International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Image Database Security Using Multilayer Multi Share Visual Cryptography

Apurva A. Mohod [1], Prof. Komal B. Bijwe[2]

[1, 2]Amravati University, P.R. Pote college of Engineering and Management, Kathora Naka, Amravati

Abstract: ***In this paper, we are presenting a novel technique of multilayer multi share Visual Cryptography in which image is encrypted at multiple levels using sterilization algorithm. In encryption secret image is converted into monochromatic image i.e. Red, Green and Blue channels are separated and each channel encrypted using sterilization algorithm. It is a bitwise operation. Shares obtain at each level are stored in database using that database image is encrypted to further levels. For decryption all the shares are need to be superimposed in proper sequence using desterilization algorithm. By stacking shares with same keys, original secret image is revealed.***

Keywords: Multilayer, Multishares, Sterilization, Visual Secret Shares,Security,bitwise operation.

1. Introduction

Visual Cryptography (VC) is a technique which encrypts the image and converts it into unreadable format and by decrypting the image original secret image is obtained. Encryption is the process of transforming the image into some other image using an algorithm so that any unauthorized person cannot recognize it. Visual cryptography is extended up to secret sharing. Visual secret sharing encrypt a secret image into transparent parts which are called as shares such that stacking a sufficient number of shares reveals the secret image. It is a obtain from secret sharing scheme given by Adi Shamir in 1979 in which they showed how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k – 1 pieces reveals absolutely no information about data D[1]-[3]. Visual cryptography can also be somewhat deceiving to the inexperienced eye, in such a way that, if an image share were to fall into the persons hands, it would look like an image of random noise or bad art.

Early Visual Cryptography Systems are mainly focused on black-and-white secret images. If the original image is not black and white, for example, a gray-scale image, dithering is employed to preprocess the original image that could degrade the image quality. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast. Pixel expansion, which means that each secret share is of size several times bigger than the original image. In these cases all participants who hold shares are assumed to be honest, that is, they will not present false or fake shares during the phase of recovering the secret image. Two important parameters which govern the quality of reconstructed images are m (pixel expansion rate which represents the loss in resolution from the original image to the shares) and α (the relative difference in weight between the superimposed shares that come from one color level (e.g. black) and another color level (e.g. white)). For image Integrity, a good VCS should bring the value of m close to one (i.e. no pixel expansion) and α as large as possible [4]-[6].

2. Previous Work

Visual cryptography was originally invented and pioneered by *Moni Naor and Adi Shamir* [7] in *1994* at the Eurocrypt conference. The (k, n) Visual Cryptography Scheme can decode the concealed images without any cryptographic computations. It contain black and white pixel only and it was for sharing single secret. The secret image is divided into exactly two random shares i.e. Share1 and Share2. To reveal the original image, both shares are required to be stacked. They use complementary matrices to share a black pixel and identical matrices to share a white pixel. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black. This implies that the superimposition of the shares represents the Boolean OR function.

Until year *1997* visual cryptography schemes were applicable to only black and white images. First colored visual cryptography scheme was developed by *Verheul and Van Tilborg* [8] for sharing single secret. Colored secret images can be shared with the concept of arcs or maximum distance separable codes. In colorful visual cryptography one pixel is transformed into m sub pixels, and each subpixel is divided into c color regions. In every sub pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacking of sub pixels. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3.The share generated were meaningless.

Nakajima, M. and Yamaguchi, Y.[9],developed Extended visual cryptography scheme (EVS) in *2002*. An EVC provide technique to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography. Generally, visual cryptography suffers from the deterioration of the image quality. It showed a method to improve the image quality of the output by enhancing the image contrast beyond the constraints given by the previous studies. The method enables the contrast enhancement by extending the concept

of error and by performing half toning and encryption simultaneously. This paper also describes the method to improve the quality of the output images.

Extended visual cryptography was proposed recently to construct meaningful binary images as shares using hypergraph colourings, but the visual quality is poor to overcome these problem in *2006, Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo*[10],suggested a novel technique named halftone visual cryptography to achieve visual cryptography via halftoning. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. This paper focuses on developing a general halftone visual cryptography framework, where a secret binary image is encrypted into high-quality halftone images, or halftone shares. In particular, the proposed method applies the rich theory of blue noise half toning to the construction mechanism used in conventional VC to generate halftone shares, while the security properties are still maintained. The proposed method utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares carrying significant visual information. The visual quality of obtained halftone shares is observably better than any available visual cryptography method known to date. It maintains good contrast and security and increases quality of the shares.

In *2012, Somdip Dey*[11] proposed a novel method for visual cryptography, which consist of three stages: 1) First, a number is generated from the password and each pixel of the image is converted to its equivalent eight binary number, and in that eight bit number, the number of bits, which are equal to the length of the number generated from the password, are rotated and reversed; 2) In second stage, extended hill cipher technique is applied by using involuntary matrix, which is generated by same password used in second stage of encryption to make it more secure; 3) In last stage, they perform modified Cyclic Bit manipulation. First, the pixel values are again converted to their 8 bit binary format. Then 8 consecutive pixels are chosen and a 8X8 matrix is formed out of these 8 bit 8 pixels. After that, matrix cyclic operation is performed randomized number of times, which is again dependent on the password provided for encryption. After the generation of new 8 bit value of pixels, they are again converted to their decimal format and the new value is written in place of the old pixel value. This system provides high level of security to the image.

Simple Visual Cryptographic technique is insecure. This cryptographic technique involves dividing the secret image into n shares and a certain number of shares (m) are sent over the network. The decryption process involves stacking of the shares to get the secret image. To overcome this problem *Manika Sharma, Rekha Saraswat in 2013*[12] proposed a cryptographic technique for color images where they are using color error diffusion with XOR operation. The shares are developed using Random number. The key generated for decryption process is sent securely over the network using RSA algorithm. Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. The simplest form of the algorithm scans the image one row at a time and one pixel at a time. The current pixel is compared to a half-gray value. If it is above the value a white pixel is generated in the resulting image. If the pixel is below the half way brightness, a black pixel is generated. The generated pixel is either full bright or full black, so there is an error in the image. The error is then added to the next pixel in the image and the process repeats.

In 2014 Shubhra Dixit, Deepak Kumar Jain and Ankita Saxena[13]proposed an approach for secret sharing using randomized VSS in which they propose new visual cryptography algorithm for gray scale image using randomization and pixel reversal approach. (2, 2) randomize visual cryptography in practice where the shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel. The original secret image is divided in such a way that after OR operation of qualified shares reveals the secret image. In the (3, 3) visual secret sharing scheme shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel and storing the final value of the share pixel after reversal into the shares in round robin fashion. The result of the three shares obtained after OR operation using stacking of all these qualified shares the original secret reveal.

3. Proposed Work

1. Algorithm for Encryption:-

Step 1:-The image which we have to encrypt should be select here.
Step2:-In this 0 level stage, the image is converted to monochromatic one i.e. Red, Green and Blue channels are get separated from original image and obtain 3 shares. In the Red share G=B=0, Green share R=B=0 and for Blue, R=G=0.
Step 3:-Each color share is further encrypted into 8 shares. i.e. R+G+B=8+8+8=24 shares the operation is done at 1st level of encryption. This encryption is done with the key provided by sterilization process.
Step 4:-In this 2nd level 8 encrypted shares of each color make group of 3,3 and 2 shares for further encryption.
Step 5:-From above 3 shares obtained using this share finally encrypted red, green, blue color shares generated. This operation is perform at level 3
Step 6:- In this conditional box, It checks for the condition for encrypting all the 3 shares. Unless and until all the 3 shares are encrypted it process in the loop.
Step7:-In this last level of encryption all the 3 share get combined and finally encrypted share obtained. Save the encrypted image to database.

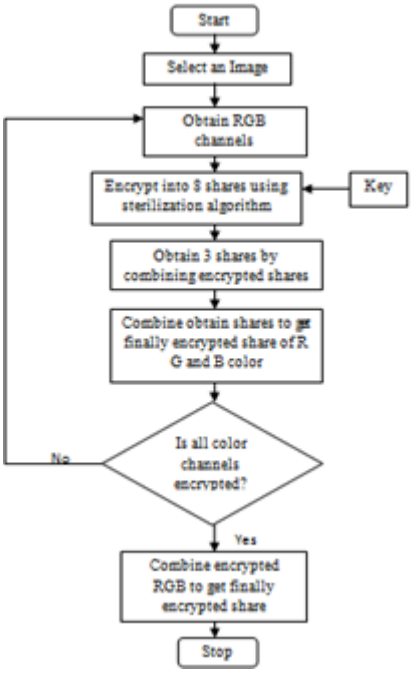

Figure 1: Flow chart for Encryption of an Image

2. Algorithm for decryption

Step 1:- Select the encrypted image.
Step 2:- Separate encrypted Red, Green and Blue Share from an encrypted share.
Step 3:-Further decrypt each red, green and blue into 3 shares. i.e. R+G+B=3+3+3=9 shares.
Step 4:- Decrypt each share into 8 shares, i.e. for decrypting red share split first share into 3 shares, second into 3 shares and third into 2 shares.
Step 5 :-By using the 8 shares of each color obtain single share in next step using desterilization algorithm.
Step 6 :- The condition has to be check that all color shares are decrypted or not, if all the shares decrypted then go for next process, Otherwise set the process in loop.
Step 7 :- At this last stage of decryption combine all the decrypted Red, Green and blue share and finally decrypted image is going to be revealed.

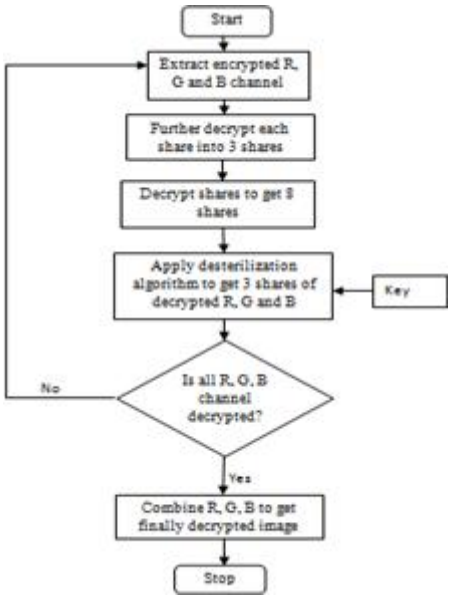

Figure 2: Flow Chart for Encryption of Image

4. System Implementation and Testing

This module focuses on the implementation aspects of Image encryption. Following are the steps for it.
Step1: (Initialization Process)
For image encryption user has to select encryption menu and load the image which has to be encrypted. The image must contain Red, Green and Blue component. Whatever image has been chosen it is resizes to 200*200 pixels.

$I = \frac{dI}{dR.dG.dB}$

Where R=Red, G= Green and B = Blue

Step2: (Encryption at level 0)
Make the loaded image monochromatic by separating channels i.e. red green and blue and then used those channel for further encryption.

$I_R = \frac{dI}{dR}$ Where G=B=0
$I_G = \frac{dI}{dG}$ Where R=B=0
$I_B = \frac{dI}{dB}$ Where R=G=0

Step3: (Image encryption at level 1)
Create 8 blank shares for each Red, Green and Blue channel. Perform image encryption by using sterilization algorithm. Here image is going to be encrypted using key. i.e. R+G+B=8+8+8=24.
Level 1:-

$$dIL_{1R} = \frac{dI_1}{dz} + \frac{dI_2}{dz} + \frac{dI_3}{dz} + \ldots\ldots\ldots \frac{dI_8}{dz}$$
$$= \frac{1}{dz}(dI_1 + dI_2 + dI_3 \ldots\ldots\ldots dI_8)$$

$$dIL_{1G} = \frac{dI_9}{dz} + \frac{dI_{10}}{dz} + \frac{dI_{11}}{dz} + \ldots\ldots\ldots \frac{dI_{16}}{dz}$$
$$= \frac{1}{dz}(dI_9 + dI_{10} + dI_{11} \ldots\ldots\ldots dI_{16})$$

$$dIL_{1B} = \frac{dI_{17}}{dz} + \frac{dI_{18}}{dz} + \frac{dI_{19}}{dz} + \ldots\ldots\ldots \frac{dI_{24}}{dz}$$
$$= \frac{1}{dz}(dI_{17} + dI_{18} + dI_{19} \ldots\ldots\ldots dI_{24})$$

Step4: (Image encryption at level 2)
Create 3 blank shares for each channel and set it as per processing. i.e. total 9 channels are obtained. This encryption is done by grouping of 3, 3 and 2 shares obtained from previous step. The grouping of 3 shares gives single encrypted image. For this 8 bit of red share is set to red bit of blank share. The red bit obtained from second share is set to green bit to next level and red bit of third share is stored to blue component. Same operation performs for green and blue.
Level 2

$$dIL_{21R} = \int_{i=1}^{3}(dI_1 + dI_2 + dI_3)$$
$$dIL_{22R} = \int_{i=1}^{3}(dI_4 + dI_5 + dI_6)$$
$$dIL_{23R} = \int_{i=1}^{2}(dI_7 + dI_8)$$
$$dIL_{21G} = \int_{i=1}^{3}(dI_9 + dI_{10} + dI_{11})$$
$$dIL_{22G} = \int_{i=1}^{3}(dI_{12} + dI_{13} + dI_{14})$$
$$dIL_{23G} = \int_{i=1}^{2}(dI_{15} + dI_{16})$$

$$dIL_{21B} = \int_{i=1}^{3}(dI_{17} + dI_{18} + dI_{19})$$

$dIL_{22B}=\int_{i=1}^{3}(dI_{20}+dI_{21}+dI_{22})$
$dIL_{23B}=\int_{i=1}^{2}(dI_{23}+dI_{24})$

Step5: (Image encryption at level 3)
Combine encrypted 3 shares of each channel to get finally encrypted image of each color, i.e, Red, green and blue. Here also similar operation is performing to combine shares. To create single encrypted image from 3 shares. Set red bit of image to red bit of next level of encrypted image. Set red bit of second share to green bit of next level share and red bit of last share is set to blue share of next level. Similar operation has to be performed for green and blue channel.

$dIL_{3R}=\int_{1}^{3}(DIL_{21R}+DIL_{22R}+DIL_{23R})$
$dIL_{3G}=\int_{1}^{3}(DIL_{21G}+DIL_{22G}+DIL_{23G})$
$dIL_{3B}=\int_{1}^{3}(DIL_{21B}+DIL_{22B}+DIL_{23B})$

Step6: (Image encryption at level 4)
Combine each color encrypted image to give finally encrypted image. Set red bit of finally encrypted monochromatic image to red bit of finally encrypted image. Green bit is set to green and blue is set to blue.The processing at first level of encryption is done by using sterilization algorithm. The detail working of algorithm is as shown. Each
pixel is combination of Alpha, Red, Green and Blue channel. Shares created by sterilization algorithm.

$dIL_f=\int_{1}^{3}(dIL_{3R}+dIL_{3G}+dIL_{3B})$

- **Sterilization algorithm:-**

Step 1 – Select share from level 0
Step 2- For Red process first 8 bits|| green process middle 8 bits|| blue last 8bits
Step 3- For Red share
i. Create 8 blank shares for Red G=B=0,For Green R=B=0,For Blue R=G=0.
ii. Apply 8-integer key to first pixel of share from left to right.
iii. Set bit value from step 1 to the blank share associated with key value.
iv. if bit value of share=1
then set blank share=255
else
set blank share=0
v. If key=end then apply it in circular pattern to next pixel.
vi. Repeat step i to v for each pixel.
Step 4 – Repeat step 2 and 3 for green and blue share from step 1.
Step 5 - stop

- **Splitting image into Red, Green and blue channel**.

Fig. 4.2 Separation of R,G,B Channels

Each pixel is separated into R,G,B. For Red channel G=B=0, For Green R=B=0 and for Blue R=G=0.For example first pixel value is [213 198 222]

- **Bitwise Operation**

Each channel is represented in binary format.
Red Channel – [213,0,0] - 11010101
Green Channel - [0,198,0] - 11000110
Blue Channel - [0,0,222] – 11011110

- **Key Generation**

n this section, 8 integer key is generated. Here multiple keys are going to be generated as each pixel is encrypted using keys. Maximum number of keys provides more security as it required more prediction and complexity for decryption to an intruder. User can select any number of keys manually or randomly. For ex. Key selected for first pixel is 48127536.

- **For Red channel**

Create 8 blank shares and set the first level encrypted shares by using key and sterilization algorithm. Key – 48127536

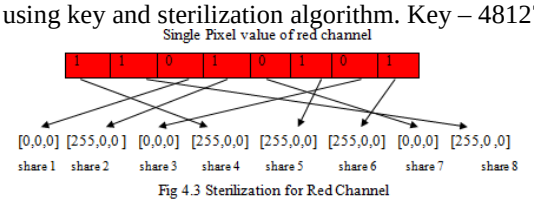

Fig 4.3 Sterilization for Red Channel

As key provided is 48127536 for the first pixel of image then take the number from key if it is 4 then set the blank share no.4,second number is 8 then 8th number share is set, Next key number is 1 then set 1st number share and so on. If bit number of red channel is 1 then set particular blank share as 255, otherwise set it 0.

- **For Green Channel :-**

Similar operation is going to perform on green channel. Create 8 blank shares.Key-75861324

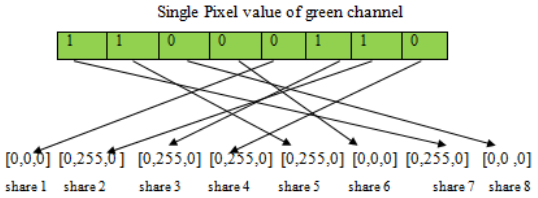

Fig 4.4 Sterilization for Green Channel

Here the operation perform is similar to that of encryption of red channel. Key provided for the pixel is 75861324.so set 7th share by using same technique. Now green shares are going to create hence put R=B=0.and set only green bits.

- **For Blue channel :-**

Similar operation that is performing for red and green encryption is used here.Key :- 84127536

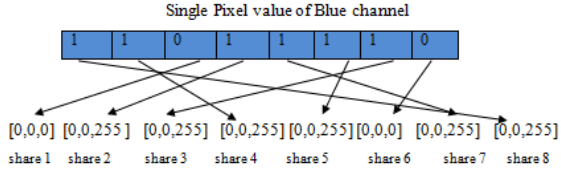

Fig 4.5 Sterilization for Blue Channel

The sterilization algorithm works on this blue channel is exactly similar to that of red and green channel. As here R=G=0.So set the value of green share only.

Table 1: Mean Intensity

Name of Input Image	Mean Intensity Of Original Image	Mean Intensity of Encrypted Image	Mean Intensity Of Decrypted Image
Img1.jpg	113.322	127.573	113.322
Img2.bmp	113.453	128.839	113.453
Img3.png	79.509	126.756	79.509
Img4.jpg	127.762	128.228	127.762
Img5.bmp	104.247	122.655	104.247

Table 2: Entropy

Name of Input Image	Entropy Of Original Image	Entropy Of Encrypted Image	Entropy Of Decrypted Image
Img1.jpg	7.4295	7.6351	7.4295
Img2.bmp	7.4247	7.8339	7.4247
Img3.png	7.5306	7.7891	7.5306
Img4.jpg	7.7613	7.8965	7.7613
Img5.bmp	7.7706	7.9035	7.7706

Table 3: PSNR and MSE:

Name of Input Image	PSNR Original with Encrypted Image	MSE Original with Encrypted Image
Img1.jpg	8.6899	8791.97
Img2.bmp	9.2215	7779.12
Img3.png	7.8407	10690.76
Img4.jpg	8.7402	8690.78
Img5.bmp	8.1558	9942.60

5. Conclusion & Future Scope:

5.1 Conclusion

Visual Cryptography is fastest growing stream. Day to day new inventions is adding more importance to it. Every technique has its pros and cons. Secret Sharing Scheme divide image into number of shares. These shares are meaningless and nothing can be reveal from individual share. For revealing the secret number of shares should be superimpose to obtain original image. Various techniques invented for Visual Cryptography lack in quality of reconstructed image also pixel expansion and various problems.

In this propose work new concept of sharing the color image at multiple levels has given which provided more security to the encryption. Initially image is separated into Red, Green and Blue channels and then Sterilization Algorithm is used. It provides keys which are used to encrypt every pixel. Each level consist database of particular number of shares, by using that database image is encrypted. For revealing the original image all the shares are required to be superimposed using the keys. By stacking shares in proper sequence original image will obtain. The concept is extremely secure as shares are encrypted at multiple levels using the keys without which one can never decrypt the image.

5.2 Future Scope

Every image is a combination of Alpha, Red, Green and Blue Channel. In this propose work image is encrypted by separating Red, Green and Blue channels, in future Alpha channels can also be add to sterilization process which provide more security to image. Also this concept can also be used for stenography in which text or image can be hiding behind each encrypted share.

References

[1] Sagar Kumar Nerella, Kamalendra Varma Gadi , RajaSekhar Chaganti," Securing Images Using Colour Visual Cryptography and Wavelets", *International Journal of Advanced Research in Computer Science and Software Engineering* , Vol. 2, Issue 3,pp.163-168, March 2012.

[2] Quist-Aphetsi kester, Laurent nana,Anca Christine Pascu,,"A Novel Cryptographic Encryption Technique of Video Images using Quantum Cryptography for satellite Communication," *IEEE* 978-1 -4799-3067-8/13 ©2013.

[3] Shubhra Dixit,Deepak Kumar Jain, and Ankita Saxena, "An Approach for Secret Sharing Using Randomised Visual Secret Sharing," *IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies* ,978-1-4799-3070-8/14 $31.00 © 2014

[4] Roberto De Prisco and Alfredo De Santis," On the Relation of Random Grid and Deterministic Visual Cryptography", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 9, NO. 4, APRIL 2014

[5] Mr.M.Venkatesh, Mr.S.Rajesh,"Security Analysis of Visual Secret Sharing Scheme," *M.Venkatesh et al, International Journal of Computer Science and Mobile Applications*, Vol.2 Issue. 1, pg. 127-134, January-2014.

[6] Adi Shamir,"How to share a secret," *ACM*, N0014-76-C-0366, vol. 22, November 1979.

[7] Naor, M. and Shamir, A.,"Visual cryptography,"*In Proc. Eurocrypt 94, Perugia,Italy, Springer Verlag*, May 912, LNCS 950, pp.112.,2010

[8] E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing

Schemes," *Designs, Codes and Cryptography, 11(2)* , pp.179–196, 1997.
[9] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography For Natural Images," *Journal of WSCG*,v10i2. 303-310,2002.
[10] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," *in Proc. of IEEE International Conference on Image Processing,Barcelona, Spain*, VOL. 15, NO. 8, August 2006.
[11] Somdip Dey," Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI Method: SD-EI Ver-2", *International Journal of Cyber-Security and Digital Forensics*, 2012.
[12] Manika Sharma, Rekha Saraswat," Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 2, Issue 10, April 2013.
[13] Naor, M. and Shamir, A.,"Visual cryptography,"*In Proc. Eurocrypt 94, Perugia, Italy, Springer Verlag*, May 912, LNCS 950, pp. 112.,2010

Author Profile

Apurva A. Mohod Received Bachelor of Engineering in Information Technology from SGB Amravati university & Pursuing Master of Engineering in Computer Science and Engineering from P.R.Pote(Patil) College of Engineering & Mgt, Amravati, College of Engineering and Management, Amravati.

Prof. Komal B. Bijawe Received Master of Engineering in Computer Science and Engineering from SGB Amt University. Working as assistant professor in P.R.Pote(Patil) College of Engineering & Mgt, Amravati.