A New Approach in LSB Based Image Steganography to Enhance Network Security

[1]**Susmita Soni,** [2]**Abhinav Soni**
[1]M-Tech, Marudhar Engineering College, Bikaner
[2]B-Tech, JUIT, Solan, Himachal Pradesh

***Abstract*— Steganography is used to hide the existence of secret data and it can be defined as the study of covert communication. In this way, if it provides covert communication successfully, the secret message does not attract the attention from eavesdroppers and attackers.**
In this paper, the secret message is embed into a carrier image and hence, the taxonomy of current image steganographic technique i.e. digital watermarking has been presented. In this paper the secret message is hidden into Least Significant Bit of the color components of the carrier image.

***Index Terms*—ASCII, LSB, RGB image, YCbCr image**

I. INTRODUCTION

Steganography comes from the Greek steganos (covered or secret) and graphy (writing or drawing). Steganography is an art of providing covert communication. It can be defined as the hiding of confidential information within other, seemingly harmless images, graphics or sounds [1].

Steganography is very old methods used around 440 B.C. Steganography is hiding a confidential message within an ordinary file.

In Steganography, the confidential message is hide in an image or text or any other audio file and produce a stego file as output. A stego key is used to hide the confidential information into these carrier files. The main aim of Steganography is to communicate securely in a completely undetectable manner and to avoid suspicion of secret data [2]. The main difference between Cryptography and Steganography is that Cryptography scrambles the confidential message so that it becomes difficult to read [4] whereas Steganography hides the existence of secret message.

II. IMAGE BASED STEGANOGRAPHIC SYSTEM

Steganographic systems have one general principle. According to that, in fig. 1, sender X wants to send a confidential message M to receiver Y. Sender X does not want that the confidential message is access by any third party except receiver Y. For this sender X use a carrier image C to hide the secret message M. Sender X embeds the secret message M into carrier image C with the help of stego key K. By this process Sender X gets stego image S as output. Stego image S is look identical to the carrier image C. Therefore, the stego image S represents the original carrier image C along with the secret message M embedded inside stego image.

After embedding process, sender X sends this stego image S to receiver Y over transmission channel. The main aim of steganographic system is to provide covert communication so that the secret message is not seen to anyone. On receiver side, Y retrieves the secret message M from stego file S by using stego key K which was used to embed the secret message. Only the sender and the intended recipient should have the stego key [5].

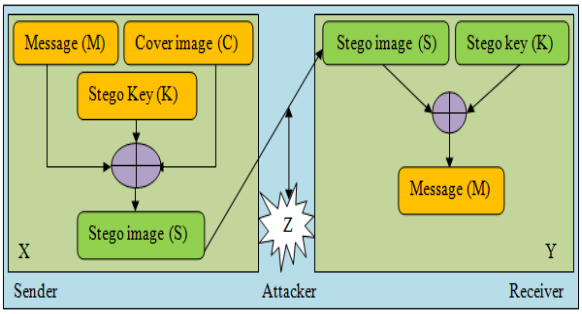

Fig. 1: Steganographic System

ISSN: 2278 – 1323

III. Least Significant Bit Technique

Least Significant Bit insertion is very common and easy approach in Image Steganography which is used to embed the secret message into an image. In this approach, the confidential information is put in the least significant bits of the pixel in an image. This technique is very easy and common for image, audio and video steganography [3,6]. The resulting stego image is look identical to the cover image.

For example, in a 24 bit color image, we want to insert S whose binary value is 01010011 into it. Each pixel uses eight bits for the intensity of red, green and blue. We need 3 pixels for hiding letter S [7].

Pixel/Color	RED	GREEN	BLUE
Pixel 0	00100111	11101001	11001000
Pixel1	00100111	11001000	11101001
Pixel 2	11001000	00100111	11101001

After inserting S into the above sequence the embedded image will be look like this

Pixel/Color	RED	GREEN	BLUE
Pixel 0	0010011**0**	1110100**1**	1100100**0**
Pixel1	0010011**1**	1100100**0**	1110100**0**
Pixel 2	1100100**1**	0010011**1**	11101001

In this way secret message is embedded into an image through LSB insertion method. It is very difficult for human eye to see a difference between the original and the stego image as there are only slightly differences in color.

IV. Proposed Work

During transmission of secret message, the attacker somehow manages to know that there is some confidential information transferring. In order to overcome this problem a model is proposed. In this model, steganography is used for hiding the secret message into a carrier file so that it becomes difficult for the attacker to feel the existence of the secret message in the carrier file and in this way the transmission will be secured.

For embedding a secret message into a carrier image we are using Simple Watermarked Embedded System.

In Proposed Work, we will input our secret message which is to be embedded into a carrier image to form stego image.

For example, our secret message is **HELLO**

To embed our secret message into carrier image, first of all, we have to change our RGB image into YCbCr image.

Suppose our RGB image is shown in fig. 2.

Fig. 2: RGB image

Now we change our carrier RGB image into YCbCr image.

Fig. 3 shows the conversion of the images.

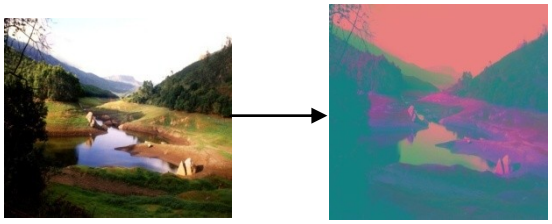

Fig. 3: Conversion of RGB image into YCbCr image

Fig. 4 shows the carrier YCbCr image into which we will go to embed our secret message **HELLO**

ISSN: 2278 – 1323

Fig. 4: Carrier YCbCr image

Now the embedding process of secret message is start. For this, we will have to calculate the ASCII (American Standard Code for Information Interchange) values of each characters of secret message. Then calculate the binary values of these ASCII values and these binary values are then inserted into the LSB (Least Significant Bit) of the carrier YCbCr image.

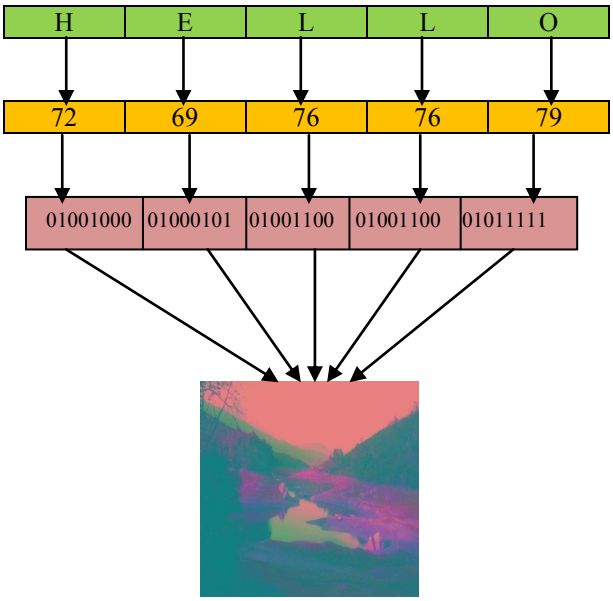

Fig. 5: Embedding Process of secret message

From fig. 5, we can see that our secret message **HELLO** is now hidden into YCbCr image.

Now convert the YCbCr image containing secret message into RGB image. That RGB image will be our stego image which is shown in fig. 6.

YCbCr image with Secret message

Stego image

Fig. 6: Conversion of YCbCr into Stego image

Note:- *Extraction process of secret message is just reverse process of Embedding Process*.

A. Proposed Algorithm

The embedding process of secret message into carrier image is as follow:

Inputs: Secret message and Carrier Image

Output: Stego image

1. First of all read the bits of secret message.

2. Read the input image.

3. Convert the input RGB image into YCbCr image.

4. Break the pixel of YCbCr image into color components.

5. Get the LSB of the color components.

6. Substitute one LSB bit of color component (from step 5) with one bit of secret message.

8. Repeat step 6 for the remaining bits of the secret message.

9. Now convert the output image into RGB form i.e. stego image.

V. RESULT

Various results and observations are taken during proposed work. Memory and Time overhead are calculated during work.

Fig. 7 shows the embedding window where our secret message is to be embed into a carrier image.

ISSN: 2278 – 1323

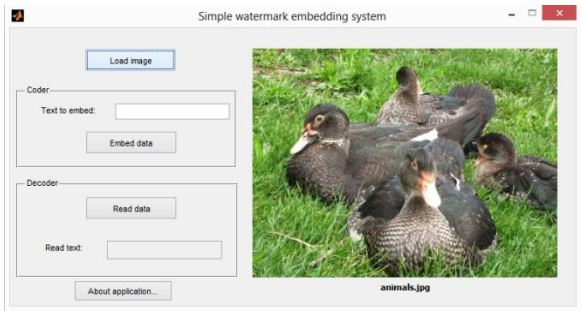

Fig. 7: Embedding Window

Fig. 8 shows the embedding window where we have inserted our secret message HELLO into carrier image.

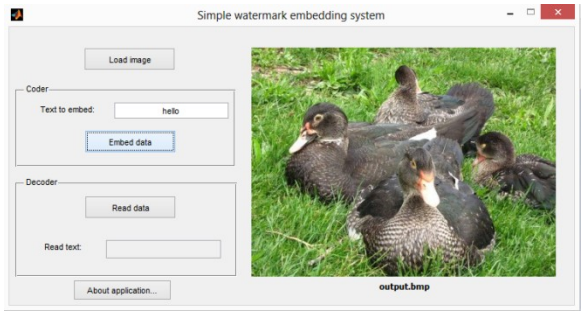

Fig. 8: Embedding window after inserting message

In fig. 9, when we click the "Read Data" button, we retrieve our original message.

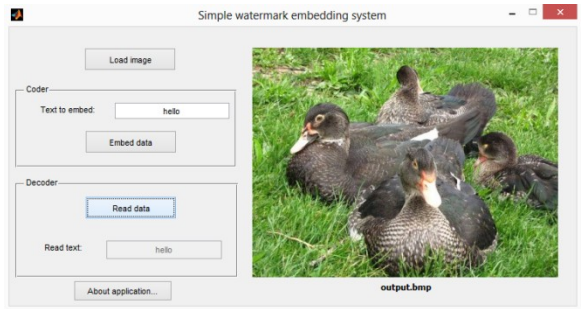

Fig. 9: Window showing our original message by Extraction process

Similarly other carrier image of plane which embed our secret message "image steganography".

Fig. 10 and Fig. 11 shows both the embedding and extraction of secret message.

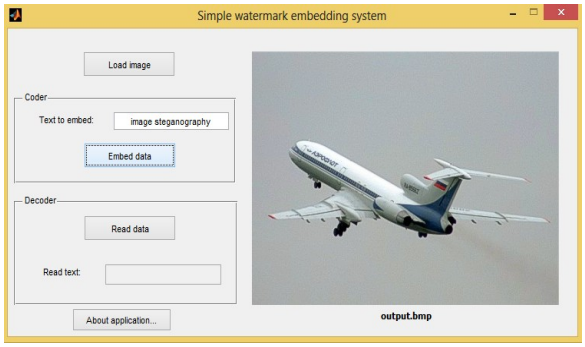

Fig. 10: Embedding Window after inserting message

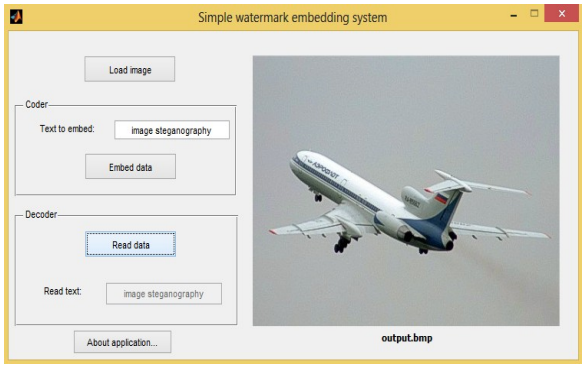

Fig. 11: Window after retrieving the message

The performance of both embedding and extraction process can be defined by calculating the following aspects:

1. Memory Overhead
2. Time Overhead

IMAGE	MEMORY OVERHEAD		
	Input image size (in bytes)	Stego image size (in bytes)	Difference (in bytes)
Animals	63809	36832	26977
Plane	22663	10583	12080

Table. 1 Memory Overhead

IMAGE	TIME OVERHEAD		
	Embedding Time (in seconds)	Extraction Time (in seconds)	Total Time (in seconds)
Animals	0.4878	0.0555	0.5433
Plane	0.4818	0.0543	0.5361

Table. 2 Time Overhead

ISSN: 2278 – 1323

VI. CONCLUSION

In this paper, the secret message is embedded into a carrier image. Different images of different size gives slightly time differences in process of embedding and extraction of secret message and for memory overhead, different size of images consume less memory which leads to high security of secret message. Thus this system provides more security to confidential information. Embedding the secret message into an image is too much secure.

ACKNOWLEDGEMENT

Hardwork always give us fruitful results, and this paper is an example of hardwork, dedication and proper guidance of my teachers, friends and my family. Here I would like to express my thanks to all of those, who helped me to complete the paper.

REFERENCES

[1] A.Joseph Raphael, Dr.V Sundaram "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.
[2] Neil F. Johnson & Sushil Jajodiya, "Steganalysis: The Investigation of Hidden Information", in the *Proceedings of the 1998 IEEE Information Technology Conference,* Syracuse, New York, USA, September 1st - 3rd, 1998.
[3] N.F. Johnson and S. Jajodiya, "Exploring Steganography: Seeing the Unssen", *IEEE,* pp. 26-34, 1998.
[4] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods," *International Journal of Digital Evidence*, Fall 2003 Voulme 2 Issue 2.
[5] Domenico Bloisi and Luca Iocchi, "Image Based Steganography and Cryptography".
[6] Alain C. Brainos II, "A Study Of Steganography And The Art Of Hiding Information".
[7] Samir K Bandyopadhayay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee, Poulami Das, "A Tutorial Review on Steganography".

ISSN: 2278 – 1323