International Journal of Engineering Research & Management Technology ISSN: 2348-4039
September-2015 Volume 2, Issue-5
Email: editor@ijermt.org www.ijermt

A New Method in Image Steganography

Diwakar Aggarwal[1], Deepika Sharma[2]
Student, CSE, MIT, Meerut, UP, India[1]
Faculty,CSE , MIT, Meerut,UP, India[2]

ABSTRACT:
"Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). In this paper, a new Steganography technique is presented, implemented and analysed. The proposed method hides the secret message based on searching about the non-identical bits between the secret messages and image pixels values. The proposed method is compared with the LSB benchmarking method. It is implemented to hide the secret message "Hello world" on two Bmp images, with size (128*128) and (298*298) respectively. The results of the proposed and LSB hiding methods are discussed and analyzed based on MSE and PSNR values. The proposed method is efficient, simple and fast it robust to attack and improve the image quality.

KEYWORDS: Steganography, Least Significant Bit, Bmp Image, Secret Information

1 **INTRODUCTION**:

"Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). However, in the hiding information the meaning of Steganography is hiding text or secret messages into another media file such as image, text, sound, and video.

Steganography ancient origins traced back to 440BC. It was started by the Greeks by shaving the slaves hair heads and writing the message on their heads, after the hair had been grown, they were sent to their allies in order to communicate with them without the enemies knowledge. As well as, the invisible ink used for hiding the secret messages by the American revolutionaries during the USA revolution. Also it was used in both world wars by German army. Another Steganography technique is the spam mimic software which developed by wayner in (2003), this software was developed to detect and hide the secret messages in text file based on set of protocols.

The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The
main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information. if suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.

The main terminologies used in the Steganography systems are: the cover message, secret message, and secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending

on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.

In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e. image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the stego file by email or chatting, or by other modern techniques. The stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender.

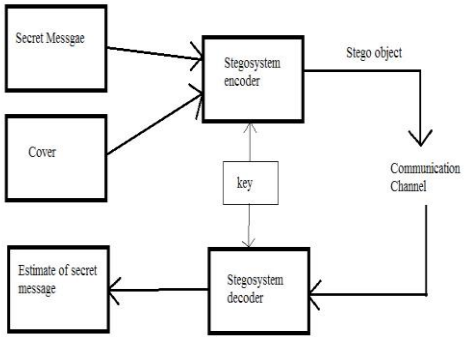


Figure1 Steganography System Scenario

Many carrier messages can be used in the recent technologies, such as image, text video and many others. The image file is the most popular used for this purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (black-white), gray scale and red-green-blue (rgb) images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent from 00000000 for black and 11111111 for white pixels. The gray scale image has 8 bits values per pixel represent by (00000000) for black and (11111111) for white pixels. in this research paper the gray scale images are used as a carrier message to hide the secret messages by the least significant bit hiding method (lsb) as well as the proposed method.

2. LEAST SIGNIFICANT BIT HIDING TECHNIQUE (LSB):

LSB is the most popular Steganography technique. it hides the secret message in the rgb image based on it its binary coding. Figure 2 presents an example about pixel values and shows the secret message. LSB algorithm is used to hide the secret messages by using algorithm 1. LSB makes the changes in the image resolution quite clear as well as it is easy to attack

ALGORITHM (1) L EAST SIGNIFICANT BIT HIDING ALGORITHM.
INPUTS: GRAY SCALE IMAGE, SECRET MESSAGE.
OUTPUT: SEGOS IMAGE.
BEGIN
SCAN THE IMAGE ROW BY ROW.
ENCODE THE SECRET MESSAGE IN BINARY.
START SUB-ITERATION 1:
CHOOSE ONE PIXEL OF THE IMAGE
HIDE ONE BY ONE BITS OF THE SECRET MESSAGE IN EACH PIXEL IN THE LEAST SIGNIFICANT BITS.
SET THE IMAGE WITH THE NEW VALUES.
END SUB-ITERATION 1.
SET THE IMAGE WITH THE NEW VALUES AND SAVE IT.
END

GRAY SCALE IMAGE PIXEL

0	1	1	0	1	0	0	1

3 THE PROPOSED METHOD:

LSB hiding technique hide the secret message directly in the least significant bits in the image pixels, hence that affect the image resolution, which reduce the image quality and make the image easy to attack. As well as this method is already has been attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the non-identical values between the secret messages and image pixels, see Figure 3. The proposed method is used to hide the secret messages by using algorithm 2.

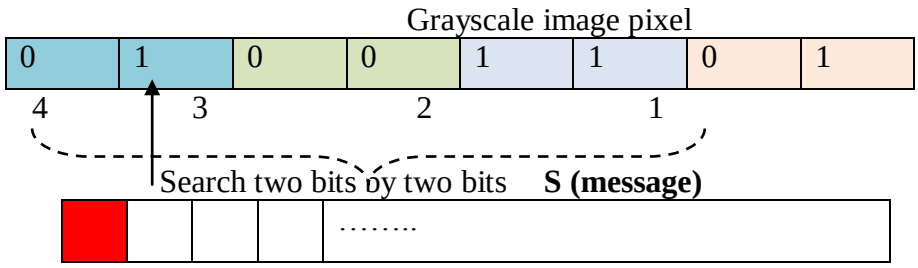


Figure 3 New Method in Image Steganography

Algorithm (2) the Proposed Hiding Algorithm
Inputs: Greyscale image, secret message.
Output: Stego image.

Begin
Scan the image row by row.
Encode the secret message in binary.
Start sub-iteration 1:
Choose one pixel of the image and encode it in binary.
Hide one by one bits of the secret message in each pixel by searching about the non-identical.
If the least bit of non-identical is satisfied then set the image with the new values.
Otherwise twist the non-identical bits and set the image with the new values
End sub-iteration 1.
If no non-identical bits are found hide the message in the last bit of pixel
Set the image with the new values and save it.
End

The LSB and the proposed hiding algorithms have been implemented in the Matlab on i5 2.50 GHZ in 2015. The two methods are applied to hide the secret message "Hello World" on two Bmp images, the first with size (128*128) and called “The Lena image” see Figure 4a, while the second one with size (298*298) and called "The Baboon image", see Figure 4b.

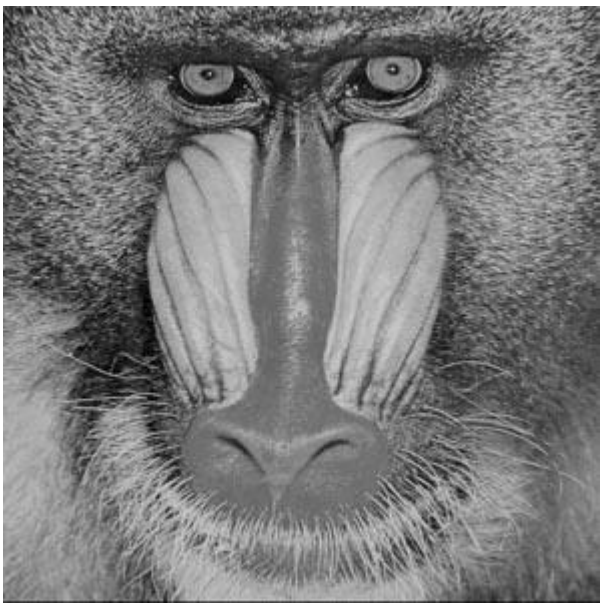
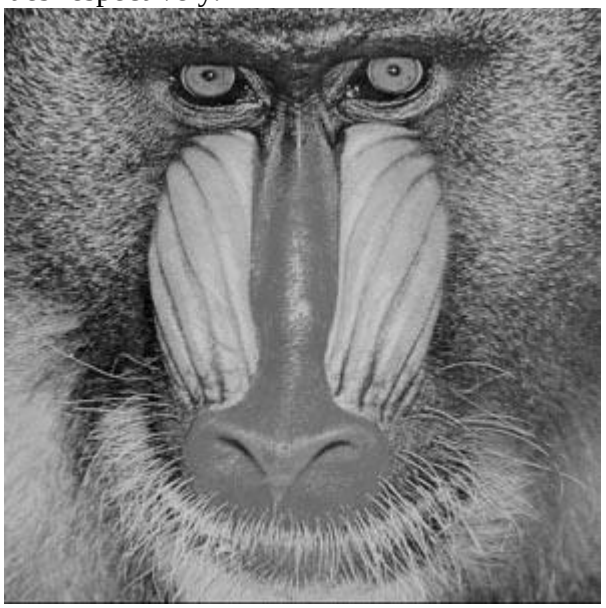


Figure 4 Two Bmp images: (a) The Lena image) (b) The baboon image

4 DISCUSSIONS AND ANALYSIS:

The proposed method and the LSB hiding methods, hiding every single bits of the secret message in one pixel of the image. The secret message used in this paper has 11 characters which are 88 bits, to hide those bits 88 pixels are needed.. In this paper, the results of the proposed and LSB hiding methods are analyzed based on MSE and PSNR values. Figure 5 shows the resultant images and the analysis table which present the MSE and PSNR values respectively.

(a)



(b)

	Lena	Baboon
PSNR	52.5395	69.1905
MSE	0.0913	0.0107

	Lena	Baboon
PSNR	52.5395	69.1905
MSE	0.0913	0.0107

(c)

Figure 5 the resultant images and the analysis table obtained by the proposed hiding method when applied on the (a) 4a and (b) 4b images.

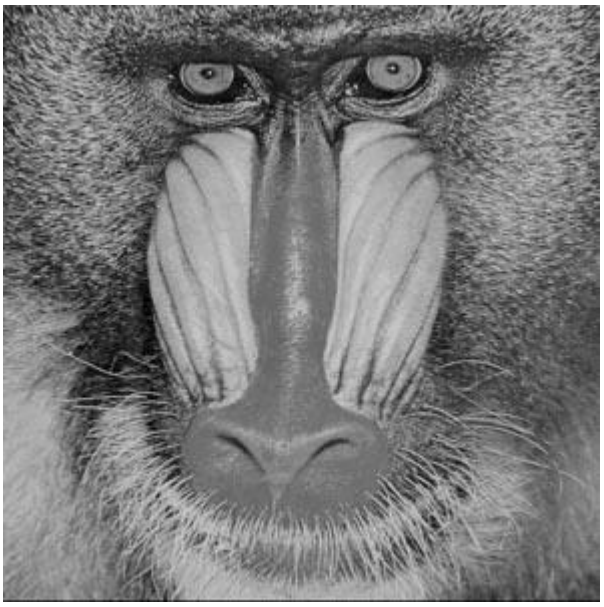


Figure 6 the resultant images and the analysis table obtained by the LSB hiding

5 CONCLUSIONS:

In this paper, a new Steganography technique was presented, implemented and analyzed. The proposed method hides the secret message based on searching about the non-identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The proposed and the LSB hiding methods were implemented to hide the secret message "Hello World" on two Bmp images, with size (128*128) and (298*298) respectively. The results of the proposed and LSB hiding methods were discussed and analyzed based on the MSE and PSNR. This paper conclude that the proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This paper concluded that the LSB hiding method is the worst case of the proposed method. the result obtained by the proposed method and the LSB hiding method in terms of ratio of accuracy in improving the image quality.

REFERENCES:

1. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).
2. C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.
3. H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.
4. J,Corporation,Steganography.http://www.webopedia.com/TERM/S/steganography.html. 2005.

.