

Enhanced Least Significant Bit algorithm For Image Steganography

Shilpa Gupta¹, Geeta Gujral² and Neha Aggarwal³

¹ Department of computer science, Manav Rachna College of Engineering
Faridabad, India
dear.sanva@gmail.com

² Department of computer science, Manav Rachna College of Engineering
Faridabad, India
geetagujral.mrce@mrei.ac.in

³ Department of computer science, Manav Rachna College of Engineering
Faridabad, India
aggarwal.neha83@gmail.com

Abstract

The rapid development of data transfer through internet has made it easier to send the data accurate and faster to the destination, but in order to transfer the data securely to the destination without any modifications, there are many approaches like steganography. This paper introduces the concept of steganography using a new Algorithm “Enhanced LSB Algorithm”, which has negligent distortion as compared to the Least Significant Bit Algorithm.

Keywords: Carrier Image, Enhanced Least Significant Bit, Image Steganography, Information Hiding, Least Significant Bit, Steganography

1. Introduction

The word ‘Steganography’ comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and thus means, literally, covered writing. It is a data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. The goal of steganography is to hide messages inside the images in such a way that does not allow any “enemy” to even detect that there is a secret message present in the image. Steganography attempts to hide the existence of communication [1]. The basic structure of Steganography is made up of three components:

- i. The Carrier image,
- ii. The Message,
- iii. The Key

The carrier can be a painting, or a digital image. It is the object that will ‘carry’ the hidden message. A key is used to decode/decipher/discover the hidden message. This can

be anything from a password, a pattern, a black-light, or even lemon juice.

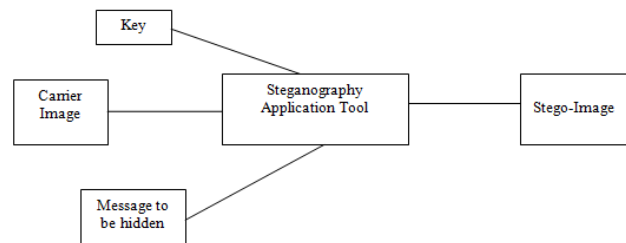


Fig 1. Block Diagram of Steganography

2. LEAST SIGNIFICANT BIT TECHNIQUE

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP's or possibly another image format such as GIF [2]. The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components. Suppose that we

have three adjacent pixels (9 bytes) with the RGB encoding [7]

```
10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011
```

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

```
10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010
```

Here the number 300 was embedded into the grid, only the 5 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.

1) Least Significant Bit Algorithm
ALGORITHM 1

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in RGB component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
4. After that Message is hidden using Bit Replacement method.

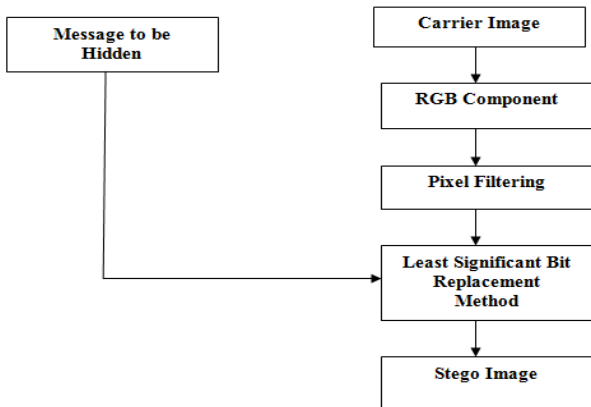


Fig 2. Algorithm of Least Significant Bit

From 4 to 6 keywords should follow the abstract (as a subheading

3. PROPOSED WORK

ENHANCED LEAST SIGNIFICANT BIT TECHNIQUE

LSB algorithm hide information in the least significant bit of each color i.e. RGB of the carrier image. The problem states from the fact that modifying the three colors of a pixel produces a major distortion in the resulting color. So the one method that would introduce more efficiency and less distortion is Enhanced Least Significant Bit.

Enhanced LSB algorithm works in the spatial domain. It improves performance of LSB by hiding information in only one of the three colors that is blue color of the carrier image.

2) Enhanced Least Significant Bit Algorithm
ALGORITHM 2

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in Blue component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Enhanced Least Significant Bit (ELSB) of every pixel to hide information, leaving most significant bits (MSB).
4. After that Message is hidden using Bit Replacement method.

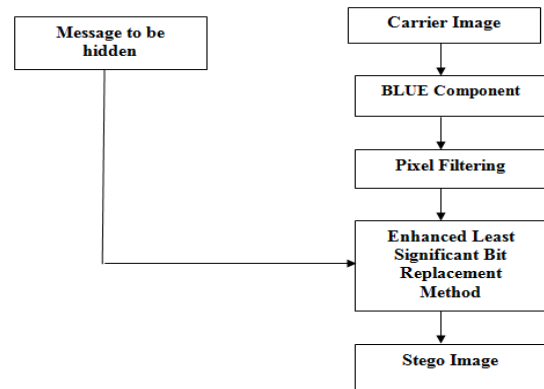


Fig 3. Algorithm of Enhanced Least Significant Bit

4. CONCLUSION

In this paper the existing Least Significant Bit Algorithm has been analyzed and found to have a more amount of distortion, so a new method has been proposed "Enhanced Least Significant Bit (ELSB)". It improves the performance of the LSB method because information is hidden in only one of the three colors that is BLUE color of the carrier image. This minimizes the distortion level which is negligent to human eye.

Comparative Analysis of Least Significant Bit and Enhanced Least Significant Bit Encoding Technique

If a pixel of the cover image with the RGB (Red-Green-Blue code) color A8A8A8 # is used, binary

10101000-10101000-10101000 to hide the message 111, the result would be (10101001-10101001-10101001):

Results obtained hiding the message 111 in the pixel 10101000-10101000-10101000 with the LSB method

Table 2: Results with LSB method

	Hexadecimal	Decimal	Red	Green	Blue
Original pixel	A8A8A8	11053224	168	168	168
Modified pixel	A9A9A9	11119017	169	169	169

The three least significant bits of the pixel have changed, introducing a small distortion, but the difference between the old and new color represents a leap of 65793 colors in the scale of colors.

Enhanced LSB method that would introduce more efficiency and less distortion would store the 3 bits of information to hide in the same color. Using the same example, the 3 bits of information will be introduced in the 3 LSB bits of blue color

(10101000-10101111-10101111):

Results obtained hiding the message 111 in the pixel 10101000-10101000-10101000 with the ELSB method:

Table 2: Results with ELSB method

	Hexadecimal	Decimal	Red	Green	Blue
Original Pixel	A8A8A8	11053224	168	168	168
Modified Pixel	A8A8AF	11053231	168	168	175

In this case the leap in the scale of colors is 7.

References

- [1] K.B.Raja, C.R.Chowdary, Venugopal K R, and L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Department of Computer Science Engineering, Bangalore 2005 IEEE
- [2] V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011)
- [3] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images" World Academy of Science Engineering, and Technology 50 2009

- [4] H. Yang, X. Sun, G. Sun. "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution". Journal: Radio engineering Year: vol. 18, 4Pages/record No.: 509-516, 2009.
- [5] Shashikala Channalli and Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE vol. 1, no.3 2009.
- [6] S. Venkatraman, A. Abraham, M. Paprzycki, "Significance of Steganography on Data Security", International Conference on Information Technology: Coding and Computing (ITCC'04), 5-7 April 2004.
- [7] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, June/July 2005

Shilpa Gupta is pursuing her M.Tech, final year (computer Science and Engineering) degree from Manav Rachna College of Engineering, Maharishi Dayanand University. Her areas of interest are steganography, cryptography

Geeta Gujral received M.Tech (Computer Science and Engineering) degrees with Hons. from Maharishi Dayanand University in 2009. Presently, she is working as an Assistant Professor in Computer Science and Engineering Department in Manav Rachna College of Engineering, Faridabad. Her areas of interest are Ad-Hoc Networks, steganography

Neha Aggarwal is pursuing her M.Tech, final year (computer Science and Engineering) degree from Manav Rachna College of Engineering, Maharishi Dayanand University. Her areas of interest are data mining, clustering, steganography.