Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 84 (2015) 33905-33909

ISSN: 2229-712X

Implementation of LSB Steganography Technique on FPGA for Highly Secured Image

Jayashri Gokul Gurav[1], Jaikaran Singh[2] and Mukesh Tiwari[2]
[1]VLSI Design, Department of E&TC, SSSIST, Sehore.
[2]Department of E&TC, SSSIST, Sehore.

ARTICLE INFO

Article history:
Received: 20 May 2015;
Received in revised form:
15 July 2015;
Accepted: 23 July 2015;

Keywords
LSB Steganography algorithm,
FPGA,
Image processing,
C Languge.

ABSTRACT
Steganography is skill of hiding secret messages or hiding secret images so that only the writer and the intended recipient are aware from hidden information .Steganography is an powerful technique in terms of any type of carrier which is hiding technique that develops stimulating structures to fruitfully & successfully hide information (may be a text or an image) in color images. Digital steganography is basically about hiding a file in, or adding a file to, another file, called the carrier file, such that the carrier file is not changed enough to raise suspicion that something may be concealed within it or appended to it. The steganography scheme on hardware platform shows huge potential by means of various advantages such as high speed implanting, specific hardware dependency, and low power consumption etc. Current developments favor using digital images, carrier files as the cover file to hide another file that contains the secret information in the form of either text or image that means carrier file. Hardware stenographic modules applied in a processor platform like FPGA which offer some essential additions to the existing benefits of software based stego systems. It also offers the Embedding rate which is very high when compared to the systems in software domain. LSB method representing a high imbedding capacity.

Introduction

The term steganography is derived from the Greek word and literally means “covered writing” Steganography allows people to communicate secretly. A steganography system consists of three elements: cover element which hides the secret message, the secret element and the stego element which is the cover object with message embedded inside it.

There are many methods for concealing messages in an images in such a manner that the modifications made to the image are perceptually invisible. However, the question whether they result in images that are statistically indistinguishable from unhampered images has not been adequately explored. This paper describes Least Significant Bit based Steganography and under what condition can an observer distinguish between Stego images (Images with a secret message) and Cover-images (Images without any secret message).When large redundant bits present in the digital representation of an image, so images are the most popular cover objects for steganography.

Typically, gray images use 8 bits, whereas colored utilizes 24 bits to describe RGB model. The Aim of the this project work, intended to demonstrate LSB steganography, a powerful technique for data and image security, its implementation on FPGA and calculate its parameters like PSNR, BER,MSE for its to analyze its hiding capacity [1]

Steganography is the art of writing secret messages or hiding secret images so that only the both the parties that means sender and the intended recipient are aware of the hidden information .Steganography is an information hiding technique that utilizes lifting schemes to effectively hide information (may be a text or an image) in color images. The steganography system on hardware FPGA platform shows huge potential by means of multiple advantages such as high speed embedding, specific hardware dependency and low power consumption etc.

Hardware steganography modules implemented in a processor platform like FPGA offer some important additions to the existing benefits of software based stego systems. It also provides the Embedding rate which is very high when compared to the systems in software domain. LSB method representing a high imbedding capacity

Objective of Work

In our project an algorithm is designed to hide a secret image within CVR image to shield the confidentiality of the image. Steganography Imaging system (SIS) is a system that is capable of hiding the data inside the image. The system is using two layers of security in order to maintain data privacy. Using LSB algorithm we are replacing the list significant bit of cover image with a secret image.

Literature survey

As in this paper, the secret data is only a message (or code word) or carrier which is hided inside image using steganography technique. Here algorithm is used SIS which is not having a high embedding capacity.[2] In our project we are hiding an image to a image by using LSB .

In this paper, the algorithm LSB is used but this is applied on the message bits . As in our project we are hiding an image to a image by using LSB ad also we are implementing on hardware with effective results.[3]

According to this paper, the complexity of frequency analysis increases quickly and largely on a poly-alphabetic message because it implements the entire ASCII table and it can have more than one character represent another. Here we are not using such ASCII table due to this the complexity of frequency decreases. [4]

Tele:
E-mail addresses: jayu.gurav@gmail.com

This paper describes a method for integrating together cryptography and steganography through image processing. Here the algorithm is used is ISC extracting process.[5]

So here we are using LSB algorithm as an ISC has optimum cryptographic performance, by proving that it is equivalent to Vernam cipher.

Where research with this paper is the images are get compressed through JPEG format to retrive it fast at receiver. But JPEG is a lossy compressed file. Therefore to avoid this problem we taking combination of some JPG,TIF,PNG and BMP format which is a lossless compressed file.[6]

Problem definition

The aim of our project is to encrypt and decrypt the stego image. The stego image is the image which hide the secret image over an cover image using LSB algorithm and FPGA hardware

System development

From [1] we need to show block of encryption &decryption method of steganography

Block diagram

Encryption method

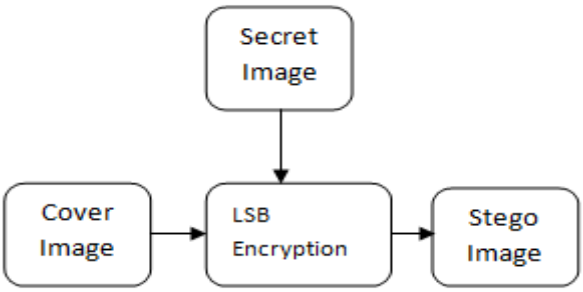


Fig 4.1.1(a) : Block diagram of encryption of an image

Decryption method

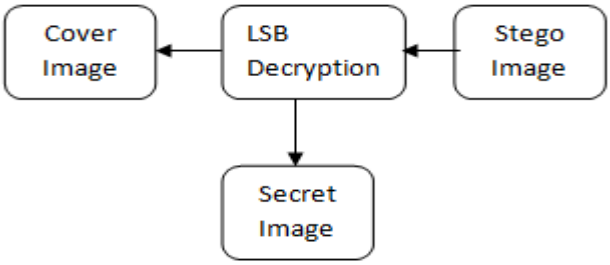


Fig 4.1.2(b) :Block diagram of decryption of an image

Block diagram explanation

Interfacing with FPGA kit

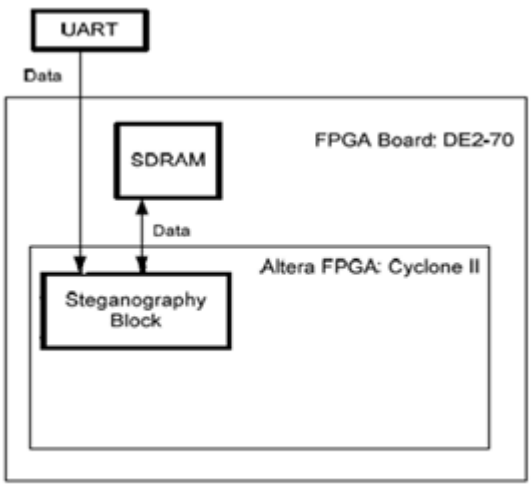


Figure 2. System overview

It consists of

1). SDRAM
2). UART interface
3). Steganography unit

The steganography block is implemented in the FPGA chip Cyclone-II. Both Cyclone-II and SDRAM are parts of the FPGA board DE2-70.

SDRAM: It is called "Synchronous" DRAM because the memory is synchronized with the clock speed that the computer's CPU bus speed is optimized for. The faster the bus speed, the faster the SDRAM can be. SDRAM speed is measured in Megahertz, which makes it easy to compare the processor's bus speed to the speed of the memory. The SDRAM chip on DE2 board has the capacity of 64 Mbits(8 Mbytes).It is organized as 1M *16 bits *4 banks.

UART interface

A UART (Universal Asynchronous Receiver/Transmitter) is the microchip with programming that controls a computer's interface to its attached serial devices. Specifically, it provides the computer with the RS-232C Data Terminal Equipment (DTE) interface so that it can "talk" to and exchange data with modems and other serial devices. As part of this interface, the UART also Converts the bytes it receives from the computer along parallel circuits into a single serial bit stream for outbound transmission

Steganography unit

The steganography block implements LSB steganography method by concealing the secret information in the CVR using a combination of 2-bit and 3-bit LSB steganography, referred to as 2/3-LSB. Each CVR pixel is represented by three bytes. A single byte of the secret information is concealed in the three bytes of a CVR pixel as shown in Figure 4.2.2.

LSB Algorithm

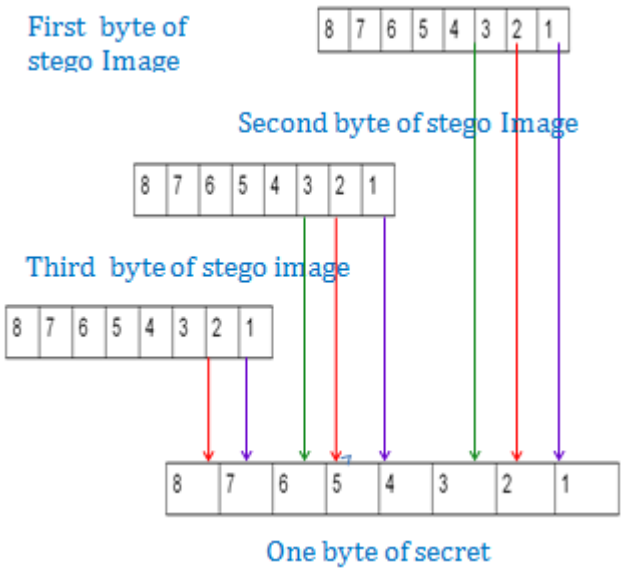


Fig 4.2.2: Concealing mechanism inside a stegnograp

FPGA SPARTEN 3

A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing—hence "field-programmable".

Spartan 3 Embedded Dev board:

- Benefits Supports VHDL, Verilog ,C
- JTAG Programming | Debugging
- Image processing development
- Supports
- Xilinx ISE

- Xilinx EDK
- System Generator(MATLAB)
- Accel DSP

Software used

Mat lab

MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran.

System specification

- FPGA Sparten3
- Microcontroller (P89v51RD2)
- Resistor
- Capacitor
- Crystal-3.57MHz,11.0592MHz
- LCD (16 x 2)
- Regulators- L7812/ L7805/ L7912
- Rectifier diodes 1N4007
- Zigbee module.

Methodology

In this section we are going to describe the method using LSB Steganography techniques. The Observations & conclusions are made on the basis of three parameters Mean Square Error (MSE), Bit Error Rate (BER), Peak Signal to Noise Ratio (PSNR).

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar (or different) the stego-image compared with CVR. The following metrics are used in the literature including the work of [6]

• Mean Squared Error (MSE) is computed by performing byte by byte comparisons of the CVR and stego-image. The computation can be expressed as follows:

$$MSE = \frac{1}{M*N}\sum_1^M \sum_1^N (fij - gij)^2$$

Where M, N are the number of rows and columns in the CVR matrix, fij is the pixel value from CVR, and gij is the pixel value from the stego-image. Higher value of MSE indicates dissimilarity between compared images.

• Bit error rate (BER) computes the actual number of bit positions which are changed in the stego-image compared with CVR.

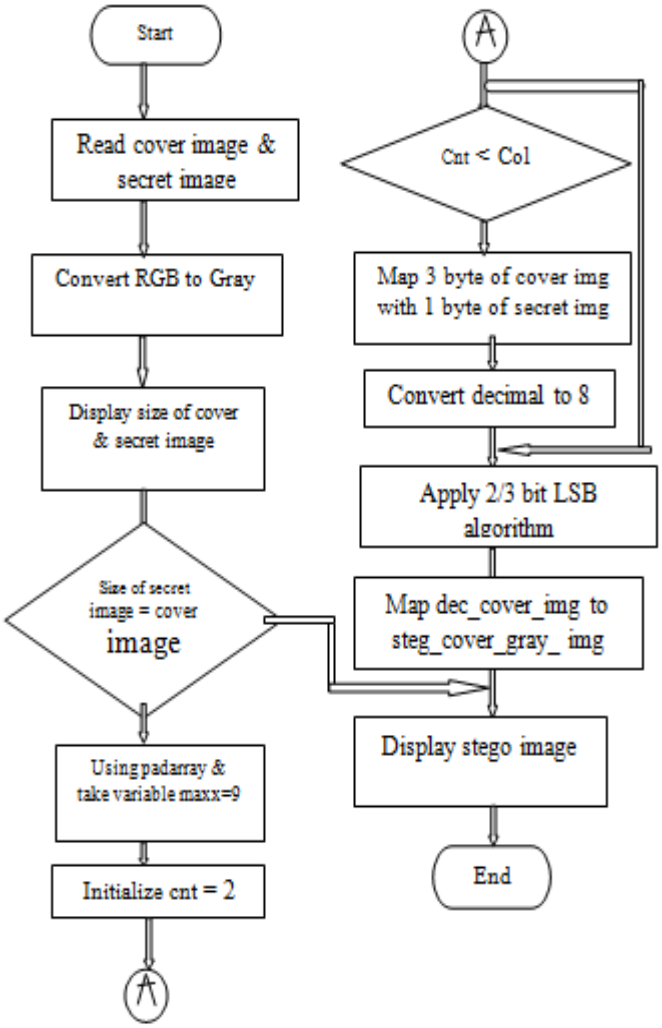
• Peak signal-to-noise ratio measures in decibels the quality of the stego-image compared with the CVR. The higher PSNR the better the quality. PSNR is computed using the following equation:

$$PSNR = 10\log_{10}\frac{L2}{MSE}$$

For above LSB of two pixels, we compute the three metrics and obtain the following values: MSE=0.77, BER=0.032, PSNR=113.36dB.When we considering two different images i.e. Secret & Cover FALL.jpg & PEPPERS.png respectively. Several LSB steganography techniques were implemented, where $1 \le n \le 8$ using several images of several types. The image metrics were computed for the images across the various LSB experiments. We use methodology with MATAB software where we consider count. Consider Cnt=2; Where Our assumptions are i is the row of secret image and j is the column of secret image .Maximum value of LSB steganography we take 9.i.e. Maxx=9;Read 3 pixels of cover image and convert that into binary. As we create three maximum counts for three pixels of cover images which we are converted RGB into Gray.

Read a pixel of secret image and convert that onto binary after we converts this binary no.s of gray images into decimal no. for conversion of cover image. Mix 2 images :Convert mixed image into decimal's sign it to output image. Similarly creating for secret image by calculating decimal to binary & again binary to decimal. Jump by 3 pixels this is incrementing columns of secret image.

Flow chart



Explanations

Input Images

Take input as secret image & cover image. Convert these images cover & Secret images into gray images with help of commands. Display size of both images. By using Pad array function equal size of both images. Taking maximum variable is max count.& map steganographed image & original image. Initialze Count is equal two in loop function due to cont is less than column.

LSB Encryption & Decryption Methods

1 By taking 3 bytes of cover images & 1 byte of Secret image are mapped.

2 After taking convert each pixel value of cover & Secret images from decimal to binary.

3 Applying 2/3 LSB algorithm on cover image using secret image.

4 Mapped the decimal cover image to steganography image.

5 Displaying Both Images.

Observation & results

Input images are

Fig.8.1.1(a)Lena.bmp

Fig.8.1.2(b)Fall.jpg

Fig.8.1.3(c) Leaf.jpg

Fig.8.1.4(d) Cameraman.tif

Fig.8.1.5(e) Peppers.png

Fig 10. Krishna.jpg

Encryption Process

Before Encryption

Col / Row	1	2	3
1	77	111	182
2	141	117	176
3	172	148	169

Ex :3*3 matrix of cover image

After Encryption

Col / Row	1	2	3
1	77	108	183
2	141	117	178
3	173	149	173

Ex 3*3 matrix of stego image.

Result Table

Hardware Results

In the following table, we have listed various combination of SECRET & CVR images with different size & different formats. We have also shown the calculated MSE,PSNR,BER for each of these combinations.

Sr no	Images		MSE	BER	PSNR
	Secret	Cover			
1	Fall.jpg	Peppers. png	0.77	0.03	113.36
2	Leaf.jpg	Fall.jpg	0.79	0.031	113.12
3	Leaf.jpg	Krishna. jpg	0.83	0.032	112.57
4	Leaf.jpg	Lena.bmp	0.77	0.032	110.22
5	Peppers.png	Lena.bmp	1.100	0.04	106.35
6	Peppers.png	Moon.tif	0.86	0.053	112.30
7	Cameraman. Tif	Lena.bmp	0.73	0.035	110.85

Conclusion

After the implementation of this project, it can be concluded that the steganography can be effectively used to hide data or image into an another image without any loss. The main advantage of our project is that any size of image can be hided through LSB algorithm with high speed & High PSNR of transmission by using FPGA kit.

The scope of the project is to limit unauthorized access and provide better security during image transmission. In this project, the proposed approach finds the suitable algorithm for embedding the secret image in an image using steganography which provides the better security pattern for sending secret image through a network. Video transmission through image. Hiding graphical figures through images

References

[1] Jayashri Gokul Gurav, Prof.Mukesh Tiwari, Prof. Jaikaran Singh “High Secured Image by LSB Steganography Technique using Matlab”, IJRITCC,ISSN 2321-8169,1836-1840

[2] Rosziati Ibrahim and Teoh Suk Kuan “Steganography Algorithm to Hide Secret Message inside an Image” (Johor, Malaysia) Received: November 25, 2010 / Accepted: January 10, 2011 / Pu blished: February 25, 2011.

[3] Randomizers Saeed Mahmoudpour and Sattar Mirzakuchaki “Hardware Architecture for a Message Hiding Algorithm with Novel” International Journal of Computer Applications (0975 – 8887) Volume 37– No.7, January 2012. CPSC 350 Data Structures: Image Steganography.

[4] NickNabavian nabav100@chapman.edu nov.28,2007 “Image based steganography and Cryptography Domenico Bloisi and Luca Iocchi Dipartimento di Informatica SistemisticaSapienza University of Rome, Italy , dec.31,2008

[5] S. Areepongsa, N. Kaewkamnerd, Y. F. Syed, and K. R. Rao

"Exploring On Steganography For Low Bit Rate Wavelet Based Coder In Image Retrieval System" The University of Texas at Arlington, Box 19016, TX 76019 IEEE Papers :
[6] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method 978-1-4673-1550-0/12/$31.00 ©2012 IEEE
[7] D.Kahn, The Codebreakers, Macmillan, New York, 1967.
[8] B. Norman, Secret Warfare, Acropolis Books, Washington, D.C., 1973.
[9] H.S. Zim, Codes and Secret Writing, William Morrow, New York, 1948.
[10] J. Brassilet et al., "Document Marking and Identification using Both Line and Word Shifting," Proc. Infocom95, IEEE CS Press, Los Alamitos, Calif., 1995.
[11] P. Wayner, Disappearing Cryptography, AP Professional, Chestnut Hill, Mass.,1996
[12] E. Koch, J. Rindfrey, and J. Zhao, "Copyright Protection for Multimedia Data," Proc. Int'l Conf. Digital Media and Electronic Publishing, Leeds, UK, 1994.
[13] W. Bender et al., "Techniques for Data Hiding," IBM Systems J., Vol. 35, Nos. 3 and 4, 1996, pp. 313-336.
[14] I.J. Cox et al.,"Secure Spread Spectrum Watermarking for Multimedia,"Tech. Report 95-10, NEC Research Inst., Princeton, N.J., 1995.