Increase the Capacity Amount of Data Hiding to Least Significant BIT Method

Ghadah Al-Khafaji, Hazeem B. Taher, Nura Anwer Abdulzahara

Abstract- In this paper a new strategy to increase the number of bits hiding in each image for LSB method is suggested to give more data capacity with high secure stegano image. The technique of hiding a private message within a file in such a manner that third party cannot know the existence of matter or the hidden information. The purpose of Steganography is to create secrete communication between the sender and the receiver by replacing the least significant bits (LSB)of the cover image with the data bits depending on the type of the pixel class if it is edge then exchange two bits else one bit exchanged.

Keywords: Image steganography, text hiding, Least Significant Bit algorithm.

I. INTRODUCTION

In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Security has become a critical feature for thriving networks and in military alike. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect military messages, E-mails, credit card information, corporate data and personal files [1]. Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Today, thanks to modern technology, steganography is used on text, images, sound, signals, and more [2]. A good strategy to guarantee irrecoverability is to cover the secret data not using a trivial method based on a predictable algorithm, but using a specific random pattern based on a mathematical algorithm [3]. Steganography hides the very existence of the message by embedding it inside a carrier file of some type. An eavesdropper can intercept a cryptographic message, but he may not even know that a steganographic message exists. Cryptography and Steganography achieve the same goal via different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning [1]. Steganography includes the hiding of media like text, image, audio, video files. In another media of same type or of different type. Later the message hidden in the selected media is transmitted[4]. An *image* steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method.

Manuscript Received on June 2014.

Dr. Ghadah Al-Khafaji, Baghdad University, College of Science, Iraq.
Dr. Hazeem B. Taher, Thi-Qar University, College of science, Iraq.
Nura Anwer Abdulzahara,Thi-Qar University, College of Science, Iraq.

Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a *cover image* in steganography, and the message-embedded image is called a *stego image* [4]. Most of the algorithms that work in the spatial domain using a LSB method as the algorithm for information hiding, that is, hide one bit of information in the least significant bit of each color of a pixel.

II. PROBLEM DEFINITION

The aim of this paper is to hide the data over an image using least significant steganographic algorithm and to send the stego file to the destination where the retrieving of the secret data is done.

III. PROBLEM SOLUTION

The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of the project is modified the classic LSB method depending the edge detection concept as indication to increase the amount of data hiding in the same cover with high security level of transferring.

IV. EDGE DETECTION TECHNIQUES

Edge detection aims at identifying points in a digital image at which the image brightness changes sharply or more formally has discontinuities. Following edge detectors are handy:

1) Sobels Edge Detector - 3×3 gradient edge detector

2) Prewitt Edge Detector - 3×3 gradient edge detector.

3) Canny Edge Detector - non-maximal suppression of local gradient magnitude.

4) Zero Crossing Detectors - edge detector using the Laplacian of Gaussian operator. In this paper work we are using canny edge detector. This method was proposed by John F. Canny in 1986 [5]. Even though this method is quite old but is still used because of its precision in edge detection. The main advantage of this method is elimination of multiple responses to a single edge. It also having good localization property, means the detected edges are much closer to the real edges. The response of this detector is also good, as the original edge does not result in more than one detected edge. The Canny algorithm uses four filters (Kx , Ky , G, ϑ) to detect horizontal, vertical and diagonal edges in the blurred image as bellow:

$$K_x = \begin{matrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{matrix}$$

$$K_y = \begin{matrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{matrix}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

$$G = |K_x| + |K_y|$$

$$\vartheta = \arctan\left(\frac{K_x}{K_y}\right)$$

V. LSB METHOD

LSB (Least Significant Bit) steganography can be described as follows: if the LSB of the pixel value I(i, j) is equal to the message bit m to be embedded, I(i, j) remain unchanged; if not, set the LSB of I(i, j) to m. The message embedding procedure can be described using an Equation as follows;

$$I_s(x,y) = \begin{cases} I(x,y) - 1 & LSB(I(x,y) = 1 \; and \; m = 0 \\ I(x,y) & LSB(I(x,y)) = m \\ I(x,y) + 1 & LSB(I(x,y) \neq 0 \; and \; m = 1 \end{cases}$$

For example, if a pixel of the cover image with the RGB (Red-Green-Blue code) color is used, binary 10101000-10101000-10101000, and 1 bit with value 1 is set on each LSB bit of each color component, to hide the message 111, the result would be 10101001-10101001-10101001:

VI. PROPOSED ALGORITHM

The data hiding patterns using the steganographic technique in this project can be explained using the simple block diagram figure (1). In this section, algorithms for different processes used both in the sending side and receiver sides are described which are illustrated below:

A- Algorithm for message embedding

1- Read the secret data (message).
2- Convert the message to binary vector D.
3- Determine the length of the message m.
4- Read the cover image (carrier) I.
5- Apply the edge detection filter to produce edge image E.
6- Scan the edge image E to determine the number of place hiding in the original image (2 place for edge pixel and 1 place for background) T.
7- Compare if T≠m goto step 4 to read a new image.
8- Apply LSB technique, the LSBs of the pixel are changed depending on the pattern bits and secret message bits. If the E(i,j) is edge value then change 2-bit else change 1-bit.
9- Repeat step 8 untill all bits in d are exhausted.
10- Finally, the produced image (carrier) is sent to the receiver.

B- Algorithm for message extracting

1- Read the stego image (carrier) I.
2- Apply the edge detection filter to produce edge image E.
3- For each pixel of image I if the pixel value is edge then extract 2-bits else if it is background then extract 1-bit only.
4- Put the bits extracted in the vector.
5- Repeat step 3 for each of the stego pixels.
6- Convert the data extracted to character types.
7- Display the extracted message.

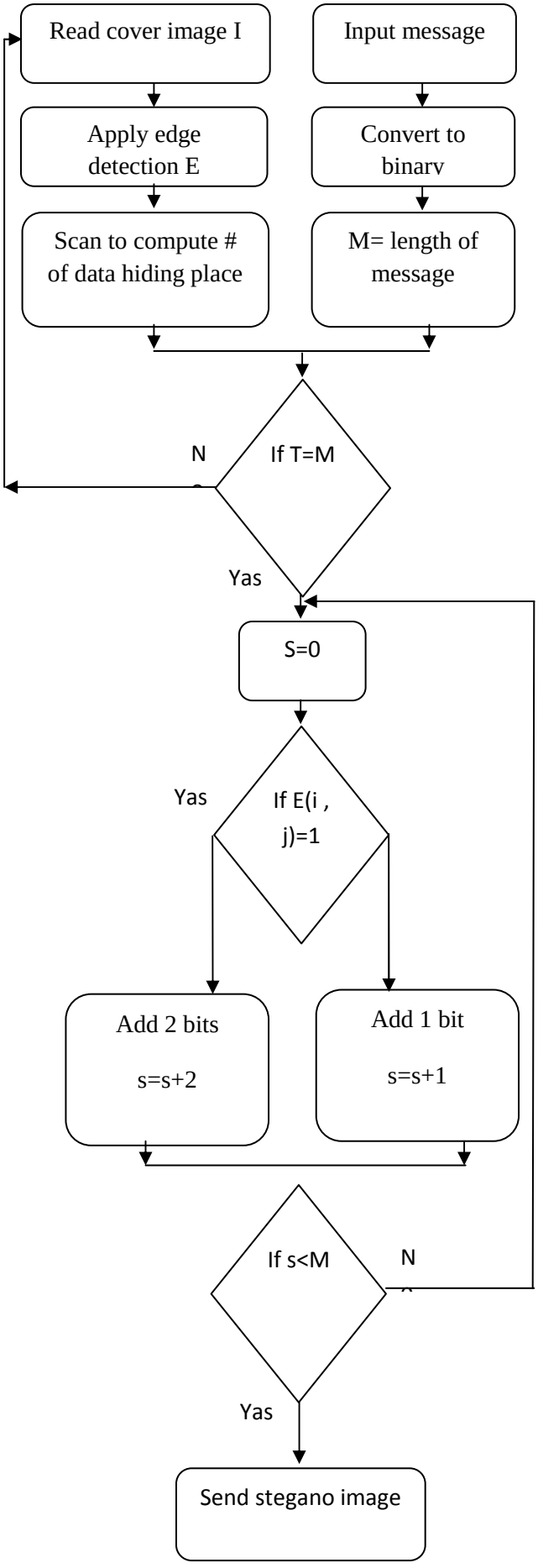


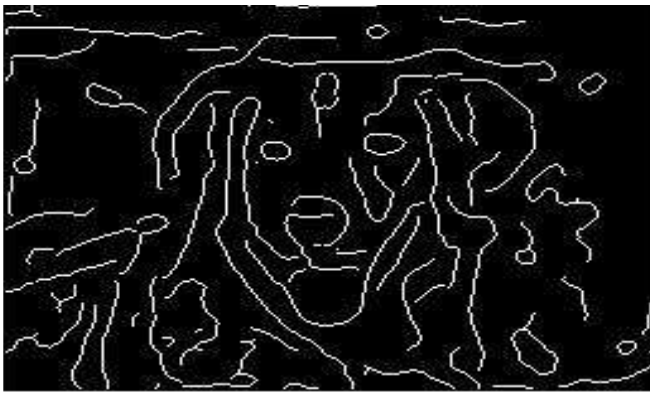
Figure (1) stegano digram.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

VII.EXPERIMENTAL RESULT

This section presents some of experimental results obtained. The figure 2 shows the original image(cover)that have size (194*259).Figure 3 shows the edge image and figure 4 shows the stegano image. The number of bits added increases by 2900 bits. Table 1 shows the value of data hiding for other images.

Figure(2) Original Image.



Figure(3) Edge Detection Image.

Figure(4) Stegano Image.

VIII. CONCLUSIONS

This paper proposed a new strategy to increase the number of bits that hiding in the carrier image depending on the type of the pixel is it edge or not. The number of bits stored in the edge pixel is more than the background pixel. Additionally, the high level of security is used because the distribution of the secret message bit is not striate.

REFRENCES

[1] S. Narayana1, G. Prasad, " Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions", Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010

[2] I. J. Kadhim, " A New Audio Steganography System Based on Auto-Key Generator", AL-Khwarizmi Engineering Journal, Vol.8, No.1, pp27-36, 2012.

[3] Y. Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications, Vol. 60, 4, December 2012.

[4] N. Jain, S. Meshram, S. Dubey, “Image Steganography Using LSB and Edge – Detection Technique". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[5] V. Saini1, R. Garg, " A Comparative Analysis on Edge Detection Techniques Used in Image Processing",IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN : 2278-2834 Volume 1, Issue 2 (May-June 2012), PP 56-59 www.iosrjournals.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.