques
Mahmoud E. Hodeish, Vikas T. Humbe	An Optimized Hal-ftone-Visual Cryptography Scheme Using Error Diffusion-2018 [18]	Binary and Gray Scale Images	Improves and reduces the pixel expansion problems, Eliminate requirement codebook design, They also reduces the random pattern of the share images and Evaluate the performance analysis using different statistical methods

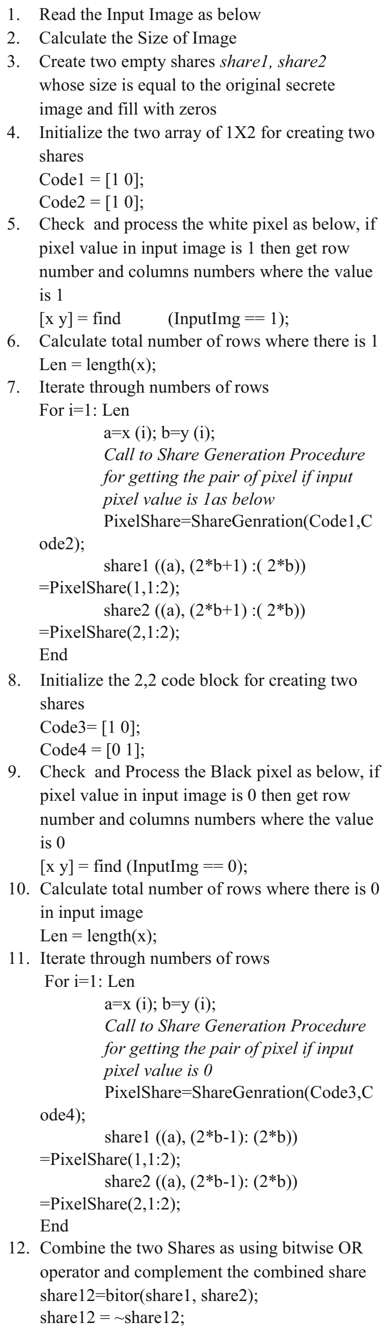
(*continued*)

Table 2. (*continued*)

Name of Authors	**Title of scheme and year of publication**	**Type of Image**	**Used techniques**
Shivendra Shivani	Verifiable Multi-tone Visual Cryptography-2017 [17]	Gray Scale and Color Image	For a pixel in share a self-embedding verifiable bit is added for the prevention of cheating and testing the integrity of the pixel. Overcomes the problem of random shares, requirement of codebook.
Mahmoud E. Hodeish, Linas Bukauska, Vikas T. Humbe	An Optimal (k, n) Visual Secret Sharing Scheme for Information Security 2016 [15]	Binary Image	(k, out of n) scheme based on designed codebook, and transport of matrices, n-Vector, and XOR boolean operation are used
Angel Rose, A Sabu, M Thampi	A Secure and Verifiable Scheme for Secret Image Sharing 2015 [14]	Binary Image, gray scale image	Arnold transformation technique Bit-Plane Complexity Steganography, Mean-Square-Error (MSE) and Structural-Similarity-Index value test
Souvik Roy and P. Venkateswaran	"Online Payment System using Steganography and Visual Cryptography" 2014 [13]	Binary Image, gray scale image	text based steganography, and Visual Cryptography
Rajendra A B and Sheshadri H S	"Visual Cryptography in Internet Voting System" 2013 [16]	Gray Level Image	2-out-of-2 Visual Cryptography

sharing scheme and problems such as alignment problem, distortion, thin line problem occurred while combining the share are minimized.

Algorithms for the Proposed Method



```
1.  Read the Input Image as below
2.  Calculate the Size of Image
3.  Create two empty shares share1, share2
    whose size is equal to the original secrete
    image and fill with zeros
4.  Initialize the two array of 1X2 for creating two
    shares
    Code1 = [1 0];
    Code2 = [1 0];
5.  Check  and process the white pixel as below, if
    pixel value in input image is 1 then get row
    number and columns numbers where the value
    is 1
    [x y] = find          (InputImg == 1);
6.  Calculate total number of rows where there is 1
    Len = length(x);
7.  Iterate through numbers of rows
    For i=1: Len
            a=x (i); b=y (i);
            Call to Share Generation Procedure
            for getting the pair of pixel if input
            pixel value is 1as below
            PixelShare=ShareGenration(Code1,C
    ode2);
            share1 ((a), (2*b+1) :( 2*b))
    =PixelShare(1,1:2);
            share2 ((a), (2*b+1) :( 2*b))
    =PixelShare(2,1:2);
    End
8.  Initialize the 2,2 code block for creating two
    shares
    Code3= [1 0];
    Code4 = [0 1];
9.  Check  and Process the Black pixel as below, if
    pixel value in input image is 0 then get row
    number and columns numbers where the value
    is 0
    [x y] = find (InputImg == 0);
10. Calculate total number of rows where there is 0
    in input image
    Len = length(x);
11. Iterate through numbers of rows
     For i=1: Len
            a=x (i); b=y (i);
            Call to Share Generation Procedure
            for getting the pair of pixel if input
            pixel value is 0
            PixelShare=ShareGenration(Code3,C
    ode4);
            share1 ((a), (2*b-1): (2*b))
    =PixelShare(1,1:2);
            share2 ((a), (2*b-1): (2*b))
    =PixelShare(2,1:2);
    End
12. Combine the two Shares as using bitwise OR
    operator and complement the combined share
    share12=bitor(share1, share2);
    share12 = ~share12;
```

Share Generation Procedure which is invoked in previous algorithms works as below.

ShareGenration(codea, codeb) Procedure

```
1.  Create two variable from 1x2 array codea as
    below
    a1 = codea (1);
    a2 = codea (2);
2.  Create two variable from 1x2 array codeb as
    below
    b1 = codeb (1);
    b2 = codeb (2);
3.  Assign codea and codeb to array in
    in = [codea
          codeb];
4.  Create the out array of size in and fill the zeros
    out = zeros(size(in));
5.  Select the random number between 0 and 1 and
    multiple this with 1.9 to get the floor value
    either 0 or 1 as below
    RandomNumber = floor(1.9*rand(1));
6.  If (RandomNumber == 0)
       out = in;
    elseif (RandomNumber == 1)
            codea(1) = a2;
            codea(2) = a1;
            codeb(1) = b2;
            codeb(2) = b1;
            out = [codea
                   codeb];
    End of IF

7.  Finally return the out array as below
    Return out
8.  End of Procedure
```

4 Experimental Result

The result obtained using the above algorithm and procedure is presented as below. Figure 2 shows the input binary sample secrete image, Fig. 3 and Fig. 4 shows the generated share, share 1 and share2, and finally Fig. 5 shows the secrete image after combining the two shares.

5 Discussion and Performance Analysis

5.1 Pixel Expansion

The pixel expansion problem is reduced 100% using the scheme proposed. The size of the secret image and the size of the generated share image, and image after reconstructed using shares is exactly the same size that is represented in Fig. 2, 3, 4 and 5.

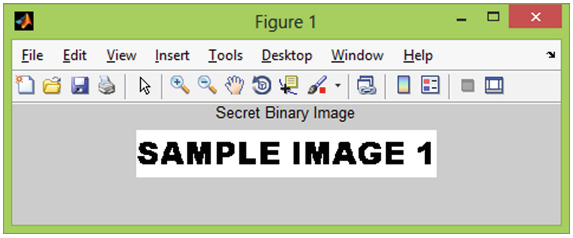


Fig. 2. Input binary sample secrete image

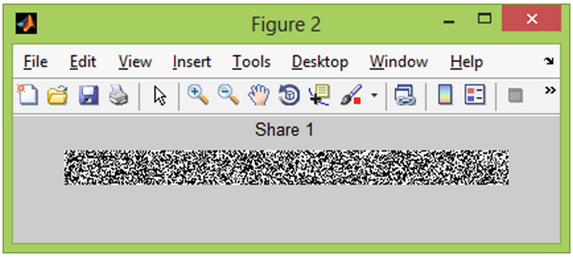


Fig. 3. Generated share, share 1

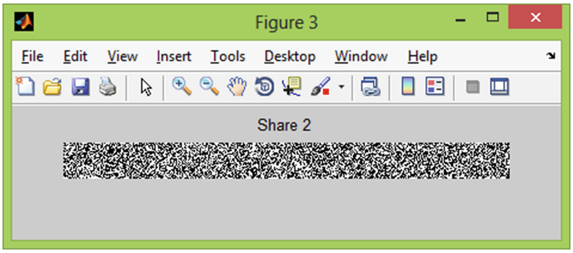


Fig. 4. Generated share, share2

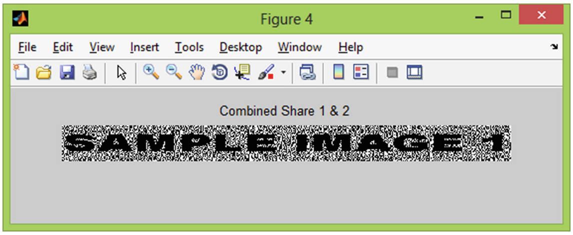


Fig. 5. Secrete image after combing two shares, share1 and share2

5.2 Contrast and Statistical Analysis

The image obtained after reconstruction is without the distortion of pixels, and that is the output displayed in Figs. 1, and Fig. 5. To estimate the quality of a reconstructed secret image and to demonstrate that the reconstructed secret image is of the same quality as of the original secret image, there are a variety of statistical analysis metrics of image restoration as presented below.

5.3 Mean Square Error

The formula to calculate Mean-Square-Error (MSE) [19] mathematically is presented as below.

$$\mathrm{MSE} = \frac{1}{\mathrm{MX\ N}} \sum_{i=1}^{M} \sum_{j=1}^{N} (\mathrm{h_{ij}} - \mathrm{h_{ij}}\prime)^2 \tag{1}$$

Where $\mathrm{h_{ij}}$ and $\mathrm{h_{ij}}\prime$ are the pixel values of original image and reconstructed secrete image, respectively

5.4 Peak-Signal-to-Noise-Ratio

Peak-Signal-to-Noise-Ratio (PSNR) [20] is also a mathematical and or engineering formulation calculated by using MSE and by the help of the Eq. 2 presented below.

$$\mathrm{PSNR} = 10 * \mathrm{loglog}\, \frac{\mathrm{R}^2}{\mathrm{MSE}} \tag{2}$$

Statistically, when the value of PSNR = 1, it indicates that the scheme proposed delivers the extreme visual quality.

5.5 Universal-Index-Quality (UIQ)

Universal-Index-Quality (UIQ) can be calculated with the help of Eq. 3 displayed below[21].

$$UIQ = \frac{4\sigma_{zy}\underline{xy}}{\sigma_x^2 + \sigma_y^2\left[\left(\underline{x}\right)^2 + \left(\underline{y}\right)^2\right]} \tag{3}$$

Image deformation modeling operation can be performed with UIQ by using the three three parameters listed below.

1. Correlation loss,
2. Luminance distortion, &
3. Contrasts distortion

The range of the UIQ value is between *-1* to +*1*. The positive and a strong Linear-Correlation among the two pictures X and Y exists, if the UIQ values are close to +*1*. The UIQ value is *-1* then it represents there is a negative relationship between the two pictures and at the last the value of UIQ is zero then it represents that there is no any relationship between the two pictures [21].

5.6 Maximum Difference (MD)

This Maximum-Difference (MD) analysis factor is mainly used to determine the error among original secret information images and reconstructed secret information image. This MD factor is straight proportional with the contrast of image given and dynamic range and that can be can be determined using the Eq. 4 as displayed below [22]

$$\mathrm{MD} = \max\left|\mathrm{x_{ij}} - \mathrm{y_{ij}}\right| \tag{4}$$

5.7 Average Difference (AD)

The Average-Difference is used to calculate the differentiation between the two images; that is the original image and image obtained after the reconstruction. The formula to calculate the Average-Difference (AD) of the original secret information image and the image obtained after the reconstruction of the secret image and that is estimated with the Average-Difference metrics as listed below [23].

$$\mathrm{AD} = \frac{1}{\mathrm{M\ X\ N}}\sum_{\mathrm{i=1}}^{\mathrm{M}}\sum_{\mathrm{j=1}}^{\mathrm{N}}\left(\mathrm{X_{ij}} - \mathrm{Y_{ij}}\right) \tag{5}$$

In the above equation, the value of X, and Y are used to presents the secrete image that is in original form and the calculated or the reconstructed secrete image. All those values that are illustrated above are represented in Table 1.

Tables 1 shows the value of MSE, MD and AD are equal and which is zero, The value of PSNR is infinity ∞ and the values of UIQ is 1 presented and persuade that the reconstructed image and the original secrete images have been completely extracted without any loss or damage of important and meaningful information of the reconstructed image. Table 3 represented those values.

We compare our method with previously known method the result obtained using different statistical measures are presented in Table 4.

Table 3. Shows the different metrics of statistical analysis metrics Obtained in experiment

Statistical Metrics	Value Obtained in Experiments
MSE	0
PSNR	∞
UIQ	1
MD	0
AD	0

Table 4. Results of comparison between the previously known methods and the proposed method using statistical measures

Scheme	**Type of Image**	**Expansion of Pixel**	**Super-imposition Method**	**Aspect Ratio**	**Quality of Revealed Image**
Zhou et al.'s scheme [4]	Binary(m x n)	$p = 4$	OR Operation	Changed	Better quality
Zhongmin Wang et. al.'s [5]	Binary(m x n)	$P = 4$	OR Operation	changed	Lossless
Mahmoud E. Hodeish et. al.'s [15]	Binary Halftone	P = 2	XOR Operation	changed	Lossless
Chang-Chou Lin [8]	Grey Level	P = 4	OR Operation	changed	Lossy
F. Liu et. al [9]	Color	$P = 4$	OR operation	changed	Lossy
The Proposed Scheme	Binary	$p = 1$	XOR Operation	unchanged	Lossless

6 Conclusion

In this paper a new secure (2, 2) secrete sharing scheme is developed to securely transmitting the images over network. The proposed approach provides secured shares and overcome the problems such as pixel expansion, alignment problem, extensive codebook design, flipping Issues, and distortion problem. Shares generated through this system are secure because share are depends on the random value, and while combining the two share problems of share alignment is minimized, also there is no distortion of shares, share size is minimum, and finally flipping issue is minimized. We have compared our results with previously known method, and we found more contrast optimal shares. The proposed method can be further modified for color images, and for creating verifiable shares.

References

1. Moni Naor and Adi Shamir, "Visual Cryptography," Eurocrypt, 1994
2. Jonathan weir and weiQi, Yan "Visual Cryptography and its Application", Ventus Publishing Aps, eBook, pp.1-144, 2012.
3. Ecaterina Moraru (Valica), "Visual Cryptography", Published in: Technology, Art & Photos on Slide share, pp. 1-38, 2008.
4. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo," Halftone Visual Cryptography", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, pp. 2241-2453, AUGUST 2006

5. Zhongmin Wang, Student Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo, "Halftone Visual Cryptography via Error Diffusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, pp. 383-396, SEPTEMBER 2009
6. G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, "Visual cryptography for general access structures", Proc.ICAL96, Springer, Berlin, 1996, pp. 416-428, 1996
7. Abhishek Parakh and Subhash Kak "A Recursive Threshold Visual Cryptography Scheme", CoRR abs/0902.2487, 2009
8. Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters, v.24 n.1-3, 2003.
9. F. Liu, C.K. Wu, X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2009.
10. C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998
11. S. J. Shyu, S. Y. Huanga, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, p. 3633-3651, 2007
12. Tzung-Her Chen n, Chang-Sian Wu," Efficient multi-secret image sharing based on Boolean operations", Signal Processing Volume 91, Issue 1, pp. 90-97, January 2011.
13. Souvik Roy and P. Venkateswaran," Online Payment System using Steganography and Visual Cryptography", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2014.
14. Angel Rose A, Sabu M Thampi," A Secure Verifiable Scheme for Secret Image Sharing 2015", Procedia Computer Science 58, pp.140-150, 2015
15. Mahmoud E. Hodeish, Linas Bukauska, Vikas T. Humbe," An Optimal (k, n)Visual Secret Sharing Scheme for Information Security", Elsevier- Procedia Computer Science 93, pp.760 – 767, 2016.
16. Rajendra A B and Sheshadri H S "Visual Cryptography in Internet Voting System", IEEE, pp. 60-64, 2013.
17. Shivendra Shivani, "VMVC: Verifiable multi-tone visual cryptography", Springer, Multimed Tools Application, https://doi.org/10.1007/s11042-017-4422-6, pp.1-20, January 2017.
18. Mahmoud E. Hodeish and Vikas T. Humbe, "An Optimized Half tone Visual Cryptography Scheme Using Error Diffusion", Springer, Multimed Tools Application pp 1-17, January 2018.
19. Chen, C.Y., Chen, C.H., Chen, C.H., Lin, K.P., 2016. An automatic filtering convergence method for iterative impulse noise filters based on PSNR checking and filtered pixels detection. Expert Syst. Appl. 63, 198–207.
20. Shankar, K., Eswaran, P., February 2017. RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Commun. 14 (2), 118–130. https://doi.org/10.1109/CC.2017.7868160.
21. Wang, Z., Bovik, A.C., 2002. A universal image quality index, IEEE Signal Process Lett.9 (3), 81–84.
22. Rajkumar, S., Malathi, G., 2016. A comparative analysis on image quality assessment for real time satellite images. Indian J. Sci. Technol. 9, 1–11
23. Ece, C., Mullana, M.M.U., 2011. Image quality assessment techniques in spatial domain, IJCST 2 (3).