A REVIEW ON FPGA-BASED SECRET DATA HIDING IN DIGITAL IMAGE USING STEGANOGRAPHY

[1]Ms. Vaishnavi V. Phiske, [2]Dr. Nilesh N. Kasat
[1]PG student, [2]Asso. Professor
Department of Electronics and Telecommunication, Sipna COET, Amravati, Maharashtra, India.

Abstract : Security of information is very important in terms of communication and the secrecy of how to decode it.Steganography is hiding of secret message within an ordinary message and the extraction of it at its destination. It is beneficial for securely storing sensitive data. It is one of the very powerful and popular techniques used for hiding information. Designing steganography in hardware helps to speed up steganography. In this paper, hardware implementation of LSB steganography technique is performed using MATLAB and FPGA, in which secret data is concealed within digital image and extraction of secret data on the FPGA.

IndexTerms **- Data hiding, FPGA, LSB, MATLAB, Steganography.**

I. INTRODUCTION

The last decade has witnessed the rapid development in information technologies and the wide availability of digital consumer device. Digital representation of information makes it possible to illegally produce an unlimited number of perfect copies. But at same time this leads to the hacking vulnerability and duplicity of the original information. The secrecy of digital information ought to be maintained once being communicated over the web. Interest for information hiding techniques has grown in the last few years. The most modern technique to this problem is digital steganography scheme. In a large number of applications, it is desired that the communication to be done in secrete. Data should be more secured while transmitting it. The steganography is the latest technique to send data safely to receiver. Image steganography is one of the most widely acceptable data hiding techniques. It is concerned with transmitting a secret message while hiding its existence.

Steganography is the art and science of embedding a secret text in a cover image without leaving a remarkable track on the cover image. The secret text is hidden in the cover image and the resulting image is called a "stego-image". The stego-image is passing through a communication channel. At the receiving, a pre-processing stage is applied to the received stego-image, then the secret text can be extracted from it. The most popular and frequently method of Steganography is the Least Significant Bit embedding (LSB). This paper focuses on a LSB based image steganography algorithm as it considered as one of the famous approaches that used for embedding the existence of the secret text in a cover image in which the LSBs of a cover image are changed according to the bit stream of the secret text to be hidden.

II. LITERATURE REVIEW

The originality of the digital data is altered during the process of transmission and sharing over internet. Hence there exists a problem in sending the data in a imperceptible manner. Data hiding is one of the methods to hide the secret data in the host content and transmit in an effective manner. Various authors proposed methods in order to secure the data.

Dr. Ahlam Fadhil Mohmmad, Nada Abdul Kanai, Sana Sami Mohammad [1] have developed a new method for FPGA implementation of secured steganography system. In this paper, reversible steganography scheme has been presented, different from the schemes using adaptive LSB method and LFSR techniques. This work showed attractive results especially in the high throughputs, better stego-image quality, requires little calculation and less utilization of FPGA area. Shreedeep Gangopadhyay, Bhaskar Banerjee [2] presents a methodology for implementing real-time image processing applications on a reconfigurable logic platform using Xilinx System Generator (XSG) for Matlab. In general, this work deals with explorations of the application of image processing particularly in the field of hidden data transmission, copyright protection.

FPGA implementation of digital watermarking system is presented by K. Tamilvanan, R. B. Selvakumar [3]. This paper proposes Discrete Wavelet Transform (DWT) to authenticate the multimedia image and it can convert the image from spatial domain to frequency domain. This System is developed on Xilinx Spartan3 FPGA device using embedded development kit (EDK) tools from Xilinx. S. Raveendra Reddy, Sakthivel S. M. [4] have developed the verilog based FPGA implementation of data hiding in grayscale image using the concept of the LSB Matching technique. In this verilog based data hiding process the secret digital signature is hidden in the host image then analyzed with the PSNR value and Payload capacity.

Prof. L. K. Chouthmol, Mr. R. V. Rathod [5] have proposed FPGA implementation of Data hiding in Images. This research provides a hardware solution for information hiding in 8-bit gray scale image using Least Significant Image. Steganography technique followed by Image compression using Discrete Wavelet Transform. This work focuses on the image steganography with an image compression using least significant bit with Discrete Wavelet Transform on FPGA Spartan III EDK. Hardware Implementation of LSB Steganography using MATLAB and FPGA is presented by Prof. Sheetal G. Khadke and Apurva S. Mahajan [6]. The system represents 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.

A. A. Prabhune and S. M. Joshi [7] have developed a information hiding technique for data security using FPGA. The algorithm implements data embedding algorithm which is capable of hiding more secret data while keeping the stego-image quality degradation imperceptible. At the receiver end user enters the password, if that password is correct then that authorize user can be able to extract data from video frame. E. A. Elshazly, Safey A. S. Abdelwahab, et al [8] proposed LSB based image steganography algorithms for embedding data in color images. In this work, algorithms are performed using MATLAB software and implemented using FPGA. The proposed algorithm is based on embedding the signature of the transmitter and the length of secret text in the Red channel and the secret text itself in the other two channels. The experimental results prove that the proposed algorithm can embed larger secret text (up to 98,304 characters) with better results of PSNR and NCC, compared to the previous algorithms.

Data hiding in a digital image with FPGA implementation is presented by Premalatha P, Amsaveni A [9]. This paper discusses economical implementation of a low-complexity steganography system with digital image as host system. Simulink block is designed for embedding and extracting process and the same block can be converted to VHDL code and the same will be implemented in FPGA. This technique provides a higher PSNR and NCC value. Harini V and Vijayaraghavan V [10] have proposed a technique for enhancement of secret data communication through encrypted data embedding in colour images. It is implemented in FPGA. The design architecture when implemented on FPGA Spartan III offers high processing speed, which might give an impulse for the researchers to a very fast, programmable & cost effective hardware solution in the area of Secure Communication.

With the literature review, various observations are drawn as mostly LSB techniques are employed for image steganography. Now-a-days, FPGA implementation provides excellent results than MATLAB implementation in terms of processing time, power and area requirement.

III. PROPOSED WORK

For a successful data hiding, the technique should embed the secret data without altering the cover image and extract the hidden information from an image with the high degree of knowledge integrity. Following block diagram shows the proposed method to hide the existence of the embedded information.

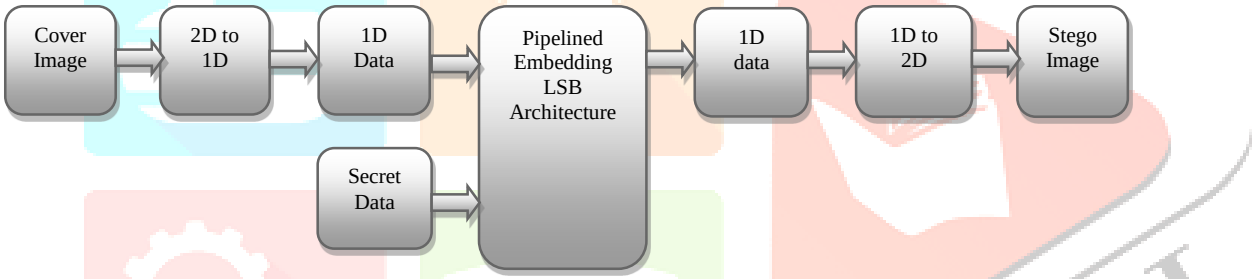

Fig -1: Embedding Process

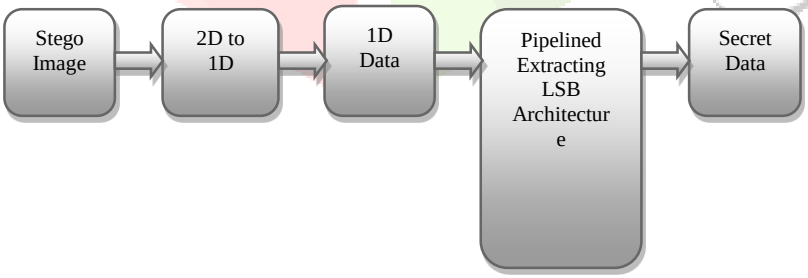

Fig -2: Extraction Process

The embedding process includes cover image as input, pre-processing stage, post processing stage and stego image as output. In the pre-processing stage, the cover image is converted to its pixel value. The secret data is converted to its corresponding to its binary value. The least significant bits of each pixel value is replaced by binary value of secret data. The post-processing stage involves combining the cover image and secret data which results in stego image using MATLAB. In LSB steganography, the information is hidden within the last bits of the pixels of the cover image. Mostly the value after replacement is same as pixel value. Hence there is no change in cover image before and after steganography.

Extraction will be the reverse process of embedding and retrieves the secret data from image. Before applying to the LSB architecture, this stego image is converted into its 1D signal using MATLAB. In FPGA, secret data is extracted from 1D signal by using VHDL code. The secret data is recovered and download on the FPGA kit. Here, the embedding phase of the proposed algorithm is performed using MATLAB and extraction phase is implemented using FPGA.

FPGA based data hiding system seems to be an interesting option since its capacity for parallel processing could allow multi-channel processing. The FPGA contains logic components that can be programmed to perform complex mathematical functions making them highly suitable for the implementation of matrix algorithms. FPGA helps to solve both security and processing speed.

IV. CONCLUSION

In this paper, we presented a review on FPGA based secret data hiding. Steganography technique is implemented by using LSB technique to the secret image to get the better results. Designing steganography in hardware helps to speed up steganography. The main goal of steganography is to ensure that the transmitted message is completely masked, thereby ensuring that the message is accessible only to the intended receiver and not to any intruders or unauthorized parties. The steganography will continue to grow in importance as a protection mechanism.

REFERENCES

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

[2] Shreedeep Gangopadhyay, Bhaskar Banerjee, "Image processing and data hiding framework on FPGA based platform ", ISSN (P):2320-2084, Volume-1, Issue-3, May-2013.

[3] K. Tamilvanam, R. B. Selvakumar, "FPGA implementation of digital watermarking system ", IJCSMC, Vol.3, Issue.4, April 2014, pg 1321-1327.

[4] S. Raveendra Reddy, Sakthivel S. M., "A FPGA Implementation of Data hiding using LSB matching method", IJCST, Volume 03, Issue 04, April 2014, pg 1321-1327.

[5] Mr. R. V. Rathod, Prof. L. K. Chouthmol, "FPGA implementation of Data hiding in Images", IJAREST, ISSN (0):2393-9877, ISSN (P):2394-2444, Volume 2, Issue 12, December-2015.

[6] Apurva S. Mahajan, Prof. Sheetal G. Khadke, "Hardware Implementation of LSB Steganography using MATLAB and FPGA", IJCST-Volume 3, Issue 4, Jul-Aug 2015.

[7] A. A. Prabhune, S.M. Joshi, "Information Hiding Techniques for Data Security Using FPGA", IJARCSSE, volume 6, Issue 1, January 2016.

[8] E. A. Elshazly, Safey A. S. Abdelwahab, R. M. Fikry, S. M. Elaraby, O. Zahran, M. EI-Kordy, "FPGA Implementation of Robust Image Steganography Technique based on Least Significant Bit in Spatial Domain", International Journal of Computer Application (0975-8887), Volume 145-No. 12, July 2016.

[9] Premalatha P, and Amsaveni A, "Data hiding in digital image with FPGA implementation", 2016 Online International Conference on Green Engineering and Technologies.

[10] Harini V, Vijayaraghavan V, "FPGA Implementation of Secret data sharing through Image by using LWT and LSB Steganography Technique", IJESC, June 2017, volume 7, Issue No. 6.

[11] Jayaram Bhasker, " A VHDL Primer ".

[12] Douglas L. Perry, " VHDL: Programming by Example ", Fourth Edition, McGraw-Hill.

[13] A. K. Jain," Fundamentals of Digital Image Processing ", Pearson Education.