Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparison of LSB and MSB Based Image Steganography

Kanika Anand
ECE
SDDIET(KUK), Barwala,
Panchkula, India

Er. Rekha Sharma
ASSIT. PROFF. ECE
SDDIET(KUK), Barwala,
Panchkula, India

Abstract:- ***Steganography is an art of communication that hide the secret (i.e. message, information or communication in any form) data over a public channel. Hiding the occurrence of communication can be done by superimpose a secret message into cover message (i.e. an stego image) which the sender and the receiver can suspect only but third party cannot suspect the secret message. Therefore, in order to protect the secret messages from the third party there are many algorithms to hide the secret message. The algorithms are very complex i.e., number of steps are too much in the algorithm previously proposed but the value of PSNR is still less by that method. Now the proposed algorithms used for implementing the LSB based Steganography & MSB based Steganography for both gray scale and color images reduces the complexity and also indicate which one is better on the basis of BER and PSNR.***

Keywords:-LSB, MSB, STEGANOGRAPHY, Cryptography, BER, PSNR

I. INTRODUCTION

Cryptography was created as a technique for securing the secrecy of communication many different methods have been developed to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret but may also be necessary to keep the existence of the message secret. The technique used to implement this, is called Steganography..

Steganography can also be used for illegitimate reasons. For instance if someone was trying to steal data ,they could conceal it in another file or files and send it out in an innocent looking email or file transfer. Furthermore a person with a hobby of saving pornography, or worse, to their drive, may choose to hide the evidence through the use of Steganography. And, as was pointed out in the concern for terroristic purposes, it can be used as a means of covert communication.

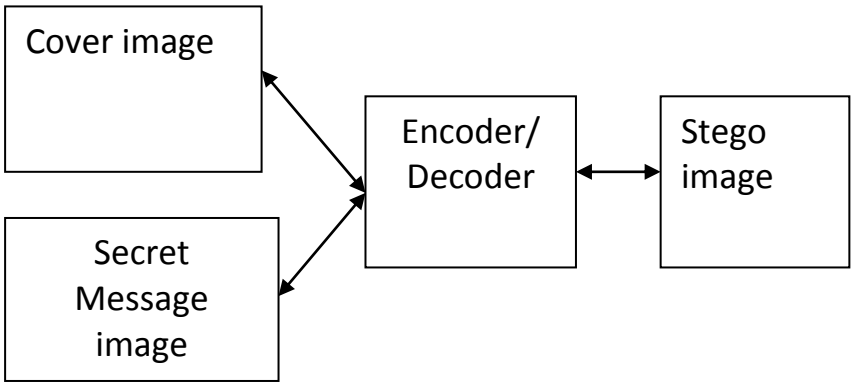

Figure1.Steganography

COVER IMAGE:-This is a real image in which we hide the secret message.
SECRET MESSAGE: - contains the message which wants to transfer.
STEGO OBJECT: - Combination of COVER IMAGE and SECRET MESSAGE.

Steganography differs from cryptography in the sense way where cryptography only keeping the contents of a message secret , Steganography and cryptography are both ways to protect information from unwanted parties or third party but neither technology alone is perfect.

1.1 Steganography techniques

Steganography (a rough Greek translation) has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. The exploration of steganography from its earliest instances through potential future application is defined by the Steganography techniques and these techniques are classified as:

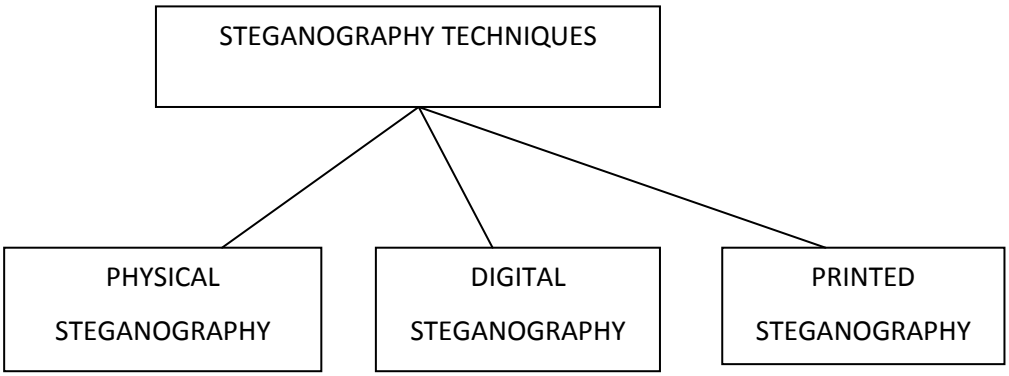

Figure 2 Types of Steganography

1.1.1 Physical steganography

Steganography has been widely used including recent historical time and the present day. Possible permutations are endless and known examples include:

- Hidden messages within wax tablets: in ancient Greece, people wrote messages on the wood, and then covered it with wax upon which an innocent covering message was written.
- Hidden messages on messenger's body: also in ancient Greece.
- Hidden messages on paper written in secret inks, under other messages on the blank part of other messages.
- Messages written in Morse code on knitting yarn.

1.1.2 Printed steganography

Digital steganography output may be in the form of printed documents. A message, the plaintext, may be first encrypted by traditional means, producing a cipher text. Then, an innocuous converted is modified in some way to as to contain the cipher text, resulting in the stego text. For example, the letter size, spacing, typeface, or other characteristics of a cover text can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. Francis Bacon developed bacon's cipher as such a technique.

1.1.3 Digital steganography

Modern Steganography entered the world in 1985 with the advent of the personal computer applied to classical steganography problems. Development following that was slow, but has since taken off, going by the number of steganography program available: the Steganography Analysis and research Centre have identified over 725 digital steganography applications. Digital Steganography techniques include:

- Concealing message within the lowest bits of noisy images or sound files.
- Concealing data within encrypted data. The data to be concealed is first encrypted.
- Chaffing and winnowing.
- Pictures embedded in video material (optionally played at slower or faster speed).
- Content- Aware Steganography hides information in the semantics a human user assigns to a data gram. These systems offer security against a non- human adversary/warden.

1.1.3(a) Least Significant Bit (LSB) It is a common, simple approach to embedding information in a cover image[1]. The least significant bit (in other words, the 8^{th} bit) of some or all the bits inside an image is changed to a bit of the secret message the technique for increased capacity of information hiding in LSB's method gives better performance in all the parameters and is a safe technique for embedding secret messages.[3]

For example a grid for 3 pixels of a 24- bit image can be follows:-

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is embedded into the Least Significant Bit of this part of the image, the resulting grid is as follows:

(00101101 0001110**0** 01011110)
(10100110 1110010**0** 00001100)
(11011010 1010110**1** 01101011)

Although the number was embedded into the first 8 bits of the grid, only the 3 underlines bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [2]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the color. In its simplest form LSB makes use of BMP images, since they use lossless compression[7].

1.1.3(b) Most significant bit(MSB):- It is a common, simple approach to embedding information in a cover image. The most significant bit (in other words, the 1st bit) of some or all the bits inside an image is changed to a bit of the secret message. For example a grid for 3 pixels of a 24- bit image can be follows:-

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is embedded into the Least Significant Bit of this part of the image, the resulting grid is as follows:

(0**0**101101 **0**0011100 01011110)
(1**1**100110 **1**1100100 00001100)
(1**0**011010 **1**0101101 01101011)

Although the number was embedded into the first 8 bits of the grid, only the 5 underlines bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color, changing the MSB of a pixel results in small changes in the intensity of the color. The human eye cannot perceive these changes thus the message is successfully hidden.

1.2 Uses of Steganography

Steganography can be used anytime we want to hide a data. There are many reasons to hide data but they reach to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention.

Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Steganography takes advantage of these areas, replacing them with information (encrypted mail for instance). Steganography has long been in use, even before the invention of the computer. For example, warning nations used invisible ink and macro dots to communicate message covertly. However, computer technology has been Steganography to the next level.

II. PROPOSED METHODOLOGY

The proposed methodology covers this basic approach used for implementing the LSB based Steganography & MSB based Steganography for both gray scale and color images. The first major challenge is to find out the comparison between LSB & MSB based Steganography methods and to check which method is better and the second one is to

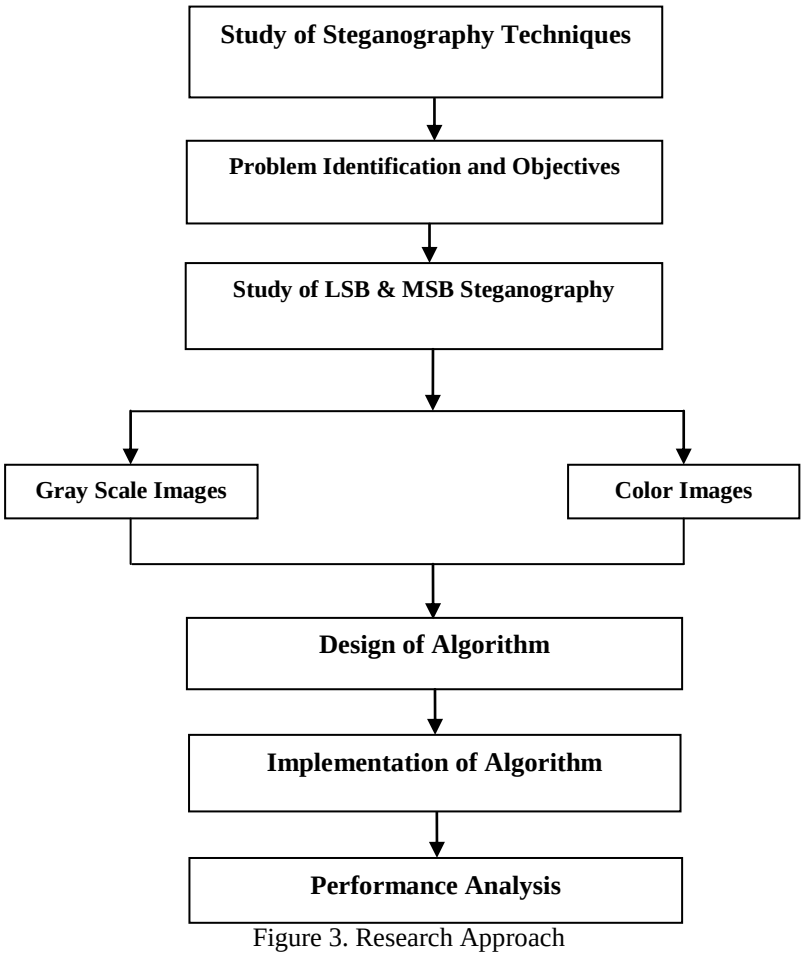

Figure 3. Research Approach

reduce the computational complexity of the algorithm. The solution to check whether LSB Based Steganography is better or MSB based Steganography is better depends on the values of Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). So the main solution is to find the value of Mean Square Error (MSE) as lowest as possible & Peak Signal to Noise Ratio (PSNR) as much as possible to show the good quality of the stego image and to check which method is better.

III. CONCLUSION

In this a data hiding method by improved LSB substitution & MSB substitution process is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity. A good balance between the security and the image quality is achieved. This method is applicable on both gray scale & color images. . Experimental results show the effectiveness of the proposed method. The results obtained in my result paper also show significant improvement in PSNR than the method proposed in Ref. [8] with respect to image quality and computational efficiency & also in MSE.It has also been concluded that LSB based Steganography is better than MSB based Steganography on the basis of values of MSE & PSNR as shown by the experimental results due to too much difference in the original image and the stego image in case of MSB based Steganography.

REFERENCES

[1] *S. Lekshmi R, Wilscy. M and C.E. Veni Madhavan, "*Improving the Reliability of Detection of LSB Replacement Steganography", International Journal of Network Security & its Applications (IJNSA), Vol. 2, no. 4,pp. 247- 254, October 2010.

[2] *S. Gupta, G. Gujral and N. Aggarwal*, "Enhanced Least Significant Bit Algorithm for Image Steganography", International Journal of Computational Engineering & Management, Vol. 15, pp. 40- 42, July 2012.

[3] *H.B. Kekre, D. Mishra, R. Khanna, S. Khanna and A. Hussaini,*"Comparison between the basic LSB Replacement Technique & Increased Capacity of Information Hiding in LSB's Method for Images", International Journal of Computer Applications, Vol. 45, no. 1, pp. 33- 38, May 2012.

[4] *A. Asthana, S. Joshi*, "An Adaptive Steganography Technique for Gray & Colored Images", International Journal of Advanced Research in Computer science & Software Engineering, Vol. 2, pp. 41- 45, May 2012.

[5] *I. Diop, S.M Farssi, O. Khouma, H.B Diouf, K. Tall and K. Sylla*, " New Steganographic Scheme based of Reed-Solomon Codes", International Journal of Distributed and Parallel Systems, Vol. 3, no. 2, pp. 81- 89, March 2012.

[6] *A. Agarwal, A.K. Vasta*, "A Novel Steganography Technique for Gray and Colored Images", Journal of Global Research in Computer Science, Vol. 3, no. 3, pp. 24- 28, March 2012.

[7] V. Tyagi, A. Kumar, R. Patel, S. Tyagi and S. Singh Gangwar, "Image Steganography Using Least Significant Bit with Cryptography", Journal of global Research in Computer Science, Vol. 3, no. 3, pp. 53- 55, March 2012.

[8] V.K. Sharma and V. Shrivastava, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimizing detection", Journal of Theoretical and Applied information Technology, Vol. 36, no. 1, pp. 1- 8, Feb 2012.

