Webpage: www.ijaret.org

Volume 3, Issue VIII, Aug 2015
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Design and Evaluation of Visual Crypto System

Preeti[1], Manisha Gahlot[2]

[1]M.Tech Scholar
South Point Institute of Tech. & Management
meenunashier27@gmail.com
[2]Assistant Professor,
South Point Institute of Tech. & Management
mani_sehra@yahoo.com

Abstract-*In the field of communication, security is an important issue nowadays. Digital communication has seen exponential enlargement in the past few decades. As a result, the security of digital data has become a field of far-reaching research since piracy and unofficial use of such data is common because of the ease with which data can be pretended or tampered. It is now common to transfer multimedia data via the Internet. Visual Cryptography (VC) is a special cryptographic technique where decryption is done by a certified user by simply overlaying the shares. It uses the quality of human vision to decrypt encrypted images. It does not require complex calculation. The basic idea of the visual cryptography scheme is to split a secret image into number of arbitrary shares which alone reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the shares. For security concern; it also ensures that hackers cannot scrutinize any clues about a secret image from individual cover images. So, there is a need to design a method by which a binary image could me encrypted and decrypted easily in a secure manner. Watermarking is a prospective method for protection of ownership rights on digital audio, image, and video data. It helps to identify the true owner of the digital information. This technology is one of the possible methods to protect digital information. An image data encoding technique using combination of image encryption and visual cryptography has been proposed in his research work. This hybrid technique takes the advantages of both techniques and emerge as an efficient algorithm in terms of security and efficiency. Since, we are encoding the target image before inputting it into visual cryptography, this modification enhance the security of proposed method. MATLAB R2013a has been taken as an implementation platform. Image processing toolbox and generalized MATLAB toolbox has been taken as implementation tools.*

Keywords: *Cryptography, Visual Cryptography, Security, Sharing, Stacking.*

1. INTRODUCTION

Cryptography

Cryptography refers to the study of mathematical techniques and related aspects of Information security like data confidentiality, data Integrity, and of data authentication. Cryptography as the study of secret (crypto) writing (graphy) can be defined as the science of using mathematics to encrypt and decrypt data back. It allows two people, commonly known as Alice and Bob, to communicate with each other securely. This means that an eavesdropper known as Eve will not be able to listen in on their communication [5].

2. VISUAL CRYPTOGRAPHY

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 in to 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 introduced by first in 1994 Noar and Shamir [2] [9]. Visual cryptography is a cryptographic technique which all ows visual information (e.g. printed text, hand written notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the identity of computers. It is a technique of cryptography which enables the decryption of images without using computer [8]. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation [7]. This property makes visual cryptography especially useful for the low computation load requirement [2]. Visual cryptography schemes are characterized by two parameters: the expansion corresponding to the number of sub pixels contained in each share and the contrast, which measures the “difference” between black and white pixels in the reconstructed image. Combining the shares together reveals the information. Minimum two shares are needed for revealing the secret image [5]. In Visual Cryptography Scheme (VCS) there are five phases i.e. halftoning, shrare Generation, Embedding secret, Extracting secret, reveal secret [7].

3. MODEL OF VISUAL CRYPTOGRAPHY

In this section we formally define VCS model, as well as (k, n)-threshold VCS scheme that was proposed by Naor and Shamir.

Definition 1: Hamming weight: The number of non-zero symbols in a symbol sequence. In a binary representation, Hamming weight is the number of "1" bits in the binary sequence.

Definition 2: OR-ed k-vector: Given a j x k matrix, it is the k-vector where each tuple consists of the result of performing Boolean OR operation on its corresponding jx1 column vector [1].

Definition 3: An VCS scheme is a 6-tuple (n, m, S, V, a, d). It assumes that each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white sub pixels. The resulting structure can be described by an nxm Boolean Matrix S= [Sij] where Sij = 1 iff the jth sub pixel in the ith share is black. Therefore, the grey level of the combined share, obtained by stacking the transparencies, is proportional to the Hamming weight H (V) of the OR-ed m-vector V. This grey level is usually interpreted by the visual system as black if H (V) ≥ d and as white if H (V) < d-am for some fixed threshold 1≤d≤ m and relative difference a> 0. a m, the difference between the minimum H(V) value of a black pixel and the maximum allowed H(V) value for a white pixel is called the contrast of a VCS scheme [1].

Definition 4: VCS Schemes where a subset is qualified if and only if its cardinality is k, are called (k, n)-threshold visual cryptography schemes. A construction to (k, n)-threshold VCS consists of two collections of n x m Boolean matrices C0 and C1, each of size r. To construct a white pixel, we randomly choose one of the matrices in C0, and to share a black pixel, we randomly choose a matrix in C1 [1]. The chosen matrix will define the color of the m subpixels in each one of the n transparencies. Meanwhile, the solution is considered valid if the following three conditions are met:

[1.] For any matrix S in C0, the "or" operation on any k of the n rows satisfies H(V) < d-a m.

[2.] For any matrix S in C1, the "or" operation on any k of the n rows satisfies H (V) ≥d.

[3.] For any subset {i1 i2,... iq} of {1, 2,.. .n} with q< k, the two collections of q x m matrices Bt for t€{0,1} obtained by restricting each n x m matrix in Ct(where t = 0,1) to rows i1,i2, ...,iq are indistinguishable in the sense that they contain the same matrices with the same frequencies. In other words, any q x n matrices S0 €B0 andS1 €B1 are identical up to a Column permutation [1].

Condition first and second defines the contrast of a VCS. The third condition states the security property of (k, n)-threshold VCS. If we have not been given k shares of the secret image, one cannot gain any hint in deciding the color of our pixel, regardless having any amount of computation resources. [1]

4. BLACK AND WHITE VISUAL CRYPTOGRAPHY SCHEME

Sharing Single Secret: In this encoding scheme a binary image is divided into two shares, Share 1 and Share 2. If pixel is white one of the above two rows of **Table1** is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table1 is chosen to generate Share1and Share2. Here each share pixel code denote two white and two black pixels each of share alone gives noise clue about the pixel whether it is white or black [2].

Table1: Naor and Shamir's scheme for encoding a binary pixel into two shares [2]

Pixel	Probability	Share$_1$	Share$_2$	Share$_1$ ⊗ Share$_2$
□	50%	◧	◧	◧
	50%	◨	◨	◨
■	50%	◧	◨	■
	50%	◧	◧	■

To hide a binary image into two meaningful shares author suggested spatial-domain image hiding schemes. These two secret shares are embedded into two gray level cover images. To decode the hidden messages, embedding images can be superimposed. Balancing the performance between pixel expansion and contrast author recommend a (2, n) scheme based on combination.

The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated.

5. SCHEME TO SECURE IMAGE SHARES

Visual Cryptographic Encryption

In this phase author will do visual cryptography encryption. It consists of generation of shares using any basic visual cryptography model. In our proposed scheme, a (2, 2) VC share creation is performed. Each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub pixels. A black pixel is shared into two complementary blocks of four sub pixels. All the pixels in the secret image are encrypted similarly using this scheme. The shares can be either Vertical, Horizontal or Diagonal shares. Any single share is a random choice of two black and two white sub pixels, which looks medium grey. When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black) [3].

The visual secret sharing scheme assumes that the message consists of a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. The resulting structure can be described by an n × m Boolean matrix S = [sij] where sij=1 iff the th sub pixel in the th transparency is black. When transparencies in i1, i2...ir in S. The grey level of this combined share is proportional to the Hamming weight H (V) of the “or” ed m-vector V. This grey level is interpreted by the visual system of the users as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$.

Hiding the Shares using Digital watermarking

This phase embeds image shares into some cover images using digital watermarking. Result of this phase will be different meaningful shares consist some cover image. Discrete cosine transformation (DCT) is used for convert the image into frequency domain. DCT can be interpreted as decomposition into a set of frequency coefficients having the same bandwidth on a logarithmic scale. The obtained coefficients are real number values. The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. The algorithm for embedding the watermark is following.

Step 1: Set minimum coefficient difference.
Step 2: Set the size of the block in cover image to be used for each bit in watermark.
Step 3: Read in cover object.
Step 4: Determine size of cover image
Step 5: Determine maximum message size based on cover object and block size.
Step 6: Read in the message image.
Step 7: Reshape the message to a vector.
Step 8: Check that the message is not too large for cover.
Step 9: Pad the message out to the maximum message size with ones.
Step 10: Process the image in blocks.
Step 11: Transform block using DCT.
Step 12: If message bit is black then value of frequency coefficient (5, 2) > (4, 3).
Step 13: End if
Step 14: If message bit is white then value of frequency coefficient **(**5, 2) < (4, 3).
Step 15: End if
Step 16: Adjust the two values such that their difference >=k.
Step 17: Transform block back into spatial domain.
Step 18: Move on to next block, at the end of row move to next row.
Step 19: Exit [3]

Sharing a Secret Image in Binary Images with Verification: This scheme uses a watermark image to verify the reconstructed secret image so that a defined participant does not need to execute shadow verification during both the shares reconstruction phase and the revealing phase. Scheme can be divided into two procedures: (1) the shares construction procedures, and (2) the revealing and verifying procedures [6]. First, during the shares construction procedure, the dealer generates two shadows, called *SA* and *SB*, from the secret image *I* and a binary watermark *L*. Second, the dealer applies a torus automorphism to permute two generated shadows. During the revealing and verifying procedure, participants repermute two collected shadows and later reconstruct a secret image *I′* and an extract watermark *L′* [6].

Visual Cryptography and Secret Fragment Visible Mosaic Images

For the data hiding visual cryptography and secret fragment visible mosaic images plays a very important role. Mosaic is a different type of art manufactured by generating small pieces of any materials, such as stone, glass, tile, etc. First target image is selected; the given secret image is then divided into rectangular tiles, which then are fit into similar blocks in the target image. Next, the colour characteristic of each tile image is transformed to be that of the corresponding block in the target image, resulting in a secret mosaic image which looks like the selected target image [4].

Mosaic Image Creation

In this first phase, Shamir secret sharing algorithm is used by which a secret is divided into parts, giving each participants its own unique part, some of the parts or all of them are needed in order to reconstruct the secret counting on all participants to combine together, the secret might be impractical and therefore sometimes the threshold scheme is used. Now fit the title of the secret image into the target block of a preselected target image. After this transforming the colour characteristic of each tile image in the secret image to become that of the corresponding target block in the target image and rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block. After the rotation relevant information is embedding into the created mosaic image for future recovery of the secret image. In this way we get the output secret fragment visible mosaic [4].

Secret Image Recovery

In this second phase, extracting the embedded information for secret image recovery from the mosaic image, and recovering the secret image using the extracted information by secret image recovery algorithm. In this phase result will be calculated and optimize if required result is in the form of delay and accuracy [4].

6. PROPOSED METHODOLOGY

1. Reading of target image.
2. Conversion of watermark image into binary one.
3. Calculation of size of watermark image matrix.
4. Calculation of total number of elements in watermark.
5. Requesting ciphering key from user.

Encryption of watermark

6. Declaration of loop according to the total number of watermark elements.
7. Generation of random sequence according to the size of watermark image.
8. Conversion of random matrix into binary one.
9. Declaration of outer and inner loop according to rows and columns of watermark matrix.
10. Xoring of binary random sequence and binary watermark so as to encrypt the watermark.
11. Display of original watermark and encrypted watermark.

Visual cryptography

12. Calculation of size of input binary secret image
13. Creation of share 1 according to the size of input binary secret image
14. Creation of share 2 according to the size of input binary secret image
15. Processing of White pixel.
16. White pixel share combinations.
17. Finding of white pixel indices in input binary secret image.
18. Calculation of number of rows of white pixel.
19. Random permutation the share generation.
20. Generation of share 1 and share 2 randomly for white pixel.
21. Processing of Black pixel.
22. Black pixel share combinations.
23. Finding of black pixel indices in input binary secret image.
24. Calculation of number of rows of black pixel.
25. Random permutation the share generation.
26. Generation of share 1 and share 2 randomly for black pixel.
27. Calculation of MSE and PSNR of share 1 and share 2.
28. Display of share 1 image.
29. Display of share 2 image.
30. Overlapping of share 1 and share 2 using or operation.
31. Display of overlapped image.

Decryption of watermark

32. Calculation of size of new watermark image matrix.
33. Calculation of total number of elements in watermark.
34. Requesting deciphering key from user.
35. Declaration of loop according to the total number of watermark elements
36. Generation of random sequence according to the size of watermark image
37. Conversion of random matrix into binary one
38. Declaration of outer and inner loop according to rows and columns of watermark matrix.
39. Xoring of binary random sequence and binary watermark so as to encrypt the watermark
40. Display of decrypted watermark.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Calculation of Performance Parameters

41. Calculation of mean square error between original target image and recovered image.
42. Calculation of peak signal to noise ratio between original target image and recovered image.
43. Calculation of correlation value between original target image and recovered image.

7. EXPERIMENTAL RESULTS

An image data encoding technique using combination of image encryption and visual cryptography has been proposed in his research work. This hybrid technique takes the advantages of both techniques and emerge as an efficient algorithm in terms of security and efficiency. Since, we are encoding the target image before inputting it into visual cryptography, this modification enhance the security of proposed method. MATLAB R2013a has been taken as an implementation platform. Image processing toolbox and generalized MATLAB toolbox has been taken as implementation tools. Two images 'PREETI.png' and 'crypt.png' has been taken as target images for experimental purpose. The size of these images is 550 x 550. Image encryption method is aplied on this image so as to encode this image. This image will go further for visual cryptography and 2 shares of this encoded image will be generated named share 1 and share 2. These shares will undergo for overlapping so as to recover encoded image. Then this encoded image will further go for decoding or reverse encoding procedure and original target image will be recovered. Figure 1 is snapshot of target image with encrypted image. Figure 2 is the snapshot of share 1. Figure 3 is the snapshot of share 2. Figure 4 is the snapshot of overlapped share. Also, some output performance parameters i.e. PSNR of share 1 and share 2, MSE and PSNR of target image and recovered image has been calculated. Figure 6 is the snapshot of MATLAB command window showing PSNR of share 1 and share 2. Figure 7 is the snapshot of MATLAB command window showing PSNR, MSE of target image and recovered image. Also, a table has been prepared showing the values of these parameters for image 'PREETI.png' and 'crypt.png'.

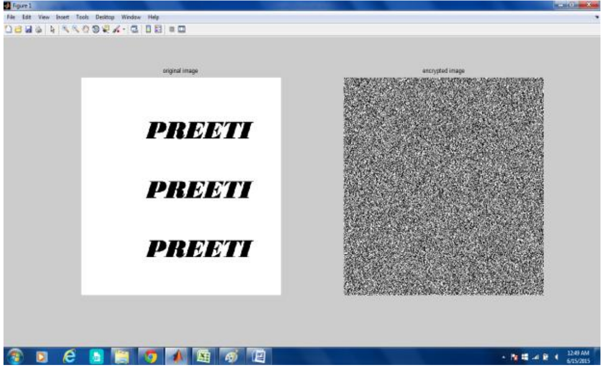


Figure 1: snapshot of target image with encrypted image

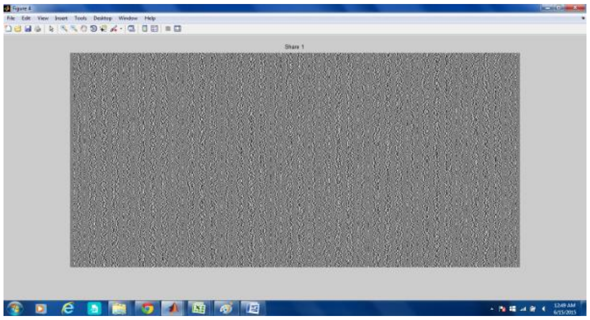


Figure 2: snapshot of share 1

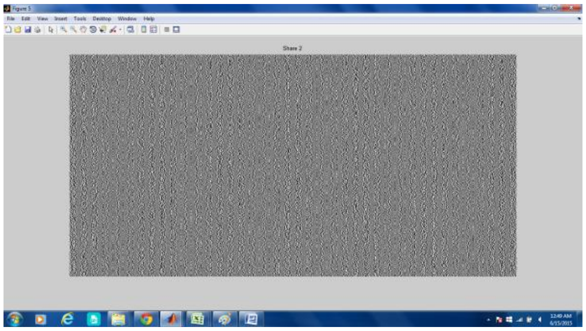


Figure 3: snapshot of share 2

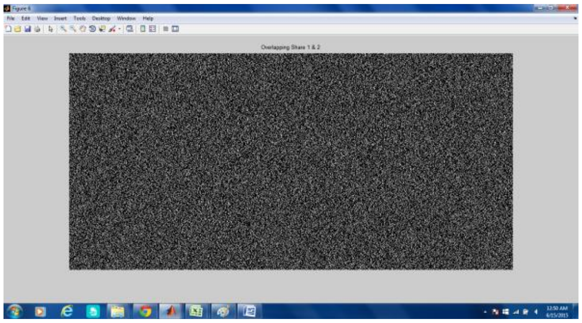


Figure 4: snapshot of overlapped share

Also, some output performance parameters i.e. PSNR of share 1 and share 2, MSE and PSNR of target image and recovered image has been calculated.

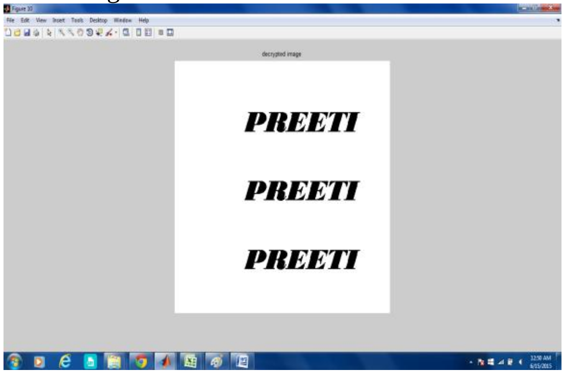
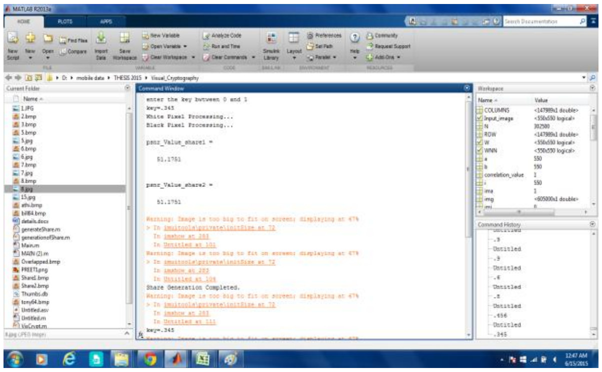


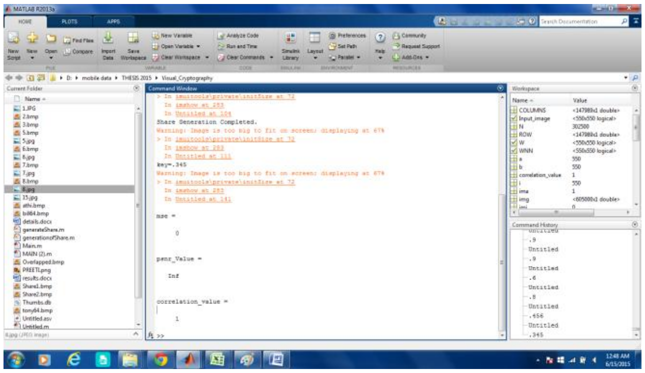
Figure 5: snapshot of overlapped share

Also, some output performance parameters i.e. PSNR of share 1 and share 2, MSE and PSNR of target image and recovered image has been calculated.



```
enter the key bwtween 0 and 1
key=.345
White Pixel Processing...
Black Pixel Processing...

psnr_Value_share1 =

   51.1751


psnr_Value_share2 =

   51.1751

Warning: Image is too big to fit on screen; displaying at 47%
> In imuitools\private\initSize at 72
  In imshow at 283
  In Untitled at 101
Warning: Image is too big to fit on screen; displaying at 47%
> In imuitools\private\initSize at 72
  In imshow at 283
  In Untitled at 104
Share Generation Completed.
Warning: Image is too big to fit on screen; displaying at 47%
> In imuitools\private\initSize at 72
  In imshow at 283
  In Untitled at 111
key=.345
```

Figure 6: snapshot of MATLAB command window showing PSNR of share 1 and share 2



```
> In imuitools\private\initSize at 72
  In imshow at 283
  In Untitled at 104
Share Generation Completed.
Warning: Image is too big to fit on screen; displaying at 67%
> In imuitools\private\initSize at 72
  In imshow at 283
  In Untitled at 111
key=.345
Warning: Image is too big to fit on screen; displaying at 67%
> In imuitools\private\initSize at 72
  In imshow at 283
  In Untitled at 141

mse =

     0


psnr_Value =

   Inf


correlation_value =

     1

>>
```

Figure 7: snapshot of MATLAB command window showing PSNR, MSE of target image and recovered image

Table 1: MSE, PSNR for share 1, share 2, 'PREETI.png' and 'crypt.png'

S. No.	File name	File size	PSNR of Share 1	PSNR of share 2	MSE b/w input and extracted image	PSNR b/w input and extracted image	Normalized correlation value b/w input and extracted image
1.	PREETI.png	550 x 550	51.1751	51.1571	0	infinity	1
2.	crypt.png	550 x 550	51.1751	51.1751	0	infinity	1

8. CONCLUSION & FUTURE SCOPE

Visual Cryptography provides one of the secure ways to transfer images on the Internet. The main advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. A new advanced visual cryptographic technique has been introduced in this present research work. An image data encoding technique using combination of image encryption and visual cryptography has been proposed in his research work. This hybrid technique takes the advantages of both techniques and emerge as an efficient algorithm in terms of security and efficiency. Since, we are encoding the target image before inputting it into visual cryptography, this modification enhance the security of proposed method. This work also solve the problem of security of encoded images i.e. share 1 and share 2 as scam can access all communication channels but cant reconstruct the secret image random permutation is used for creation of shares. Proposed method also overcomes pixel expansion related problem. The performance analysis of the proposed method reveals that the proposed encryption method is ideal. Yet many possible enhancements and extensions can be made to improve further. In future the proposed system can be extended such that it can be applied to all types of image formats like jpg, jpeg, png, tif, gif etc.

REFERENCES

[1] Debasish Jena, Sanjay Kumar Jena, "A Novel Visual Cryptography Scheme", International Conference on Advanced Computer Control, DOI 10.1109/ICACC.2009.109.

[2] Thottempudi Kiran1, K. Rajani Devi, "A Review on Visual Cryptographic Scheme", Journal of Global Research in Computer Science, Volume 3, No. 6, June 2012, ISSN-2229-371X.

[3] Jagdeep Verma, Dr. Vineeta Khemchandani, "A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA) www.ijera.com Vol. 2, Issue 1, Jan-Feb 2012, pp.1121-1125 112, ISSN: 2248-9622.

[4]] Rucha R. Raut, Prof. Komal B. Bijwe, "A Survey Report on Visual Cryptography and Secret Fragment Visible Mosaic Images", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 3, Issue 10, October 2014 ISSN 2319 – 4847.

[5] Aswathy. S, "Watermarked LTVC Scheme", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1167-1170, ISSN: 0975-9646.

[6] Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu, "Sharing a Secret Image in Binary Images with Verification", Journal of Information Hiding and Multimedia Signal Processing , ISSN 2073-4212, Ubiquitous International Volume 2, Number 1, January 2011.

[7] Shital B. Pawar, Prof. N. M. Shahane, "Visual Secret Sharing Using Cryptography", International Journal of Engineering Research, Volume No.3, Issue No.1, pp : 31-33 , 01 Jan. 2014 ISSN:2319-6890.

[8] M. Bharathi, R. Charanya and T. Vijayan " Halftone Visual Cryptography & Watermarking" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April - 2013 ISSN: 2278-0181.pp. 2747-2752.

[9] Namrata Joshi and Vishal Sharma" A Review New Methodology for Visual Cryptography in Color Image Based on Cyclic Shift Pixel Method" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 6, August – 2012 ISSN: 2278-0181. Pp. 1-4.