Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Performance Analysis of Data Hiding Using Adjacent Pixel Difference Technique

**Jagbir Singh**
*Dept. of ECE,*
*GZS-PTU Campus, Bathinda, India.*

**Savina Bansal**
*Dept. of ECE*
*GZS-PTU Campus, Bathinda, India.*

**R.K. Bansal**
*Dept. of ECE*
*GZS-PTU Campus, Bathinda, India.*

***Abstract: Steganography aims at hiding a text/message in an image in such a way that only receiver knows its existence. A natural image has many smooth areas. In recent years, various techniques are used for hiding data in the smooth areas of the image using digital image processing with varying degree of goodness. The prime goal is to enhance the data hiding capacity without much deteriorating the quality of the picture under consideration. Locating the best position in an image that will achieve the desired goal is a critical design issue. This work attempts to deal with this issue and analyses the impact of data hiding on high edge density and low edge density areas on some of the standard benchmark images. The underlying steganography algorithm used is Adjacent Pixel Difference (APD) technique available in literature. The simulation results reveal that the performance parameter PSNR tends to deteriorate in high density edge area as compared to low edge density area as the image block size area is varied.***

***Keywords: Steganography, Histogram Modification, Adjacent Pixel Difference (APD), Edges, PSNR, Capacity.***

## I. INTRODUCTION

Due to the rapid development of multimedia and internet, presently it has become easier for the hackers to edit, modify and duplicate the data. Now a day it necessitates finding appropriate protection because of the sensitivity of information. Steganography deals with the techniques used for protection of information. Itis the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message [10]. It is kind of security through obscurity.The steganography is used in applications, which includes confidential communication,secret data storing, for providing protection against data alteration. The secret information can be stored in cover files like text, image, audio and video. Most of the steganographic techniques hide secret data in images as it is relatively easy to implement [10]. The most important property of the cover source is the amount of data that can be stored in it without changing its properties. Many researches are working in this area and have proposed different techniques with varying capacities and with varying degree of success for hiding the data. Recently the neighbouring pixel difference techniques have gained interest among researches. It is a technique [1] in which difference of neighbouring pixel is taken of an image and the corresponding histogram is obtained. From the histogram peak points and zero points are calculated for embedding the data, as discussed ahead.However, there remain several issues which need to be resolved before an efficient steganography system is developed. Some of these include:

i) Locating the best position in an image which might result in lower PSNR degradation
ii) How to increase the data hiding capacity?
iii) How to increase the imperceptibility?
iv) How to increase the robustness?

Inthis paper, we have investigated the issues of locating the appropriate location in a given image and have taken up the Adjacent Pixel difference (APD) technique [1] as the baseline algorithm. Three different benchmark images are taken and fixed message size is stored in all of them. The picture quality is measured by means of PSNR using MATLAB platform and compared. Certain terminologies pertaining to image analysis are discussed below:

*Histogram:* The histogram represents the graphical representation of the tonal variation of digital images in image processing. It represents the number of pixels for each tonal value. The x-axis represents the tonal variations and y-axis represents the number of pixels in particular tonal value as shown in Fig 1 (b).

**Fig 1 (a) Lena Image**

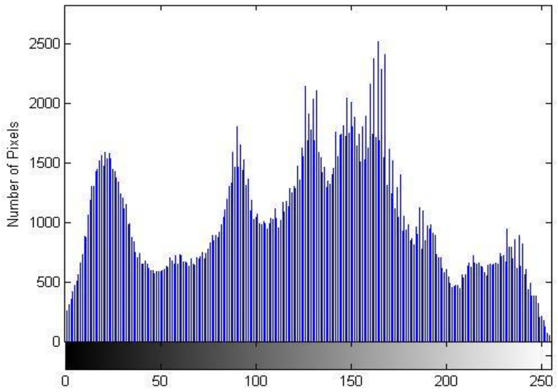


**Fig 1 (b) Histogram of Lena Image**

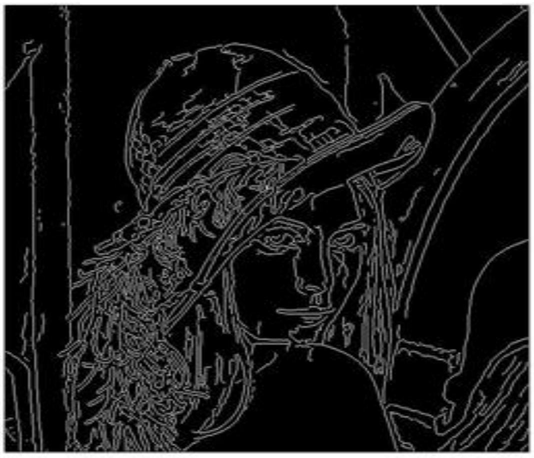


**Fig 1 (c) Edges in Lena Image**

*Edges:* Edges in images are area with strong intensity contrast. It represents jump in intensity from one pixel to other pixel. It is a boundary between two regions. Many edge detection methods [7] are used for detecting the edges of an image. In this paper 'Canny' method is used for edge detection Fig 1 (c). The paper is organized as follows: Next Section presents a brief overview of the steganography works available. SectionIII presents the Adjacent Pixel Difference (APD) algorithm, and Section IV describes the present work and the results obtained.

## II. LITERATURE REVIEW

Yuan-Yu Tsai et.al in proposed a reversible data hiding algorithm for gray-scale images [2]. The results revealed better in terms of embedding capacity and imperceptibility.Yu-Chiang Li et al. [1] presented data hiding using Adjacent Pixel Difference (APD) which used the histogram of the pixel difference for increasing the capacity of embedded data. The results were shown to have better embedding capacity and quality of image after hiding a data. proposed novel reversible data hiding algorithm, which could recover the original image from marked image after extracting a hidden message. This method used the zero or minimum points of the histogram of an image for embedding a data into the original image and the results were found to be better than that of other algorithms in terms of PSNR. In [6], ZaidoonKh. Al-Ani *et al.* provided a brief overview of the different types of steganography techniques and their classification. In [3] Zhao et al. proposed a steganography method to embed the secret data into compressed images, video files so as to achieve a high embedding rate. N Senthil Kumara and R Rajesh presented image segmentation using an edge detection technique [7]. In [8] H. Motameni *et al*. proposed the method of hiding a text message in gray scale image. The results were noticed to be better in terms of security as that of existing method by converting an original image into binary image. T Morkel *et al.* [5], presented techniques used for image steganography and their uses. They tried to find the requirements of good steganography system and their uses according to the application. The results were concluded to be better in terms of efficiency of image segmentation as that of existing method. Hamid A Jalab *et al*. [9], presented a new information hiding system to make a steganography more secure. The results were found to be better in terms of security by using executive file as a cover file. In [10] Abbas Cheddad*et al*. proposed different methods of existing steganography with some common standards by providing some embedding algorithm.

## III. OVERVIEW OF APD ALGORITHM

In this paper, data hiding is done using an Adjacent Pixel Difference technique as proposed in [1].Thebasic schemeoutline of the present work using APDalgorithm is as follows:

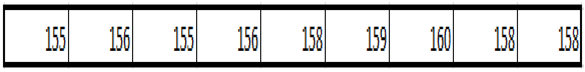
i) Choose any gray-scale image in jpg format
ii) Find edges by using the 'Canny' command
iii) Choose a block of any size at any location of the image
iv) Calculate the adjacent pixel difference of pixels in that particular block
v) Obtain the histogram
vi) Calculate Peak Points (PP) and Closet Zero points (CZP)
vii) If PP>CZP, then shift each pixel value in the range, [ZP+1, PP-1], to the left hand side by decreasing the pixel value by one unit
viii) If PP<CZP, then shift each pixel value in the range, [PP+1, ZP-1], of the histogram to the right hand side by increasing the pixel value by one unit
ix) Shifting of histogram generates free space for embedding the data
x) With peak point value, embed a bit of hidden data
xi) If embedded bit is "1", then shift the pixel from PP to ZP by one
xii) If embedded bit is "0', then pixel value does not change

These steps are explained with an example as given below:

**Ex: Data (1010) hiding in a 3x3 image**

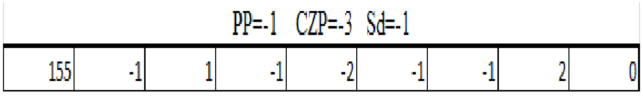
| | | |
|---|---|---|
| 155 | 156 | 155 |
| 159 | 158 | 156 |
| 160 | 158 | 158 |

**a) Host Image Array**



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 155 | 156 | 155 | 156 | 158 | 159 | 160 | 158 | 158 |

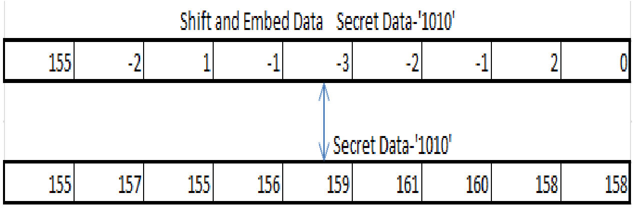
**b) Arranging pixels in raster scan order**



PP=-1 CZP=-3 Sd=-1

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 155 | -1 | 1 | -1 | -2 | -1 | -1 | 2 | 0 |

**c) Calculation of Adjacent Pixel Difference (P')**



Shift and Embed Data Secret Data-'1010'

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 155 | -2 | 1 | -1 | -3 | -2 | -1 | 2 | 0 |

Secret Data-'1010'

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 155 | 157 | 155 | 156 | 159 | 161 | 160 | 158 | 158 |

**d) Shifting and Embedding of Data**

| | | |
|---|---|---|
| 155 | 157 | 155 |
| 156 | 159 | 161 |
| 160 | 158 | 158 |

**e) Stego-Image after embedding Data**

**Fig 2: An Example of the data hiding using APD**

Consider a sample image with 3x3 pixels as shown in Fig 2(a); assume the secret data to be hidden as '1010'.In step 1,APD scans the original image in inverse scan-order as shown in Fig 2(b). After scanning pixel difference is generated in Fig 2(c). In next step,APD selects one pair of peak point and zero point, namely (-1,-3) and shiftsthe value of 'P' and embeds the data as shown in Fig 2(d).The Stego-Image after embedding data using APD is shown in Fig 2(e).

## IV. PRESENT WORK

In this work, we have analysed the APD algorithm by taking three benchmarking images namely 'Lena', 'Tiffany' and 'Baboon' as shown in Fig 3. Basically our purpose is to detect the most appropriate location in an image, where the data can be embedded without much degradation of original image by calculating their PSNR.For this purpose we focused on different locations of the image and embedded a fixed size data by varying the block sizes. As the block size increases the number of edges tends to increase and its impact is analysed on the stego-image. The APD algorithm as described in section III was used, the images were taken in jpg format and their edges were calculated using MATLAB platform. Performancemetrics as used in the work are detailed below:

**a) Lena** **b) Tiffany** **c) Baboon**

**Fig 3: Benchmark Images used**

*Peak Signal to Noise Ratio (PSNR):* This parameter computes the peak signal to noise ratio between two images. This ratio is used as a quality measure between original and embedded image. It is measured in decibels (dB). Higher the value of PSNR better is the quality of reconstructed image.

$$\boldsymbol{PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20.\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)}$$

Here $MAX_I$ represents the maximum possible pixel value of an image. When the pixels are represented using 8 bits per sample, its value will be 255. The term MSE (Mean Square Error) represents the mean of the square of the differences in the pixel values between corresponding pixels of the two images and is given by:

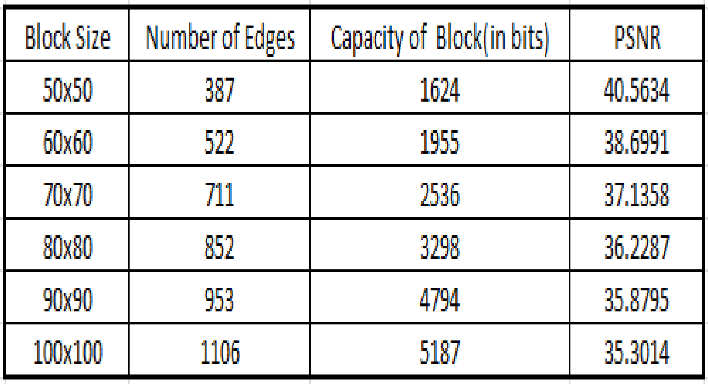
$$\boldsymbol{MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2}$$

*Capacity:* It is amount of data that can be safely hidden into the cover image without being detected. Higher the capacity, higher is the amount of data that can be embedded.

*Performance Analysis:* The results as obtained on 3-benchmark images by varying block sizes are given below:

*a)* *Lena Image:* The JPEG image of Lena is taken with bit size as 512x512. There are two different locations (Location 1 and Location 2) reflecting higher and lower edge densities selected in the image as shown in Fig4 and Fig 6. APD algorithm is applied on these locations and results obtained are shown in Table I, Table II, Fig 5 and Fig 7. The size of the embedded data is taken as 1076 bits for all the test cases.

**Table I: Performance Analysis for Lena image at Location 1**



| Block Size | Number of Edges | Capacity of Block(in bits) | PSNR |
|---|---|---|---|
| 50x50 | 387 | 1624 | 40.5634 |
| 60x60 | 522 | 1955 | 38.6991 |
| 70x70 | 711 | 2536 | 37.1358 |
| 80x80 | 852 | 3298 | 36.2287 |
| 90x90 | 953 | 4794 | 35.8795 |
| 100x100 | 1106 | 5187 | 35.3014 |

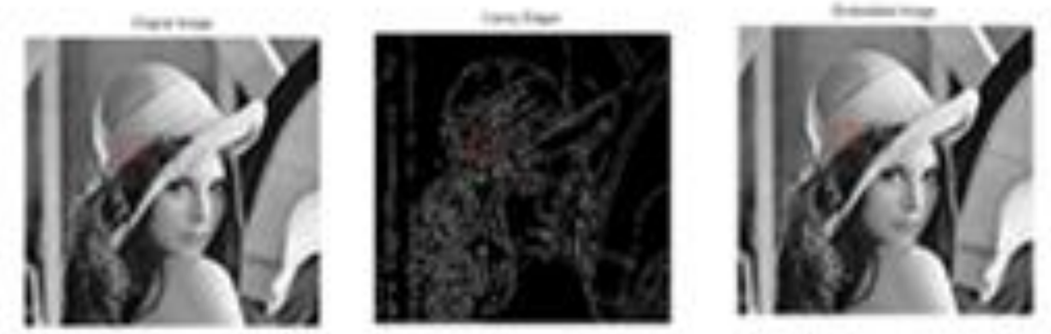


**Fig 4: a) Original Image b) Edges in Image c) Embedded Image at Location1**

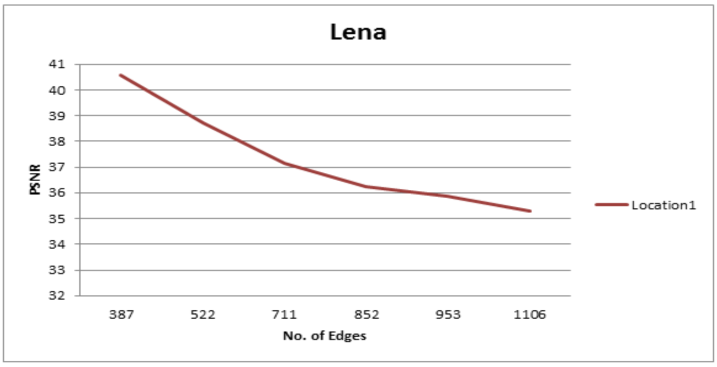


**Fig 5: PSNR vs. Edges at Location 1**

**Table II: Performance Analysis for Lena image at Location 2**

| Block Size | Number of Edges | Capacity of Block(in bits) | PSNR |
|---|---|---|---|
| 50x50 | 218 | 1655 | 59.3856 |
| 60x60 | 221 | 2474 | 56.1623 |
| 70x70 | 396 | 3290 | 54.3413 |
| 80x80 | 513 | 4282 | 53.3213 |
| 90x90 | 670 | 5368 | 49.6498 |
| 100x100 | 740 | 6538 | 47.3776 |

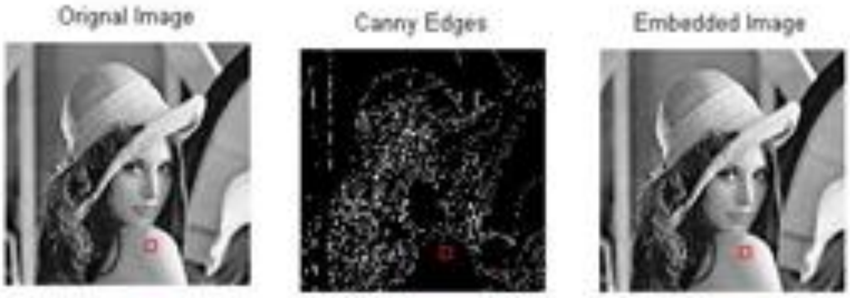


**Fig 6: a) Original Image b) Edges in Image c) Embedded Image at Location 2**

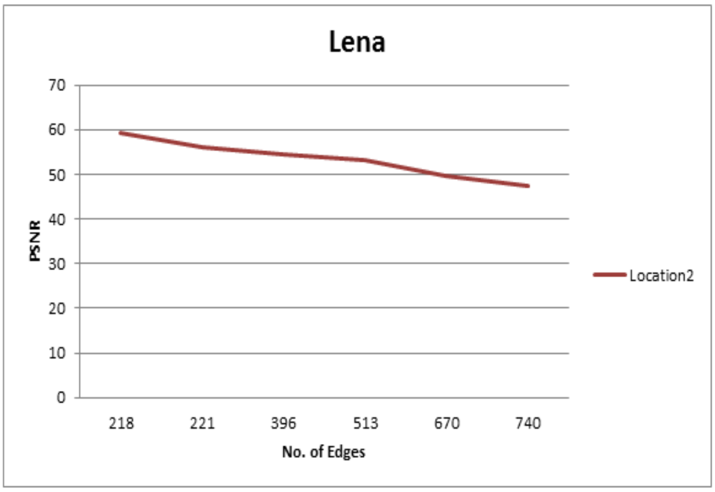
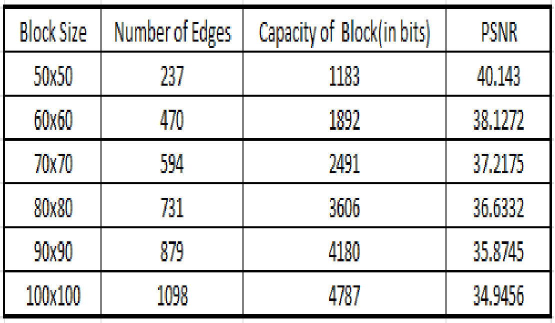


**Fig 7 PSNR vs. Edges at Location 2**

b) *Tiffany Image:* The JPEG image of Tiffany is taken having a size 512x512 and two different locations reflecting higher and lower edge densities are selected as shown in Fig 8 and 10. APD algorithm is applied on these locations and results obtained are shown in Table III, Table IV, Fig 9 and Fig 11.

**Table III: Performance Analysis for Tiffany image at Location 1**



| Block Size | Number of Edges | Capacity of Block(in bits) | PSNR |
|---|---|---|---|
| 50x50 | 237 | 1183 | 40.143 |
| 60x60 | 470 | 1892 | 38.1272 |
| 70x70 | 594 | 2491 | 37.2175 |
| 80x80 | 731 | 3606 | 36.6332 |
| 90x90 | 879 | 4180 | 35.8745 |
| 100x100 | 1098 | 4787 | 34.9456 |

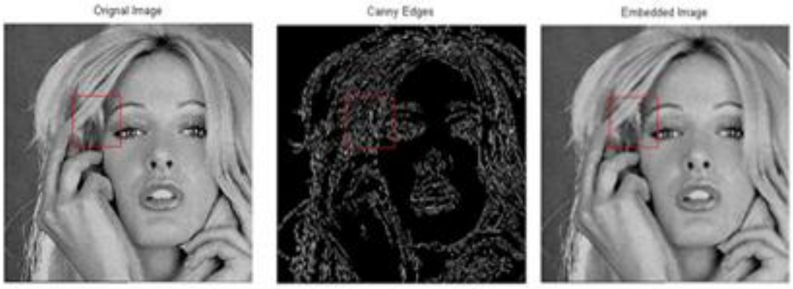


**Fig 8: (a) Original Image (b) Edges in Image (c) Embedded Image at location 1**

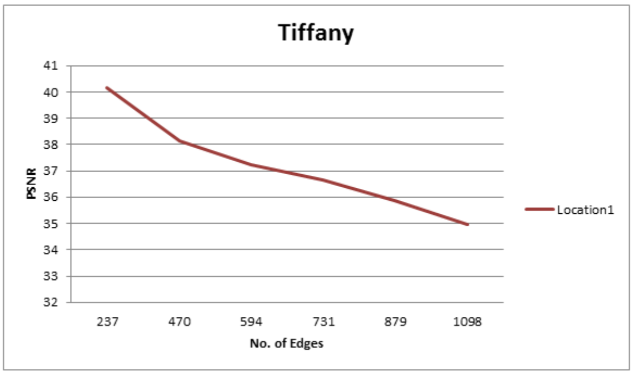
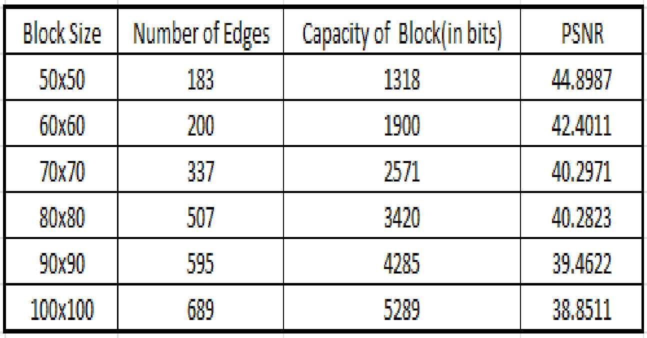


**Fig 9 PSNR vs. Edges at Location 1**

**Table IV: Performance Analysis for Tiffany image at Location 2**



| Block Size | Number of Edges | Capacity of Block(in bits) | PSNR |
|---|---|---|---|
| 50x50 | 183 | 1318 | 44.8987 |
| 60x60 | 200 | 1900 | 42.4011 |
| 70x70 | 337 | 2571 | 40.2971 |
| 80x80 | 507 | 3420 | 40.2823 |
| 90x90 | 595 | 4285 | 39.4622 |
| 100x100 | 689 | 5289 | 38.8511 |

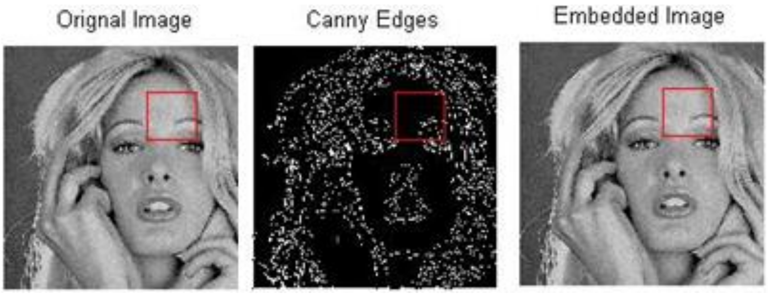


**Fig10 (a) Original Image (b) Edges in Image (c) Embedded Image at Location 2**

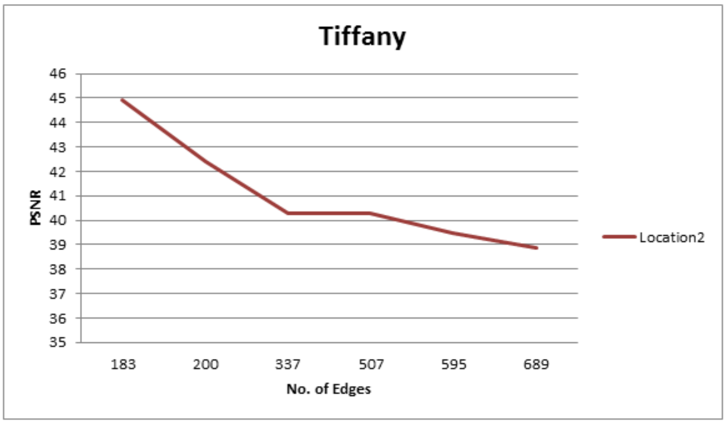
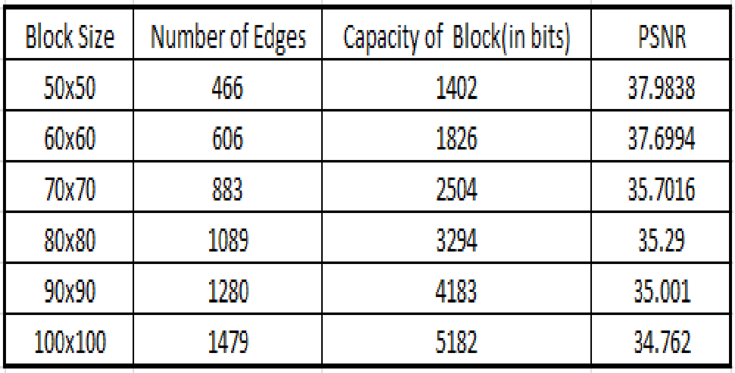


**Fig 11 PSNR vs. Edges at Location 2**

*c) Baboon Image:* The JPEG image of Baboon is taken having a size 512x512 and two different locations reflecting higher and lower edge densities are selected as shown in Fig 12 and Fig 14 respectively. The APD algorithm is applied on these locations and results obtained are shown in Table V, Table VI, Fig 13 and Fig 15.

**Table V: Performance Analysis for Baboon image at Location 1**



| Block Size | Number of Edges | Capacity of Block(in bits) | PSNR |
|---|---|---|---|
| 50x50 | 466 | 1402 | 37.9838 |
| 60x60 | 606 | 1826 | 37.6994 |
| 70x70 | 883 | 2504 | 35.7016 |
| 80x80 | 1089 | 3294 | 35.29 |
| 90x90 | 1280 | 4183 | 35.001 |
| 100x100 | 1479 | 5182 | 34.762 |

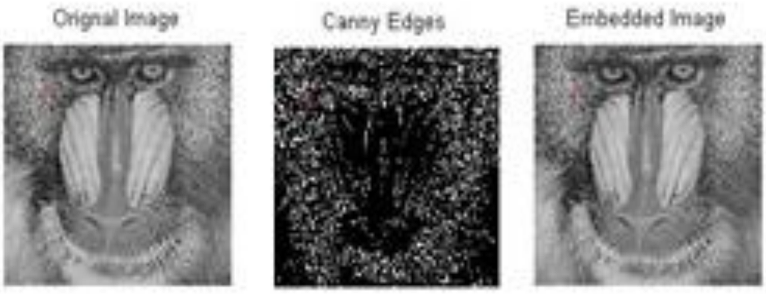


**Fig12: (a) Original Image (b) Edges in Image (c) Embedded Image at Location 1**

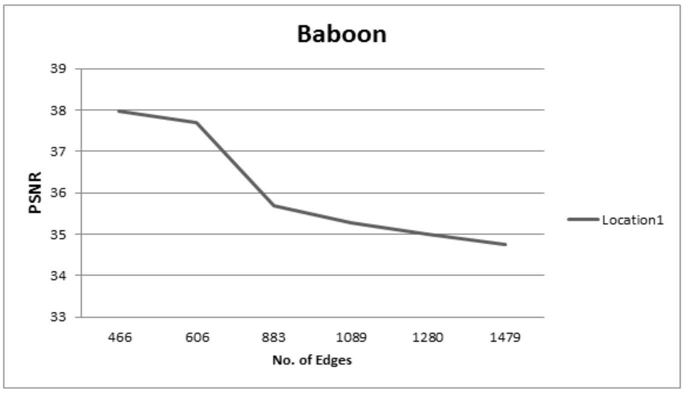


**Fig 13: PSNR vs. Edges at Location 1**

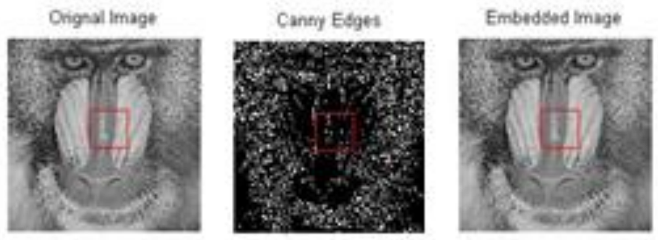
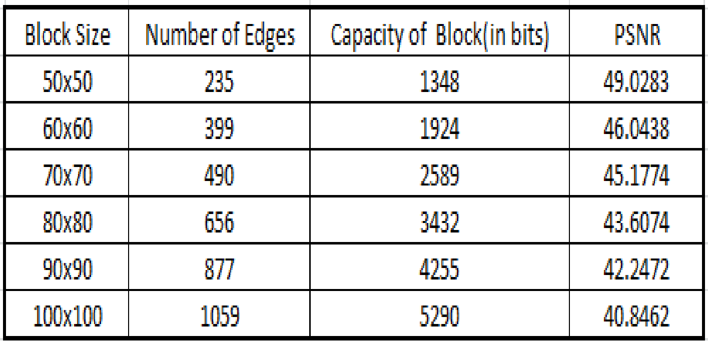


**Fig 14 i) Original Image ii) Edges in Image iii) Embedded Image at Location 2**

**Table VI: Performance Analysis for Baboon image at Location 2**



| Block Size | Number of Edges | Capacity of Block(in bits) | PSNR |
|---|---|---|---|
| 50x50 | 235 | 1348 | 49.0283 |
| 60x60 | 399 | 1924 | 46.0438 |
| 70x70 | 490 | 2589 | 45.1774 |
| 80x80 | 656 | 3432 | 43.6074 |
| 90x90 | 877 | 4255 | 42.2472 |
| 100x100 | 1059 | 5290 | 40.8462 |

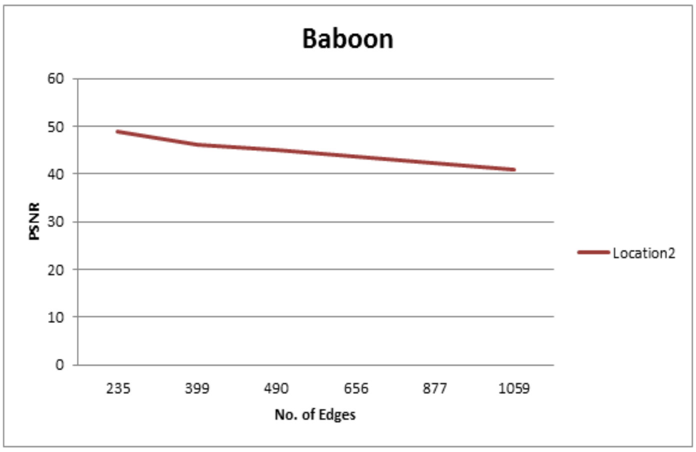


**Fig 15: PSNR vs. edges at Location 2**

## V. CONCLUSION

From the results obtained in section IV, it is gatheredthat as the block size increases the data hiding capacity increases accordingly due to the increased availability of potential hiding places. Further, it is seen that for the tested scenarios, hiding of same size dataat location2 results in lesser PSNR deterioration as compared to location 1. It reflects that data hiding could be more beneficial at those locations that have lesser number of edges. It is also seen that PSNR at edges reduces roughly by 12% as compared to that at non-edges. So edges are the most sensitive areas of an image that should be handled carefully during storage of information.The present work is carried out with gray scale images and with.jpg image format, though in future it can be extended to other formats and colour images.

## REFERENCES

[1] Y.C. Li, C.M. Yeh and C.C. Chang, “*Data hiding based on the similarity between neighbouring pixels with reversibility*”, Elsevier Journal of Digital Signal Processing, Vol. 20, pp.1116–1128, 2010.

[2] Y.Yu Tsai, D.S. Tsai and C.L. Liu, “*Reversible data hiding scheme based on neighbouring pixel differences*”, Elsevier Journal of Digital Signal Processing, 2012.

[3] Z. Zhao, N. Yu, and X. Li, “*A novel video watermarking scheme in compression domain based on fast motion estimation*”, in Proc. of IEEEInt’l Conference on Communication Technology, pp. 1878-1882, 2003.

[4] Z. Ni, Y.Q. Shi, N. Ansari and W. Su, “*Reversible data hiding*”, IEEE Trans. on Circuits and System for Video Technology, Vol 16, pp. 354–362, 2006.

[5] T. Morkel, J.H.P. Eloff and M.S. Olivier, "*An overview of image steganography*", in Proc. of 5th Annual Information Security South Africa Conference (ISSA), 2005.

[6] Z. AL.Ani, AAZaidan, B BZaidan and H. O. Alanazi, "*Main Fundamentals for Steganography*", Journal of Computing, Vol. 2,2010. (ISSN: 2151-9617)

[7] N.S.Kumaran and R. Rajesh, "*Edge Detection Techniques for Image segmentation -A Survey of Soft Computing*", International Journal of Recent Trends in Engineering, Vol. 1, pp.250-254,2009.

[8] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami, "*Labeling Method in Steganography*", in Proc. of World Academy of Science, Engineering and Technology, pp. 349-353, 2007.(ISSN: 1307-6884)

[9] H.A. Jalab, A .AZaidan and B.B Zaidan, "*New Design for Information Hiding with in Steganography Using Distortion Techniques*", IACSIT International Journal of Engineering and Technology Vol. 2, pp. 72-77, 2010 (ISSN: 1793-8236).

[10] A.Cheddad, Joan Condell, K.Curran and P.McKevitt, "*Digital Image Steganography: Survey and Analysis of Current Methods*", Signal Processing, Vol 90, pp. 727-752, 2010.