FPGA Implementation of Image Steganography: A Retrospective

[1]Jatin Chaudhari, [2]Dr. K.R.Bhatt

[1]P.G. Student, [2]Associate Professor
EC Dept., SVIT, Vasad, India
[1]jatinchaudhari@hotmail.com, [2]krbhattec@gmail.com

***Abstract*-- Steganography is the art of hiding a Secret message within a cover message in such way that only intended recipient have knowledge about secret message. Cover message can be image, audio, file etc. In this paper we have focused on FPGA system of Steganography for Image file. First we discuss the basics of Image Steganography and then focus on review study of embedded FPGA system of Image Steganography**.

***Index Terms*—Steganography, FPGA, X-Box, LFSR**

I. INTRODUCTION

Since the ancient times people have been interested in hiding secret messages. Both cryptography and steganography achieve this aim, but using the different way as we next explain. Steganography is an ancient technology which has applications even in today’s modern society. A Greek word meaning “covered writing,” steganography has taken many forms since its origin in ancient Greece. During the war between Sparta and Xerxes, Dermeratus wanted to warn Sparta of Xerxes‟ pending invasion. To do this, he scraped the wax off one of the wooden tablets they used to send messages and carved a message on the underlying wood. Covering it with wax again, the tablet appeared to be unused and thereby slipped past the sentries‟ inspection. However, this would not be the last time steganography would be used in times of war. In World War II, the Germans utilized this technology. Unlike the Greeks, these messages were not physically hidden; rather they used a method termed “null ciphering.” Null ciphering is a process of encoding a message in plain sight. For example, the 2nd letter of each word in a message could be extracted to disclose a secret message [1]. Although its roots lay in ancient Greece, steganography has continually been used with great success throughout history. Today steganography is being incorporated into digital technology. The techniques have been used to create the watermarks that are in our nation’s currency, as well as encode music information in the ever-popular mp3 music file. Copyrights can be included in files fingerprints can be used to identify the people who break copyright agreements. However, this technology is not always used for good intentions; terrorists and criminals can also use it to convey information. According to various officials and experts, terrorist groups are “hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, and other Web sites. This aspect of steganography is what sparked the research into this vast field and Education and understanding are the first steps toward security. Thus, it is important to study steganography in order to allow innocent messages to be placed in digital media as well as intercept abuse of this Technology.

Steganography is concerned with sending a secret message while hiding its existence. The word *steganography* is derived from the Greek words *steganos*, meaning ’covered’, and *graphein*, meaning ’to write’[2]. On the other hand, cryptography is not concerned with hiding the existence of a message, but rather its meaning by a process called *encryption*. The word *cryptography* is derived from the Greek word *kryptos*, meaning ’hidden’ [3].

Due to advances in ICT (Inverse Cryptography technology), majority information will be stored electronically. So the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. Steganography is a technique of concealing information in digital media [2]. In contrast to cryptography, the encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown [3]. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video, and images.

II. OVERVIEW OF STEGANOGRAPHY

The main goal of steganography is to communicate securely in a completely undetectable manner [4] and to avoid drawing suspicion to the transmission of a hidden data [5]. It is not to keep others from knowing the Concealed information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed [6]. The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message.

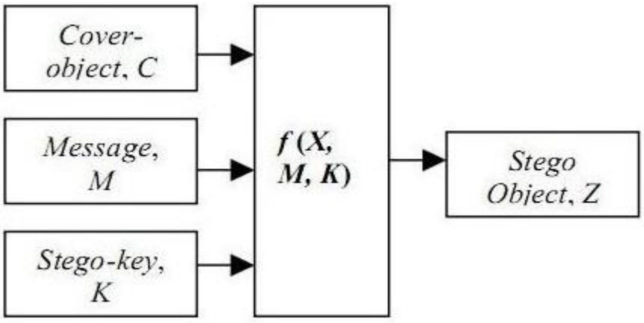

Figure 1: Basic model of Steganography

Based on the cover object steganography can be classified as shown in Figure 2.

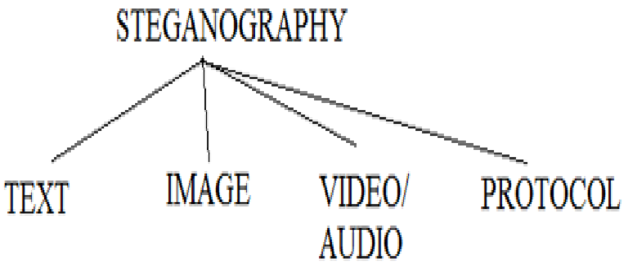

Figure 2: Classification of Steganography

III. IMAGE STEGANOGRAPHY

Image steganography techniques can be divided into two groups: those in the Spatial Domain and those in the Transform Domain [7]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [8].

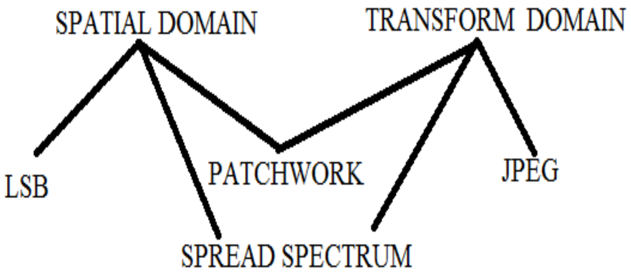

Figure 3: Categories of Image Steganography

Least significant bit (LSB) insertion technique is a common, simple approach to map information in a cover image. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message.

For example when using a 24-bit a bit of each of the red, green and blue colour components can be used for embedding a Secret image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)
(1010011**0** 1100010**1** 0000110**0**)
(1101001**0** 1010110**0** 0110001**1**)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in a cover image will require to be modified to conceal a secret message using the maximum cover size [9].

IV. FPGA HARDWARE APPROACH

Several Image steganography algorithms have been proposed for securing digital image in the current literature. Here is a brief browsing of FPGA implementation to execute secure Steganography algorithms. Authors of [10] have implemented chips capable to execute successfully steganography in spatial domain using X-Box Mapping algorithm.

These design basically based on mapping of different values from x-boxes. First Image have been encrypted using cryptography then each pixel is divided into group of 2-bit. Mapping a value in ciphered image with X-box value which is generated by X-or property followed by bit insertion in cover image to formation Stego image.

Generation Procedure for X-Box:

X-Boxes are a 2x2 matrix, where 16 (0 to 15) values are stored. To put values in X-boxes, Author uses X-OR property: 0 XOR 0 = 0, 1 XOR 1 =0 and 0 XOR 1 = 1, 1 XOR 0= 1.

For example 13 is inserted in any one of the four X-Boxes as follow: 13=1101=11 XOR 01=10 thus the position of 13 is 2nd row and 1st column as shown in Figure 4.

	0	1
0	0	4
1	13	9

Figure 4: X-Box

Then, take the cipher encrypted image pixel and divided 8-bit value into 2-bits. For Example,

$$(1\ 4\ 9)_{1\ 0}= (10010101)\ 2$$

B1= 10;
B2=01;
B3=01;
B4=01;

X-box Mapping & Bit Insertion

Now they just map the values of B1, B2, B3, and B4 from the X-mapping box. First take B1 =10; Then search the value of 1st row and 0th column of the X-I box; after mapping we get the value (13) 10= (1101) 2cSimilarly we get mapping values for the B2, B3, B4; we get in the same way 11,14,1 sequentially. After getting the new mapping values we insert these values into the cover image using LSB insertion and they got the Stego image.

Table 1: The PSNR that they have getting for some images

Image	Capacity	Size(pixel)	PSNR (dB)
Lena.jpg	25%	64	31.11
Cameraman.jpg	25%	64	31.78
Koala.jpg	25%	64	31.87
Penguin.jpg	25%	64	31.80

In the next work done by Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, they have proposed method steganography model [11]. In which it consists of: steganography unit, Nios processor, SDRAM and UART interface. The steganography block and Nios processor are implemented in the FPGA chip Cyclone-II. Both Cyclone-II and SDRAM are parts of the FPGA board.

The Author have implement LSB steganography method by hiding the secret information in the cover media using a combination of 2-bit and 3-bit LSB steganography, referred to as 2/3-LSB.

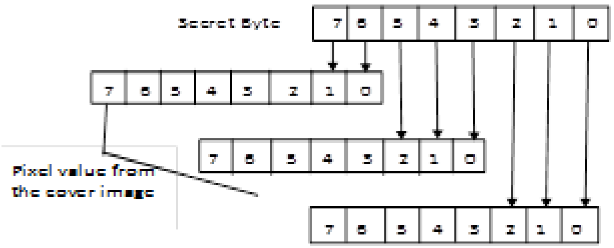

Figure 5: Hiding technique to 2/3 LSB method

It is simply memory access and it maps one secret byte to one Cover data pixel. Author have developed the Nios processor which is embedded processor and it is a part of the FPGA board. The processor execute programs loaded in the SDRAM memory to control the operations. It also serves as interface between the system and SDRAM. The processor receives and sent data from UART to SDRAM. The processor interface the Steganography to SDRAM.

Table 2: Simulation Result for clown, Baboon and Lena

Design	MSE	BER	PSNR(dB)
Clown	6.0	0.15	40.3
Baboon	5.2	0.15	40.3
Lena	2.2	0.15	40.3

Dr. Ahlam Fadhil Mahmood et al [12] have proposed FPGA Based LSB Embedder and Extractor It consists of six parts: Address Generator (AG), Color Space Converter (CSC), block memory, Steganography Embedd Unit (SEU), Steganography Extract Unit (DSEU) and main controller (MCU). AG is responsible for calculating the addresses which are used to access the block memory using six nine bit LFSRs units. AG generates random addresses and it composed of six LFSR operates in Parallel. Our eye is less sensitive to hue and Saturation. If the colour information is stored in the intensity and colour format then processing speed can be made faster. So Author have Use CSC to converted RGB colour Space to YCrCb Colour Space. They uses Single Port Ram for each Channel to Store Steganography Image SEU and DSEU Unit are to Embedded and Extract the Secret image and all above Unit is Control by Main Controller. The proposed embed and extract algorithms are implemented using MATLAB Simulink and System Generator and Synthesis result are Shown in Table.3

Table 3: Synthesis Result

Slices	2411 out of 13696 17%
Frequency(MHz)	107.75
Throughput(Mbps)	3 pixel/ Clock cycle
Latency	0.065µsec

Table 4: Comparison of Times

Image	Size	Software	Hardware	Ratio
babbon	512*512	2.6727	0.00418	639.4
pepper	512*512	2.6727	0.00418	639.4
boat	512*512	1.3421	0.00209	642.1
sailboat	512*512	2.6727	0.00418	639.4

V. CONCLUSION

This paper has discussed some steganographic techniques which are proposed on field programmable gate array. Mainly the spatial domain and techniques are taken into account. After going through the synthesis results for respective techniques, we have observed that FPGA is the best solution for the efficient image processing. X-box Mapping approach is better because without stego key, no one can extract the original information from the stego-image. 2/3 bit LSB technique is simple than the LFSR based technique but LFSR Based technique Gives better security as it generates the random address to fetch the cover data and then it embedded the secret image. Also Future work can be done by incorporated above the methods to build the Steganography unit and also we can work into transform domain for better security.

REFERENCES

[1] Kevin Curran, “An Evaluation of Image Based Steganography Methods,” International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2.

[2] J. Fridich, and R. Du, “Secure Steganographics Methods for Palette Images”, In Information Hiding, 3rd International Workshop, Springer 1999, pp. 47-60.

[3] Khalil Challita and Hikmat Farhat, “Combining Steganography and Cryptography: New Directions,” International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208. The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[4] J. Zollner, H. Federrath, H. Klimant, et al., “Modeling the Security of Steganographic Systems”, in 2nd Workshop on Information Hiding, Portland, April 1998, pp. 345-355.

[5] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., “Information Hiding – A survey”, Proceedings of the IEEE, 87:07, July 1999.

[6] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sunder Singh, “Hiding Encrypted Message in the Feartures of Images,” IJCSNS International Journal of Computer Science and Network Security, VOL. 7, No.4, April 2007.

[7] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001.

[8] Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, Visual Image Signal Processing, 147:03, June 2000.

[9] Krenn, R., “Steganography and Steganalysis”, http://www.krenn.nl/univ/cry/steg/article.pdf.

[10] Mr. Jagadeesha. D.H, Mrs. Manjula.Y, Dr. M. Z. Kurian, "FPGA IMPLEMENTATION OF X-BOX MAPPING FOR AN IMAGE STEGANOGRAPHY TECHNIQUE," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 6, June 2013.

[11] 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.

[12] Dr. Ahlam Fadhil Mahmood, Nada Abdul Kanai, Sana Sami Mohmmad, "An FPGA Implementation of Secured Steganography Communication System," Tikrit Journal of Engineering Sciences/Vol.19/No.4/December 2012, (14-23).