RESEARCH ARTICLE OPEN ACCESS

Steganography Scheme Based on LSB Embedding Technique with Different Image Format

Mrs. Aparna Singh Kushwah, Ruchika Daharwal
Assistant Professor Electronics and Communications Department UIT-RGPV, Bhopal
Student Assistant Professor Electronics and Communications Department UIT-RGPV, Bhopal
Corresponding auther: Mrs. Aparna Singh Kushwah

ABSTRACT: To increase the security of messages sent over internet steganography is used. Various steganography techniques have been proposed so far. Least Significant Bit steganography is one such technique in which least significant bit of pixels of the image is replaced with data bits. This approach has the advantage that it is simplest one to understand, easy to implement and results in stego-images that contain embedded data as hidden. The disadvantage of Least Significant Bit is that it is vulnerable to stego analysis and is not secure at all. So as to make it more secure, the least significant bit algorithm is modified to work in different way.
The proposed method performs a selection of suitable direction for secret byte embedding so as to minimize the bit changes in the cover image when a secret data is embedded. This paper reports a new algorithm for LSB (Least Significant Bit) replacement based image steganography for RGB color images. The directional aspects of embedding data are explored to develop an improved LSB embedding technique.
Keywords: Cover Image, Secret Message, LSB Technique, Different Format

Date of Submission: 18-06-2018 Date of acceptance: 03-07-2018

I. INTRODUCTION

Steganography is the process of hiding information into an object such that informal eyes can neither identify the meaning of hidden message nor even recognize its existence. Hiding messages or information techniques are gaining much attention today. This is largely due to the fear of encryption services getting outlawed and the owners who want unauthorized access to information [1]. With the advancement in computing technology, the need for private and personal communication has increased. To provide security to messages, steganography is one such technique [2]. There are many ways to hide information in digital images that is what is called steganography, such as Least Significant Bit, Masking and filtering, algorithms and transformations [3]. Out of these, least significant bit scheme is the most common technique used in steganography. This works exactly in the same way its name sounds like; the significant bits of cover image are altered so that information can be embedded within it [4]. To the human eye, changes in the values of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object [5]. As more number of least significant bits of a pixel are used to hide information, it generated distortion to the cover image.

II. RELATIVE WORK

There have been a large number of embedding techniques proposed in the literature which generally falls either in the category of Spatial Domain or Transform Domain [6] Embedding. These techniques work on difference approaches on cover image with different constraints but with the same objective of securing and maximizing hidden data. In Spatial Domain methods, approach is used on the principle of tuning the parameters of the cover-image so that the difference between cover-image and the stegoimage is little and imperceptible to the human eye. One of the reasons of acceptability of these kinds of approaches is simple algorithmic nature and ease of mathematical analysis [7]. The most widely known image based on modifying the least significant bit (LSB technique). As the resolution and depth of color increase in an image, the impact of manipulating the LSB becomes less noticeable. Hence high resolution images are preferred for use as cover-images. On the other hand, there are number of transform embedding approaches which includes Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [7]. Irrespective to the domain, transform coefficients are selected to mix with the secret data so that information is not visible to human eye.

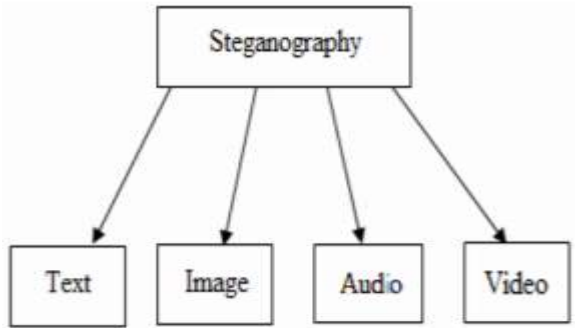

Figure 1: Ways to achieve Steganography

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of text elements. Hiding secret messages in text can be a very challenging task because the text files contains very little redundant data that can be replaced with secret message and therefore reliable decoding and minimum visible change are somewhat conflicting [8]. Most common types of text steganography are Line-Shift Coding, Word-Shift Coding and Feature Coding [8]. Image steganography is the most popular technique being used in digital world of today. This is because of limited power of human visual system. Any kind of text whether it is plain text or cypher text or an image itself can be hidden inside a cover image. An image consists of hundreds of colors pixels and an increase or decrease in the brightness of colors by one or two points does not make much difference to a human eye. Most common steganography is Least Significant bit apart from masking and filtering techniques. Audio Steganography is the way of hiding secret message in which secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file [8]. Human Auditory System (HAS) is unable to differentiate among sounds that vary a very little when compared among themselves and this weakness is exploited to encode secret messages in audio without being detected. Most common audio steganography techniques are LSB Coding, Phase Coding, Echo Hiding and Spread Spectrum [8]. Before choosing an encoding technique for audio, two things need to be considered that are the digital format of the audio and transmission media of the audio.

III. LSB (LEAST SIGNIFICANT BIT)

LSB technique is implemented in spatial domain. The technique converts image into shaded Gray Scale image. This image will be act as reference image to hide the text. Using this grey scale reference image any text can be hidden. Single character of a text can be represented by 8-bit. If the reference image and the data file are transmitted through network separately, we can achieve the effect of Steganography. Here the image is not at all distorted because said image is only used for referencing. Any huge amount of text material can be hidden using a very small image. Decipher the text is not possible intercepting the image or data file separately. So, it is more secure. In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to stegano-analysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains - for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today. From one of our reference paper we found that in LSB steganography, to conceal the message the least significant bits of the cover media's digital data are used. The useful feature of the LSB steganography techniques is LSB replacement that makes LSB stegnography as simple. To reflect the message it needs to be hidden, LSB replacement steganography flips the last bit of each of the data values.

Consider an 8-bit gray scale bitmap image where each pixel is stored as a byte. And it also representing in a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

The letter C whose binary value is 1000001. To hide this binary value it can replace the LSBs of these pixels to have the following new gray scale values:

11010011
01001010
10010110

IV. PROPOSED METHODOLOGY

Cover-Image: An image in which the secret information is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc. The cover image is sometimes called as the "host".

Stego-Image: The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

Payload: The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

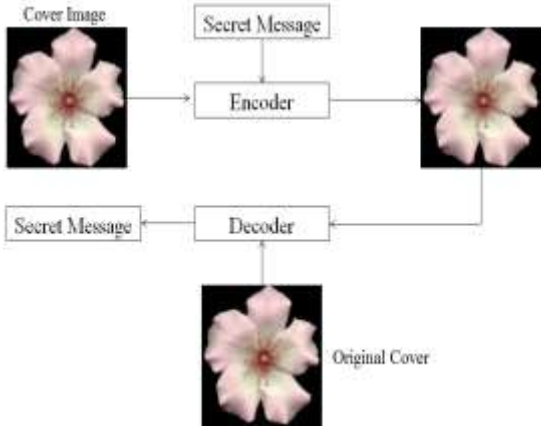

Figure 2: Flow Chart of Proposed Methodology

This technique works best when the file is longer than the message file and if image is grayscale.

When applying LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

S(i, j) = C(i, j)-1, if LSB (C(i, j)) = 1 and SM = 0

S(i, j) = C(i, j)+1, if LSB (C(i, j)) = 0 and SM = 1

S(i, j) = C(i, j), if LSB (C(i, j)) = SM

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and "SM" id the next message bit to be embedded. S(i, j) is the Stego image.

The proposed method follows a directional embedding technique for achieving maximum image quality in the stego image. The proposed method performs a selection of suitable direction for secret byte embedding so as to minimize the bit changes in the cover image when a secret data is embedded.

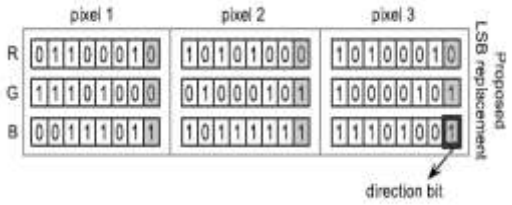

Figure 3: LSB embedding of the byte 11110000 in the cover image using the proposed method.

As you can see in Fig. 3, the byte 11110000 is embedded in a reverse order (00001111) in the original cover image for minimizing the number of alterations. Here also, we take three consecutive pixels (say p1, p2 and p3) for embedding a byte of information. Firstly, the red channels of p1, p2 and p3 are replaced with secret bits, followed by their green and blue channels. A direction bit is added at the 9-th bit which indicates that the preceding data is in stored in a reverse order. A value for the direction bit indicates a normal forward direction of storing data while a value 1 for the direction bit indicates that the data is stored in reverse direction. It can be noted that the number of bit changes required is 8 whereas in the proposed method shown in Fig. 3 requires no bit alterations. Instead of using only one directional bit per byte of secret data, we can also integrate more directional bits to indicate more directions of storing secret data within the cover image. However, this would decrease the embedding capacity of the cover image.

V. SIMULATION RESULT

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language. A proprietary programming language developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[y(i,j)-x(i,j)]^2$$

$$PSNR = 10\log_{10}(L*L/MSE)$$

Figure 4: Open the Graphical User Interface (GUI) Window

Figure 5: Window for LSB Steganography

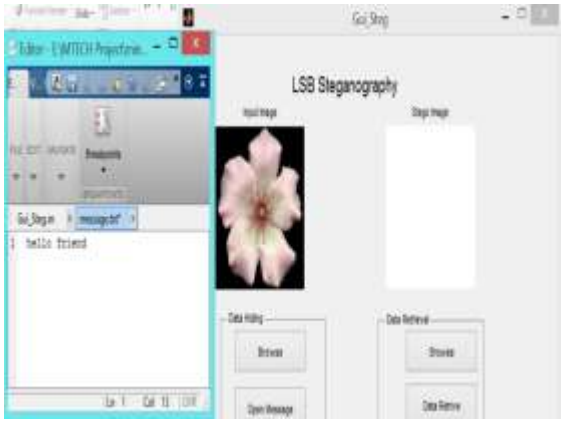

Figure 6: Window for Inter the Message

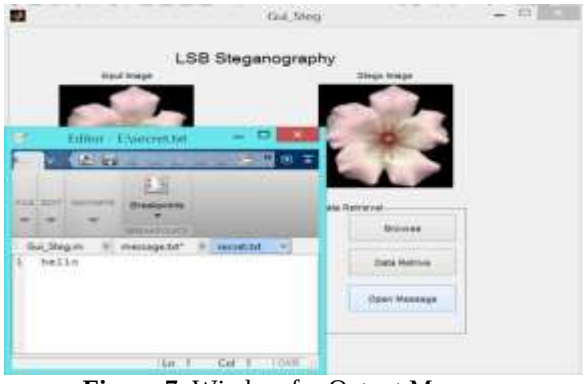

Figure 7: Window for Output Message

Table 1: Result for Different Image with 50 Characters

Image	**Image Type**	**Characters**	**Parameter**	
			MSE	PSNR
Flower Image	.jpg	50	0.0017	52.34 dB
Lena Image	.jpg	50	0.0014	53.54 dB
Building Image	.jpg	50	0.0012	53.98 dB
Tiger Image	.jpg	50	0.0014	52.89 dB

Table 2: Result for Different Image with 200 Characters

Image	**Image Type**	**Characters**	**Parameter**	
			MSE	PSNR
Flower Image	.bmp	200	0.0081	46.55 dB
Lena Image	.bmp	200	0.0084	46.01 dB
Building Image	.bmp	200	0.0092	46.21 dB
Tiger Image	.bmp	200	0.0090	45.88 dB

VI. CONCLUSION

As compared with the traditional Least Significant Bit algorithm, the data hiding steganography method presented in this paper was found to be of increased imperceptibility to stego analysis attacks on the cover image. Therefore, this method is best suited for the purposes of communication applications. The recommended mode of transmission of stego images is through email attachments or web postings.

The results indicate that the proposed method performs well especially when embedding secret data at higher LSB bit positions. There are few methods that try to improve the quality of stego image by embedding secret data only in the channels of least importance. The proposed method can also be combined with those methods but it would naturally result in a reduction in the embedding capacity.

REFRENCES

[1]. Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan, Usman Ali and Muhammad Naeem, "An Improved Image Steganography Technique based on MSB using Bit Differencing", Sixth International Conference on Innovative Computing Technology, IEEE 2016.

[2]. Ghazanfari, K., Ghaemmaghami, S., Khosravi, S. R., "LSB++: An improvement to LSB+

Steganography", TENCON IEEE Conference, Bali, pp. 364-368, IEEE 20111.

[3]. Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," IJMECS, Vol. 4, No. 6, pp. 27-34, 2012.

[4]. Jianhong Sun, Yingjiang Li, Xiaohui Zhong, Junsheng Li, "A Scheme of LSB Steganography Based on Concept of Finding Optimization Pixels Selection," Software Engineering and Knowledge Engineering: Theory and Practice Volume 115, pp. 155-160, 2012.

[5]. A. D. Ker, "Steganalysis of LSB matching in grayscale images," Signal Processing Letters, IEEE, Vol. 12, Issue 06, pp. 441- 444, 2005.

[6]. Lee Y.K., B. G., "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding," Advances in Image and Video Technology, Springer Berlin Heidelberg, 2010, pp. 349-360.

[7]. Yambin Jina Chanu, Themrichon Tuithung, Kh Manglem singh, "A Short Survey on Image Steganography and Steganalysis Technique", IEEE 2012.

[8]. Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image," IEEE Trans. International Congress on Image and Signal Processing, pp. 252-255, IEEE 2012.

[9]. Masoud Nosrati, Ronak Karimi, Mehdi Hariri, "An introduction to steganography methods," World Applied Programming, Vol (I), No (3), ISSN: 2222-2510, August 201 I, pp. 191-195.

[10]. 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, 2009.

[11]. S. S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography," International Journal of Scientific & Technology, research Volume I, Issue 6, July 2012 ISSN 2277-8616 68 ijstr©20 12 www.ijstr.org.

[12]. Bing Song and Zhi-hong Zhang, "One improved LSB steganography algorithm," Proc. SPIE 8784, Fifth International Conference on Machine Vision (ICMV 2012): Algorithms, Pattern Recognition, and Basic Technologies, 87840V (March 13, 2013); doi: I 0.1117/12.2013923; http://dx.doi.org/10.1117/12.20 13923.

[13]. Yu Qiudong, X.-W. L., "A New LSB Matching Steganographic Method Based on Steganographic Information Table," Second International Conference on Intelligent Networks and Intelligent Systems, China, 2009, pp. 362 - 365.

[14]. YiYu x., Wang A., "Revisit LSB Matching," Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010, pp. 410--413.

Mrs. Aparna Singh Kushwah "Steganography Scheme Based on LSB Embedding Technique with Different Image Format "International Journal of Engineering Research and Applications (IJERA) , vol. 8, no.6, 2018, pp.71-75