Data Hiding In Digital Image Processing Using Steganography: A Review

[1]Rajani, [2]Muhammad Tauheed Khan
[1]M.Tech Student, [2]Professor,
Department of ECE, AFSET, Faridabad, Haryana, India

***Abstract* - Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It is always non visible. In this message more important than original signal. Steganography has various useful applications. The main objectives of steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. These are the main factors which make it different from other techniques watermarking and cryptography. This paper includes the important steganography methods and the main focus is on the review of steganography in digital images.**

***Keywords* - Steganography, Histogram, Adjacent Pixel Difference (APD), PSNR, Capacity**

I. Introduction

Steganography is the art of concealing a message, image or file within another message, image or file. Steganography is used to secure the message. One of the major requirements of data hiding is that the hidden data must be imperceptible. The use of steganography has many advantages and are very useful in digital image processing which makes them suitable for a wide variety of applications. In this modern area, internet offers great convenience in transmitting large amounts of data in different parts of the world. However, the safety and security of long distance communication remains an issue. In order to solve this problem of security and safety has led to the development of steganography schemes. Steganography is different from watermarking and cryptography. The main objective of steganography is to to hide the existence of the message itself, which makes it difficult for an observer to figure out where exactly the message is. On the other hand, cryptography techniques tend to secure communications by changing the data into a form so that it cannot be understand by an eavesdropper. And in watermarking logo is more important than information. Steganography is the type of hidden communication that means "covered writing" (from the Greek words stego or "covered" and graphos or "to write"). In 1550, Jerome Cardan, an Italian mathematician, proposed a scheme of secret writing where a paper mask with holes is used. The user needs to write his secret message in such holes after placing the mask over a blank sheet of paper. Then remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text [1]. In this 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 [2]. The picture quality is measured by means of PSNR using MATLAB platform and compared.

II. Literature Review

Yuan-Yu Tsai et.al in proposed a reversible data hiding algorithm for gray-scale images [3]. The results revealed better in terms of embedding capacity and security. 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 [4] 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 [5]. In [6] 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.* [7], 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*. [8], 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 [9] Abbas Cheddad*et al.* proposed different methods of existing steganography with some common standards by providing some embedding algorithm.

III. APD Algorithm

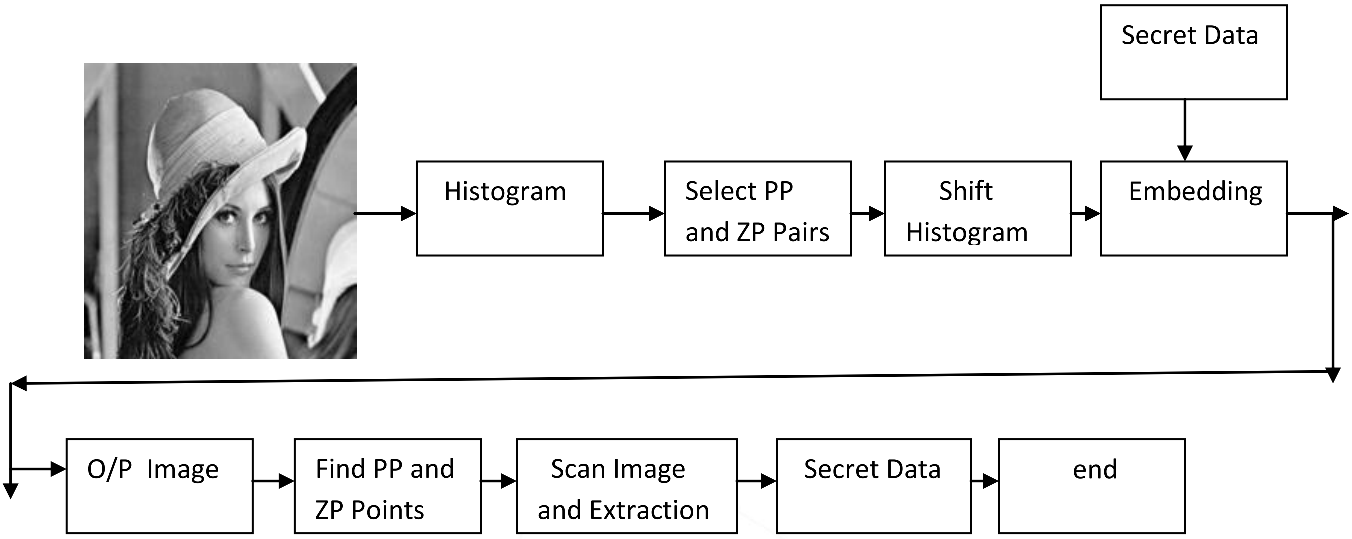

Fig.1: Flow chart of the APD method including Data embedding and data extraction Process

Step 1: For a given image, Produce the histogram of the cover image. Fig.1 shows the histogram of image.
Step 2: Find the peak point and zero points.
Step3: 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.
Step 4: 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.
Step 5: Shifting of histogram generates free space for embedding the data.
Step 6: With peak point value, embed a bit of hidden data.
Step 7: If embedded bit is “1”, then shift the pixel from PP to ZP by one.
Step8: If embedded bit is “0‟, then pixel value does not change.
Step9: In extraction process same find PP and ZP.
Step 10: Scan the the image and extract the message.

Histogram: The histogram represents the graphical representation of the tonal variation of digital images in digital 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.2: lena

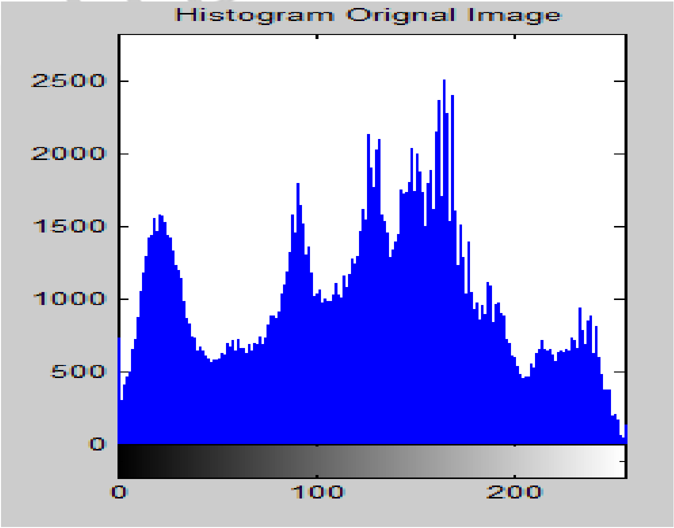

Fig.2: a). Histogram of lena image

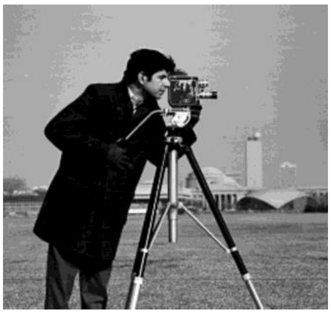

Fig .3: cam

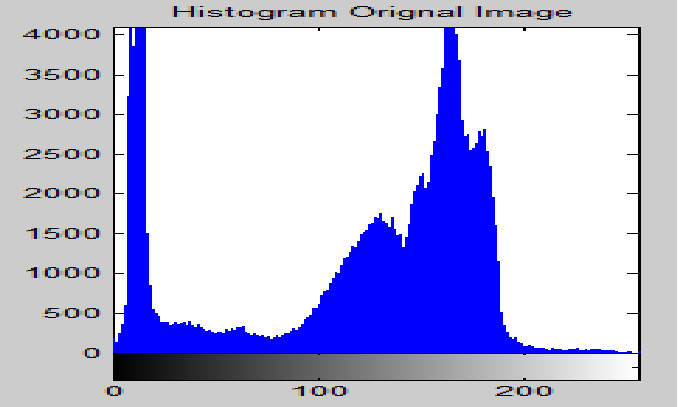

Fig.3 b). Histogram of cam image

Analysis: Three common requirements, security, capacity, and imperceptibility, may be used to rate the performance of steganographic techniques. As a performance measure for image distortion due to embedding, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images .

$$\text{PSNR} = 10log1o(R^2/MSE)$$

R is the maximum fluctuation in the input image data type and MSE is the Mean Square Error. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

IV. Conclusion

This paper reviewed the main steganographic techniques. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and security). As a performance measure for image distortion due to embedding, the well-known peak-signal-to noise ratio (PSNR). It compute peak signal to noise ratio between two images, in decibels. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image.

References

[1] S.B. Sadkhan., “Cryptography: Current status and future trends”, in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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)

[7] 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.

[8] 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).

[9] 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.

[10] Da-Chun Wu, Wen-Hsiang Tsai, “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters 24 (2003) 1613–1626.