International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 8, October - 2012

Title: Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images

AUTHOR:

Mr. Rohit Garg

M-Tech Scholar

MMEC, Mullana University, Mullana

CO-AUTHOR:

Mr. Tarun Gulati

Assistant Professor

MMEC, Mullana University, Mullana

ABSTRACT:

Steganography is the practice of hiding one piece of information inside of another. The most common example is watermarking. Art and science of covering information in such a way that its presence is unnoticed. It comes from the Greek word steganos (covered) and graptos (writing), literally covered writing, in the sense of a hiding message. In Steganography the text or image in question is invisible although it resides in the interior of an apparently normal piece of other information, like a text, an image or a soundtrack unlike cryptography where the message is clearly visible although you need the key to decipher it , in this case the information cannot be seen unless the correct procedure is applied to the text or image where it resides. Computer files (image, sound recordings, even disks) contain unused or insignificant areas of data. Steganography take advantage of these areas, replacing them with information. Steganography has long been in use, even before the invention of the computer. Nowdays, messages are typically hidden within digital images, videos and audio. This paper focuses on two techniques, Least Significant Bit (LSB) and Most Significant Bit (MSB), Embedding using digital images as a medium. The terminology is that a message is hidden within a cover image to produce a stego-image.

Introduction:

Since the rise of the internet one of the most important factors of information technology communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep existence of the message secret. The technique used to implement this is called Steganography.

Steganography is the art and science of invisible communication. This is accomplishing through hiding information in their information, thus hiding the existence of the communicated information. The word Steganography is derived from the Greek word “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”.The goal of Steganography is to hide the data from

a third party. Generally message will appear to be something else: images, articles, shopping lists, or some other cover text and classically, the hidden message may be in invisible ink between the visible lines of a private letter.

Steganography can also be used to allow communication within an underground communication. Throughout history Steganography has been used to secretly communicate information between people.

Examples:

1. During World War 2 invisible ink was used to write information on piece of paper so that the paper appeared to the average person as just being blank piece of paper.
   Liquids such as urine, milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye.

2. In Ancient Greece they used to select messengers and shave their head they would then write a message on their head. Once the messages have been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secret message.

METHODS OF HIDING DATA IN DIGITAL IMAGES:

There are two types of methods in digital images:-

1. **Least Significant Bit (LSB)**
   Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit of some of all of the bits inside an image is changed to a bit of a secret message. When using 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a bit. LSB makes use of BMP images, since they use loss less compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image. Now days, BMP images of 800*600 pixels are not often used on the Internet and might arouse suspicion. For this reason, LSB Steganography has also been developed for use with other image file formats.

2. **Most Significant Bit (MSB)**
   In computing, the most significant bit (msb, also called the high-order bit) is the bit position in a binary number having the greatest value. The msb is sometimes referred to as the left-most bit due to the convention in positional notation of writing more significant digits further to the left. The MSB can also correspond to the sign of a signed binary number in one or two's complement notation. "1" meaning negative and "0" meaning positive.It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in $2^{31}..2^{0}$). Although a few CPU manufacturers assign bit numbers the opposite way (which is not the same as different endianness), the *msb* unambiguously remain the *most* significant bit. This may be one of the reasons why the term *msb* is often used instead of a bit number, although the primary reason is probably that different number representations use different numbers of bits. By extension, the most significant bits (plural) are the bits closest to, and including, the MSB.

Objective:

- To study various security techniques used in case of images.
- How LSB Steganography is inserting secret message in Least Significant bit of the pixel of image.
- How MSB Steganography is inserting secret message in Most Significant bit of the pixel of image.
- Finally, to find out the comparison between the results of LSB & MSB in terms of MSE(Mean Square Error) & PSNR(Peak Signal to Noise Ratio).

Methodology used:

Programming in MATLAB and simulation

- MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language developed by Math Works.
- It allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, and Fortran.
- This is especially helpful to solve problems with matrix and vector formulations.
- An image is nothing but a matrix or set of matrices which define the pixels value of the image, such a grey scale value in black and white images, and Red, Green and Blue or Hue, Saturation and Intensity values in color images.

❖ Algorithm of LSB Based Steganography:

Algorithm to embed text message using Grayscale Image

Step 1: Read the cover image & text message, which is to be hidden in the cover image.

Step 2: Convert text message into binary.

Step 3: Calculate LSB of each pixel of cover image.

Step 4: Replace LSB of cover image with each bit of secret message one by one.

Step 5: Write stego image.

❖ Algorithm of LSB Based Steganography:

Algorithm to retrieve text message using Grayscale Image

Step 1: Read the stego image.

Step 2: Calculate LSB of each pixel of stego image.

Step 3: Retrieve bits & convert each 8 bit into character.

Step 4: Calculate MSE & PSNR.

❖ Algorithm of MSB Based Steganography:

Algorithm to embed text message using Grayscale Image

Step 1: Read the cover image & text message, which is to be hidden in the cover image.

Step 2: Convert text message into binary.

Step 3: Calculate MSB of each pixel of cover image.

Step 4: Replace SB of cover image with each bit of secret message one by one.

Step 5: Write stego image.

❖ **Algorithm of MSB Based Steganography:**

Algorithm to retrieve text message using Grayscale Image

Step 1: Read the stego image.

Step 2: Calculate MSB of each pixel of stego image.

Step 3: Retrieve bits & convert each 8 bit into character.

Step 4: Calculate MSE & PSNR.

Formulae to find MSE & PSNR:

In case of Grayscale Images

- MSE = sum(sum(sum((I-O).^2)))/double(256*256*1)
- PSNR =10* log(255*255/MSE)

Results of LSB Based Steganography:

Original Image Stego Image

MSE between both images is 0.4939

PSNR between both images is 117.879

Results of MSB Based Steganography:

Original Image Stego Image

MSE between both images is 228.5034

PSNR between both images is 55.610

Related Work:

- In **2010**, Shreelekshmi R, M Wilscy presented a paper "Preprocessing Cover Images for More Secure LSB Steganography". In this paper they discussed a transformation method for cover images for increasing the reliability of LSB replacement steganography in spatial domain.

- In **2010**, Dr. Ekta Walia, Payal Jain and Navdeep presented a paper "An Analysis of LSB & DCT based Steganography". In this paper, they analyzed the two different schemes of steganography first was the least significant bit (LSB) based image steganogaphy and second the discrete cosine transform (DCT) based image steganography.

- In **2009**, Mamta Juneja, Parvinder S. Sandhu & Ekta Walia presented a paper "Appliaction of LSB Based Steganography Technique for 8- bit Color Images". In this paper, they describe a technique to successfully embed data in 8- bit color image.

- In **2008**, Hasan Mathkour and Batool Al-Sadoon presented a paper "A new image Steganography Technique". In this paper, they investigated diverse steganography techniques and tools.

- In **2006** "Implementation of LSB Steganography and Its Evaluation for various Bits" was presented by Deshpande Neeta, Kamalapur Snehal and Daisy Jacobs. They have presented hidden message in LSB, i.e, the eight bit inside picture pixel was changed to message bit.
- In **2004** Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon presented a paper "Image Steganography: Concepts and Practice" the main goal of steganography is to communicate securely in a completely undetectable manner. In this paper, they discussed security and capacity of the secret message in the image. They used two approaches, technique specific or universal steganalysis.

- In **2001** Jessica Fridrich, Miroslav Goljan and Rui Du State, presented a paper "Detecting LSB steganography in Color and Gray-scale Image". In this paper they discussed reliable and accurate method of detecting least significant bit (LSB) in the digital image.

Conclusion:

LSB & MSB based steganography hide the text message in LSB & MSB of cover image respectively. In this, I have found the MSE & PSNR in both cases. MSE & PSNR show the quality of the image

after hiding the message. In this, I have concluded that LSB based steganography is much better than MSB based steganography for hiding the message.

References:

[1] Mamta Juneja, Parvinder S. Sandhu and Ekta Walia, " Application of LSB Based Steganographic Technique for 8- bit Color Images", PWASET Volume 38 February ISSN, 2070- 3740, 2009.

[2] Edward Neuman, '' MATLAB Tutorials", Department of Mathematics, Board of Trustees, Southem Illinois University, Last Updated Friday, April 3, 2009.

[3] Beenish Mehboob and Rashid Aziz Faruqui, "A Steganograhy Implementation", IEEE International Symposium on Biometric & Security Technologies, ISBAST 08, 23-24, Islamabad, pp.1-5, April 2008.

[4] Hassan Mathkour and Batool Al- Sadoon, "A New Image Steganography Technique", Digital Object Identifier, version 11-18, pp. 1-4, 2008.

[5] J.C. Judge, "Steganography: Past, Present, Future", SANS white paper, 2001, http://www.sans.org/rr/papers/index.php?Id=552, 2006.

[6] Leo Lee, "LSB Steganography Information within Information", Computer Science, Section 2, April 5, 2004, http://www.cs.sjsu.edu/faculty/stamp/cs256/projects/spro4/.../Lee.doc.

[7] Deshpande Neeta, Kamalapur Snehal and Daisy Jacobs, "Implementation of LSB Steganography & Its Evaluation for Various Bits", University of Pretoria, South Africa, ISBN, Version: 07-06-04, pp. 173- 178, 2004.

[8] J.R. Krenn, "Steganography and Steganalysis", January 2004, http://www.krenn.nl/univ/cry/steg/article.pdf.

[9] K. Sullivan, O. Dabeer, U. Madhow, B.S. Majnunath and S. Chandrasekaran, " LLRT Based Detection of LSB Hiding", submitted to ICIP 2003.

[10] O. Dabeer, K. Sullivan, U. Madhow, B.S. Majnunath and S. Chandrasekaran, "Detectio of Hiding in the Least Significant Bit", Proceedings of CISS, 2003.