Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-5, June 2017
Research Paper

www.ijsrnsc.org

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

Implementation of LSB Based Steganography Algorithms in FPGA

K. Nandhini[1*], B. Gomathi[2]

[1,2]ECE, SNS College of Engineering, Anna University, Chennai, Coimbatore, India

[*]*Corresponding Author: nandhiniece.snsce@gmail.com, Tel.: +91-7010568747*

Received: 05/Oct/2018, Accepted: 14/Oct/2018, Published: 31/Oct/2018

Abstract— Data hiding is one of the crucial techniques in network security. The word Steganography denotes hiding a confidential message (like audio, image, text, video) in a host signal (like Image, video) such that an onlooker cannot detect the existing content. In this paper data drubbing is takes place by the embedding modules that transmit the data and recovering data by extraction, with and without the concept of pipelining technique and it is realized using Xilinx device Virtex-V. A comparison for the pipelined and non-pipelined mode of data is done for parameter like timing constraints, delay, and memory usage. From the outcome, it is addressed that the data embedding using pipelining mode give better results in terms of very less embedding time compared to the non-pipelined mode. As this data hiding methodology using 4 LSB Steganography algorithm involves only simple operation, it is easy to implement as FPGA chip using Verilog HDL model Language.

Keywords— Steganography, 4LSB, Xilinx device, Verilog HDL

I. INTRODUCTION

All Transmitting an information through the web is turning into a noteworthy concern, with the goal that the information concealing method are utilized by individuals through the whole world. Data stowing away is the conspicuous territories in organize security, which contains different techniques like cryptography, steganography and watermarking.

In cryptography, information can be encoded by some calculation. In spite of the fact that the message can't be perused by the passerby, it draws in meddlers effortlessly as it is in muddled frame. In spite of the fact that it is utilized for security here and there we have to anchor the message, henceforth steganography came into the photo. This issue can be overwhelmed by Steganography, which implies concealing the mystery data behind a cover medium (video or picture, sound) with the end goal that their essence is ignorant to the spectators.

Steganography is the work of art of continue emitting a document, message record, ,for example, picture, and sound, video inside another record, message, picture or video. While considering an advanced based information concealing framework few key properties should don't fprget, which may be givn underneath.

- Imperceptibility
- Embedding Capacity
- Undetectability
- Robustness

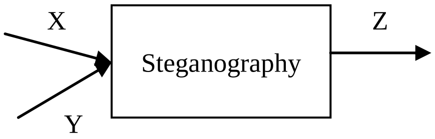

Figure 1. Block Diagram for Steganography

Where

X is the Cover files (image, audio, and video)

Y is the Message

Z is the Stego file

Cover file: It is a medium in which embedded our information. For hidden, it may be image, audio, text and video document. The different kind steganography technique use a exceptional form of cover files.

Stego-file: It is nothing but a cover file which contains confidential data (information which has to be sent) inner. This file is communicated over the channel among sender and receiver.

Message: The data or important information to be hidden or extracted. The message is also some time known as secret data. This secret message which is going to hide behind the host data.

Our work is organized in the following sections. The section II shows the previous work done by the early researchers and section III shows our proposed system in detailed manner about implementation of 4 LSB steganography algorithms using pipelining and without pipelining technique in FPGA. Result and discussion and the conclusions are in section IV and V respectively.

II. LITERATURE SURVEY

The Puja Mahajan, Prajakta Nimbalkar, Prtiksha Pawar proposes an enhanced FPGA based X-BOX mapping for a picture utilizing steganography strategy [4]. Minimum critical Bit (LSB) is a customary procedure utilized in steganography as it is simple and has a substantial covering limit. To embed diverse qualities X-Box system is utilized. In this mapping strategy, X-box will give the wellbeing of qualities and these qualities will be put away in an irregular way to enhance the security.

Jamil et al. [6] proposed a FPGA execution of LSB steganography approach on Altera group of Cyclone II FPGA instrument. The plan adjusts the trade offs Such as impalpability, fine and capacity. This paper proposed 2/3 LSB technique to gethigh quality picture and moreover to acess memory easily. Be that as it may, lapsed design is connected on Nios processor. As a final product this may limits the execution of the arrangement of principles even when contrasted with the plan discovered on FPGA device utilizing Hardware Description Language (HDL) which contain Verilog/Very High Speed Integrated Circuits (VHSIC) HDL.

.

Sathish et al. [10] proposes, another rapid reconfigurable engineering has been intended for Least Significant Bit (LSB) or multi-bit based picture steganography calculation that suits Field Programmable Gate Arrays (FPGAs) or Application Specific Integrated Circuits (ASICs) execution. The models are outlined and instantiated to actualize the total steganography framework. This framework is sufficiently able to give bigger throughput, since high degrees of pipelining and parallel activities are joined at the module level. The advanced structures are acknowledged in Xilinx Virtex-II Pro XC2V500FG256-6 FPGA gadget utilizing Register Transfer Level (RTL) consistent Verilog coding and have the ability to work progressively at the rate of 183.48 edges/second. Before the FPGA/ASIC execution, and the steganography framework is reenacted in programming to approve the ideas planned to actualize. The equipment actualized calculation is tried by changing inserting bit measure and the goals of a cover picture. As it is obvious from the outcomes exhibited that the anticipated structure is unrivaled in speed, territory and power utilization contrasted with other specialist's technique..

Elshazly et al. proposes a calculation that installs information in every segment of shading picture, where the mark of the transmitter and the length of the mystery content are covered up in Red part, while the twofold piece stream of the mystery content is covered up in Green and Blue segments of the shading picture [11]. Subsequent to inserting, the three parts are re-joined to shape a stego-picture. The stego-picture is going through a correspondence channel and a clamor might be added to it. At the recipient, the concealed content can be separated from the boisterous stego-picture with no learning of the first picture subsequent to applying a filtration in the pre-preparing stage. Utilizing MATLAB installing and removing forms are performed and utilizing Xilinx framework generator (XSG) it is executed on a field programmable door cluster (FPGA) . This calculations is actualized on FPGA has the upsides of utilizing an implanted multipliers and extensive memory. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are broke down to check and measure the factual mutilation between the cover picture and stego-picture, while the Normalized Cross Correlation (NCC) is utilized to assess the level of closeness between them. The trial results are demonstrating the productivity of the calculations and in addition demonstrating that installing bigger size of information with better aftereffects of MSE and PSNR.

III. PROPOSED SYSTEM

This paper cites about the LSB data hiding and recovering technique and presents the analyzed results for 4 Least significant bit (4 LSB). Using pipelining and without pipelining technique proposed algorithm is implemented in FPGA.

This paper proposed the steganography technique of 4 bit data hiding method which is based on LSB steganography. The LSB insertion technique recommended that data (bits of confidential data) can be swapped to the LSB of the cover medium and extraction technique recommended the data can be extracted from the stego image. Both the cover and secret image convert to binary format using MATLAB and it can be saved as a .coe file to store data in BRAM. Counter module can be used to increase the address value.
Simultaneously two data which is fetched from the BRAM and it is given to the encryption module.

The encryption process comprises

i) LSB extractor

ii) Message hiding module

In LSB extractor 4 LSB of the cover image (CI) is gets extracted. In messaging hiding module two conditions is checked which means 4 LSB of the CI and SI is equal or not. If equal means keep as it is otherwise swapping operation is performed, this two module operation can be performed in single clock cycle. Hence this module generates a stego image, and it can be displayed in a VGA monitor. Similarly stego image pixel value can be converted to binary format and it is given to the decryption module.

The decryption process comprises

i) LSB finder

ii) Message extractor.

Similarly from stego image 4 LSB get extracted after the concatenation confidential message get extracted from the stego image.

A. Steganography block

The proposed methodology for LSB steganography is contain two-step approach, namely,

- Encryption
- Decryption

The Encryption process consists Encryption algorithm module, which include LSB extractor and message hiding module. The designed system reads the confidential Message (Image) in the form of decimal, before embedding into the cover medium the decimal value is converted into the binary format.

Encryption is the core part of the drubbing process in data hiding technique. This module acquire two inputs, namely, secret message (binary) and extracted 4 LSB of the mask image, hence it produce stego image which are shown in Figure 2. Similarly perform this operation for entire pixels of cover and secret image from this stego image get generated.

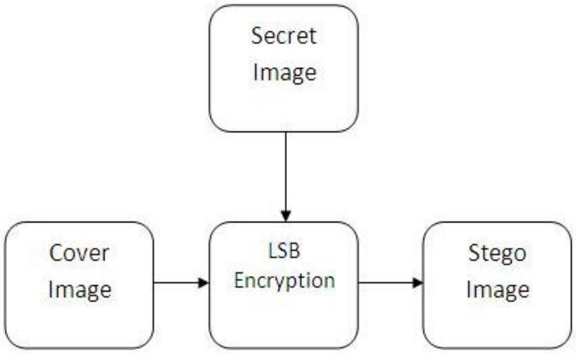

Figure 2. Block diagram of Encryption Algorithm

Conversely, the decoding module performs the LSB finder and extractor which is shown in Figure 3. In this module 4 LSB get extracted from the stego image, which is identical to the binary form of secret data, secret image can be acquired from the extracted data bit

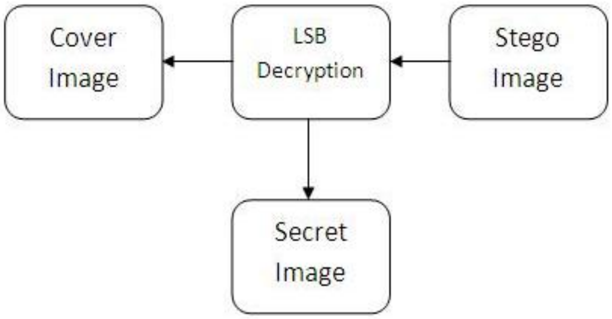

Figure 3. Block Diagram of Decryption Algorithm

B. LSB Algorithm

The algorithm procedure for proposed method has two parts which is cited below;

Encryption Algorithm

Step 1: Read the cover and secrete image which is to be hidden in the cover image.

Step 2: Convert confidential image pixel in to binary format.

Step 3: Separate 4 LSB of each pixels of cover image.

Step 4: Replace 4 LSB of cover image with 4 MSB of secret image .

Step 5: Replace 4 LSB of cover image with 4 LSB of secret image.

Step 6: Repeat step 4 & 5 for entire pixels in cover image.

Step 7: Write stego image.

Decryption Algorithm

Step 1: Read the stego image.

Step 2: Extract LSB of each pixels of stego image.

Step 3: Concatenate the extracted bit.

Step 4: Convert it into secret image.

C. Flow chart for Encryption Algorithm

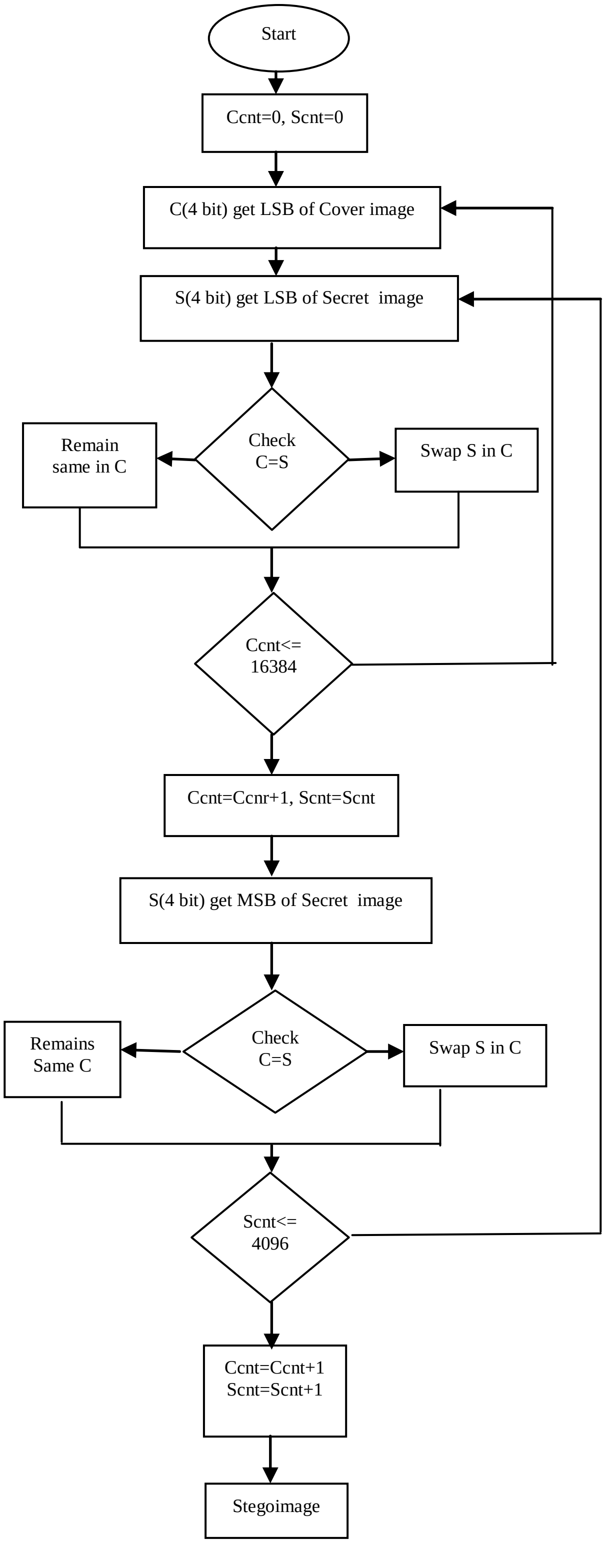

Figure 4. Flow chart of Encryption Algorithm

D. Flow chart for Decryption Algorithm

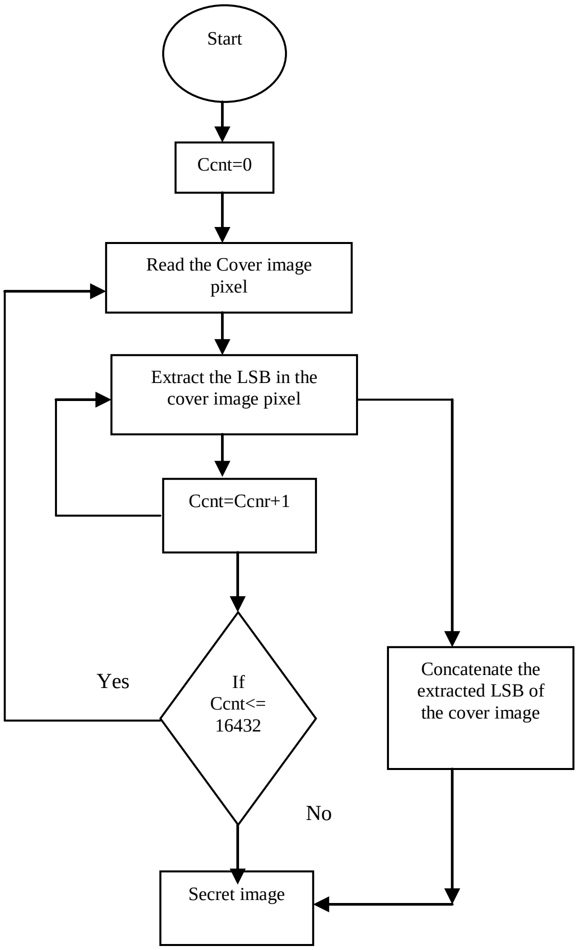
Start
Ccnt=0
Read the Cover image pixel
Extract the LSB in the cover image pixel
Ccnt=Ccnr+1
Yes
If Ccnt<= 16432
No
Concatenate the extracted LSB of the cover image
Secret image

Figure 5. Flow chart of Decryption Algorithm

Pipelining

Pipelining is one of the techniques to improve the processing speed of the processor. In pipeline concept, buffer is considering as delay initially cover image pixel and secret image pixel are stored in BRAM using IP Core Generator. CIP (Cover Image Pixel) address is incremented for every rise and fall enable signal, but SIP (secret Image Pixel) is increment for every enable rise signal and the LSB is separated from CIP (Cover Image Pixel).using LSB algorithm, encryption is performed in transmitter side and reversible operation is performed in receiver side.

IV. RESULT AND DISCUSSION

In this paper standard 8 bit gray scale test images are used for the experimentation. The CF (Carrier File) size is 128x128 and SM (Secret Message) size is 64x64 gray image and their performance was measured and compared which shown in Table. I, II and III.

TABLE .I. Source

Algorithm	Carrier file(12X128) bit	Secret message(64X64) bit
4 LSB	Lena.png 131,072	Babbon.png 32,768

TABLE .II. Performance Comparison of Encryption in MATLAB Simulation

Algorithm	Peak-SNR	SNR	MSE
4 LSB	35.6168	30.960	17.8401

TABLE .III. Performance Comparison of Decryption in MATLAB Simulation

Algorithm	Peak-SNR	SNR	MSE
4 LSB	35.6522	30.1502	17.5150

A. Simulation Results

The verilog code for the proposed model is designed and the code is simulated using Model Sim Altera 6.4a starter Edition.

Initially cover (128x128) and secret (64x64) images are taken and that image can be converted to corresponding binary value using MATLAB after that it can be saved as a Coe file to store image in a BRAM for further processing.

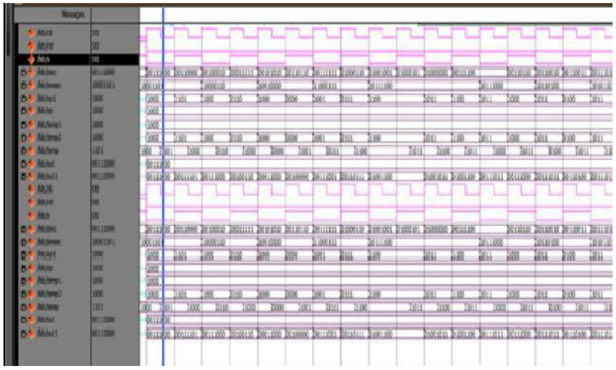

Figure 6. Simulation result for Encryption

The waveform for encryption algorithm is presented in Figure 6. This module performs the encryption which consists of LSB separator and encryption block. In this, the enable signal is used for increasing cover and secret image pixel. If the enable signal is high or low cover image pixel continuously get increased, If enable signal is low the secret image pixel get increased and the encryption process get performed.

The waveform for decryption algorithm is presented in Figure 7. This module contains LSB finder and message extractor.

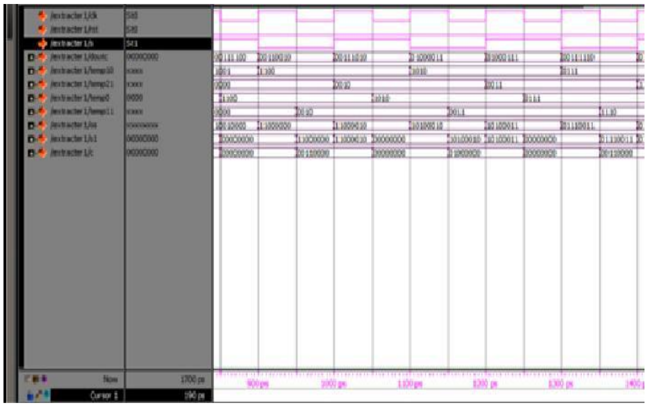

Figure 7. Simulation result for Decryption

The performance comparison of pipelining and without pipelining in the encryption and decryption side for delay and memory is shown in Table. IV and Table. V.

TABLE IV. Performance Comparison of Encryption in Xilinx

Method	Memory	Delay
Pipelining	214628KB	2.48ns
Without Pipelining	200693KB	3.648ns

TABLE V. Performance comparison of Decryption in Xilinx

Method	Memory	Delay
Pipelining	225433KB	3.019ns
Without Pipelining	214052KB	3.78ns

By comparing the result of with and without pipelining technique, memory size is increased. Buffer is consider as a delay. Processing time is reduced in both embedding and extracting side.

V. CONCLUSION

The project addresses the computation delay reduction and throughput increase for the LSB based image steganography. The algorithm does embedding in the cover medium in an invisible manner. This is achieved by implementing the encryption and decryption schemes of LSB steganography in device such as FPGA. The architectures developed in this work are new and are capable of processing in real-time since each module designed adopts high degrees of pipelining schemes. The various modules of embedding and extraction were realized using Xilinx VIRTEX-5 device using RTL compliant Verilog HDL coding. The proposed algorithm is also validated using Modelsim simulation before hardware implementation since this approach confirms the proposed concepts.

REFERENCES

[1] Hussain M, Hussain M (2013)," A survey of image steganography Techniques" International journal of Science and Technology, Vol. 97, No 18, 2014 .

[2] Tseng YC, Chen YY and Pan HK," A secure data hiding scheme for binary images", IEEE Trans Commun, vol. 50, No. 8, 2002.

[3] Fan L, Gao T, Cao Y , "Improving the embedding efficiency of weight matrix-Based steganography for gray scale images", Computer Electronics Engineering Computer, vol. 39, No. 3, 2013.

[4] Puja Mahajan, Prajakta Nimbalkar and Prtiksha Pawar," Improved FPGA base X-Box Mapping of an image using Steganography Technique", International Journal of computer Application (0975-8887), 2016.

[5] Mohd BJ, Abed S, Al-Hayajneh T and Alouneh S , "FPGA Hardware of the LSB Steganography method", Computer,Information and Telecommunication Systems (CITS), Vol.54, No. 5, 2012.

[6] Fan L, Gao T and Yang Q, Cao Y , "An extended matrix Encoding algorithm for Steganography of high embedding efficiency", Comput Electrical Engineering,vol.37, No. 6, 2011.

[7] Fan L, Gao T and Chang CC , "Mathematical analysis of extended matrix coding for steganography", In: Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013.

[8] K. Sathish Shet , A. R. Aswath, C. Hanumantharaju and Xiao-Zhi Gao," Design and development of new reconfigurable architectures for LSB/Multi-bit Image Steganography System", Springer Science + Buisness Media New York, 2016.

[9] E. A. Elshazly, Safey A. S. Abdelwahab,R. M. Fikry, S. M. Elaraby,O. Zahran and M. El- Kordy ," FPGA Implementation of Robust Image Steganography Technique based on Least Significant Bit (LSB) in Spatial Domain",International Journal of Computer Applications vol. 145,no. 12, 2016.

[10] Amirtharajan R and Rayappan JBB ," An intelligent chaotic embedding approach to enhance stego image quality",Inform Science, vol. 193, pp. 115-124, June 2012.

[11] Bassam Jamil Mohd, Saed Abed, Thaier Al- Hayajneh and Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method," IEEE Transaction on consumer Electronics, vol. 978, no. 1, pp. 4673– 1550,2012.

[12] Mamta Juneja and Parvinder Singh Sandhu, , "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, vol. l 9, No:3, pp.405-424, 2013.

[13] Upadhyay HN and Rayappan JBB," Survey and analysis of hardware cryptographic and steganographic systems on FPGA",J Applied Science, vol. 12, No. 3, pp. 201–210, 2012.

Authors Profile

Ms. K Nandhini pursed Bachelor of Engineering from P.S.R Engineering College, India in 2015 and Master of Engineering from MEPCO Schlenk Engineering College in year 2017. She is Currently working as Assistant Professor in Department of Electronic and Communication SNS College of Engineering, India since 2017. He is a member of IAENG & ISRD since 2017. She has published more than 4 research papers in reputed international Her main research work focuses on Cryptography Algorithms, Network Securityand Image Processing. He has 1.5 years of teaching experience .

Ms. B Gomathi pursed Bachelor of Engineering from K.T.V.R Knowledge Park Engineering and Technology, India in 2012 and Master of Engineering from Avinashilingam Institute for Home Science and Higher Education for Women University in year 2015. She is Currently working as Assistant Professor in Department of Electronic and Communication SNS College of Engineering, India since 2015. she is a member of IAENG & ISRD since 2015. She has published more than 10 research papers in reputed international Her main research work focuses on VLSI and Embedded . He has 3.5 years of teaching experience .