RESEARCH ARTICLE OPEN ACCESS

Review on LSB Steganography

Apurva. S. Mahajan [1], Prof. Sheetal. G. Khadke [2]
Research Student [1], Assistant Professor [2]
Department of Electronics and Communication Engineering
G.H. Raisoni Institute of Engineering & Management
Jalgaon
Maharashtra - India

ABSTRACT
This paper presents a review on the LSB image steganography. This paper also explains the different methods of the steganography, which is the technique used to hide or conceal the existence of the secret data within the cover object. It also discuss the new LSB steganography method, 2/3 LSB steganography which will be useful to hide more data within the image with less distortion in the cover image.
Keywords:- Steganography, Image steganography, 2/3 LSB steganography

I. INTRODUCTION

Steganography is the art of the hiding the data within the data carrier in such a way that no other person except sender and receiver can identify it, while the carrier occurs to be the simple file to other peoples. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [5], the data carrier may be in the form of an image, a text or an audio file. Steganography differs with the other data hiding technique like water marking in many ways for example the existence of a watermark in a document or message is many times declared openly [3], while in steganography the object to be transmitted is hidden in such a way that no one can identify it. Steganography differs from cryptography also, which does not keep the communication hidden but only scrambles the data to prevent intruders understanding the content.

Steganography is used from ancient times, the first use of steganography was reported in Greece where wax tablets were used as a medium to hide the data, another steganography method in history includes shaving the head of the messengers and tattooing the secret message on head and let the hair grow. The message can be viewed after the messengers head is shaved again [1]. Data hiding methods and techniques advanced as per time like using paper mask, invisible ink etc. now days for this purpose steganography is used in the digital formats.

In steganography almost all digital formats can be used but formats with high redundancy are more suitable for steganography. The types of main formats that can be used for steganography are as shown in figure 1.

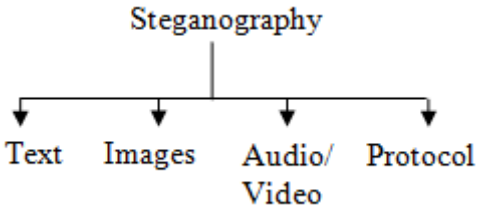

Fig. 1 Formats for the Steganography

Text steganography has a long history, which consists of the hiding the secret message within text message but it is now rarely used due to the digital text files have very small amount of redundant data.

Image steganography is the very popular type of the steganography now the days in this the data is hidden within the pixels of the cover image

In audio/video steganography, techniques used are similar to the image steganography.

In protocol steganography the secret data is hidden within messages and network control protocols used in the network transmission [2].

II. IMAGE STEGANOGRAPHY

Among the different types of steganography image steganography is mostly used. There are various methods to do image steganography like in transform domain and in image domain.LSB steganography comes in the image domain.

Image steganography consists of two images one is cover image and the other is secret images. The bits from the secret image are embedded in the cover image, as shown in figure 2

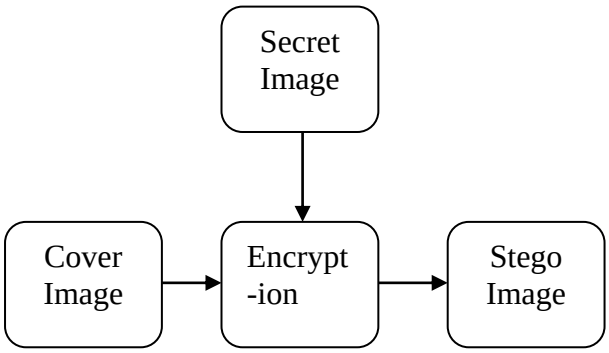

Fig. 2 Block Diagram of Encryption Process of an Image

A. *Least significant bit (LSB) steganography*

In LSB steganography the information is hidden within the last bits of the pixels of the image. The LSB is the least significant bit in the byte value of the image pixel in the image. In a 24-bit image three colours are used namely red, green and blue, they are each represented by the byte so there are three bytes per pixel in the image. An 800 × 600 pixel image, can thus store a total 1,440,000 bits or 180,000 bytes of embedded data since there are 256 possible intensities of each primary colour, change in the LSB of a pixel results in small changes in the intensity of the colours, these changes cannot be detected by the human eye - thus the message is successfully hidden.

To illustrate LSB technique, consider the following example, suppose the cover image has the following two pixel values

(0000 1010 0011 1010 0111 0100)
(1111 1101 1100 0011 1100 0111)

Also, assume that the secret bits are 101111, after embedding the secret bits, the resulting pixel values are:

(0000 101<u>1</u> 0011 1010 0111 010<u>1</u>)
(1111 1101 1100 0011 1100 0111)

The underlined bits indicate that the bits were changed from their original value. Only two bits in the cover image were modified in this process. On average about half of the bits in the cover image will be modified when embedding the secret image. LSB method given above limits the size of the secret data to eighth of the size of the cover image.

LSB steganography can be further extended to embed secret information in the least n-bits to increase the capacity of the secret information n/8 the size of the cover image but it causes distortion in the image when it goes beyond certain limits.

B. 2/3 LSB steganography

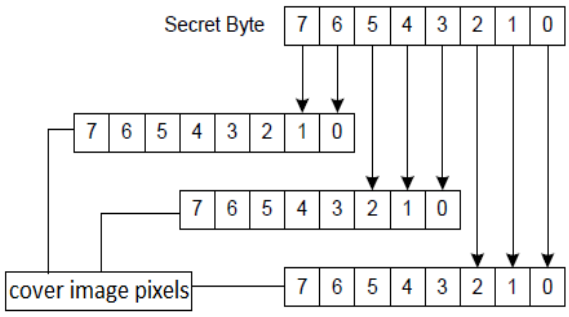

Fig.3 2/3 LSB Steganography

The steganography block implements LSB steganography method by concealing the secret information in the cover image using a combination of 2-bit and 3-bit LSB

steganography, referred as 2/3-LSB [4]. Each cover image pixel is represented by three bytes. Single byte of the secret information is concealed in the three bytes of a cover image pixel as shown in figure 3

.

III. CONCLUSIONS

This paper highlights some basic concepts about steganography and its types. It explains the LSB image steganography. The future work includes implementing hardware of the LSB steganography using matlab and FPGA, also calculating image parameters like PSNR, BER etc in the matlab.

ACKNOWLEDGMENT

Authors would like to express sincere thanks and deep gratitude to Prof. H. K. Bhangale, Head of E&C Department who extended wholehearted co-operation to complete this work successfully.

Authors are also express deep and sincere gratitude to the principal, G.H. Raisoni institute of engineering & management, Jalgaon for being a constant source of inspiration.

REFERENCES

[1] Neil F. Johnson, Sushil Jajodia, George Mason University, "Exploring Steganography: Seeing the Unseen", IEEE Computers, February 1998, pp. 26-34

[2] T. Morkel, J. Eloff and M. Olivier, "An Overview of Image Steganography," The Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, July 2005

[3] H. Wang, S. Wang, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, October 2004, Vol. 47, No. 10, pp. 76-82

[4] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, Sahel Alouneh, ’’FPGA Hardware of the LSB Steganography Method’’ computer, information and telecommunication systems, May 2012

[5] Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir, ‘’Art of Hiding: An Introduction to Steganography’’, October 2012