Analysis of Various Image Steganography Techniques Based Upon PSNR Metric

Rajkumar Yadav
University Institute of Engineering & Technology, M.D. University, Rohtak

***Abstract*—** Every common person uses internet directly or indirectly in some spheres of his life. They mainly use the internet for information sharing. Also, information sharing has the primary importance in the field of Military Services, Medical Services, Mobile Services, and Investigation Agencies etc. The main hurdle in the path of information sharing is the security of information. The information security can be achieved by Cryptography and Steganography. But now days, Steganography is the most burnt area. There are lot of research is going on steganography. In this paper, we analyze various image steganography techniques by using peak signal to noise ratio (PSNR) Metric. After analyzing the techniques, we found that 6th, 7th and 8th Bit Method provides highest PSNR values and LSB Method provides lowest PSNR values.

***Keywords*—** Steganography, cryptography, LSB, GLM, parity checker etc.

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

Steganography is the art and science of hiding information by embedding data into media. Steganography (literally meaning covered writing) [1] have been used since ancient time, for example, people used etching messages in wooden tablets and covered them with wax. They used tattooing a shaved messenger's head, letting his hair grow back, and then shaving it again when he arrived at his contact point to reveal the message. Different types of steganographic techniques have been used that employ invisible inks, microdots, character arrangement, digital signatures, covert channel, and spread spectrum communications [2].

Electronic steganography techniques use digital ways of hiding and detecting processes. Steganography is different than cryptography and watermarking although they all have overlapping usages in the information hiding processes. Steganography security hides the knowledge that there is information in the cover medium, where cryptography reveals this knowledge but encodes the data as cipher-text and disputes decoding it without permission; i.e., cryptography concentrates the challenge on the decoding process while steganography adds the search of detecting if there is hidden information or not. Watermarking is different from steganography in its main goal. Watermarking aim is to protect the cover medium from any modification with no real emphasis on secrecy. It can be observed as steganography that concentrates on high robustness and very low or almost no security [3]. Steganography, in general, may have different applications. For example, steganography can be utilized for posting secret communications on the Web to avoid transmission or to hide data on the network in case of a violation. It can be useful for copyright protection, which is, in reality, digital watermarking [4]. Copyright protection is to protect the cover medium from claiming its credit be others, with no real emphasis on secrecy. Stego Applications can involve "ownership evidence, fingerprinting, authentication and integrity verification, content labelling and protection, and usage control" [25]. Steganography techniques use different carriers (cover medium in digital format) to hide the data. These carriers may be network packets, floppy disk, hard drive, amateur radio waves [5], or general computer file types such as text, image, audio and video [6]. Restrictions and regulations are thought of in using steganography due to the threat from different laws in different countries. The law and writes (such as copyright) enforcing agencies needed in organizations are aiming to secure their information [7] but do not have clear procedures nor tools. In fact, many easy to use steganography tools are available to hide secret messages on one side of communication and detect hidden info on the other side [6].

There are various existing techniques for image steganography like LSB technique, 6^{th} & 7^{th} bit technique, 6^{th}, 7^{th} & 8^{th} bit technique, parity checker technique, GLM technique. In this paper, we analyse tha various image steganography techniques based upon PSNR values. PSNR can be calculated by using following well known formulae:

$$MSE = \frac{1}{[n \times m]^2} \sum_{i=1}^{n} \sum_{j=1}^{m} \left(x_{ij} - y_{ij} \right)^2 \text{--------} (1)$$

$$PSNR = 10 \log_{10} [(255)^2 / MSE] \text{---------} (2)$$

where n is the number of rows in the image matrix and m is the number of columns in the image matrix.

The results are calculated on three different images.

II. PSNR Analysis Of different techniques

A. LSB Technique[13]

In this method binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel. For example we will try to hide the character 'A' into an 8-bit color image. We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this:

00100101 11101011 11001010 00100011
11111000 11101111
11001110 11100111

Then each bit of binary equivalence of letter 'A' i.e. **01100101** are copied serially (from the left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern will become like this: -

00100100 11101011 11001011 00100010
11111000 11101111
11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and formatting and quantization of noise.
The results for this technique are given in Table I.

TABLE I
LSB Technique using Web Stego

Message Length	Image 1	Image 2	Image 3
4096 Bytes	17.4	18.3	17.9
16384 Bytes	16.6	16.7	16.6

B. 6th, 7th & 8th bit method[14]

In this method 6th, 7th and 8th bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message. Methods for insertion / retrieval of message in case intruder does not manipulate the recipient copies are given in section 2 in the form of algorithms. The steps explaining how to retrieve the message in case intruder changes the least significant bit of pixels of recipient copies.
The results for this technique is given in Table II.

TABLE III
6th, 7th & 8th bit technique

Message Length	Image 1	Image 2	Image 3
4096 Bytes	33.3	31.7	32.8
16384 Bytes	34.5	31.1	33.3

C. Parity Checker Technique[15]

In this section we propose an improved steganographic method which shows improvement over digital logic method described by parvinder et al [2]. Bit replacement made in host image is negligible compared to existing embedded techniques [3-9]. In the present study, at first we are using digital operations based on logic gates along with mode and multiple method to derive the hidden information from image, after that we apply modulus operator for getting remainder and quotient. For doing so, we first selected the cover image and constructed the image matrix and information matrix respectively by converting each pixel of image into bits and the information into binary form. After construction, the image matrix and information matrix is so selected that the number of their columns should be same. We proposed a novel idea of multiplication factor to reduce the number of bits used to hide the information in the image. This factor should be (n)2 as only binary numbers are considered. We take '4' as multiplication factor as there will be only 4 remainders possible 0,1,2,3. But if we take larger number then it will be difficult to select the image. For example, if we take 16 as multiplication factor then there is a possibility of 16 remainders (0, 1, 2… 15). With these more number of remainders it would be difficult to select the specified rows of image matrix for insertion of opcode bits. It means larger the multiplication factor, harder will be the image selection. Proposed methods selected the images based on mode and multiple method along with digital logic operations to insert the message such that image is not significantly degraded after embedding and embedded information is immune to modifications from intelligent attacks or manipulations. An upper bound of 0.005 bits/pixel was determined for safe LSB embedding by Jessica et al [10].
The results for this technique are given in Table III.

TABLE IIIII
PARITY CHECKER TECHNIQUE

Message Length	Image 1	Image 2	Image 3
4096 Bytes	27.4	26.3	25.9
16384 Bytes	25.6	26.7	26.6

D. GLM Technique[16]

In 2004, Potdar et al. [7] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image. Initially, the gray level values of the selected pixels (odd pixels) are made even by changing the gray level by one unit. Once all the selected pixels have an even gray level it is compared with the bit stream, which has to be mapped. The first bit from the bit stream is compared with the first selected pixel. If the first bit is even (i.e. 0), then the first pixel is not modified as all the selected pixels have an even gray level value. But if the bit is odd (i.e. 1), then the gray level value of the pixel is decremented by one unit to make its value odd, which then would represent an odd bit mapping. This is carried out for all bits in the bit stream and each and every bit is mapped by modifying the gray level values accordingly.

The results for this technique is given in Table IV.

TABLE IV
GLM TECHNIQUE

Message Length	Image 1	Image 2	Image 3
4096 Bytes	24.2	23.1	25.4
16384 Bytes	25.6	23.7	24.6

III. CONCLUSION

This paper presents the analysis of various image steganography techniques based upon PSNR analysis. The higher the value of PSNR the better will be the technique. By analysis of the various techniques we found that 6th, 7th and 8th bit method given by Rajkumar et.al provides the highest value of PSNR whereas LSB provides the lowest value of PSNR. We can conclude from the analysis that 6th ,7th and 8th bit Method provides better PSNR value than some existing investigated methods which show high robustness of 6th ,7th and 8th bit method against various noise imperfections on the transmission channel during the transfer of the information.

REFERENCES

[1] Cox, Ingemar, Bloom, Jeffrey, Miller, Matthew, *Digital Watermarking: Principles & Practice*, 2001, Morgan Kauffman Publishers, ISBN 1-55860-714-5, ch. 1-2.

[2] Katzenbeisser, S., Petitcolas, F.A.P., *Information hiding techniques for steganography and digital watermarking*, Artech House Publishers, 2000.

[3] Feng, J. B., Wu, H. C, Tsai, C. S. and Chu, Y. P., "A new multi-secret images sharing scheme using largrange's interpolation," Journal of Systems and Software, vol. 76, no. 3, pp. 327–339, June 2005.

[4] Chang, C.C, Lin, I.C, "Remarks on fingerprint- based remote user authentication scheme using smart cards," ACM Operating Systems Review, vol. 38, no. 3, pp. 91–100, Oct. 2004.

[5] Dugelay, J.L., Roche, S., "A survey of current watermarking techniques," in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. A. P. Petitcolas, Eds. Norwood, MA: Artech House, 1999, ch. 6.

[6] Shoemaker, C., "Hidden bits: A survey of techniques for digital watermarking", Independent study, EER 290, spring 2002.

[7] Wang, Y., Doherty, J.F., and Van Dyck, R.E., "A watermarking algorithm for fingerprinting Intelligence images", Conference on Information Science and Systems, The John Hopkins University, March 21-23, 2001.

[8] S. Moller, A Pfitzmann, and I. Stirand, "Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best.", in Information Hiding: First International Workshop Proceedings, vol. 1174 of Lecture Notes in Computer Science, pp. 7-21, Springer, 1996.

[9] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", Proceedings of the SPIE 2420, Storage and Retrieval for Image and Video Databases III, pp. 164-173, 1995.

[10] A. Hanjalic, G.C. Langelaar, P.M.B. van Roosmalen, J. Biemond, and R.L. Lagendijk, *Image and Video Databases: Restoration, Watermarking, and Retrieval*, Elsevier, 2000.

[11] G. Depovere, T. Kalker, J.-P. Linnartz, "Improved watermark detection using filtering before correlation", Proceedings of the 5th IEEE Conference on Image Processing, pp. 430-434, 1998.

[12] J.J.K. O Ruanaidh, S. Pereira, "A secure robust digital image watermark", Electronic Imaging: Processing, Printing, and Publishing in Colour, SPIE Proceedings, May 1998.

[13] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34

[14] Batra Sudhir, Rishi Rahul, Yadav Rajkumar, "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, July 2010.

[15] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, "A new Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.

[16] Potdar, V., and Chang, E., *Gray Level Modification Steganography for Secret Communication*. IEEE International Conference on Industrial Informatics, Berlin, Germany, 2004.

[17] Chandramouli, R., Memon, N.D., "Steganography capacity: A steganalysis perspective", Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, 2003.

[18] Pal, S.K., Saxena, P.K., Muttoo, S.K., "Image steganography for wireless networks using the handmaid transform", International Conference on Signal Processing & Communications (SPCOM), 2004.

[19] Parvez M. T. and Gutub A., "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008-Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.

[20] Eugene T. Lin and Edward J. Delp, "A Review of Data Hiding in Digital Images", Video and Image Processing Laboratory (VIPER), Indiana.