JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Histogram Based Imperceptibility Analysis of Parity Checker Method

Rajkumar

University Institute of Engineering and Technology, MDU Rohtak

Abstract: Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. This paper presents the histogram analysis of the parity checker method. Parity checker method hide the data using the concept of odd and even parity. Histogram analysis shows the alteration in the pixel intensity after insertion of the message. Experimental results show that there is very less deflection in image quality after insertion of message using parity checker method.

Keywords: Cryptography, Steganography, Security etc.

I. INTRODUCTION

Steganography is a technique of hiding information within the information or hiding one form of information into another form of information [1]. Steganography word is the combination of two Greek word “stegos” and “grafia”. Stego means “cover” and grafia means “writing” whereas Steganalysis is a technique to detect the existence of steganography. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2]. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which supposed to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. For more secure data transfer cryptography is used with steganography. In cryptography the message is encrypts with secret key and transfer it to the other end then receiver decrypt it and get original message [3, 4].

II. LITERATURE SURVEY

Zhi and Fen [5] proposed method of LSB image steganography, which was used a method called detection of random LSB. They use passive steganalysis method for detection of secret message in stego image. This method used the concept of RS in which secret message was inserted in selected part of image randomly not in fixed or predefined manner due to this steganalysis becomes difficult. In this method, gradient energy of image is analysed theoretically based on steganalysis detection method called GEFR. To hide a secret message, a pixel can be detected easily because gradient energy level varies from pixel to pixel. Khosravirad et al. [6] proposed a new LSB technique which can be applied in both spatial domain as well as transform domain. This technique uses the concept of COS which is high order statistical property. They try to find a subset of secret message in the pixel set of an image due to which less of bits are changed in image which results less change in the bits of image. They also introduced the concept of vector of features. These features help in the classification of stego image. This method is more accurate than the method proposed by Harmsen which uses second order vector feature. In Harmen's method, false alarm was about to 14.75 % while in this method, the false alarm is reduced about to 1.5 %. Zhang et al. [7] introduced a new method of LSB steganalysis which is based on statistical distribution of pixel difference in spatial domain. it can be done on high resolution images. Based on the difference of zero and non-zero values of pixels and also finds the error which is used to determine the steganographic features. It also uses Laplacian distribution. As we know that pixels are highly correlated to each other in image and zero, non-zero values occur frequently. If change in the some neighbors' pixel value then it may slightly change the intensity level of colors. Luo et al. [8] introduced a more appropriate LSB technique. They developed an improved Random scattered method called RRS method over RS. In RRS, the value of pixels is adjusted slightly in the embedded image. Firstly, the secret message is embedded in cover image using LSB and then a compensation is done dynamically on the stego image due to this RS steganalysis is decreased near the value to 0 cause inappropriate steganalysis. In this method, one is added to the pixel value of secret message which is called compensation and then uses the RS method to adjust the pixels value in image. Basically, this method provides more resistance to RS steganalysis. Cvejic and Seppanen [9] presented modification to standard LSB algorithm in which embedding is done four bit per sample due to which capacity of storing secret information is increased by 33 present. They tried to decrease the SNR value within silent parts and where the value of audio changing slowly using modified error diffusion as well as adjustment of LSB with the help of error replacement method. In this method, closed level of audio is found and then secret message is inserted into audio. After that, minimum error replacement is calculated and maximum error replacement is tried to decrease to 2k-1 caused the LSB performance improvement. Thenmozhi and Chandrasekran [10] presented a novel approach for building a secure data hiding technique of Steganography using integer wavelet transform along with cropping. Employed frequency domain to increase the robustness of the proposed steganography method. cropping function and OPAP has been utilised to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image and to increase the hiding capacity with low distortions respectively. Simulation results showed that the novel scheme outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity. Balakrishana et al. [38] proposed single digit sum (SOS) based image steganography. Proposed technique controlled the amount of change in pixel. Determined the base for computing SOS by using upper limit of pixel. Ensured that the stego image does not degrade beyond the degradation in the compressed image. Martin et al. [11] investigated whether stego-images, bearing a secret message, are statistically "natural" or not. Utilized recent results on the statistics of natural images and investigated the effect of some popular steganography techniques. Found that these fundamental statistics of natural images were, altered by the hidden "nonnatural" information. Considered the class of natural images, for which the change generally falls within the intrinsic variability of the statistics, and didn't allow for reliable detection, unless knowledge of the data hiding process is taken into account. Thenmozhi and Chandrasekran [12] presented a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Discussed the chaotic system, and its advantages for achieving the encryption of data. Applied the henon mapping (chaos) on the secret image and performed the two dimensional Discrete Wavelet Transform (2-D DWT) on the cover image of size M × N. improved the Image quality by preserving the wavelet coefficients in the low frequency sub band. Experimental results showed that the algorithm has a high capacity and a good invisibility. Prabhakran and Bhavani [13] proposed secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Performed Arnold transformation to scrambles the secret image. Also performed Discrete Wavelet Transform (DWT) is performed in both images, followed by Alpha blending operation. Applied the Inverse Discrete Wavelet Transformation (IDWT) to get the stego image. Investigated the performance of the proposed scheme by comparing various qualities of the stego image and cover image. Results showed that the proposed algorithm for steganography is highly secured with certain strength in addition to good perceptual invisibility. Das and Tuithung [14] presented the technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q were used as cover image and secret image respectively. Performed Huffman Encoding over the secret image/message before embedding and each bit of Huffman code of secret image/message was embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image became standalone information to the receiver. Experimental result showed that the algorithm had a high capacity and a good invisibility. Proposed technique showed better result in comparison with other existing steganography techniques.

III. PARITY CHECKER METHOD

In this method, the concept of even and odd parity has been used by using the parity checker. As we already know that even parity means that the pixel value contains even number of 1‟s and odd parity means that the pixel value contains odd number of 1‟s. In this method „0‟ bit is inserted at a pixel value where pixel value has odd parity and if the parity is even then odd parity is made by adding or subtracting „1‟ to the pixel value. Similarly, „1‟ is inserted at a pixel value if it had even parity. In case, if even parity is not present at that location then even parity is made over that location by adding or subtracting „1‟. In this way „0‟ or „1‟ is inserted at any location. For retrieval of message, again parity chacker is used. If odd parity is present at the selected location then „0‟ is message bit, else message bit is „1‟. Retrieval process is repeated for all locations. In this way, the message bits are retrieved bits from all the locations where these have been inserted.

IV. HISTOGRAM BASED ANALYSIS

We have taken set of 6 test images for histogram analysis. The results have been analysed in MATLAB. We have inserted 10 KB message in all the test images. After insertion of 10 KB message the stego images are generated. Histogram shows the frequency of intensity in cover image and stego image. The histograms of cover image and stego image with their respective histogram are shown by Figure 1 to Figure 6. Figure 1 shows the pepper cover image, pepper stego image with their respective histograms. Figure 2 shows the lena cover image, lena stego image with their respective histograms. Figure 3 shows the house cover image, house stego image with their respective histograms. Figure 4 shows the girl cover image, girl stego image with their respective histograms. Figure 5 shows the couple cover image, couple stego image with their respective histograms. Figure 6 shows the aerolpane cover image, aeroplane stego image with their respective histograms. The various histograms show that there is very less deflection in image intensity after insertion of 10 KB data.

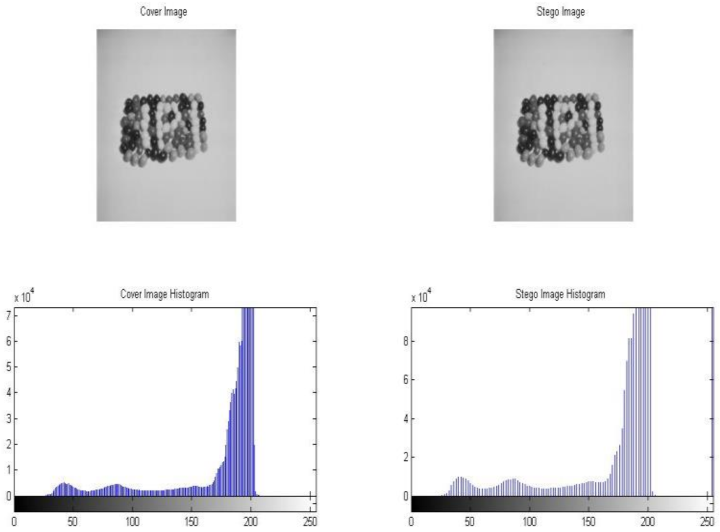

Figure 1: Cover and Stego image pepper with their respective histogram

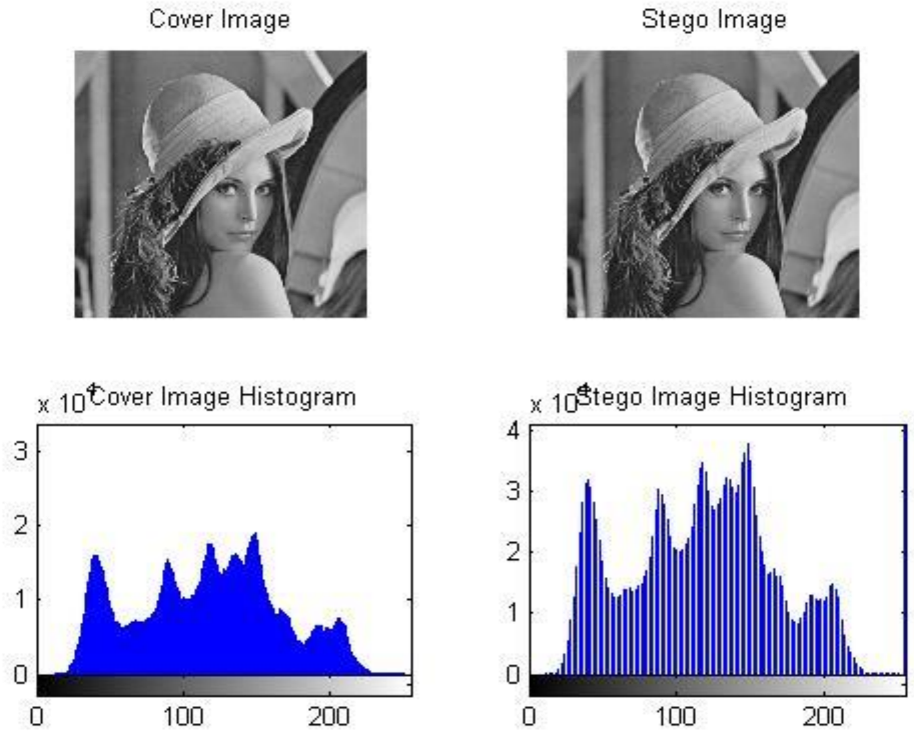

Figure 2: Cover and Stego image lena with their respective histogram

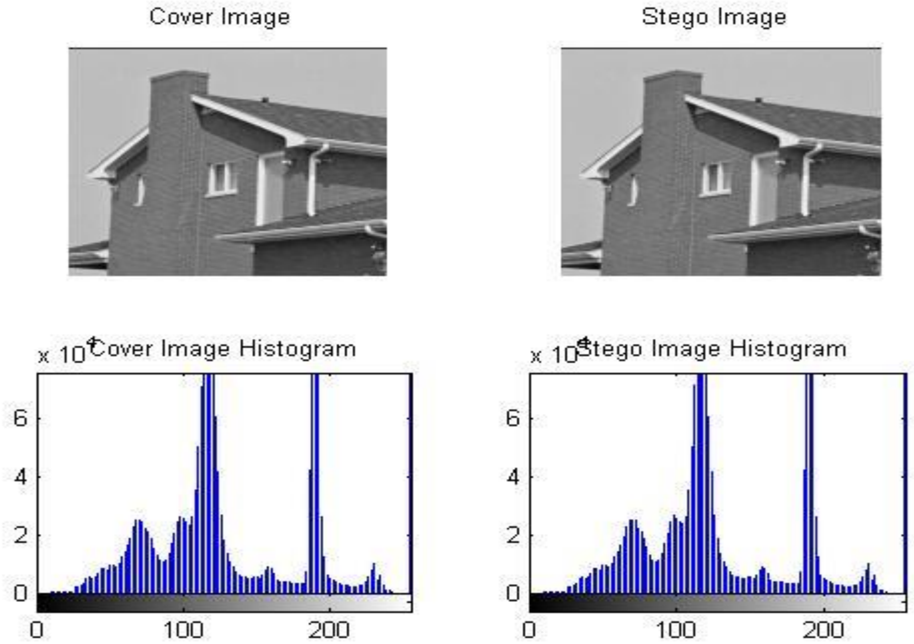

Figure 3: Cover and Stego image house with their respective histogram

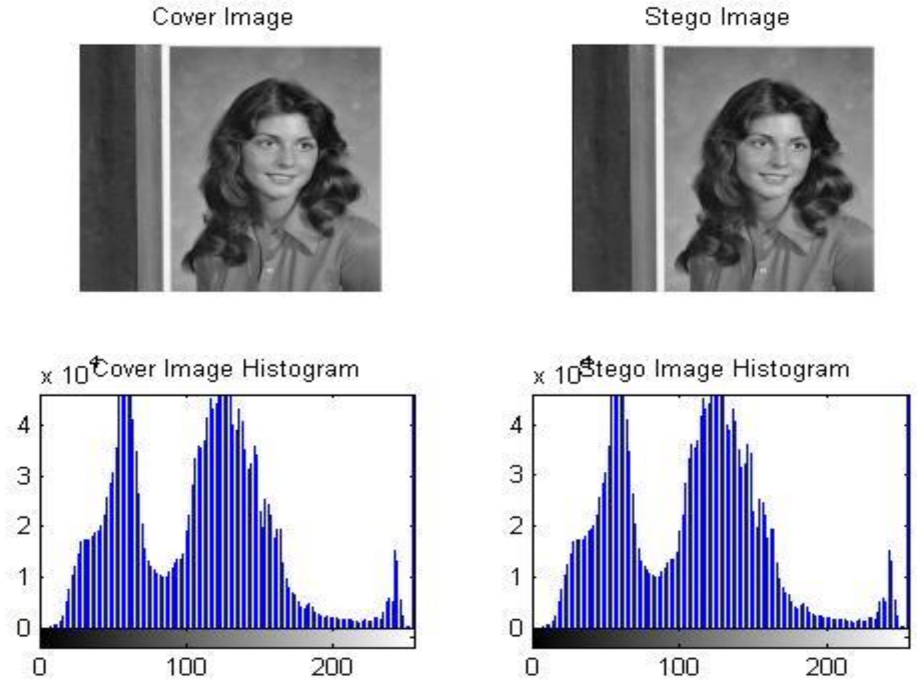

Figure 4: Cover and Stego image girl with their respective histogram

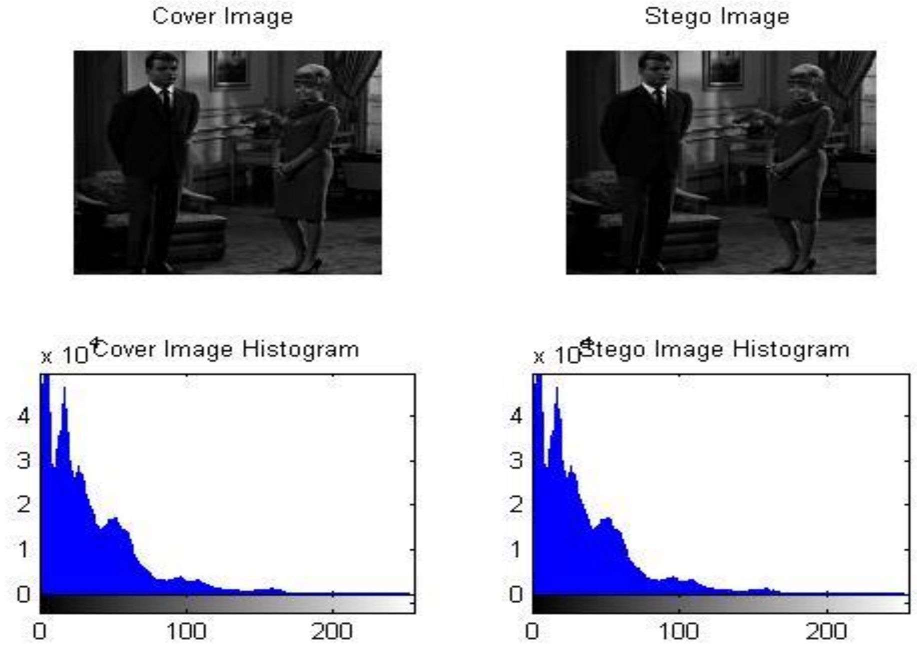

Figure 5: Cover and Stego image couple with their respective histogram

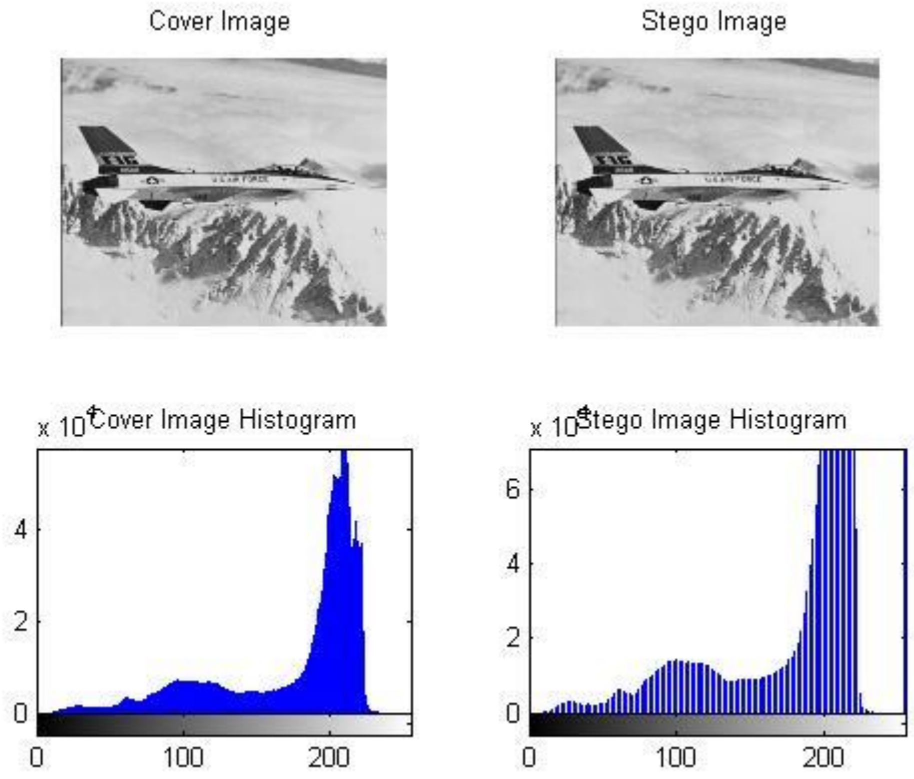

Figure 6: Cover and Stego image Aeroplane with their respective histogram

V. CONCLUSION

We have analyzed the parity checker method on the basis of histogram analysis. The experimental results show that there is very less change in image intensity after insertion of 10 KB data. This less deflection shows that parity checker method is highly imperceptible towards human visual system. In the future, we will try to develop a new technique which is highly imperceptible and can work with cryptography for better security of data.

REFERENCES

[1] S. Ahn, L.V. and Hopper, N.J.(2005)," Public-Key Steganography".

[2] Amirtharajan, R., Akila, R. and Chowdavarapu, P.D. (2010), "A Comparative Analysis of Image Steganography". International Journal of Computer Applications 2(3): 41–47.

[3] Amirtharajan, R., Ganesan, V., Jithamanyu, R. and Rayappan, J.B.B. (2010), "An Invisible Communication for Secret Sharing against Transmission Error", Universal Journal of Computer Science & Engineering Technology, 1 (2), 117-121.

[4] Anderson, R. J. (1996), "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48.

[5] Anderson, R.J. and Petitcolas, F.A.P. (1998), "On the Limits of Stegnography", IEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481

[6] Arnold, M. (2000), “Audio Watermarking: Features, Applications and Algorithms”. Multimedia and Expo. IEEE International Conf., Vol. 2, pp. 1013-1016.

[7] Bandopadhyay, S.K., BhattaCharya, D., Ganguly, D., Mukherjee, S. and Das, P. (2007), “A Tutorial Review on Steganography”.

[8] Batra, S., Rishi, R., Yadav, R. (2010), “Insertion of message in 6th, 7th & 8th bit of pixel values and retrieval in case intruder changes the least significant bit of image pixels”, International Journal of Security and its Applications, Vol . 4, No. 3.

[9] Bender, W. and Gruhl, D. (1996), “Techniques for data hiding”, IBM Systems Journal, Vol 35, Nos 3&4.

[10] Bennett, K. (2004), “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text”, Purdue University, CERIAS Tech. Report 2004-13.

[11] Brainos, II A.C. (2007),” A Study Of Steganography And The Art Of Hiding Information”.

[12] Brassil J, Low S, Maxemchuk N, O’Garman L. (1994),” Electronic Marking and Identification Techniques to Discourage Document Copying”. In: Infocom. IEEE. 1278–1287.

[13] Carlson, A.B., Crilly, P.B. and Rutledge, J.C., Communication Systems.

[14] Ravi Saini and Rajkumar Yadav “A New Data Hiding Method Using Pixel Position And Logical And Operation ”, International Journal of computer and Electronics Research(IJCER) Vol. 1, Issue 1, 2012, ISSN: 2778-5795, Peer Reviewed and Referred International Journal

[15] Gunjan Chugh, Rajkumar Yadav, Ravi Sini, A New Image Steganographic Approach Based on Mod Factor for RGB Image, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol 7, Issue 3, Pp 27-44, 2014, ISSN 2005-4254.

[16] Rajkumar Yadav, Gaurav Chawla and Ravi Saini. “Semi Pixel Difference Method For Digital Image Watermarking With Minimum Degradation In Image Quality”, International Journal Of Computer Technology and its Applications(IJCTA),Vol. 2, Number 5,pp 1297-1314, ISSN: 2229-6093, Peer Reviewed and Referred International Journal

[17] Rajkumar Yadav, Ravi Saini and Kamaldeep. “Cyclic Combination Method For Digital Image Steganography With Uniform Distribution Of Message”. Advance Computing: International Journal(ACIJ), Vol. 2, Issue 6, November 2011, ISSN: 2229-726X, Peer Reviewed and Referred International Journal

[18] Rajkumar Yadav, Kamaldeep and Ravi Saini. “Biometric Template Security By Using Invisible Watermarking With Minimum Degradation in Quality of Template”, International Journal of Computer Science and Engineering (IJCSE),Vol. 3, No. 1, Dec 2011, ISSN: 0975-3397, Peer Reviewed and Referred International Journal

[19] Rajkumar Yadav, Ravi Saini and Gaurav Chawla. “SSB-7: A New Image Steganography System For Messsage Insertion Chance Enhancement Using Bit 7”, International Journal of Computer Applications(IJCA), Vol. 24, No.4, June 2001 Impact Factor=0.835, ISSN: 0975-8887, Peer Reviewed and Referred International Journal

[20] Chan, C.K. and Chen, L.M. (2004), “Hiding data in images by simple LSB substitution”, Pattern Recognition 37 (3) 469–474.