New Information Hiding Technique using Features of Image

Deepali Singla
Punjab University,UIET,Chandigarh,India
Email: deepysingla91@gmail.com

Dr. Mamta Juneja
Punjab University,UIET,Chandigarh,India
Email: er_mamta@yahoo.com

***Abstract*—Steganography is a word derived from two Greek words i.e. Stegno and Graphy. Stegno means cover and graphy means writing. It is an important branch of information security which protects the secret information from eavesdropper. Steganography hides the existence of secret information in order to protect it. In this paper we are dealing with image steganography, in which images are used to hide the information in them. Number of image steganography techniques has been proposed so far to achieve the goals of steganography i.e. high payload, less imperceptibility and more robustness. In this paper a new steganography technique for colored image (i.e. RGB images) is introduced. This new introduced technique makes the use of features to hide more information than in other areas of image. As features are considered to be the function of edges therefore in this technique we are using hybrid edge detector to extract the features. In this technique a combination of Canny and fuzzy edge detector is used to detect the optimal edges. After detecting edges 1 bit of red, 4 bits of green and 8 bits of blue channel are used for hiding the secret message bits. For smooth areas an adaptive least significant bit based scheme is used. The newly introduced scheme achieves all the three goals of steganography appropriately.**

***Index Terms*—first term, second term, third term, fourth term, fifth term, sixth term**

I. INTRODUCTION

Steganography, Greek meaning covered writing, is a branch of information security which hides the existence of important information in order to prevent any unauthorized access [1]. Just like cryptography steganography helps in securing the crucial information. But the way of securing the information is different for both techniques. Cryptography changes the information into an unintelligent form such no one apart from the communication can understand it. Whereas steganography hides the information into an innocent media such that intruder can't detect the existence of the information. There are number of innocent media used by the steganography e.g. text, signals, videos and images etc. [2]. In this paper we are dealing with the image steganography.

Basic mechanism of image steganography is as shown in figure 1

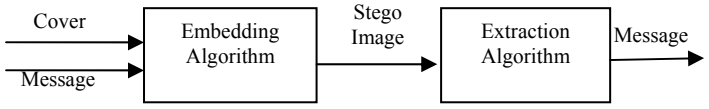

Figure 1. Basic Mechanism of Steganography

Basic terminologies of image steganography are as shown in fig.1 are cover image, message, embedding algorithm, stego image, extraction algorithm. Cover image is any innocent image used to hide the message bits. Number of image file formats are used for this purpose e.g. jpg, gif and bmp etc. We generally deals with bmp i.e. bit map image file format because it has lossless compression [3].

Image steganography is generally grouped into two categories i.e. spatial domain image steganography and transform domain Image steganography. In spatial domain image steganography original pixel values are used for hiding the secret information whereas in transformation domain transformed pixel values are used for hiding the information [4].

There are three goals of image steganography techniques i.e. high payload capacity, high imperceptibility and more robustness. Payload capacity deals with number of bits used per pixel for hiding the secret information. Imperceptibility means intruder is not able to detect the existence of message in the image. This is measured using a parameter named peak signal to noise ratio (PSNR). Higher the PSNR higher will the imperceptibility be. Robustness means the ability to resist attacks [5].

In this paper a new image steganography technique is proposed using hybrid edge detector and high capacity embedding technique for color images. This paper is organized as follows: section 2 presents the literature survey. Section 3 describes the newly propose image steganography technique. Section 4 describes the results and discussion of the newly proposed technique. Section 5 presents the conclusion and future scope.

© 2014 ACADEMY PUBLISHER
doi:10.4304/jetwi.6.2.237-242

II. LITERATURE SURVEY

Number of image steganography techniques has been introduced so far, the simplest method that has been introduced is LSB substitution technique. In this technique least significant bits of the image pixel are used for secret message bits embedding [6]. This technique achieves high imperceptibility but as it was a very simple technique that is why it is unable to resist the attacks e.g. sample pair analysis [7], difference image histogram [8] and blind detection algorithm [9]. To add so complexity in the above mentioned technique randomization is added to this technique and a tool named 'Hide and seek' has been introduced [10]. But Laplace formula attacked this tool very easily [11].

In these techniques the properties of the image was not considered to hide the data in the image. Further authors have considered the property of image that contrast areas of image can be used to hide the more secret data bits rather than in the brighter areas. On this basis a technique named 'first filter algorithm' has been introduced. Laplace formula is used for edge detection in this technique. But this technique was not much more robust [12].

In 2006 another adaptive technique was introduced which considered high frequency components of the image to be edged part of the image. So this technique uses high frequency components for embedding. This method achieved considerable advantage over the other adaptive steganography methods which do not specify the number of bits that can be hidden into an image [13] [14] [15] [16]. This technique makes the use of multi band filter to detect high frequency component, but if there is only a small difference in the cut off frequency at receiver end then extracted data will not be same as the embedded data [17].

In 2007 a random LSB technique has been introduced which make the use of Robert cross filter for edge detection. This technique added the concept of cryptography to the steganography i.e. the secret message is encrypted using data encryption standard (DES) before embedding [18].

In 2008 hybrid of pixel value differencing technique and LSB replacement [19] with some modifications has been introduced. In this technique embedding is done according to the level attained by the pixels. To find the level of a pixel, its difference with the neighbor pixel is taken into consideration. But in this method the embedding table that is used at the sender end must be send to the receiver also [20].

In 2009 a new technique has been introduced which make the use of four neighbor pixel and eight neighbor pixel relationship instead of using two neighbor pixel relationship for evaluating the level [21].

In 2010, a hybrid edge detection based image steganography technique has been introduced. The hybrid detector used in this technique is combination of canny edge detector [22] and fuzzy edge detector [23]. 3-4 bits of each edge pixel and 1-2 bits of smooth area pixels are used for embedding [23].

Another edge based image steganography technique has been introduced in 2010. This technique combined the results of all basic edge detectors. After getting the final edge matrix 6 bits of edge pixel and 2 bits of smooth area pixel are used for embedding the secret message bits [24].

In 2011 another edge based technique has been introduced in which sobel edge detector in horizontal direction. After this difference of pixel boundary is calculated with upper pixel boundary. This pixel is used to decide the embedding rate [25].

In 2012 a parameterized canny edge detector based technique has been introduced. In this technique rather than using standard values of higher and lower threshold values, these values are defined by the user. This property makes this technique more robust [26].

In 2013, combination of canny edge detector and enhanced Hough transform for edge detection. This technique provided another layer of security by encrypting the message with advanced encryption standard (AES) [27]. For embedding in smooth area adaptive modified LSB based technique was used and for edge areas 4 bits of green channel and 8 bits of blue channel are used for embedding [28].

III. THE PROPOSED METHOD

As explained above in the literature survey human visual system is less sensitive to the changes in non-continuous areas rather than changes in the continuous areas. Because of this reason we used to hide more data in the edge areas rather than in the smooth areas. For this purpose we have to find the edge areas first. In the proposed method we are using a hybrid edge detector i.e. combination of canny edge detector and the fuzzy edge detector. Hybrid edge detector is used to find the optimal and more number of edge pixels. Edge pixels are used to embed more number of secret bits, more number of edge pixels will result in higher payload capacity. After detecting edges secret data is embedded in the image. For edge pixels 4 bits of green channel and 8 bits of blue channel are replaced with secret message bits. For smooth area pixels adaptive LSB based technique is used. In section 3.1 a description of canny edge detector and fuzzy edge detector that are used in proposed method is given.

A. Canny Edge Detector

It is the classical edge detector which is considered to be optimal edge detector. This detector has basic three aims.

- Good detection.
- Good Localization.
- Minimizing the false edge detection rate.

Canny edge detector works in multiple stages. These stages are explained as fellow.

Stage1: smooth image using Gaussian filter.

Stage 2: gradient image of the smoothened image is found using Robert/sobel operator in horizontal and vertical direction.

Stage 3: detecting the thin lines only i.e. removing the pixels that are not the part of edge.

© 2014 ACADEMY PUBLISHER

Stage 4: two threshold values i.e. upper and lower threshold are used to minimize the false edge detection rate.

B. Fuzzy Edge Detector

In Fuzzy edge detector fuzzy inference rules are mentioned which are used to get the edge pixels from a given image. Each pixel in the image is given a membership value on the basis of membership function. On the basis of the membership value of the pixel, it is decided whether it is an edge pixel or a continuous area pixel.

In the fuzzy edge detector mentioned in [28] there are 8 inference rules on the basis of which each pixel is given a membership value. After this; defuzzification is done to get the final edge image. The properties of this edge detector are as given bellow:

- It has considered the eight neighbor pixel relationship while deciding whether a pixel is an edge pixel or not.
- It has also taken into consideration the application of continuity.

Membership function used in this detector is given below:

$$\text{ISLARGE}(X)\begin{cases} 1 \text{ if } |X|>C \\ |X|/C \text{ if } |X|<=C \end{cases} \quad (1)$$

In the above given membership function C is calculated using Fuzzy entropy principal and X is difference of a pixel i with the pixel j where j is present diagonally opposite to the pixel i in 8 neighbor pixel relationship. The membership value of each pixel i.e. μ_{ijk}= Islarge(G_{ijk}).

In proposed method results of both above discussed edge detectors are ORed and the resultant edge image is obtained. After this, embedding in the image on the basis of edge and non-edge pixel is done. In section 3.2 embedding procedures for edge areas and non-edge areas are described.

C. Embedding Technique for Edge Pixel

As mentioned already that HVS is less sensitive to changes in the edge areas, so our aim is to embed more secret message bits into edge area. In RGB image each pixel consists of three bytes. Each byte is representing one of the three colors i.e. red, green and blue. Red pixel contributes most to the brightness of the image and blue contributes the least. This gives an idea that more number of blue color bits of a pixel can be used for embedding than red color bits.

In this scheme we are using 4 bits of green channel and 8 bits of blue channel and 1 bit of red channel for embedding the secret information.

D. Embedding Technique for Non-Edge Pixel

For non-edge pixel we are using Kekre 2009 [30] algorithm with some modifications in it. This is an adaptive method which takes pixel value under consideration for deciding the number of bits to be used for embedding. Embedding is done on the basis of following table.

TABLE I.
ADAPTIVE EMBEDDING IN SMOOTH AREA

Pi_red	Pi_blue	Pi_green	Utilized bits
255-240	255-240	255-240	Green 4 bits Blue 8 bits
239-224	239-224	239-224	Green 3 bits Blue 7 bits
223-192	223-192	223-192	Green 2 bits Blue 6bits
191-0	191-0	191-0	Green 1 bits Blue 5 bits

Above table describes the number of bits to be embedded into the different channel corresponding to the range in which they fall.

E. Embedding at Sender End

At sender end cover image is given as the input and stego image is taken as output. This mechanism is shown in figure 2. The stego image is get by following the below mentioned steps:

Step1: Apply hybrid edge detector (Canny + fuzzy) on the cover image I and get edge image.

Step 2: Apply AES (advanced encryption standard) cryptography algorithm on the message to be hidden.

Step 3: Embedding Encrypted message into cover image.

- For edge pixels use embedding technique described in section 3.3.
- For non-edge pixels use embedding technique described in section 3.4.

Step 4: Resulting stego image I' is send to receiver.

F. Extraction at Receiver End

At receiver end stego image is received and it is considered that cover image is present at both ends. This mechanism is shown in figure 3. For extracting the message at receiver end following steps are followed:

Step1: Apply hybrid edge detector on the original cover image to get the edge pixel position and smooth area pixel position.

Step2: Using these positions extract message from the stego image.

Step3: Decrypt the extracted message Using AES algorithm to get the original message.

© 2014 ACADEMY PUBLISHER

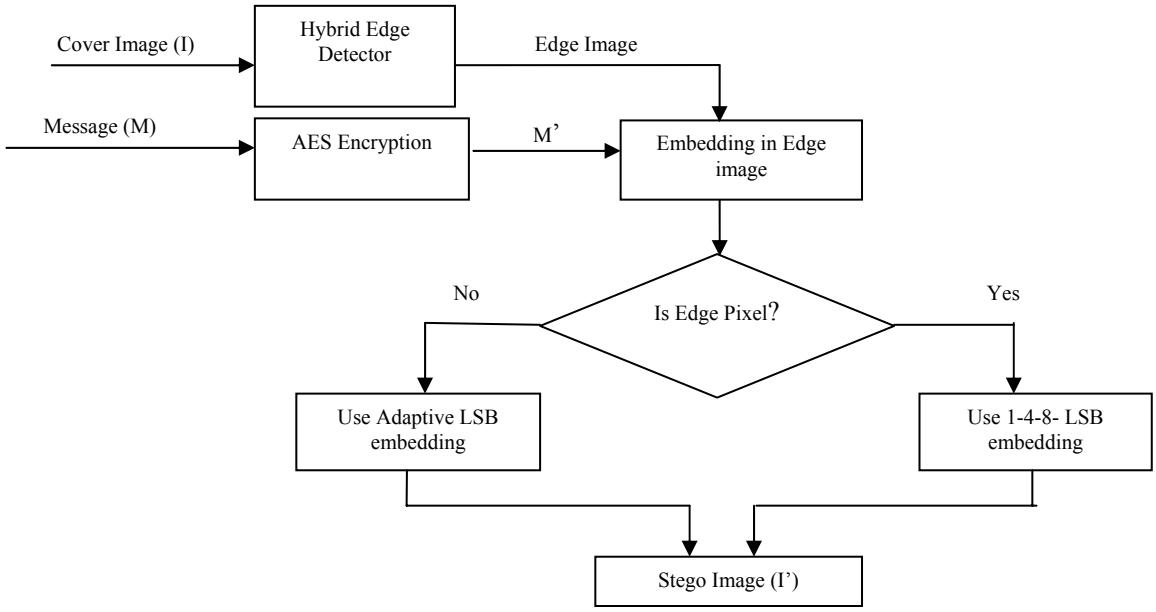

Figure 2. Embedding Mechanism at Sender end

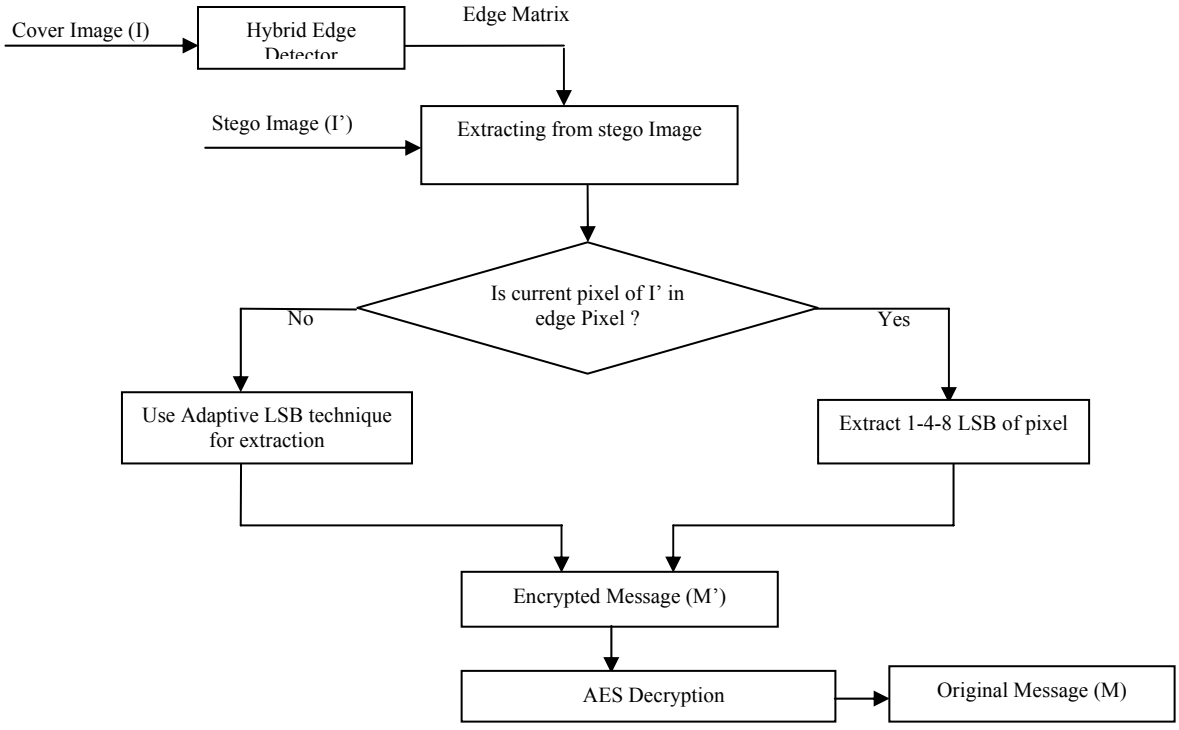

Figure 3. Extraction Mechanism at receiver end

IV. Experimental Results

The above proposed technique based on hybrid edge detector is analyzed in this section. The performance of a given steganography technique depends upon how accurately it has achieved the basic three goals of steganography i.e. high payload, imperceptibility and more robustness. All these three goals depend upon the quality of the stego image obtained as the result of the steganography technique. The quality of stego image is measured using the parameters i.e. Mean square error (MSE) and PSNR.

© 2014 ACADEMY PUBLISHER

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j}-Y_{i,j}\right)^2 \quad (2)$$

In the above given equation M and N are the dimensions of the image. $X_{i,j}$ and $Y_{i,j}$ represents the cover image pixel and stego image pixel at the position i, j.

$$PSNR = 10\log_{10}\left(\frac{I_{max}^2}{MSE}\right)dB \quad (3)$$

In the above given equation I_{max} is the maximum the maximum intensity in the cover image. On the basis of these parameters we are comparing our method with the hybrid edged approach explained in [24] and with the performance of other basic edge detectors based steganography using 6 bits of edge pixel and 2 bits of smooth pixel. The following table shows the results of applying different edge detectors used in these techniques.

Following tables shows the comparison of proposed method with the other method.

TABLE II.
COMPARISON OF THE DIFFERENT METHODS WITH PROPOSED TECHNIQUE FOR LENA IMAGE.

Methods / Parameter	Sobel	Prewitt	Robert	Gaussian	Canny	Hybrid	Proposed method
MSE	9.855	9.279	8.514	14.659	17.999	32.751	12.455
PSNR	38.19	38.45	38.82	36.46	35.57	32.97	46.68

TABLE III.
COMPARISON OF THE DIFFERENT METHODS WITH PROPOSED TECHNIQUE FOR TEMPLE IMAGE.

Methods / Parameter	Sobel	Prewitt	Robert	Gaussian	Canny	Hybrid	Proposed method
MSE	14.726	14.658	10.252	22.061	25.601	45.365	11.344
PSNR	36.44	36.47	38.02	34.69	34.04	31.56	48.24

V. Conclusion

The proposed method is a hybrid approach using hybrid edge detector, 1-4-8 LSB technique and adaptive LSB technique. The proposed method is working on the principal that more number of bits can be embedded in contrast area than in brighter areas. The proposed method has achieved desirable quality with high capacity. The proposed method is prone to many attacks as it has achieved a high quality stego image.

References

[1] Artz, D., "Digital Steganography: Hiding Data within Data," IEEE Internet Computing Journal,vol. 5(3), pp. 75-80,2001.

[2] Anderson R. J., "Stretching the Limits of Steganography," Springer Lecture Notes in Computer Science, vol.1174,pp. 39–48, 1996 .

[3] Westfeld A, J. Camenisch et al., "Steganography for Radio Amateurs— A DSSS Based Approach for Slow Scan Television", Springer-Verlag Berlin Heidelberg, pp. 201-215, 2007.

[4] M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information," Proceedings of 2009 12th International Conference on Computer and Information Technology, pp. 21-23, 2009.

[5] A. Shaddad, J. Condell, K. Curran, and P. Mckevtt., "Biometric inspired digital image steganography," Proceedings of 2008 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 159-168, 2008.

[6] Thien, C. C., Lin, J. C., "A Simple and High-Hiding Capacity Method for Hiding Digit-By-Digit Data in Images Based On Modulus Function," Pattern Recognition, vol. 36, pp. 2875-2881, 2003.

[7] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis", Proceedings of 2003 IEEE Transaction on Signal, vol.51, 2003.

[8] T. Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference histogram", Proceedings of 2003 IEEE, vol. 3, pp. 545-548, 2003.

[9] L. Zhi, S. A. Fen and Y. Y. Xian,"A LSB steganography detection algorithm", Proceedings of 2003 IEEE ISPIMRC, pp. 2780-2783, 2003.

[10] Maroney, C. Hide and Seek 5 for Windows 95, computer software and documentation, originally released in Finland and the UK.

[11] Katzenbeisser. S,Fabien, Petitcolas. A.P., "Information hiding techniques for steganography and digital watermarking",Artech House, Norwood, MA 02062, USA, 1999.

© 2014 ACADEMY PUBLISHER

[12] Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography", Proceedings of the Computing Women's Congress, 2006.
[13] R. Chandramouli, N.D. Memon and G. Li, "Adaptive Steganography," Proceedings on Security and Watermarking of Multimedia Contents III, Special session on Steganalysis, SPIE Photonics West, pp. 69-78, 2002.
[14] Karen Bailey, Kevin Curran and Joan Condell, "An Evaluation of Pixel based Steganography and Stego detection Methods," The Imaging Science Journal, vol. 52, pp. 131 - 150, 2004.
[15] Elke Franz and Antje Schneidewind, "Adaptive Steganography Based on Dithering," Proceedings Of the 2004 workshop on multimedia and security, ACM, Magdeburg, Germany, 2004.
[16] M. M. Amin, M. Salleh, S. Ibrahim, M. R. K.Atmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography," 4th national Conference on Telecommunication Technology, NCTT 2003, IEEE, pp. 21 – 25, 2003
[17] Santosh Arjun, N. and Atul Negi, "A Filtering Based Approach to Adaptive Steganography," 10th Conference, TENCON 2006, IEEE, pp. 1-4, 2006.
[18] Manglem Singh, Birendra Singh and Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images," IJCSNS, vol. 7, 2007.
[19] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, vol. 152, pp. 611–615, 2005.
[20] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, vol. 3, pp. 488-497, 2008.
[21] Hossain, M. Al Haque and S. Sharmin, F., "Variable rate Steganography in gray scale digital images using neighborhood pixel," 12th International Conference Dhaka, Information Computers and Information Technology, ICCIT '09, 2009.
[22] J. Canny, "A Computatinal Approach to Edge Detection," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 8, pp. 679-687, 1986.
[23] Wen-Jan Chen a, Chin-Chen Chang, T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, pp. 3292–3301, 2010.
[24] Rangarajan, B. Bose, Sasidhar and John Bosco, "Security Building at the Line of Control for Image Stego", International Journal of Computer Applications, vol. 12(5), 2010.
[25] Hussain, M. and Hussain, "Embedding data in edge boundaries with high PSNR," Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, 2011.
[26] Youssef Bassil, "Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 60, 2012.
[27] Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.
[28] Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," J Inf Process Syst, vol. 9, 2013.
[29] Talai Z., Talai A., "A Fast Edge Detection using Fuzzy Rules", International Confrence on Communication and Control Application, pp. 1-5, 2011.
[30] H. B. Kekre, Archana Athawale, Pallavi N. Halarnkar, "Performance Evaluation Of Pixel Value Differencing And Kekre's Modified Algorithm For Information Hiding In Images", ACM International Conference on Advances in Computing, Communication and Control, 2009.

© 2014 ACADEMY PUBLISHER