Recursive Visual Cryptography for Multiple Secret Image Sharing

Jesalkumari Varolia, R. R. Sedamkar

Abstract: ***The concept of traditional visual cryptography encrypts one image by converting it into random pixel image.This paper uses recursive visual cryptography to encrypt more than one color images.This method is also solving the problem of Pixel expansion as for recursive Visual Cryptography the original image is not necessarily double the size of secret image.This method solves the problem of reconstructing image as it uses XOR based Visual Cryptography.***

Index Terms**:** ***Visual Cryptography, Pixel expansion, Encryption, Decryption, MSR, PSNR***

I. INTRODUCTION

In this era of digital media concern of private data security(i.e Image, Msg.) has increased. Naor andAdi Shamir has proposed Visual cryptography method where image is encrypted using algorithm but there is no need of algorithm at decryption end to reveal the visual information. [4]Human visual system can decrypt the image without any processing of shares. Main moto of visual cryptography is secret sharing. Encryption process splits each pixel of original image is given to share and during the decryption process the shares are stacked pixel by pixel to unhide the original image. Each split is on separate share, and decryption is performed by superimposing pixels. When all *n* shares were stacked, the original image is revealed. If secret image is leaked no single participant is pointed all are equally responsible as it is impossible to retrieve secret image from random noised image.Brute force method can give so many possible images the actual message can not be guessed. [2]

The secret message(image) can be recovered by superimposing the all shares together. The secret image is of black and white pixels. The operation of is the logical operation OR which human visual system can deal with. VCS (k out of n) takes a secret image as input, and generates shares that can recover the secret image and less than k share images cannot get any information about the secret image. Visual cryptography is proposed with XORoperation[13] which gives better contrast of a reconstructed image.

Drawbacks of OR based Visual cryptography:

- Increase in resolution.
- Visibly reduced contrast .
- It works well with halftoned image but not working with true colors.
- If image is of high resolution (more number of pixels) stacking becomes difficult.

Revised Manuscript Received on December 22, 2018.

Mrs. Jesalkumara Varolia, Department of Computer Engineering, Thakur College of Engineering and Technology, Mumbai, India.

Dr. R.R. Sedamkar, Department of Computer Engineering, Thakur College of Engineering and Technology, Mumbai, India.

II. BACK GROUND AND PRELIMNERIES

A.Traditional v/s XOR Based Visual Cryptography

VC scheme using an XOR operation to share a binary image was presented by Itzkovitz [2]. More general definition is - A (k, n) VC scheme S = (C0, C1) consists of two collections of n x m binary matrices C0 and C1. Encryption of image is same as traditional but decryption can not be done by human eye system. This method requires machine for decryption. Table 1 gives the (2,2) XOR based VCS Share generation with 1x2 resolution for black and white pixels.To generate share for a white (black) pixel, random matrix from C0(C1) is chosen and distributes its rows as shares for both participants of the system.

Table 1.(2, 2) XOR-BASED 1X2 RESOLUTION VISUAL CRYPTOGRAPHY SCHEME

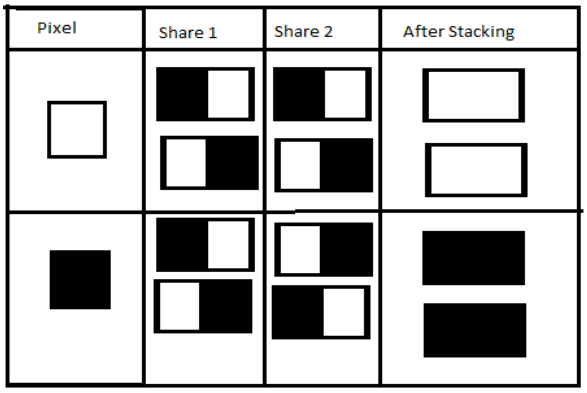


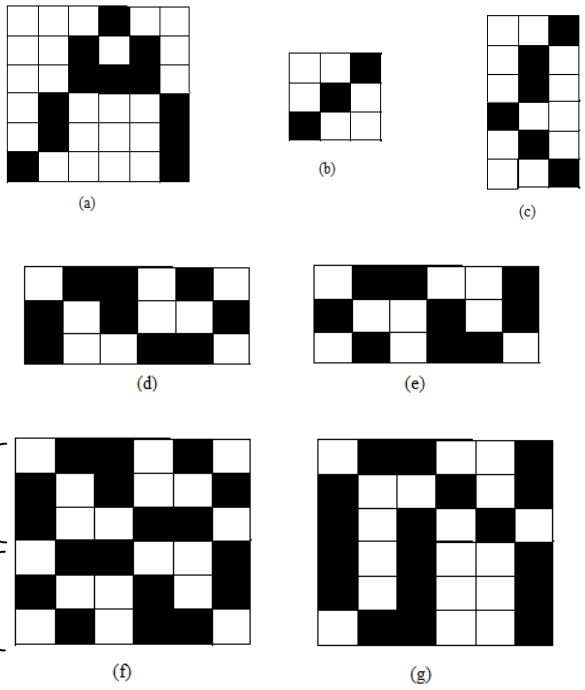
Table 1 [15], shows that 2 subpixels are generated from a pixel of the original image where one pixel is whiter and other is black. Pixel is selected through random algorithm from each pattern. If the pixel is white one of the row is selected for share generation from Table I is randomly selected to encode the pixel into 2 shares.The resolution will be changed to 1x2 from 1x1 for shares.

B. Recursive Visual cryptography

Recursive information hiding is a technique where more than one messages can be hidden in one of the shares of the original secret image. Wecan hide patients report, personal detail and hospital record in one image. The first secret image is personal information, second secret image is hospital record and original image is a report.The first small secret image is divided into different shares using visual cryptography. These shares are placed in the next level to create the shares of larger secret information. The shares distributed at each consecutive level so that no one has access to all the shares of the smaller images, unless until all participants come together to reveal the secret

information.

Example is given in Figure to explain the concept. Here three images are considered where in original image (6x6) patient's record is there, Secret message 1(3x3) is about patient's medical details and secret message 2 (6x3)is patient's personal detail. First Visual cryptography is to be applied on secret message 1 image of size 3x3 and two shares are generated of size 6.



To generated share 1 of secret message 2 image both the shares of secret message 1are concatenated which makes share1 of size 6x6

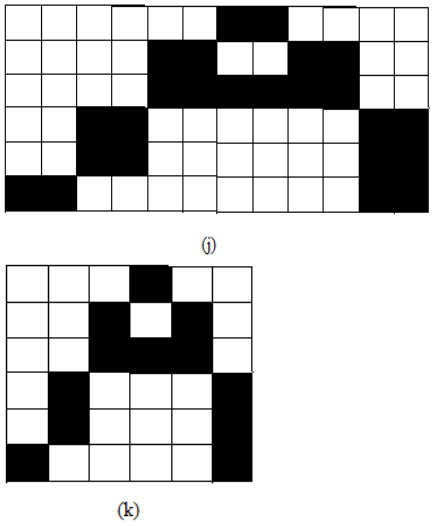
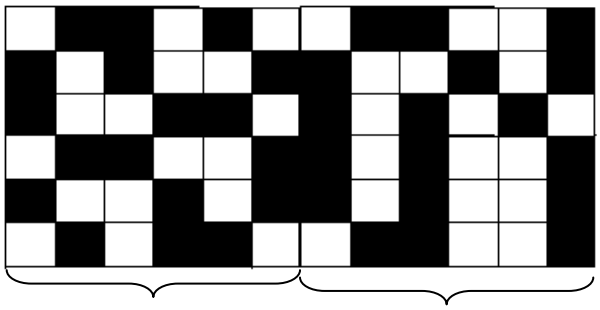


Fig.1 (a)Original Message (6x6) (b) Secret Message 1(3x3) (c) Secret Message 2 (6x3) (d) Share 1 of Secret Message 1(3x6) (e) Share 2 of Secret Message 1(3x6) (f) Share 1 of Secret Message 2 (6x6) (g) Share 2 of Secret Message 2 (6x6) (h) Share 1 of Original Message (6x12) (i) Share 2 of Original Message(6x12) (j) Decoded Original Image (6x12) (k) Reconstructed Original Message(6x6)

Share 2 is generated of size 6x6 with respect to share 1 such that by decoding shares using XOR based VC Secret message 2 is to be decoded. Now using these two shares of secret image 2 , share 1 of Original secret is generated. For that both the shares are combined and share1 of size 6x12 is generated and share 2 of original message is generated such that it can reveal the original message of size 6x12 by decoding shares using XOR based VC. To decode the original message of same size as its original size which is 6x6here ,size reduction algorithm is used ,which is mentioned below, reconstructed image is achieved.

Size reduction algorithm.

1. Consider decoded image and one image with the size of original message with all pixels white.
2. Color the i^{th} pixel with black color if 2i-1 and 2i both pixels is black for same row (because number of rows are same) in decoded image.
3. Repeat the steps for all the pixels.



(a)

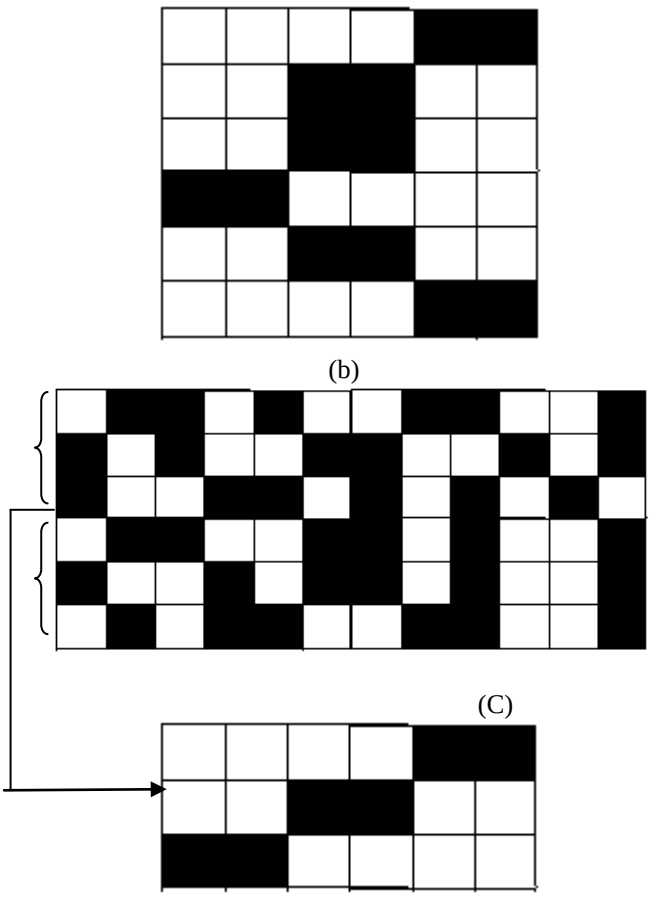


Figure 2. (a) Share 1of Original Message (6x12) (b) Decoded Secret Message 2(6x6) (c) Share 1of Original Message (6x12) (d) Decoded Secret Message 1(3x6)

In this method, first share of original image acts as Cipher (which contains hidden message) and second share acts as a key to decode original message. Shown in figure 4 that share 1 can reveal secret message 1 and secret message 2 by alone but to decode original message share 2 is needed. Share 1 can be divided in two part from the center (of same size 6x6) and by applying XOR based VCS on them we can reveal Secret image 2 and further if we bisect the first part of that division horizontally then we can reveal secret image 1 using XOR based VCS.

III. PROPOSED WORK

Comparing traditional VCS with XOR based visual cryptography; XOR based visual Cryptography gives better visual quality. Generated shares are random dots so it doesn't reveal secret information. This proposed method can deal with both grey level and colored images. Colored image is decomposed into primary colors C,M,Y but grey level image can be directly transformed into a binary image, it can be further extended for extended visual cryptography where shares are having visual meaning.

The proposed method is not working with true colors so image needs to be halftoned first. Input a colored image which should be in RGBcolormodel.Then split the image in CMY model. The purpose of using CMY is printers (usually CMY model is used as the subtractive model is more suitable for printing colors on transparencies). RGB andCMY are complementary colors, in the true color model.

Then we applied halftone algorithm onthis three images separately. There are many halftone algorithms , here error diffusion algorithm is used. We triedfloyd's algorithm, stucki's algorithm and proposed algorithm for halftoning. The coefficients for proposed method are given in fig1.The black spot represents current pixel, which is being threshold. The filter coefficients in Error Diffusion filter are indexed relative to the current pixel, which determines what percentage of quantization error, is to pass to pixel at that position, relative the current pixel.

		*	8/24	0
2/24	4/24	00	2/24	
1/24	0	4/24	2/24	1/24

Fig 3. Coefficients' of proposed method

This gives three halftoned images for each Cyan, Magenta and Yellow. Here each pixel is compared against threshold (T=127) and if intensity is greater than T make it 255 else 0.

Procedure for Encryption :

1. Read color image of RGB model as input
2. Convert RGB to CMY model.
3. Apply halftone algorithm on each (C,M,Y).
4. Generate shares for each C,M and Y by applying VCS of (2,2)
5. Combine all the share 1 to generate share 1' and Combine all the share 2 to generate share 2'
6. Read encrypted colored image shares.
7. Apply Halftone algorithm on cover images. Read different cover images for each shares.
8. Replace half 1's of cover image with respective share. And all zeros of cover image with respective share.
9. Final share is to be shared with participants.

At decryption end only the shares are to be stacked together no other computation is required to reconstruct the image. This method is Modified Visual Cryptographyscheme for colored images.

Here the resolution of share is 50% reduced than traditional Visual cryptography.

The generated halftoned shares are stamped with the cover image. These cover images can be different for different shares and it can be same for all the shares.

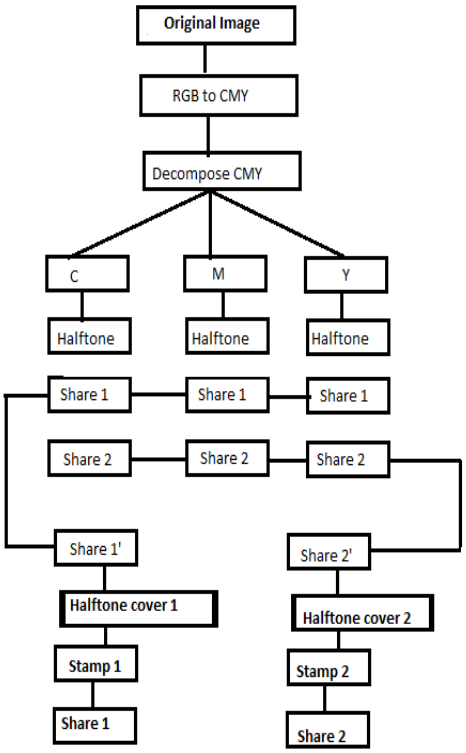


Fig 4. Generating meaningful Shares of colored images

Procedure for Stamping:
1. Read encrypted colored image shares.
2. Apply Halftone algorithm on cover images. Read different cover images for each shares.
3. Replace half 1's of cover image with respective share. And all zeros of cover image with respective share.
4. Final share is to be shared with participants.

This algorithm replaces the value of pixel with new value so image is distorted at decryption end because the shares are simply XORed not processed to maintain security.

At decryption end only the shares are to be stacked together no other computation is required to reconstruct the image.This method is Modified Visual Cryptography scheme for colored images.

Procedure for Decryption:
The shares are stacked and image is reconstructed using XOR operation.
Since the original and reconstructed image has different aspect ratio with difference in image size,first we need to resize the image to make both image equal size.There are two options to do so.

1) Resize Original image to reconstructed one
2) Resize reconstructed to Original one

Here we opted second option.
This is done specially to check image quality in terms of MSE and PSNR with respect to the original image.

IV. Result and Discussion

The complexity is directly dependent on the number of if/else conditions, as there are no other operations performed in the algorithm. Regarding the existing algorithm, as it has 4 patterns, there are 4 operations for each pixel.

1. Decomposing inCMY
2. Halftoning
3. Pixel split for Encryption
4. Merging C,M,Y shares

If we let n be the number of pixels, then the complexity of the existing method is 4n. Subsequently, in this method, there are14 if/else conditions as there are more specific comparison are being done in the process, so the complexity of the method becomes as 14n.

Two approaches for image Qualitymeasurement:-

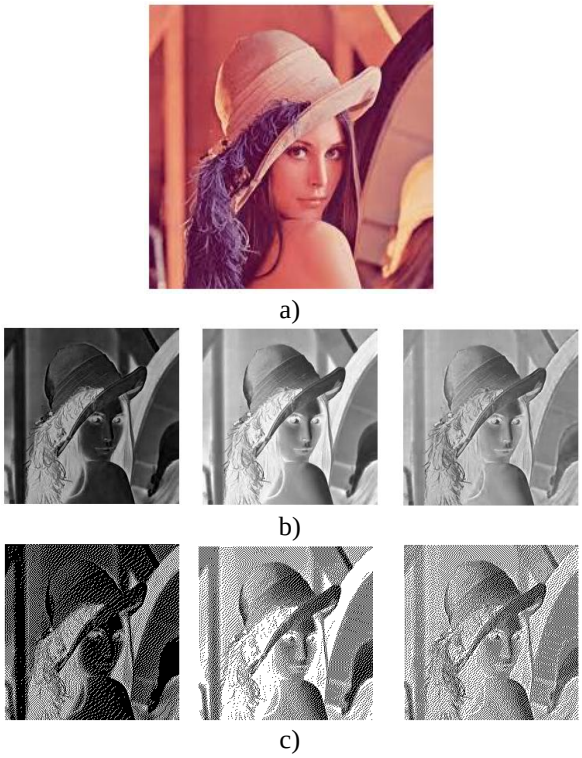
1. Subjective measurement

Participantsare selected for their visual capabilities, shown a series of test images and asked to rank the quality of the images. The method is correct butsubjective evaluation isusually not convenient, more time-consuming and expensive.

2. Objective measurement

There are algorithms for quality assessment of images and report their quality without human involvement. This eliminates the need for expensive subjective studies. Objective image is dependent on the availability of an original image, with which the reconstructed image is compared.

Fig 5 a) is the original color secret image which is to be encrypted .Firstly, image is in RGB form which is converted to CMY form as shown in Fig5 b).Then cyan , Magenta and Yellow Shares are halftoned using proposed method Fig 5 c) which gives better result thenstucki and floyd's shown in Fig 3.



a)

b)

c)

Fig 5. a) Original Image b) Decomposed Cyan , Magenta, Yellow Image c) Halftoned Decomposed Cyan , Magenta, Yellow Image

Original Image	Proposed Halftone Method	Floyd's Method	Stucki's Method
			
MSE- 0 PSNR- I Size- 225 X 225	MSE- 3.8565e+003 PSNR- 12.2689 Clock time- 5.37	MSE- 4.1689e+003 PSNR- 11.9305 Clock time- 9.81	MSE- 3.9760e+003 PSNR- 12.1363 Clock time- 12.20
			
MSE- 0 PSNR- I Size- 246 X 205	MSE- 3.3021e+003 PSNR- 12.94 Clock time- 5.35	MSE- 3.8271e+003 PSNR- 12.30 Clock time- 5.97	MSE- 3.5035e+003 PSNR-12.68 Clock time-7.15

Fig. 6 Proposed Halftone Method

Fig. 7a&b are halftoned cover images for share 1 and share 2 respectively to make shares meaningful.The cover images are halftone with the same procedure as original image.

Fig 7 a. Halftoned Cover image 1

Fig 7b.Halftoned Cover image 2

Figure 8a & b shows the stamped shares share 1 and share 2 which can be identified whose share is which. Shares are given some meaning to identify by stamping a cover image.The size of cover image has to be same as original secret image.

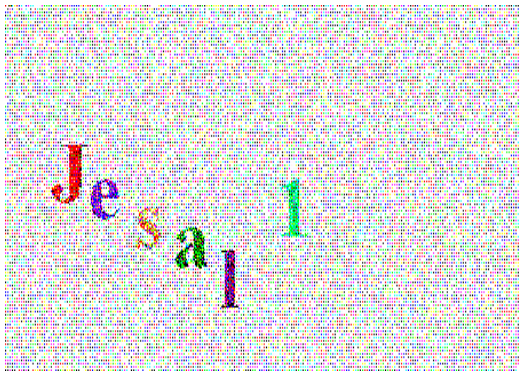


Fig 8 a. Stamped image share 1

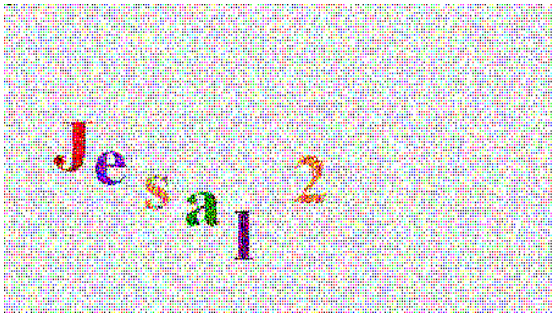


Fig 8 b. Stamped image share 2

Fig 9 shows reconstructed image at decryption side using traditional OR based VCS. The result shows reconstructed image is degraded and very less information can be extracted.

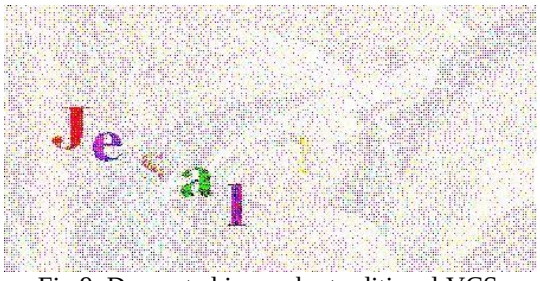


Fig.9. Decrypted image by traditional VCS

Fig 10 shows reconstructed image at decryption side using XOR based VCS. The result shows reconstructed image is degraded but better than traditional and some information is lost.

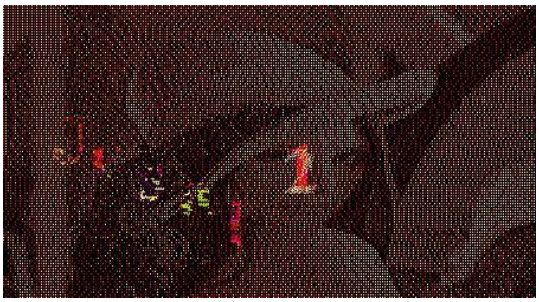


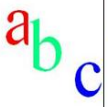
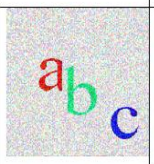
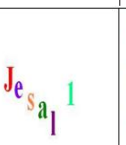
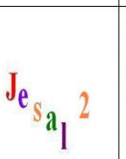
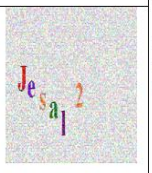
Fig.10 Decrypted using XOR-Based VCS

The Result is shown in below table II. It shows that with proposed low complex stamping algorithm the reconstructed image contrast is decreased but XOR-based VCS for colored image gives better visibility.MSE and PSNR values show the low quality of picture because the encrypted image size is changed due to proposed method of VCS. The meaningful shares makes easier for participant to identify their shares.

The cover image is also halftone color image which is stamped on share.

The stamp is not vanished from image while reconstructed which is the scope for future. The resolution is also changed which can be managed using some method.

Table 2. PROPOSED (2,2)VCS METHOD WITHMEANINGFUL SHARES

Original Image	Cover Image	Shares	Stacked image
 MSE- 0 PSNR- I Size- 225 X 225			 MSE - 1.9672e+004 PSNR - 5.1922 Size – 450 X 225
 MSE- 0 PSNR- I Size-286 x 217	 	 	 MSE- 4.8166e+004 PSNR- 1.30 Size- 572 X 217

V. ADVANTAGES OF THE METHOD

1. Manageable shares that is each share has some meaning to distinguished them from one other.
2. Better quality of reconstructed image compared to traditional VCS.
3. Pixel expansion is double the breath of original image but height is the same. One pixel is splitted in two pixels instead of four which decreases the size of share.
4. Better security because the constructed shares generates random like dots so the intruders won't get any clue of the original image.
5. It works with binary, grey level as well as colored images.
6. Colored image shares are generated in CMY model so it gives better printed hardcopy.

VI. CONCLUSION

The proposed scheme is not tolerable to attacks like rotations, cropping, scaling, contrast adjustments and translation. So we can expand it to handle these destructions. The stamped algorithm is efficient but degrades the quality of image so instead of just stacking the shares some computation at the decryption end can be done. The proposed method is better for softcopy decryption. So we can modify it to make it effective for hardcopy as well. In future we can extend this work to improve recursive visual cryptography reconstructed image quality and security. That enables to hide more than one secret images.

1. It works good for softcopy decryption but hardcopy decryption degrades the contrast of reconstructed image.
2. For stamping algorithm the size of cover image and shares must be same. So it requires resizing the cover image.
3. It can not deal with rotation, cropping , scaling or translated shares. The shares generated must be the same as they were constructed.
4. Only one secret image can be encrypted by this method.

REFERENCES

1. D. Q. Viet and K. Kurosawa, "Almost ideal contrast visual cryptography with reversing," Topics in Cryptology—CT- RSA, pp. 353–365, 2004.
2. E. Biham and A. Itzkovitz, "Visual cryptography with polarization," in RUMP Session of CRYPTO'98, 1997.
3. 3. G. Ateniese, C.Blundo, A.DeSantis and D. R. Stinson, "Visual cryptography for general access structures", Information and Computation 129 (1996), 86-106.
4. 4. M. Naor and A. Shamir, "Visual cryptography II: improving theconstrast via the cover base, in Security Protocols", M. Lomas, ed., Lecture Notes in Computer Science 1189 (1997), 197-202.
5. Naor and A. Shamir, Visual cryptography, in "Advances in Cryptology { EUROCRYPT '94", A.DeSantis, ed., Lecture Notes in Computer Science 950 (1995), 1-12
6. S. J. Shyu, "Efficient visual secret sharing scheme for color images," Pattern Recognit., vol. 39, no. 5, pp. 866–880, May 2006.
7. M. Bose and R. Mukerjee. Optimal (k, n) visual cryptographic schemes for general k. In Designs, Codes and Cryptography, volume 55, pages 19–35, 2010
8. M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary version appears in "Security Protocols", M. Lomas ed. Vol. 1189 of Lecture Notes in Compute Science, Springer-Verlag, Berlin, pp.197-202, 1997
9. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, Half tone Visual Cryptography, IEEE Transaction on image processing, vol. 15, no. 8, 2006
10. 10. W. Hawkes, A.Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).
11. 11. R. Gonzalez and R. Woods, Digital Image Processing using MATLAB, Fourth Impression, 2008.
12. 12. Yusra A. Y. Al-Najjar, Dr.Der Chen Soong Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI, International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August 2012.
13. 13. Joshi Jesalkumari.A and Dr.R.R.Sedamkar , "Modified Visual Cryptography Scheme for Colored Secret Image Sharing", in International Journal of Computer Applications Technology and Research ,Volume 2– Issue 3, 2013, pp: 350 – 356.
14. 14. P.S.Revenkar, AnisaAnjum, W .Z.GandhareGovernment Aurangabad, M.S., India"Survey of Visual Cryptography Schemes" International Journal of Security and Its Applications Vol. 4, No. 2, April,2010
15. 15. Priyanka Singh, Balasubramanian Raman, ManojMisra "A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares"- Journal Signal Processing ,2017,Volume 142 Issue C, Pages 301-319

AUTHORS PROFILE

Mrs. Jesalkumari Varolia, Assistant Professor, has 11 years of teaching experience, received M.E (Computer) in 2013,She is currently pursuing Ph.D with Department of Computer Engineering ,

Dr. R.RSedamkar, Professor & Dean (Academics) at Thakur College of Engineering and Technology ,has23 Years of teaching experience, area of specialization is Networking & Data Compression.