ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Digital Visual Cryptography Transmission Scheme by Diverse Image

Prajakta Nikam[1], Preeti Kale[2]

Department of Information Technology, MIT College of Engineering, Pune, India[1]

Assistant Professor, Department of Information Technology, MIT College of Engineering, Pune, India[2]

Abstract: Visual secret sharing (VSS) schemes split secret images in shares that are either printed on separate transparencies or are encoded and stored in a digital form. The shares can seems as noise-like pixels or as meaningful images; but shares are suspicious so there is high interception risk during transmission. To overcome this problem, we proposed Digital-image-based VSS scheme (DVSS scheme) that shares secret images via various carrier media to protect the secret during the transmission phase. The proposed DVSS scheme can hide secret image using selected natural images and generate one noise-like share. Secret image and natural images generate one noise like share. The natural shares are unaltered and inoffensive, thus minimize the transmission risk problem. We also propose scheme to conceal the noise like share to minimize the transmission risk problem. LSB and BIT steganography algorithms are used for hiding noise like share and comparative analysis is made.

Keywords: Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk, least significant bit.

I. INTRODUCTION

Visual Cryptography is a secret-sharing method that encrypts a secret image into several shares but does not requires computer or calculations to decrypt the secret image. The secret image is recovered visually simply by overlaying the encoded shares the secret image becomes clearly visible. Visual cryptography technique is invented by Moni Nair and Adi Shamir 1995[1]. They expressed a visual secret sharing scheme, where an image is broken into n shares .All n shares could decrypt the image, while any n − 1 shares does not provide any idea about the original image. Each share was printed on a different transparency, and decryption was performed by overlapping the shares [2].

Secret images can be of various types: photographs, images and others. Sharing secret images is also called as a visual secret sharing (VSS) scheme. This scheme has some disadvantage: Management of share become difficult as number of share increase. These random looking noises like shares are vulnerable to attack by attacker in middle so there is high transmission risk. Extended visual cryptography scheme (EVCS) scheme is visual secret sharing scheme solve the problem of management of shares. EVCS uses meaningful cover images to hide the share. But while recovering secret image extra noise is introduced in image and degrade the quality of secret image.

II. RELATED WORK

Visual Cryptography (VC) is a method for sharing secret image. This method was proposed by Naor and shamir [1]. VC scheme divides the secret image into share images. This share images are look like a noise images. The shares are printed on transparencies. By stacking transparencies directly, the secret images can be recovered and visually visible to human eyes without any computational devices and cryptographic knowledge. Any one share cannot recover secret image. VC is a good solution for sharing secrets when a computer is not used for the decoding process. This scheme has some disadvantage: Management of share become difficult as number of share increase. These random looking noises like shares are vulnerable to attack by attacker in middle so there is high transmission risk.

Extended visual cryptography scheme (EVCS) is another visual cryptography scheme first introduced by Naor [3].EVCS has meaningful shares and VCS contains random shares. EVCS takes secret image and n original shares images as input and outputs n shares. All n shares are meaningful images. Only qualified subset of shares can recover the secret image. Any forbidden subset of share cannot obtain any information of secret image. EVCS overcome the disadvantages of VCS as all shares of EVCS are meaningful images hence these shares are less vulnerable to attack. Bad visual quality of the shares and recovered secret image is one of the disadvantages of EVCS. Another disadvantage is that pixel expansion is large and requires complementary share images.

Embedded EVCS is a visual cryptography scheme invented by Feng Liu and Chuankun Wu [3]. To encrypt secret image take n gray scale image as input and convert them into n covering share. Covering shares are splited into blocks of s subpixel. Mo and M1 are matrices of a traditional VCS. Rows of M0 and M1 are embedded into the blocks of covering share. Finally outputs n shares. Concept of Dithering matrix is used to generate covering share.Embedded EVCS has many advantages such as it deals with gray scale input image, has smaller pixel expansion, does not require complementary share images.

Halftone visual cryptography is a technique for visual cryptography invented by Zhi Zhou [4].In this technique

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

halftoning method such as the error diffusion on a grey level image is used to obtain halftone image(HI) .This image is given to first participant. Complementary image $(\overline{HI})$ is obtained by reversing all black/white pixels of HI to white/black pixels and $\overline{HI}$ assigned to second participant. In each of share secret pixel is encrypted into halftone cell. Select only two pixel from each of share .Pixel position is same in each share. These selected pixels are secret information pixels are need to modified based on following rule:a) If pixel is white, a matrix is randomly selected from the collection of matrices Co of conventional VC.

b) If pixel is black, matrix is randomly selected from C1 . Halftoning method is better than conventional VC method for quality of share.

In halftone visual cryptography via error diffusion technique is invented by Z. Wang, G. R. Arce, and G. D. Crescenzo in 2009[6].In this technique the secret image is embedded into binary valued shares. Shares are halftoned via error diffusion method**.** Error diffusion method takes gray scale image as input and converts it into binary image. Advantages of Error diffusion are low complexity and gives good quality halftone share. Secret image pixels are hide in binary share images, by using void and cluster algorithm**.** The reconstructed secret image, obtained by overlapping .This method is good but has some problems like pixel expansion and contrast loss of original image.

User friendly Random Grid based Visual Secret Sharing scheme is invented by T. H. Chen and K. H. Tsao in 2011[8].This technique is designed to overcome problem of VCVSS schemes which worsen the pixel expansion where the size of original secret image is smaller than that of shared images. Advantages of user friendly random grid based visual secret sharing scheme are no pixel expansion, and being user-friendly. That means secret image size and original image size is same so it minimizes the problem of pixel expansion. In this method random grid R is defined as a two dimensional array of pixels. Each pixel is either transparent or opaque. Probability of number of transparent pixels and opaque pixels are same. Opacity of a random grid is 50% .

In Color image with natural shadow visual cryptography natural image is used to hide the secret information and generate one noise-like share image. During encryption process it alters the natural image so Color image with natural shadow visual cryptography suffers from texture problem that is original texture of the image will be lost[13]Using steganography techniques, secret images can be hidden in cover images that are gray images and true-color images However, the stego-images are not vulnerable to visual inspection. A method for reducing the transmission risk is an important issue in VSS schemes [10-15].

III. THE PROPOSED SCHEME

In this paper, we proposed a method to hide secret image by using printed and digital images. Fig.1 shows, the encryption process of (n, n)-DVSS scheme includes steps like image preparation, feature extraction, pixel swapping, encryption and data hiding. Steganography approach is used to hide the noise share.

Fig.1 shows encryption process where features are extracted from natural shares without altering the natural shares. Image preparation and pixel swapping processes are used for processing on only printed images. Image preparation includes three steps such as acquire image, crop image, resize image.

The feature extraction process extracts features from the natural image. Feature extraction includes Binarization, stabilization and chaos process to extract the features . Binarization process extract feature matrix from natural image. Stabilization includes balancing the number of black and white pixels of extracted feature images .Chaos process eliminate the texture of the extracted feature images and this is done by adding noise in the matrix

Encryption process performs XOR operation between feature images and secret image. To increase security of system we hide output of encryption process using data hiding technique. Here, we use steganography to hide the data. Data hiding process outputs the stego image and that image is ready to send to the destination or over the network. We use two steganography techniques LSB and BIT algorithm to hide the dataFig 2.shows class diagram for DVSS system. Class diagram shows information about class's related attributes and methods. We implement our system using java language.

A. Image Preparation Process

Image preparation process [2] has three main steps: Acquire images, crop images and resize images. Hands painted pictures are captured by using digital camera. Acquisition devices and parameter setting of the device should be same in encryption and decryption process. In next step images are cropped. At the end images are resize so they have same dimensions.

B. Feature Extraction

Features extraction process [2] extract features from printed and digital images. In the feature extraction phase, 24 bit binary feature images are extracted from each natural share. The natural shares are printed and digital images. Inputs for feature extraction are printed and digital images and it outputs feature images.

Feature extraction has three main phases: Binarization, Stabilization, Chaos. In the Binarization process, the binary feature value of a pixel is calculated.

Stabilization is used for balancing of the number of black and white pixels of an extracted feature image in each block. The number of unbalanced black pixels whose feature value is 1 is randomly chosen and then 0 is assigned for value of pixels. Stabilization process is used to balance number of black and white pixels in each block.

The chaos process removes the texture that may present in the extracted feature images and the generated share. Noise is added into original feature matrix which gives disordered matrix.

C. Encryption/Decryption Process

The proposed DVSS scheme can encrypt a true color secret image using printed and digital images and generate one noise share.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

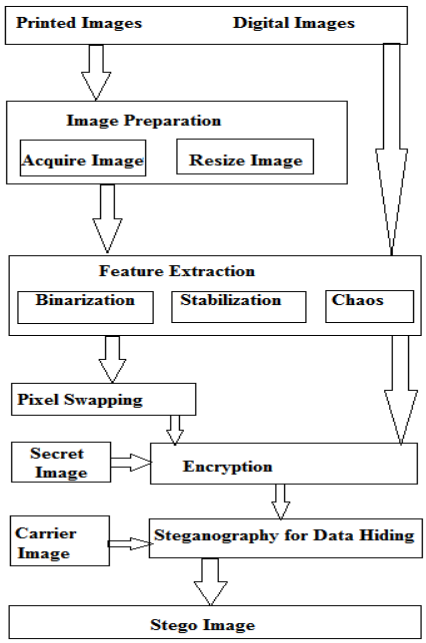


Fig 1.Encryption process of DVSS scheme

The natural images gives feature images .All feature images are combined to make one feature image with 24-bit/pixel color depth. In the encryption phase, all feature images with 24-bit/pixel color depth are XOR with secret image to generate one noise-like share with 24-bit/pixel color depth. Finally generated share is hidden by using data hiding techniques. Steganography is used to hide the data .Data hiding techniques reduce the transmission risk problem .Encryption process outputs share also called as generated share.

The input to encryption/decryption process [2] includes printed and digital images.

Step 1: Initializes random number generator G by seed ρ and it is used in feature extraction processes.

Step 2: Set all feature images in color plane to 0

Steps 3: Call Feature extraction extracts a binary feature matrix from a natural share .One feature image with a 24-bit depth per pixel is extracted from each natural share.

Step 4 : Extracted matrix is added to corresponding bit and color planes of a feature image.

Steps 5: Pixel-swapping is performed by randomly selecting a pair of pixels in a feature image

Step 6: Perform XOR operation between input image S and all feature images.

Step 7: Output image $S^{'}$

D. Share hiding using Steganography

Steganography techniques are used to conceal the noise-like share and further reduce intercepted risk for the share during the transmission phase. Here we use Image Steganography which takes the cover object as image. Image Steganography uses pixel intensities to hide the information.

Terminologies used in image steganography:

- Cover-Image: Cover image is nothing but a carrier for hidden information.
- Message: Actual information which is used to hide into images. Message could be a plain text or some other image.
- Stego-Image: After embedding message into cover image is known as stego-image.

Generally image steganography is technique for information hiding into cover-image .Message is embedded into cover image and it generates a stego-image. This stego-image is ready to sent to the other party by known medium, where the third party does not know that this stego-image has hidden message

Here we use LSB and BIT steganography algorithm which comes under Spatial Domain Methods .In spatial steganography, some bits of the image pixel values used to hide the data. Least significant bit (LSB)-based steganography [10] is a method to hides a secret message in the LSBs bits of pixel .It does not introducing any distortions in image. Changes in the value of the LSB are not visible for human eyes.

Some advantages of spatial domain LSB technique are there is very less chance for degradation of quality of the original image. More information can be stored in an image.LSB and BIT algorithms are used to hide noise like share. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane.

1) LSB algorithm:

The technique works by replacing least significant bit of red green and blue bit plane of pixel of the carrier image with information from the data in the image

Algorithm for Least Significant Bit method

Step 1: Read the cover image and data to be hidden in the cover image.

Step 2: Convert the Secret data into binary message.

Step 3: Calculate LSB bits of each pixel.

Step 4: Pick the characters from the secret data and place it in the LSB of red green and blue bit plane of pixel. Step 5: Obtained image will be stego image that contains hidden data.

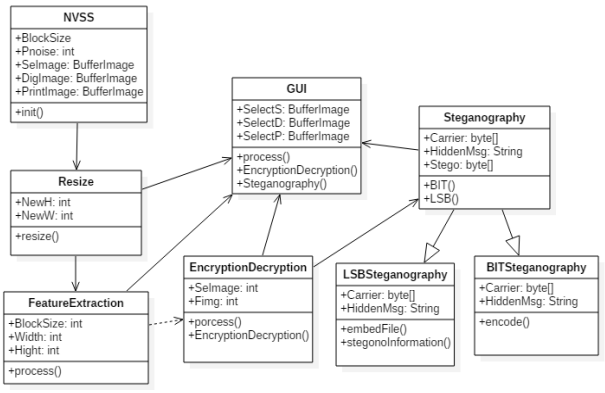


Fig 2.Class Diagram for proposed system

2) BIT algorithm:

The technique works by replacing least significant bit of red bit plane of pixel of the carrier image with information

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

from the data in the image Algorithm for Least Significant Bit method
Step 1: Read the cover image and data to be hidden in the cover image.
Step 2: Convert the secret data into binary message.
Step 3: Calculate LSB bit of red bit plane of pixel.
Step 4: Pick the characters from the secret data and place it in the LSB of red bit plane of pixel. Step 5: Obtained image will be stego image that contains hidden data

IV. PERFORMANCE EVALUATION

Here we evaluate performance of DVSS scheme by using LSB and BIT algorithm. The performance LSB and BIT algorithm for our system is evaluated by the parameters - Sum of absolute difference, Processing time, PSNR, Correlation quality. These parameters are measured for carrier image and stego image.

A.Parameters
1)Mean Absolute Error:
In more general case of image difference measurement, it may be scaled to a unit vector by:

$$MAE(x_1, x_2) = \frac{1}{n}\sum(x_1 - x_2)$$ where n is a size of x.which is known as Sum of Absolute Difference.

2). Execution Time:
Execution time is system time required for processing the images.
3). PSNR(Peak Signal to Noise Ratio):
Peak signal-to-noise ratio, often abbreviated PSNR, is an term used to calculate the ratio between the maximum possible power of a signal and the power of corrupting noise.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$PSNR = 10\log_{10}(\frac{MAX^2}{MSE})$$

Where MAX=255.
4). Correlation Quality(CQ):
Total Difference is sum of product of RGB values of carrier and Stego image. Original difference is summation of RGB value of carrier image. If the value of CQ is above 150 then images are visually accepted.

V. RESULTS

A. Experiment I

In this section, we show some results to evaluate the performance of the proposed system. Image set is shown in Fig. 3(a) to Fig 3(f).

Here we evaluate performance of DVSS scheme by using LSB and BIT algorithm. The performance LSB and BIT algorithm for our system is evaluated by the parameters - Sum of absolute difference, Processing time, PSNR, Correlation quality. These parameters are measured for carrier image and stego image. Here we take Fig. 3(e) as carrier image .We analyse DVSS system by using BIT and LSB as shown in fig.4. Fig .4(a) shows a bar graph for sum of absolute difference .Less the sum of absolute difference better the quality of stego image.

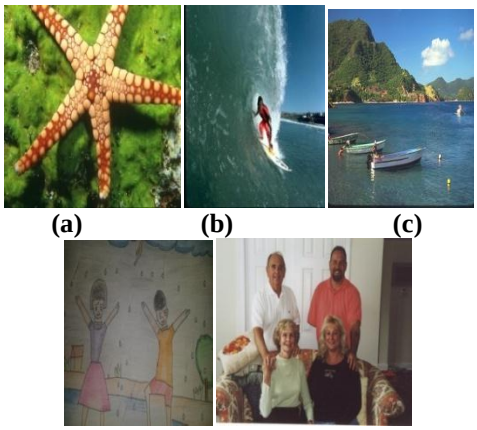
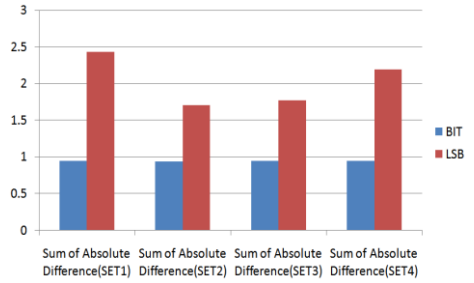
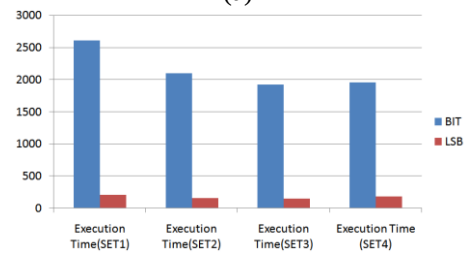


Fig.3 a) Secret image b) Digital image c) Digital image d) Printed image e) Carrier image

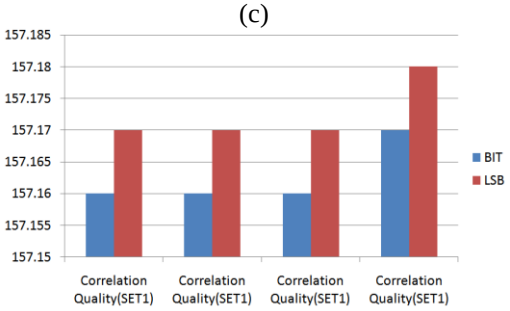


(a)



(b)

(c)



(d)

Fig.4: a) Bargraph of BIT and LSB for Sum of Absolute Difference b) Bargraph of BIT and LSB for Execution Time c) Histogram of Carrier and Stego image (BIT algorithm) d) Bargraph of BIT and LSB for Correlation Quality

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Here BIT algorithm is better than LSB. Execution time is shown in fig 4(b) from the results it is clear that BIT algorithm takes more time than LSB. Here LSB is better than BIT .We know that lower the Mean Square Error (MSE) values, better is the quality of the stego image obtained. Higher the value of PSNR better it is for the reconstruction of the image. For BIT algorithm MSE is near to zero so it gives higher value for PSNR. Higher the value of PSNR better the quality of stego image.LSB gives PSNR 45.12 db. Fig.4(c) shows histogram for BIT algorithm. There is slight change between histogram of carrier and stego image so PSNR is very high. From the results it is clear that PSNR in BIT is the best than LSB. Correlation quality is ratio of total difference and original difference. If value of CQ is above 150 then stego image is visually accepted. Both LSB and BIT gives CQ greater than 150 shown in fig.4 (d) .Here both the algorithms gives better results

B. Experiment II

Fig.5: (a) Printed image captured by Canon camera (Encryption) (b) Printed image captured by S4 mini Camera (Decryption)

This experiment gives the performance of the proposed DVSS scheme for sharing color secret images by diverse shares. The digital images and the color secret image are shown in fig.3 (a), (b),(c). The hand-painted picture is drawn on A4 paper, as shown in Fig.5 (a), (b). Hand painted picture is processed by the image preparation process. It gives two shares, one is used for encryption process and other one is for the decryption process. The share for the encryption process is captured by a digital camer Canon, as shown in Fig.5 (a). Another share is captured by the digital camera on a S4 mini, as shown in Fig.5 (b). The distortion in recovered image is introduced by different devices in capturing the hand-painted share during the encryption/ decryption phases. Recovered Image PSNR is only 9.17db .Low the PSNR high distortion is introduced in recovered image.

To minimize the variation in the content of the acquired images between the encryption and decryption processes, the type of the acquisition devices and the parameter settings of the devices should be the same or similar for encryption and decryption.

VI.CONCLUSION

We proposes DVSS scheme that can hide a digital secret image using diverse image media. The media contains randomly chosen images are unaltered in the encryption phase. Therefore, they are totally safe. The DVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed DVSS scheme can effectively reduce transmission risk, problem of management of shares and provide the highest level of user friendliness, both for shares and for participants.

We use hand-printed images for images-sharing scheme. This scheme proposes a useful concept and method for using unaltered images as shares in a VSS scheme. We use LSB and BIT steganography to hide noise share. We analyze our system using BIT and LSB by comparing Carrier image and Stego image for parameters like sum of absolute difference, execution time, PSNR, correlation quality. In this report analysis of DVSS system using LSB & BIT has been successfully implemented and results are delivered. From the results it is clear that as sum of absolute difference, PSNR in BIT is the best. BIT takes more execution time than LSB. Correlation quality is good for both the algorithm. For Pattern Analysis of the Bits BIT algorithm is more vulnerable than LSB.

REFERENCES

[1]M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2]K. H. Lee and P. L. Chiu, “Digital Image Sharing by Diverse Image Media” IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, Jan. 2014.

[3]F. Liu and C. Wu, “Embedded extended visual cryptography schemes”, IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun.2011.

[4]Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography, ”IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453 Aug. 2006.

[5]K. H. Lee and P. L. Chiu, “An extended visual cryptography algorithm for general access structures,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[6].Z. Wang, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[7]I. Kang, G. R. Arce, and H. K. Lee, “Color extended visual cryptography using error diffusion,” IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.

[8]T. H. Chen and K. H. Tsao, “User-friendly random-grid-based visual secret sharing,” IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

[9] P. L. Chiu and K. H. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[10] R. Chandramouli, N. Memon, ”Analysis of LSB based image steganography techniques,” Image Processing, vol. 3, pp. 1019-1022, October 2001.

[11]Subba Rao Y.V , Brahmananda Rao S.S , Rukma Rekha N ,” Secure Image Steganography based on Randomized Sequence of Cipher Bits”, Eighth International Conference on Information Technology,2011

[12] Alfred J. Menezes, Paul C. van Oorschot , and Scott A. Vanstone ”Handbook of Applied Cryptography” ,CRC Press 1996.

[13]Kai-Hui Lee and Pei-Ling Chiu, ”Image Size Invariant Visual Cryptography for General Access Structures Subject to Display Quality Constraints”, IEEE Transaction on Image Processing, VOL. 22, NO. 10, OCTOBER 2013

[14] Ashwathimesancla AO,” VISUAL CRYPTOGRAPHY FOR COLOR IMAGES”, International Journal of Electrical and Electronics Engineering (IJEEE) ISSN (PRINT): 2231 – 5284, Vol-2, Iss-1, 2012

[15]H. B. Kekre, Dhirendra Mishra ,Rhea Khanna, Sakshi Khanna ,“Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB’s Method for Images”, International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012

DOI 10.17148/IJARCCE.2015.49118

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

BIOGRAPHY

Prajakta Niakm Research Scholar, MIT college of Engineering, University of Pune. She has received B.E. in Information Technology from PUNE University. Currently she is pursuing M.E. in Information Technology from MIT college of Engineering, Pune University of Pune, Maharashtra, India

Prof. Preeti Kale received M.Tech in CSE. She is working as Assistant Professor in Department of Information Technology, MIT college of Engineering, Pune, India. She is having twelve year experience. Her research interest is Bioinformatics.

DOI 10.17148/IJARCCE.2015.49118