International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 6 (June 2014), PP.01-08

Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication

[1]Pooja' [2]Dr.Lalitha Y. S
[1]P.G Student Digital Electronics, Appa Institute of Engineering & Technology, Gulbarga
[2]Prof. E&CE Department Appa Institute of Engineering & Technology, Gulbarga

Abstract:- With the growth of digital media, it is becoming more prevalent to find a method to protect the security of that media. An effective method for securely transmitting images is found in the field of Visual Cryptography (VC). Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system(HVS), without the aid of computers. In this paper, a novel method of VC is presented for halftone images which represent the resultant image in the same size as the original secret image. This scheme proposed the new algorithms for the (2, 2) visual cryptography. According to visual cryptography the decryption is performed by human visual system. Proposed method based on with the aid of computer at the time of decryption. The proposed schemes are for gray scale image, color image and by stacking the shares; the resultant image achieved in same size with original secret image. The proposed scheme uses the concept of pseudo randomization and pixel reversal approach in all methods.

Keywords:- Information Security, Information hiding, Halftone image, Visual cryptography, Secret share.

I. INTRODUCTION

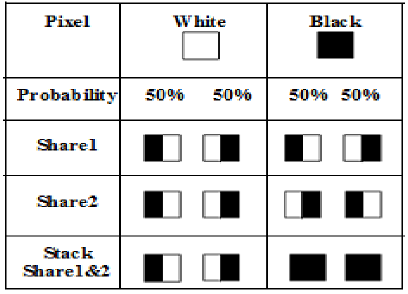
With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed.

Visual cryptography is the concept of dividing a secret image into "n" shares and revealing secret image by stacking a qualified subset of "n" shares. The scheme is perfectly secure and very easy to implement. Visual cryptography takes the input as one secret image and creates the shares by the process of encryption, later decryption is done by HVS.VC scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

The field of VC has been developed over the last several years. The original method was proposed by Naor and Shamir [1] for binary images. This provides a perfectly secure system where secret messages are contained in "shares". Individually these shares resemble random noise, but when they are stacked and aligned perfectly, their message is decrypted using only the human visual system. While this method gives security for text and binary images, the growth of digital media requires the expansion of this technique to provide security for gray and color images. Several methods have been developed for securing gray and color images, including halftoning [2], dithering [3], color subpixel groupings [4], and meaningful image shares [5, 6].Through this expansion of the original method, VC provides a secure way to store and transmit text, binary images, gray images, and color images.

II. PRELIMINARIES AND RELATED WORK

2.1 Basic (2, 2) VC scheme for gray images:



Pixel	White □		Black ■	
Probability	50%	50%	50%	50%
Share1	◧	◨	◧	◨
Share2	◧	◨	◨	◧
Stack Share1&2	◧	◨	■	■

Figure 1: Construction of (2, 2) VC Scheme

Naor & Shamir [1] implemented a (2, 2) visual cryptography where decoded image is double than that of the original secret image as pixel p expanded into two sub pixels. This is called pixel expansion, affecting the contrast of resulting image. Earlier pixel expansion and contrast optimization work revealed that researchers tried to lower expansion and optimize secret picture contrast. They also portray process of creating shares using mathematical representations. The focus is on security and contrast condition [13].

The algorithm is as follows:

1. Convert the gray-level image into a halftone image.
2. For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the rules in Fig.1. If the pixel is white, randomly select one combination from the former two rows in Fig.1 as the content of blocks in Shares 1 and 2. If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies.
3. Repeat Step 2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

2.2 *Image Halftoning:*

A halftone image is made up of a series of dots rather than a continuous tone. These dots can be different sizes, different colors, and sometimes even different shapes. Larger dots are used to represent darker, more dense areas of the image, while smaller dots are used for lighter areas. Color halftoning generates a halftone pattern for each of these inks. When these patterns are printed over each other, the human viewer will observe a color that depends on the amounts of the color inks.

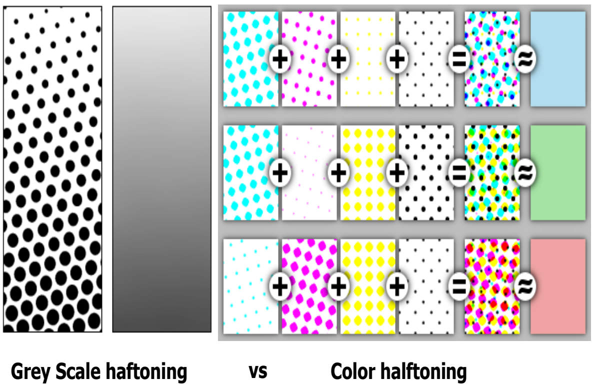


Figure 2: Image halftoning.

Visual cryptographic solutions operate on binary or binaries inputs. Natural (continuous-tone) images must be first converted into halftone images by using the density of the net dots to simulate the original gray or color levels in the target binary representation. The halftone version of the input image is used instead of the original secret image to produce the shares. The decrypted image is obtained by stacking the shares together. Because binary data can be displayed either as frosted or transparent when printed on transparencies or viewed on the screen, overlapping shares that contain seemingly random information can reveal the secret image without additional computations or any knowledge of cryptographic keys.

2.2.1 Error diffusion

Error diffusion [7], [8] produces halftone images of much higher quality than other halftone. It quantifies each pixel using a neighborhood operation.

The error diffusion scans the image one row at a time and one pixel at a time. The current pixel is compared to a threshold (127) value. If it is above the value a white pixel is generated in the resulting image. If the pixel is below the half way value, a black pixel is generated. The generated pixel is either full bright or full black.

Error is calculated which is the difference between original image and halftone image. The error is then added to the next pixel in the image and the process repeats. To which neighbor and how this error is pushed is decided by an error diffusion matrix.

		X	**7/48**	**5/48**
3/48	**5/48**	**7/48**	**5/48**	**3/48**
1/48	**3/48**	**5/48**	**3/48**	**1/48**

Figure3: Jarvis error diffusion weight matrixes

In Figure 3 error diffusion weight matrix is shown. The error occurred at the position (i, j) is weighted by 7/48 and added to the pixel value at (i+1, j). The same error is weighted by 5/48 and added to the pixel at (i+1, j+1) and so on. The same process moves to the pixel at the next position and performs the above described steps until all pixels have been proceeding.

III. EXPERIMENTAL DESIGNS

We have design some schemes on visual cryptography and visual secret sharing. The approach used for these schemes is randomization and pixel reversal. We have done several experiments and came up some new approaches of (2, 2) visual cryptography.

3.1 Randomized Visual cryptography scheme for grayscale images:

The algorithm is as follows:

Encryption:

1. Take any grayscale image as input image.
2. Convert the gray-level image into a halftone image by Jarvis error diffusion.
3. Generate the shares using pseudo randomized and pixel reversal approach as shown in fig 6.

Decryption:

4. Combine the shares to recover secret message.

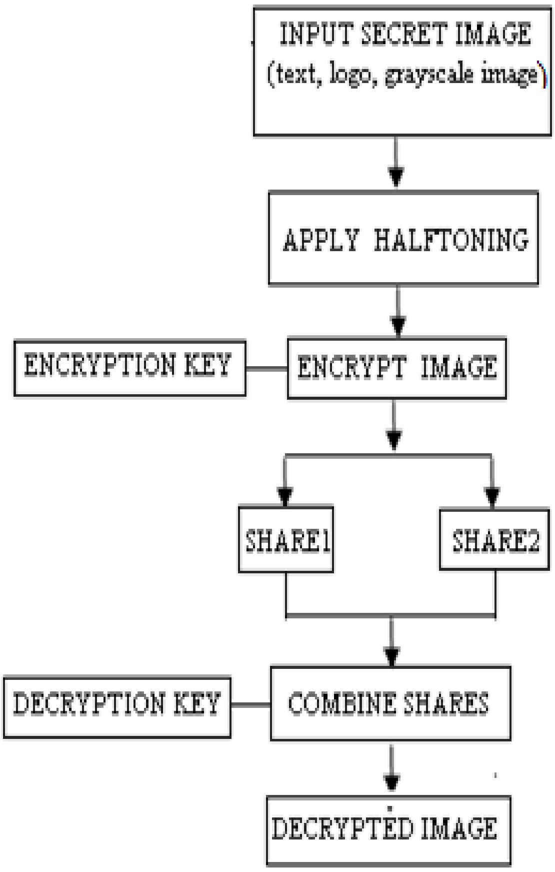


Figure4: Flow chart for grayscale image

3.2 Randomized Visual cryptography scheme for color images:

The algorithm is as follows:

Encryption:

1. Take any 24-bit color image as an input image. Each R-G-B color component is represented by 8-bits.Input image is represented by 224 =16777216 color shades. Such types of images are stored in METLAB in various forms e.g. .bmp, .tiff etc.
2. Split up color image into individual Red, Green and Blue component.
3. Using Jarvis operator we get individual R-G-B color component Halftone image. The pixel in halftone quantized image is represented by a single bit; so that the overall memory storage required will be reduced as well it reduces the number of computations.
4. Concatenating of R-G-B component into a colored Halftone image.
5. Generate the shares using pseudo randomized algorithm and pixel reversal as shown in fig 6.

Decryption:

6. Combine the shares to reconstruct secret image.

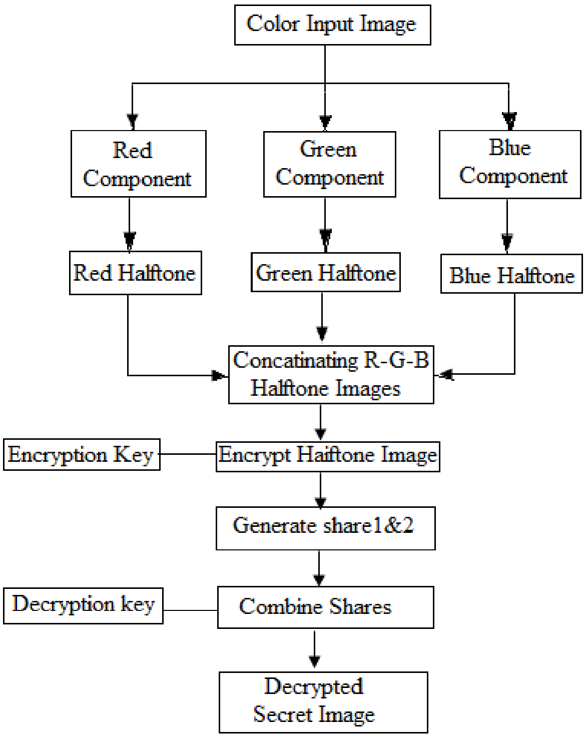


Figure5: Flow chart for color image

3.3 Pseudo Randomized Visual cryptography for halftone images (generating shares):

Encryption:

The (2, 2) visual cryptography scheme has one secret halftone (gray scale or color) image (SI) as algorithm input, where SI is said to be a matrix S_{ij} and i and j shows pixel positions and i, j = 1, 2, 3 . . . n.

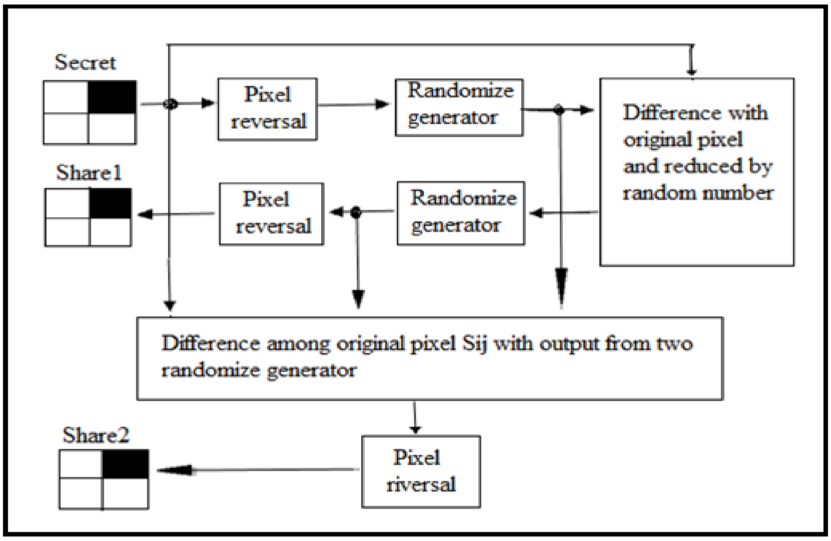
Input: Secret gray scale or color halftone image (S_{ij})

Output: Valid Shares Share 1, Share 2.

All steps of algorithm in this scheme are shown below.

1. Pixel S_{ij} with position i and j is the input called original pixel.
2. Apply pixel reversal i.e $S_{ij}' = 255 - S_{ij}$.
3. Use random number generator (0.1 to 0.9) to reduce S_{ij}' randomly.
4. Take the difference of S_{ij}' with original pixel S_{ij}.
5. Use random number generator to reduce reversed value of S_{ij}' randomly.
6. Apply pixel reversal i.e $S_{ij}'' = 255 - S_{ij}'$.
7. Store in matrix as image called share 1.
8. Take the difference of two random number generators with original pixel S_{ij}.
9. Apply pixel reversal i.e $S_{ij}''' = 255 - S_{ij}'$.
10. Store S_{ij}''' in matrix as image called share 2.
11. Repeat point 1 to 10 for all pixels from original image (i.e matrix of original image).

This algorithm is shown in Figure below:


Secret
Pixel reversal
Randomize generator
Difference with original pixel and reduced by random number
Share1
Pixel reversal
Randomize generator
Difference among original pixel Sij with output from two randomize generator
Share2
Pixel riversal

Figur6: Pseudo-Randomized Visual Cryptography (PRVC)

Pair Key Structure:

The input image has been converted to the halftone image. A pair key should be given in order to the sender and receiver to get paired mutually. If the key value matches between the sender and receiver, the receiver can further reveal the secret input message. If the pair key fails the receiver can not reveal the secret message. This structure is designed in order to promote good security level in modern visual secret sharing (VSS).

Decryption:

Decryption is done just inverse of encryption using proposed algorithm for generating the shares. This results in no loss of contrast of the original image. The following final equation is used to decrypt the shares:
Decrypted image(S) = (510-Share1-Share2+255*random generator#)**.** / (1+random generator#)

Discussions: This VC scheme use gray scale (or color) secret image. In (2, 2) visual cryptography by Naor & Shamir was implemented in [9]. Where the decoded image is twice that of original secret image because the pixel p expanded into two subpixels this effect is called pixel expansion. That affects the contrast of the resulting image. The previous work on pixel expansion and contrast optimization shows that researcher did efforts to reduce the expansion and optimize the contrast of the secret picture [10,11,12].Further they portrait the process of creating the shares using mathematical representations and mainly they focus the security and contrast condition [13].

In the previous scheme of pseudo randomized VC [14] the original secret image is divided so that it reveals the secret image after OR operation of qualified shares. And also the decoded image is darker than the secret image. Some contrast in change and impairments are visible after following these schemes. Based on observation this algorithm could not give perfect meaningless shares in case of the dark or high contrast secret image, so added preprocessing elements to change the dark or high level of gray image into lighter one (called preprocessed image). This is to be done before giving input secret image to algorithm. They defined two way of preprocessing of the input image as follows.

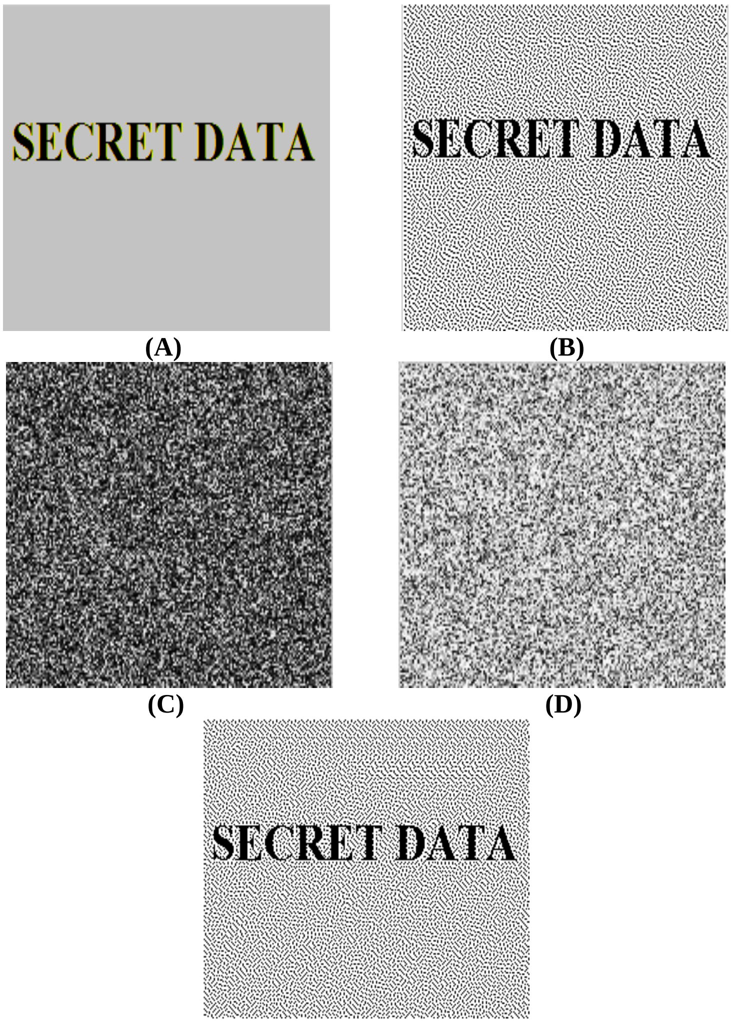
Change the pixel values to white (255) on the bases of the position of the pixel. Use odd and even combination of the pixel values in the matrix as follows:

Method 1: If i=j=odd and i=j=even1
Pixel (i, j) = 255.

Method 2: If i=odd & j=even OR i=even & j=odd
Pixel (i, j) = 255.

This preprocessing converts the secret image into lighter one in contrast.

In the proposed scheme the decoded image is same in size of original secret message there is no pixel expansion effect found. Also there is no loss of contrast of the resulting image , it is same as input image. The decoded secret image has increase the spatial resolution however mostly of visual cryptography scheme has shown the same effect in their decoded image.

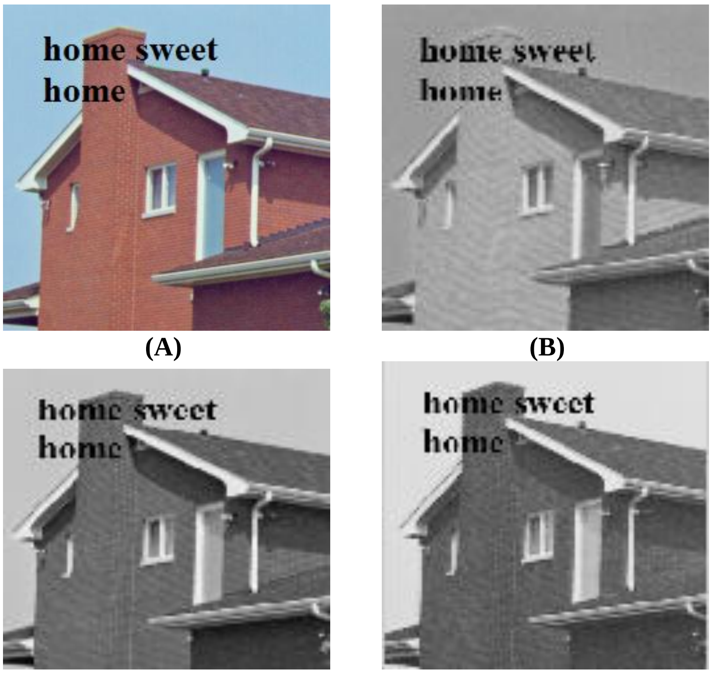


(A) **(B)**

(C) **(D)**

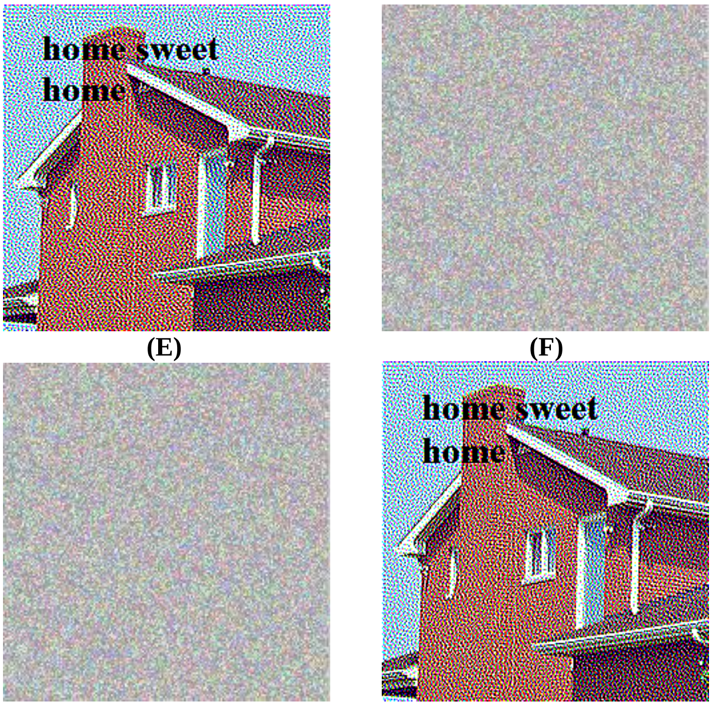
(E)

Figure 7: Pseudo-Randomized visual Cryptography results
(A) Secret Image (B) Halftone Image(C) Share 1 (D) Share 2 (E) Stacking of Share 1 and Share 2



(A) **(B)**

(C) **(D)**



(E) **(F)**

(G) **(H)**

Figure8: Pseudo-Randomized visual Cryptography results for color image (A) Secret Image (B) R Component (C)G Component (D)B Component(E)Halftone image (F) Share 1(G) Share 2 (H) Stacking of Share 1 and Share 2.

IV. RESULTS AND DISCUSSION

It is seen from figure8 that the secret image has better results without pre-processing after giving the true gray scale picture. But with the use of preprocessing the shares reveal information about the secret and this is further improved by the use of proposed algorithm. This shows the perfect meaningless stacked shares. Also it is seen from Figure9 that the secret color image has better results without pre-processing.

The comparisons of the existing and proposed works as shown in the Table2.

Table2: Comparison of algorithms

Algorithm	Complexity	Pixel Expansion	Security	Quality
Naor Shamir (basic 2×2)	Medium	Double	Increase	Poor
Proposed Technique	Less	No Expansion	Increase	Average

V. CONCLUSIONS AND FUTURE WORK

It is seen that the (2, 2) pseudo-randomized visual cryptography which generates shares, based on pixel reversal, randomized reduction in original pixel and subtractions of the original pixel. The original secret image is divided so that it reveals the secret image after inverse operation of qualified shares. This scheme reveals reduced pixel expansion, required for retrieval of the secret image and no loss in contrast of the decrypted image.

Both original and retrieved image having same sizes are the results of the proposed scheme. But pixel size increase provides easier alignment of shares which is still a research area. The proposed schemes revealed good security due to its randomness.

The proposed scheme works well for text, logo. Whereas for grayscale image and color image it works average. Because of halftoning, quality of the image is degraded.

The future work is to improve the contrast, resolution and reduce the pixel expansion in the resultant secret image. Further extend this work to use this technique with 3D images for creating the shares that have partial secret and reveal that secret by stacking to each other.

ACKNOWLEDGEMENT

I would like to give this work to my parent, who has created the author of this thesis. I would like to thank Dr.Lalitha Y.S my advisor for her understanding and research guidance.

REFERENCES

[1]. Moni Naor and Adi Shamir. Visual cryptography. EUROCRYPT, pages 1{12, 1994}.

[2]. Luiz Velho and Jonas de Miranda Gomes. Digital halftoning with space filling curves. Computer Graphics, 25(4):81{90, July 1991.

[3]. Chang-Chou Lin and Wen-Hsiang Tsai. Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24:349{358, 2003}

[4]. Young-Chang Hou. Visual cryptography for color images. Pattern Recognition, 36:1619{1629, August 2002}.

[5]. Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, and Chwei-Shyong Tsai. A novel authenticable color visual secret sharing scheme using non-expanded meaningful shares. Displays, 32:118{134, February 2011.

[6]. C-C Chang, W-L Tai, and C-C Lin. Hiding a secret color image in two color images. The Imaging Science Journal, 53:229{240, May 2005.

[7]. K. T. Knox, Error Image in Error Diffusion, Proc. Of SPIE, vol. 16, 268-279.

[8]. P. T. Metaxas, Thesis Parallel Digital Halftoning by Error Diffusion, Department of Computer Science, Wellesley College.

[9]. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo,"Half Visual Cryptography", IEEE Transaction on image processing, vol. 15, no. 8, 2006.

[10]. C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes", SIAM J. on Discrete Math. 16, 2003, 224-261.

[11]. Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, "On the Contrast in Visual Cryptography Schemes", Journal of Cryptology: the journal of the International Association for Cryptologic Research, 1996

[12]. Stelvio Cimato, Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, "Ideal contrast visual cryptography schemes with reversing", Information Processing Letters, Elsevier, www.elsevier.com/locate/ipl.

[13]. Jim Cai, "A Short Survey On Visual Cryptography Schemes", 2004 http:// www.cs.toronto.edu/~jcai/paper.pdf.

[14]. Ch.Ratna Babu, M.Sridhar, “Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security”, International Conference on Information Systems and Computer Networks, 2013.

AUTHOR’S PROFILE

Poojareddy B. Goure received her BE degree in Electronics and Communication engineering in 2012 from Visvesvaraya Technological University, Karnataka. Currently, she is pursuing M.Tech in Digital Electronics from AIET, Gulbarga, and Karnataka. She is working on the project “Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication”. Her areas of interest are Image Processing, VLSI and Software Engineering.

Lalitha Y.S was born on December 7, 1969 in India. She **received** B.E degree in Electronics and Communication Engineering and M.E. degree in Power Electronics from Gulbarga University Gulbarga, India, in 1991 and 2002 respectively. She is working as Professor in Appa Institute of Engineering & Technology, Gulbarga, India. Her research interests include image Processing, Wavelet Transform coding. She attended Four National Conferences and three International Conferences.