RESEARCH ARTICLE OPEN ACCESS

Hardware Implementation of LSB Steganography Using MATLAB and FPGA

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
Steganography is one of the very powerful and popular techniques used for hiding information. Designing steganography in hardware helps to speed up steganography and 2/3 LSB steganography method helps to hide more data. This work presents hardware implementation of 2/3 Least Significant Bit (LSB) image steganography technique using MATLAB and FPGA, in which image is concealed within another image and evaluation of image parameters of the output image.
Keywords:- Steganography, Image steganography, 2/3 LSB steganography, image parameters

I. INTRODUCTION

From the rise of the internet, the use of it for communication or data transfer has increased day by day, while the used of internet for communication has increased the security of the data transfer also becomes a main factor, for this purpose steganography can be used[1].

Steganography can be described as an 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 [5]. Various types of materials and formats can be used as a carrier like magazines, wooden tablets, image, text or an audio/video file [2].

Steganography differs from the other data hiding techniques like cryptography and watermarking etc. From these types of techniques steganography and cryptography are closely related but the main difference between them is cryptography doesn't hide the data it only scrambles it to prevent intruders from extracting the hidden data while steganography hides the data in such a way that except sender and receiver no one will suspect the presence of hidden data [3].

From ancient times steganography is used, in Greece initially wax tablets were used as a medium for steganography, after that various methods had been invented and used for steganography for example use of invisible ink, drawings, paper masks, microdot technology etc [1]. Now a day's steganography is used in digital formats. The main types of the digital formats which are used for steganography are as given below

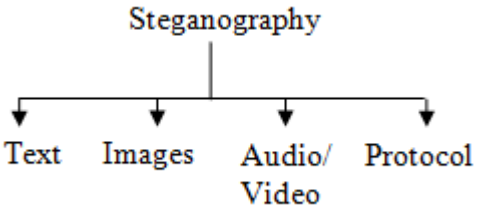

Fig. 1 Formats for the Steganography

Text steganography consists of hiding information using or within the text messages but now this technology is rarely used.

Images due to their increasing use on the internet and having high redundancy bits are the most popular cover objects for steganography. In audio steganography hiding information is possible by many ways one of them is masking. In protocol steganography information is

embedded within messages and network control protocols used in network transmission [2].

II. IMAGE STEGANOGRAPHY

Among the different kinds of steganography image steganography is mostly preferred and popular. There are various ways to perform image steganography like in transform domain and in image domain.

Image steganography includes of two images one is cover image and the other is secret image. Cover image as the name suggests used as a cover to conceal or hide the secret image. The block diagram is as shown in figure 2 given below

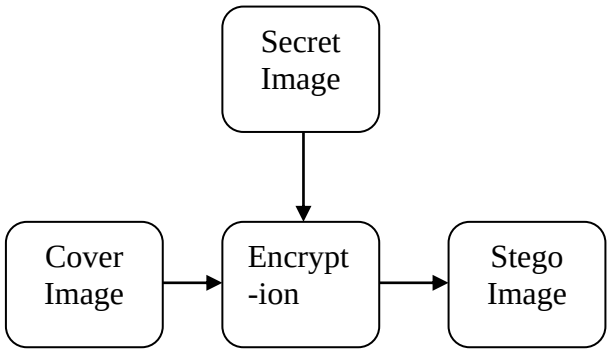

Fig. 2 Block Diagram of Encryption Process of an Image

A. *Least significant bit (LSB) steganography*

In LSB steganography the information is hidden within the last bits of the pixels of the cover image. The LSB is the least significant bit in the byte value of the image pixel in the image. To exemplify LSB technique, consider 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 111111, after concealing of the secret bits, the resulting pixel values are:

(0000 101<u>1</u> 0011 101<u>1</u> 0111 010<u>1</u>)

(1111 1101 1100 0011 1100 0111)

The underlined bits represents that the bits were changed from their original value. There are only three bits in the cover image that were modified in this process. During this process on average about half of the bits in the cover image will be modified. This method as stated above, limits the size of the secret data to eighth of the size of the cover image. It can be further extended to embed secret data 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 as the value of n increases.

B. *2/3 LSB steganography*

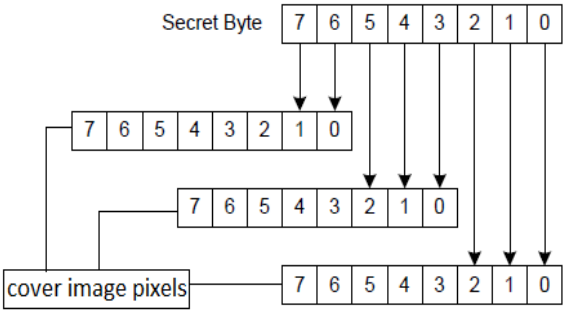

Fig.3 2/3 LSB Steganography

2/3 LSB steganography is achieved by concealing the secret information in the cover image using a combination of 2-bit and 3-bit LSB steganography, also known as 2/3-LSB [4]. Each cover image pixel is represented by three bytes and each single byte of the secret information is concealed in the three bytes of a cover image pixel as shown in figure 3.

C. *Image Parameters*

- Mean Squared Error (MSE)

MSE is calculated by byte by byte comparisons of the cover and the output stego- image. MSE can be calculated by the formula shown below

$$MSE = \frac{1}{M \times N} \sum_{1}^{M} \sum_{1}^{N} (f_{ij} - g_{ij})^2$$

Where

M, N: number of rows and columns in the cover image matrix

f_{ij} is the pixel value from cover image

g_{ij} is the pixel value from the output steganographed image.

- PSNR

Peak signal-to-noise ratio measures the quality of the stego-image compared with the cover image, higher the value of the PSNR better is the quality of the output. PSNR is calculated using the equation given below:

$$PSNR = 10\ log_{10} \frac{MAX^2}{MSE}$$

Where,

MAX is the value of maximum pixel in the image.

The PSNR is measured in decibels.

- BER

Bit error rate (BER) computes the actual number of bit positions which are changed in the output stego-image compared with cover image. BER is the unitless parameter.

III. SYSTEM DESCRIPTION

The system hardware consists of the papilio FPGA board which consists the SPARTON 3E IC and matlab software the system overview is as shown in the figure 4 below

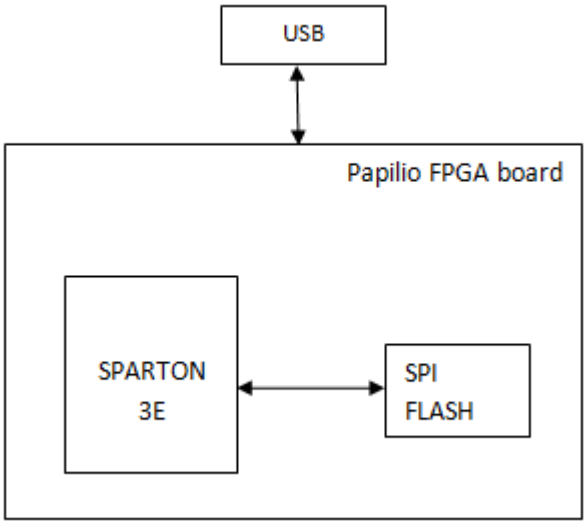

Fig.4 system

Here the papilio FPGA board is used in which SPARTON 3E IC and SPI flash memory are implemented. The program for the 2/3 LSB steganography is stored in the SPI flash memory and images are provided to the board through MATLAB. The program conceals the secret image into the cover image as described in the section II. B. The output image obtained is then given to the display by USB.

IV. RESULTS

In this section steganographed output image of the above implementation is demonstrated. The image used as a cover image is image Lena and the secret image used is the image named fall as shown in the fig. 5. Both the images are first converted into grayscale images and resized, then provided to the FPGA board where secret image is concealed within the cover image. The output obtained is as shown in the figure 6, fig. (a) is the original cover image Lena while fig. (b) is the steganographed image.

The image parameters calculated are as given below

PSNR: 53.3858

MSE: 1.2247

BER: 0.0501


Lena Fall

Fig.5 Cover image and secret image


(a) (b)

Fig.6 output images

V. CONCLUSIONS

In this paper, we implemented the 2/3 image steganography successfully by using MATLAB and FPGA and measured the output steganographed image parameters MSE, PSNR, BER.

Future work should focus on to improve the image steganography and to reduce the size of the output steganographed image.

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

[6] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001.

[7] Nani Koduri,” Steganography: Data Hiding Using LSB Algorithm”, Scribd, Feb 14, 2011