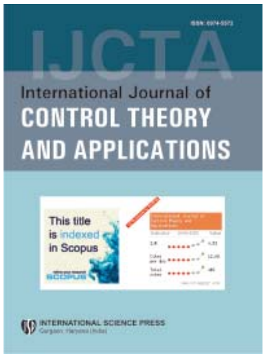

International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 9 • Number 42 • 2016

Hardware Implementation of Steganography Using LSB

Savita.D. Torvi[a] and K.B. Shivakumar[b]

[a]Research Scholar, Sri Siddhartha Academy of Higher Education Karnataka, India

E-mail: savitadtorvi@gmail.com

[b]Research Supervisor, Sri Siddhartha Academy of Higher Education

E-mail: kbsssit@gmail.com

Abstract: The communication network transfers information to the global world .in the advance development of the world web the security becomes crucial.to overcome this steganography and cryptography plays an important role to secure data while transmitting the data over the internet. In the proposed work we used both steganography and cryptography, first the input message is encrypted and then an encrypted message is embedded in image file using lsb method. And also implemented on FPGA because of their smaller size, weight and power consumption. This reduces the area, increases the speed and produced the better performance.

Keywords: *LSB, steganography, communication, FPGA.*

1. INTRODUCTION

In the recent technology computer and cyberspace are the main sources for communication, which links the distinct parts of world as one universal worldwide. In the rapid development of internet, data transmission over internet becomes the significant challenge and to protect the data while transmitting. This can be achieved by the method Steganography. As a result, the information can be transferred for longer distance. Because this has the major issue to secure the information for a longer distance. This is very essential in case of transferring confidential data. This problem can be eliminated by the use of steganography methods. This steganography is powerful method and when it is combined with encryption it gives more security.

The letter "Steganography" has two words stegno and graphia. Stegno means covered and graphy means writing, that means covered writing. It is come from Greek word. It is a data hiding method, which is used to transmit a message on a communication media where some other type of information is already being transmitted. The aim of Steganography is to hide information inside audio, video the .text or images in such a way that the hackers should not detect the secret message present inside the cover file. Steganography attempts to hide the existence of communication.

Fig1. Shows the basic model of Steganography and it has three components

1. **Contribution :** The research paper HISL is proposed for secure communication which is able to send and receive encrypted messages embedded in image file.

2. **Organization:** The paper is organized such that the related works of the proposed stegnographic model are explained in section II whereas the model is explained in section III and the performance analyses as well as the conclusions are discussed in section IV and section V respectively.

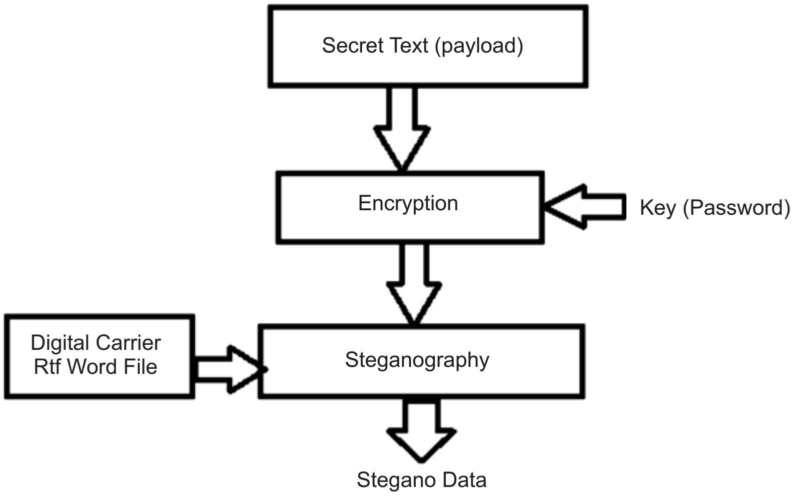

Figure 1: Basic block diagram

2. RELATED WORK

Mustafa Oman Ali and Rameshwar Rao [10] described the digital watermarking techniques by using VLSI technology based on LSB technique and shows that hardware required less area, reduction in power.

Saurabh Kumar. Presented AES encryption VLSI architecture of S-box, and shown constant area, increased speed and power.

Akshay et al., presented a new Steganographic method using Discrete Wavelet Transform

(DWT) and Least Significant bit (LSB).He was generated algorithms for transmitting captured images. He used the LSB method to hide the data in the least significant bit of image pixel. This work was implemented by XPS and VB .the image was converted into pixel format using MATLAB and adding source file and header file, converted into binary form and downloaded on FPGA.

Williams Antonio PantojaLaces and Hernandez explained an efficient hardware implementation of a low complexity steganographic system using digital images and implemented on the hardware architecture on a Field Programmable Gate Array (FPGA).

Kiran Agarwal, et al, Explained that the information can be embedded and extracted by using efficient multiplier and says that it require less area, increase in speed and high security.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

3. PROPOSED SYSTEM

Steganography is used for secure communication. Information can be hide on different files are used, because of the internet frequency digital images are commonly used.Fig1 Shows the detailed block diagram of our work. The input image is converted into binary image using MATLAB. So that it is easy for encode the information which is to be hidden and also to perform embedding operation. This model has three parts 1) Encoding 2) Embedding 3) Extraction.

1. **Encoding:** The input message is encoded by the XOR operation with the key. The same key is used for both the encryption and the extraction.

2. **Embedding:** The image is converted in to the binary image. Divide he binary image into 8 bits. The encoded message is hidden into the LSB bytes.

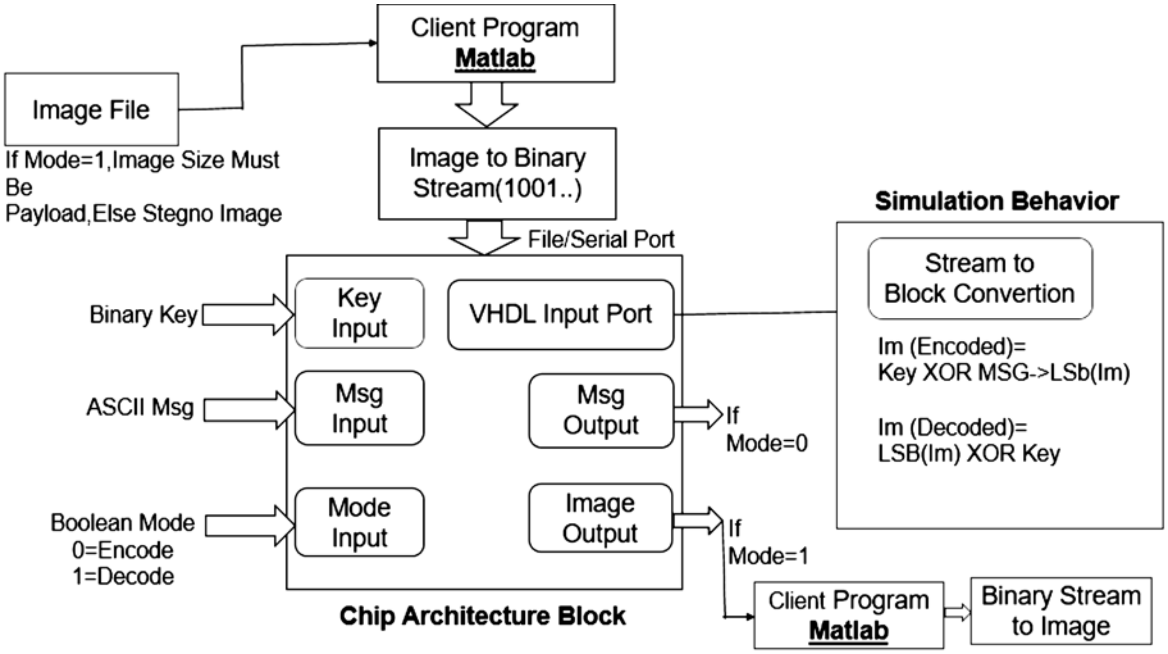

Figure 2: Detailed block diagram of the proposed work

Least Significant Bit (LSB) method: It is simple and common technique to embed the data in the cover image. Convert the image into binary *i.e.* one bit is stored in LSB of each pixel.

Example: A character ‘A’ hides into image.

ASCII value of A is 00100001

Binary image is say 0000000000000000100000010000000110000010000000101000000110000000111 ……….

Divide binary image into 8 bits

00000000, 00000001,00000010,00000011,00000100,0000010100000110,00000111

0000000**0**, **00000001**, 0000001**0**, 0000001**0**, 0000010**0**,

0000010**0**, 000011**0**, 0000011**1**

The hidden bits are underlined in the 8 bytes of the above example. Half of the bits will be changed in the LSB and we get stego image.

3. **Extraction:** The stego image is converted into binary image with MATLAB. Divide binary image into 8 bits. Then each byte is decrypt with XOR operation using key.

Data Hiding Algorithm:

Step 1: Read the cover file (image).

Step 2: convert the secret image into binary image.

Step 3: Encode the message which is to be embedding using XOR.

Step 4: Embed the encoded message using LSB.

Step 5: Write stego image.

Algorithm to receive data:

Step 1: Read the stego image.

Step 2: convert the stego image into binary.

Step 3: Convert it into secret image.

Step 4: Decrypt the bits.

Step 5: Retrieve the hidden message.

4. RESULTS

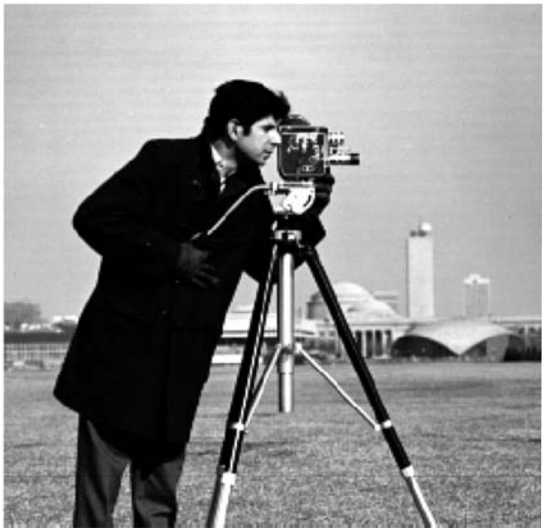

Figure 3: Input Image

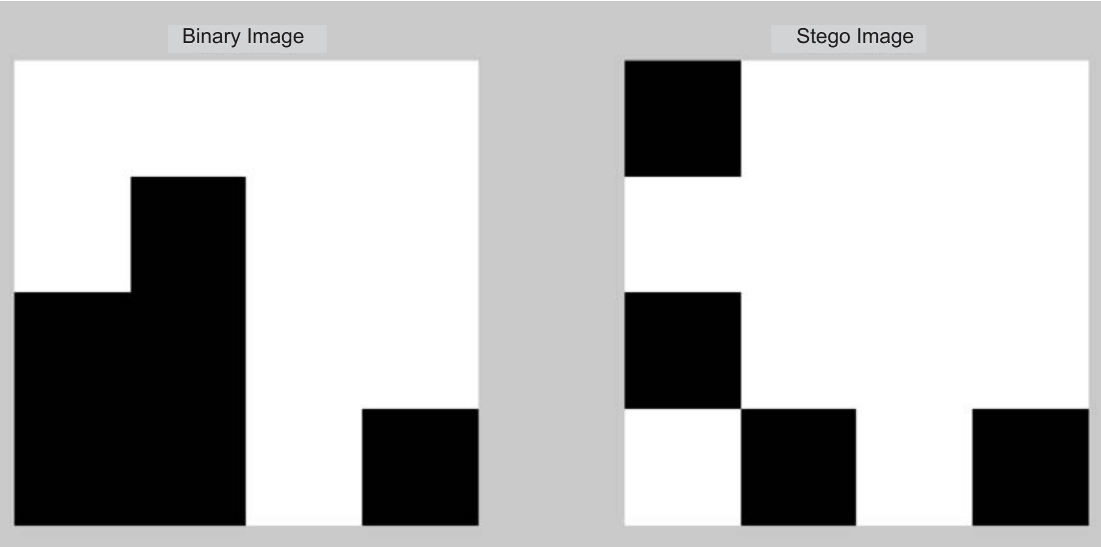

Figure 4: Binary Image

4.1. Simulated output in Xilinx

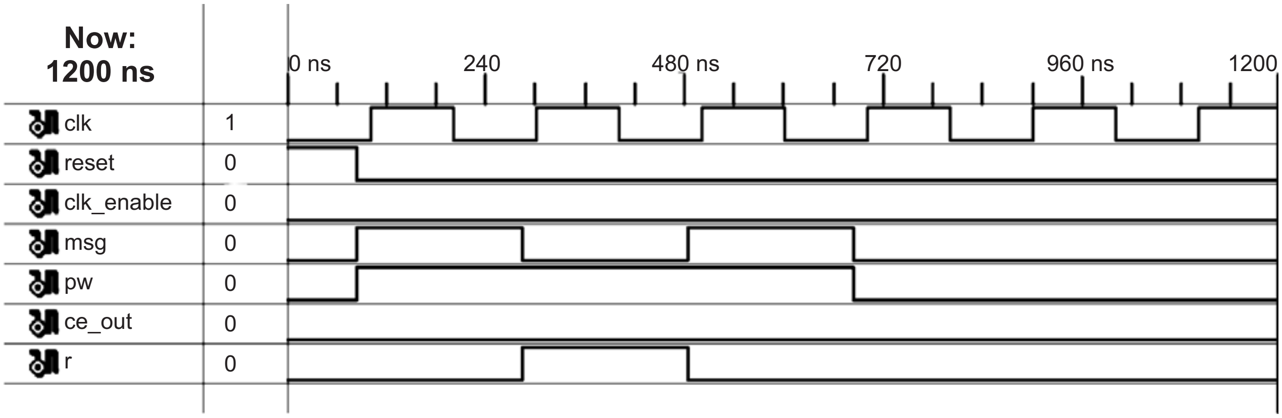

Figure 4

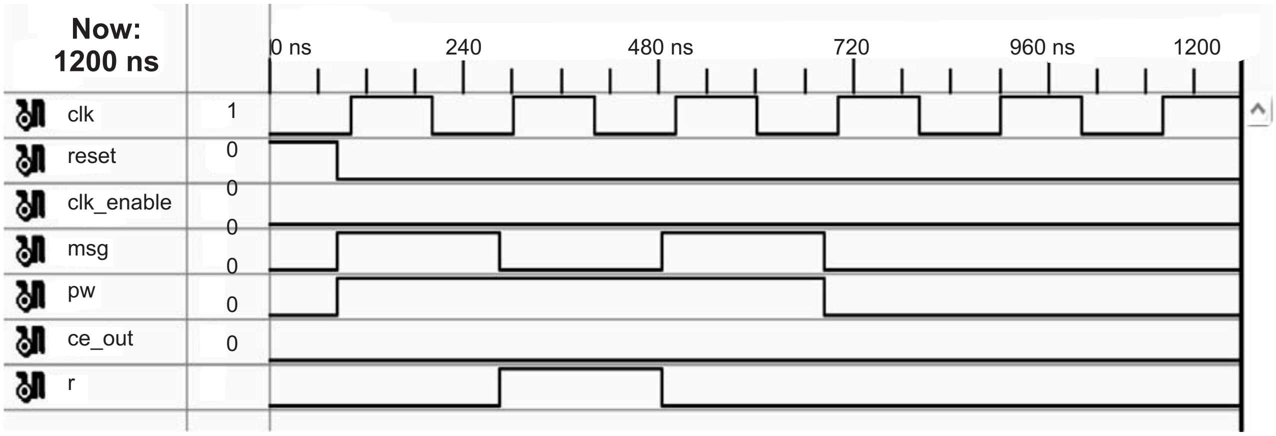

Figure 5

Figure 3 is the input image where the message will be embed and Figure4 represent the screen shots of stego image and binary image of results.

The proposed system has been verified using XILINX simulator using VHDL codes. We provided an input data of "11001001" and we received the same data at the output. And also we checked for many other inputs of 8 bits which all showing positive results. Therefore we can conclude that our system is working proper manner.

Number of Slices : 14 out of 3584

Number of Slice Flip Flops : 3 out of 7168

Number of 4 input LUTs : 8 out of 7168

Number of bonded IOBs : 7 out of 97

Number of GCLKs : 4 out of 8

Timing Report

Speed Grade: 5

Minimum period: No path found

Minimum input arrival time before clock: 3.439ns

Maximum output required time after clock: 6.56ns

Maximum combinational path delay: 6.824ns

4.2. 3 Bit RTL Schematic Diagram

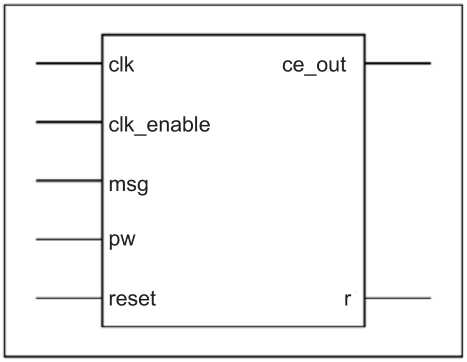

Figure 6

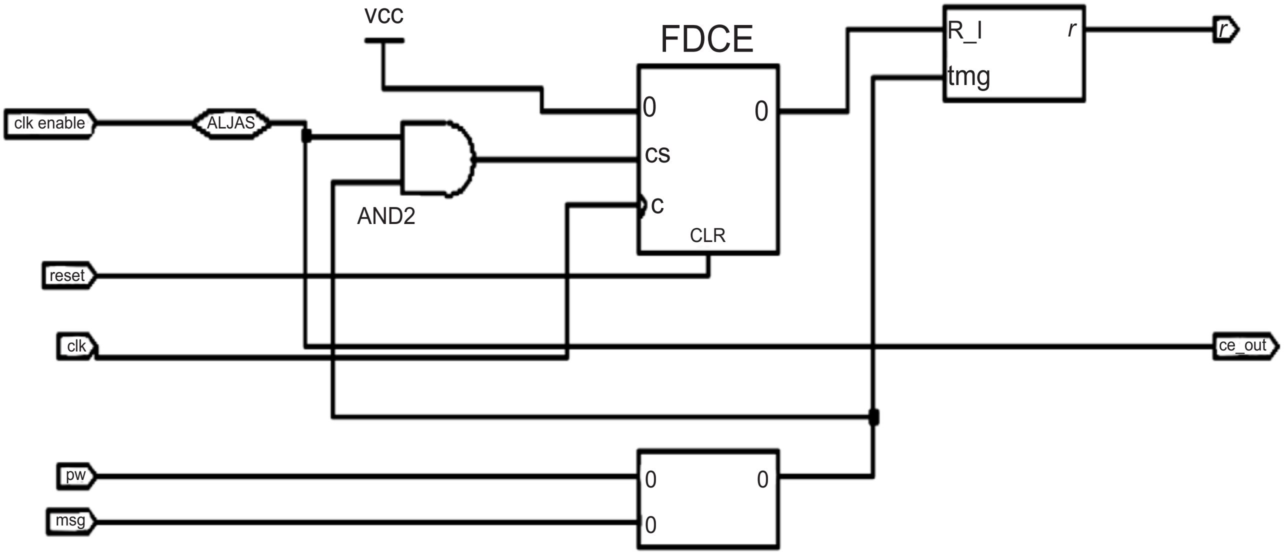

Figure 7

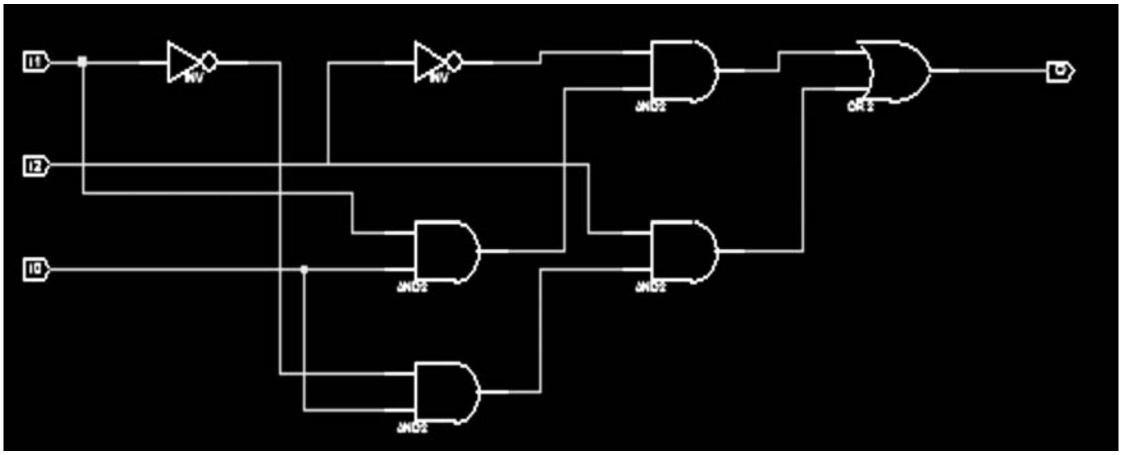

Figure 8

Table 1
Comparison table of area and graph

S. No.	*Parameters*	*A*	*B*	*C*
1.	Number of slices	115	42	10
2.	Number of 4 input LUTs	190	64	14
3.	Number of bonded IOBs	145	2	7
4.	Number of slice flip- Flops	104	64	8
	TOTAL	554	172	39

From Table 1, it is observed that [A], [B] used more no of slices, LUTS,IOBS and Flip-flops than [C]. Therefore our work takes less area to hide the message in image.

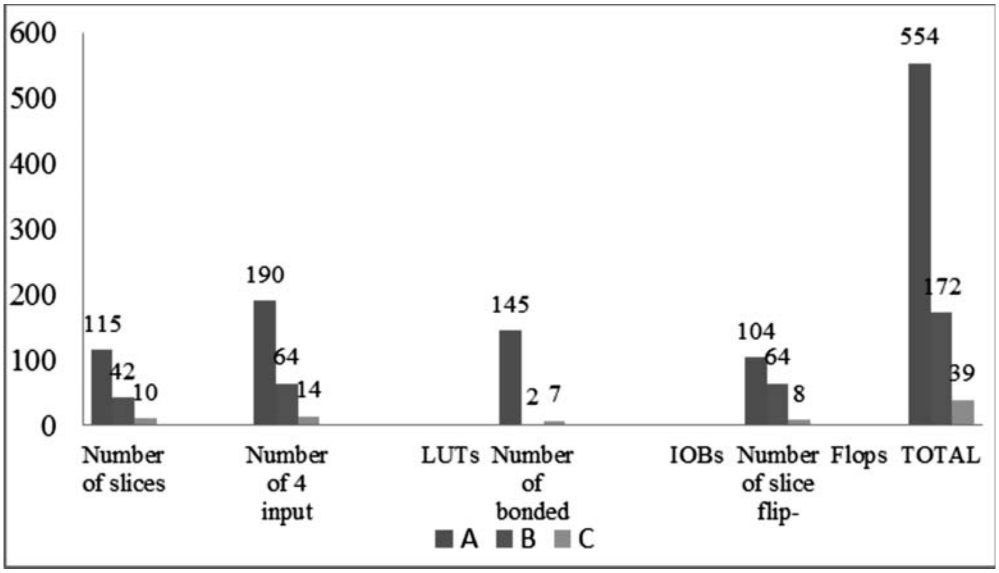

Figure 9

Table 2
Comparison table of power, speed, area and *psnr* and graph

S.No.	*Parameters*	*A*	*B*	*D*	*C 3 bit*	*C 8 bit*
1.	Power(*mw*)	2.16	–	–	13	24
2.	Speed(*ns*)	250	–	65	7.18	6.5423
3.	Area		–	17%	2%	
4.	PSNR(dB)	51.58	45	51.2	85.91	84.56

From Table 2 it is observed that [A], [B], [D] and [c] is our work. Comparing all the four our work takes less time and less area to hide data in to the image.

1. S. Raveendra Reddy* and S. M. Sakthivel "A FPGA Implementation of Dual Images based Reversible Data Hiding Technique using LSB Matching with Pipelining". Indian Journal of Science and Technology, Vol 8(25), DOI: 10.17485/ijst/2015/v8i25/80980, October 2015.
2. "FPGA Implementation of Image steganography using LSB and DWT". December 2015.

4.3. Results for 8 bit data

The following results are obtained for 8bit data.

PSNR: 90.58db

AREA: 132mb

POWER: 24mw

SPEED: 0.542ns

Number of Slices:	5 out of	68	0%
Number of Slice Flip Flops:	1 out of	1536	0%
Number of 4 input LUTs:	7 out of	1536	0%
Number of bonded IOBs:	21 out of	97	21%
Number of GCLKs:	1 out of	8	12%

4.4. 8 Bit Simulated Output

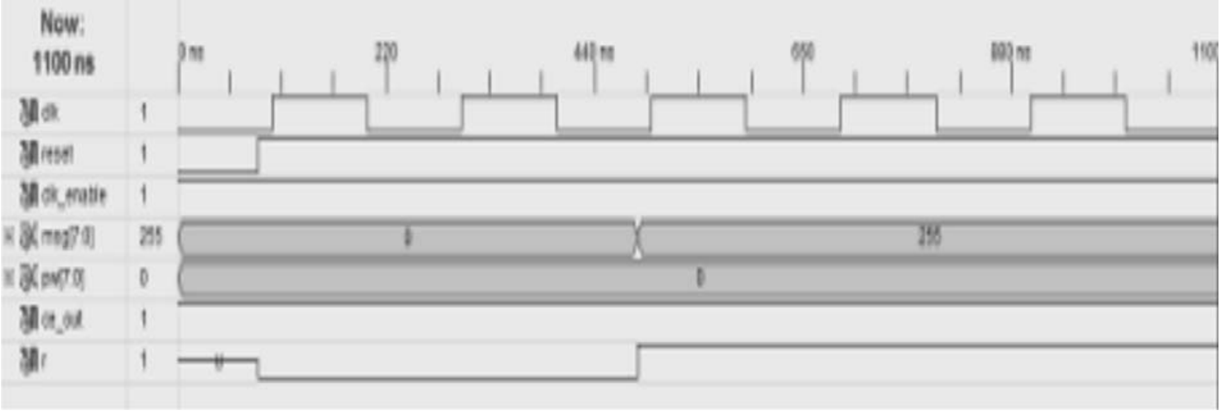

Figure 10

4.5. 8 Bit RTL schematics

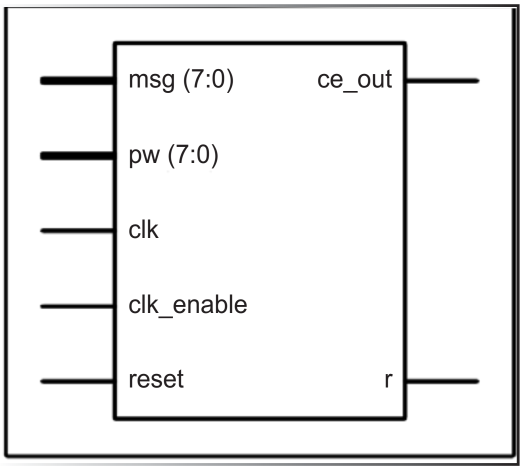

Figure 11

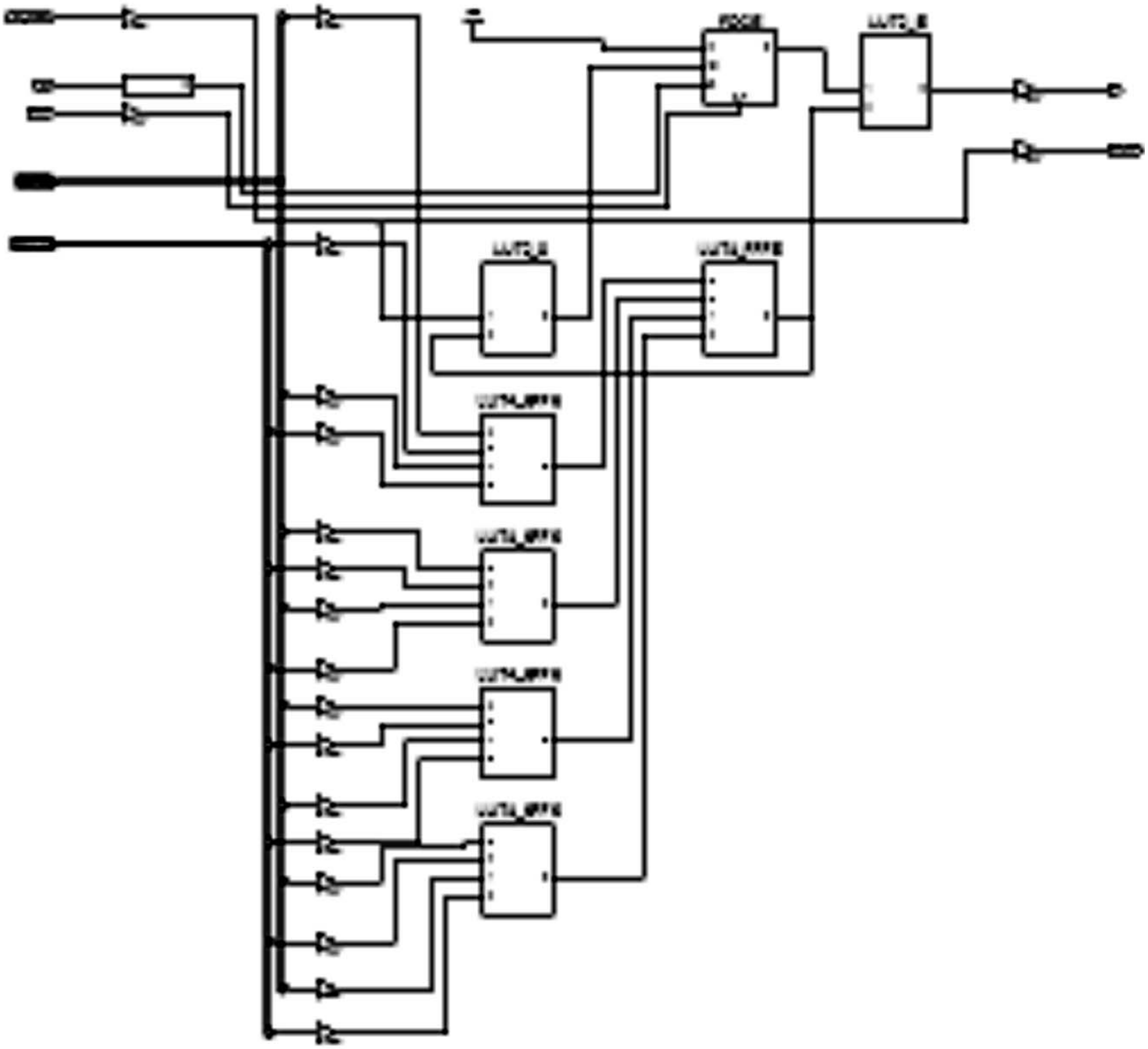

Figure 12

5. CONCLUSION

In this paper we have implemented a real time application of image steganography using LSB method. It is experimentally shown that proposed method is more effective than existing method and performance is also increase due to less time.

In future different spatial and transform domain methods and random based LSB method can also be used and implement on FPGA which will increase the speed.

REFERENCES

[1] Ahlam Fadhil Mahmood, et al, "An FPGA Implementation of Secured Steganography Communication System", Tikrit Journal of Engineering Sciences/Vol.19/No.4/December 2012, (14-23)

[2] Mustafa Osman Ali, Rameshwar Rao"Digital image watermarking basics, and Hardware implementation", International journal of modeling and optimization, vol.2, No 1, February 2012

[3] Saurabh Kumar, "An improved VLSI Architecture of S-Box for AES Encryption" International Conference on Communication Systems and Network Technologies. 2013 IEEE

[4] Akshay A. Jadhav; R. V. Babar; M. S. Gaikwad "Hardware implementation of digital watermarking system for real time captured image transmitting" Pervasive Computing (ICPC), 2015 International Conference 2015

[5] Williams Antonio Pantoja Laces; Jose Juan Garcia- Hernandez "FPGA implementation of a low complexity steganographic system for digital images" Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference 2015.

[6] Kalpana Shete, Mangal Patil, J. S. Morbale "FPGA Implementation of Image Steganography Using LSB and DWT "IJCSN International Journal of Computer Science and Network, Volume 4, Issue 6, December 2015.