



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

An Optimized FPGA Implementation of LSB Replacement Steganography Using DWT

Maya C S¹, Sabarinath G²

Department of Electronics and Communication, St. Joseph's College of Engineering and Technology, Palai, India^{1,2}

Abstract: This work focuses on the image steganography with an image compression using Discrete Wavelet Transform (DWT) on FPGA Spartan III Evaluation Development Kit (EDK). Current trends support digital image files as the cover file to hide another digital file with secret message or data. At receiver side, using Inverse Discrete Wavelet transform, both original image as well as hidden data can be successfully extracted. The design architecture when implemented on FPGA Spartan III offers a processing time of just 13.79 ns, which might give an impulse for the researchers to a very fast, programmable & cost effective hardware solution in the area of Secure Communication.

Keywords: Steganography; Lifting Scheme; Stego image; Wavelets; encoding

I. INTRODUCTION

The secrecy of digital information should be maintained when being communicated over the internet. An ideal steganography technique embeds secret message into the carrier image with imperceptible change in the image. The Least Significant Bit (LSB) algorithm is used to insert the bits of the hidden message into the Least Significant Bits of the pixels. A new approach for detecting Least Significant Bit (LSB) steganography in digital images is introduced here. Digital images have high capacity to store data and information. The data can be manipulated which cannot be detected by human eye [2]. A successful method of information hiding is more difficult using colour images than that of gray scale images. This paper presents an information hiding technique that utilizes the Discrete Wavelet transforms to effectively hide data in colour images.

Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for steganography, and thus the importance of image steganography. Embedding secret information inside images requires intensive computations, and therefore, designing steganography in hardware speeds up steganography. For a successful information hiding technique, it will result the extraction of hidden data from an image with high degree of data integrity.

The rest of the paper is organized as follows. Section II deals with system description. Section III introduces literature survey. Section IV introduces Stegosystem. Section V illustrates Encoding of the message. Section VI describes decoding the hidden data. Section VII explains proposed system. It finally concluded with simulation results and discussions.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

II. SYSTEM DESCRIPTION

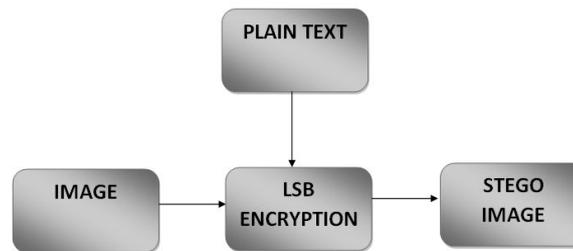


Fig.1 Encryption Algorithm

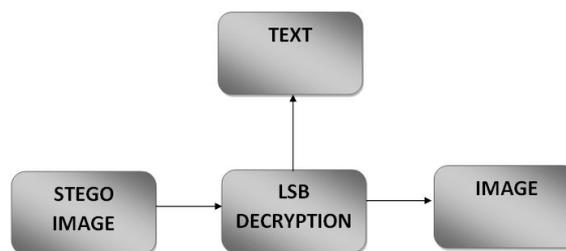


Fig. 2 Decryption Algorithm

Steganography is the art of hiding secret information into innocent data in a way that prevent detection of hidden messages. Digital images are suitable for hiding secret information. An image which contain secret message is called cover image. First, there will not be any visual difference between cover image and stego image. Second, the method of information hiding should be reliable. So, it is impossible for someone to extract the secret message, if they have no any special extracting method and a proper secret key. Third, the maximum length of the secret information should be as long as possible.

Message encoding on an image using Integer Wavelet Transform, which divided into two parts, one portion is encryption other is description. In encryption part there is a digital image in which we encode secret message by removing LSB of image pixel and add our secret message on corresponding LSB position, then the output image is called stego image. For retrieve the secret message program splits the image into its colour channels and applies the inverse wavelet transform to each channel to the level specified by the user. When the inverse wavelet transformation is completed, the program retrieves the message out of the pixels of the cover image.

III. LITERATURE SURVEY

T. Morkel [6] intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganography techniques are more suitable for which applications. Although only some of the main image steganography techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. In [7], a high-performance JPEG steganography along with a substitution encryption methodology is proposed. The approach uses the discrete cosine transform (DCT) technique which used in the frequency domain for hiding encrypted data within image. Experimental results show that the visual and the statistical values of the image with encrypted data before the insertion

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

are similar to the values after the insertion thus reduces the chance of the confidential message being detected and enables secret communication. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).

Jondhale [8] proposes the method of embedding the secret text data in spatial domain of a given 8 bit gray scale image followed by image compression using IWT on hardware Spartan III (XC3S200TQ144-4) using Lifting Scheme .A successful information hiding should result in the undistinguishable Stego image to be transmitted via internet as well as the extraction of the hidden data from this Stego image with high degree of data integrity. This research provides a hardware solution for data hiding in 8 bit gray scale image using well known LSB Image Steganography technique, followed by image compression using IWT so as to efficiently utilize network bandwidth for high speed operation. Also it is noticed that at receiver side using Reverse IWT both original image as well as hidden data can be successfully extracted. The design architecture when implemented on FPGA Spartan offers a processing time of 19.11 Sec for 128*128 gray scale image of bit depth 8 bits which might give an impulse for the researchers to a very fast, programmable & cost effective hardware solution in the area of Secure Communication. This design implementation required XPS EDK 10.1 software platform along with Matlab 7.5 & Visual Basic Studio 6 to display images on computer screen. This work focuses on an alternating method, that is, Least Significant Image Steganography using Discrete Wavelet Transform. When it is implemented on FPGA Spartan III, it offers a processing time of 13.79 ns for 128 x 128 gray scale images. So this work optimizes the processing time of Least Significant Image Steganography using Discrete Wavelet Transform. The implementation done with XPS EDK 10.1 software platform along with Matlab 7.5 and Visual Basic 6 to display image on computer screen. The conversion of true color image into gray scale image as well as resizing of image into (128 * 128) format was carried out using Matlab 7.5 Image Processing Toolbox.

Bassam and Sahel [9] proposed an FPGA hardware implementation of LSB steganography method. This work made an analysis on n-bit LSB. From the analysis PSNR of 2-bit LSB is 44.1dB for Baboon image and for 3-bit LSB, PSNR is 37.9dB, for the same image. The 2/3- LSB provide good image matrices and its performance is between 2-bit and 3-bit LSB, that is 37.9dB for the same Baboon image.

IV. STEGOSYSTEM

A stego-system is a combination of both embedding algorithms and a cover image. Figure.3. shows the graphical version of a stego system.This paper introduces a secret message encoding method which makes use of wavelets. Wavelets will breakdown the stream into high frequency and low frequency parts, known as Details and Trends. Lifting technique allows for variations in levels of transformation, selecting the regions on cover image to be manipulated, type of wavelet transformation to be applied and how far apart in the image each piece of the message to be encoded. This type of comparison can be done if a bitwise comparison of the cover image is done with this stego image.

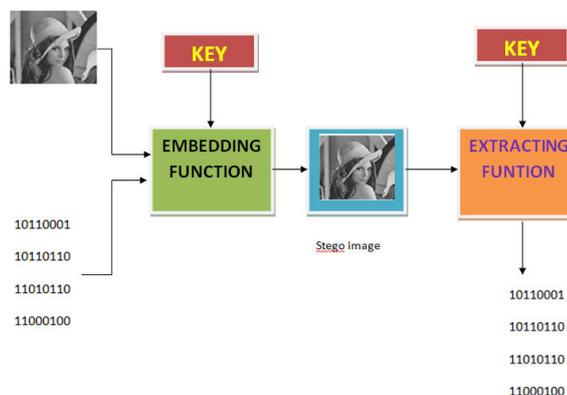


Fig.3 Stegosystem

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

V. ENCODING OF THE MESSAGE

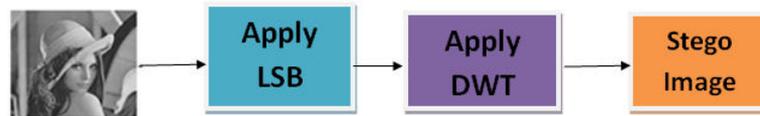


Fig.4 Encoding of the message

Steps for encoding the hidden data are,

- Apply LSB replacement.
- Use Discrete Wavelet Transform.
- Store as regular image.

VI. DECODING OF HIDDEN DATA

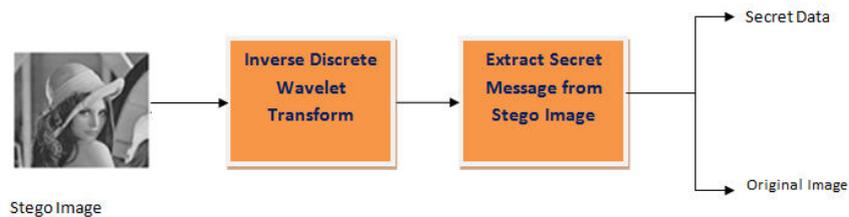


Fig.5 Decoding of hidden data

Steps for decoding of hidden data are,

- Take the Inverse Discrete Transform of modified image.
- Then extract secret bits of data from this image.
- And combine these bits into an actual message.

VII. PROPOSED SYSTEM

A. Least Significant Bit(LSB) Insertion

8 bits are used for the representation of characters in ASCII code. The value of DWT coefficients can be manipulated slightly without being noticed by visual inspection after the image is reconstructed using the manipulated DWT coefficients. This work concentrated that the bits of ASCII characters can be included in the DWT coefficients without resulting in a visible appearance in the stego image. The LSB insertion algorithm is used to insert the bits of the hidden message into Least Significant Bits of the pixels. This method is used to embed the significant amount of the information with no visible degradation of the cover image. One major advantage of the LSB algorithm is that it quick, easy and it also work well with grayscale images.

B. Process of Adding a Message

The process of embedding data to the pixels of an image is a multistep process. The ASCII character stream is split into two bit pairs. A Discrete Wavelet Transform is applied to an image. Then the two bit pairs are inserted into the image is either the trends or details in the Frequency Domain. Finally the inverse process is applied to reconstruct the image.

C. Encoding a Message in the Image

The ASCII character stream is split into 4 two-bit pairs per character. The 2 LSBs of a pixel is replaced with these two bit pairs. These two bit pairs are then stored in an array for manipulating later. Then the lifting scheme is applied to the image. Lifting scheme is applied three times because the image is split into 3 colour channels. The program then automatically adjusts the encoding according to the decomposition level of Wavelet Transform.

If the transformations are complete the two bit pairs in the ASCII characters are then hidden in the pixels of the processed image. The offset value of the colour channel is specified by the user and determines which bits are used to

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

hide each subsequent two bit pair of ASCII character. Hiding can be done by performing the bitwise AND operation with 0 and the two bits of the pixel value. It will set the two bits to 0. Then the two bit pairs to be hidden is then combined with the pixels by bitwise OR operation. This process effectively sets the pixel bits to the message bits.

D. Decoding of the Message

The flow of this process starts in the same way as the encoding process. The program splits the image into its colour channel and then applies the inverse wavelet Transform to each channel. When the transformation is completed the original message is retrieved out of the pixels of the cover image.

VIII. SIMULATION RESULT AND DISCUSSIONS

This work is implemented on MatlabR2010a and the Parallel processor Xilinx FPGA Spartan III. The processing time obtained when implemented on Matlab is 0.446 sec while the processing time obtained from Xilinx FPGA Spartan III is 13.79ns(72.495MHz). So this work optimize the processing time of Least Significant Bit replacement image steganography in digital images using Discrete Wavelet Transform.

A. Matlab Simulation Results

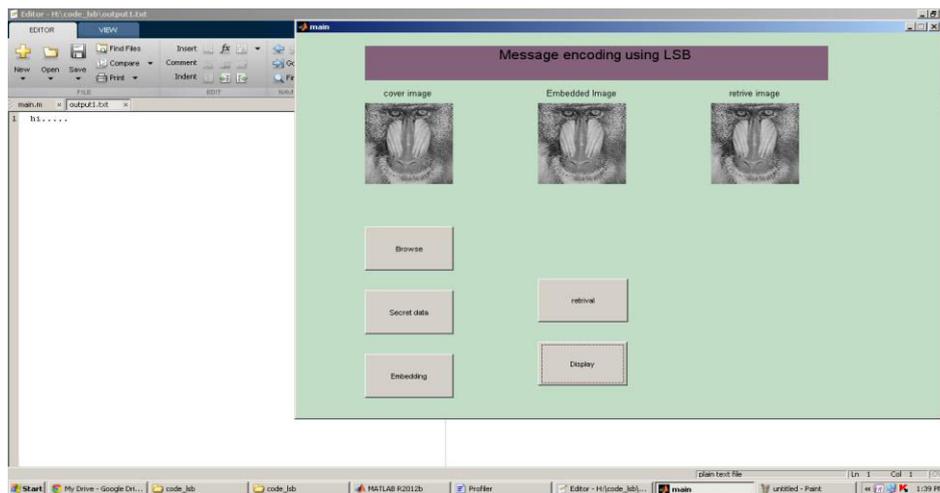


Fig.6 Retrieving secret data and hidden messages

Profile Summary
Generated 31-Jul-2013 13:41:54 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
gui_mainfcn	1	0.446 s	0.000 s	
main	1	0.446 s	0.000 s	
openfig	2	0.319 s	0.286 s	
gui_mainfcn>local_openfig	2	0.319 s	0.000 s	
main>main_OpeningFcn	1	0.127 s	0.016 s	
imshow	3	0.111 s	0.000 s	
newplot	6	0.095 s	0.015 s	
graphics/private/cio	6	0.079 s	0.000 s	
cla	6	0.079 s	0.000 s	

Fig.7 Profile Summary of Matlab Simulation

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

B. FPGA Implementation Results

The transformations in the digital images can be manipulated to some extent which cannot be detected by human eyes. An example of such manipulation is the insertion of secret information which is known as information hiding. In this research we embed the secret text data in a given 8-bit gray scale image followed by image compression using Discrete Wavelet Transform on hardware Spartan III. A successful information hiding will result in the undistinguishable stego- image which can be transmitted via internet. This design implementation required Xilinx Platform Studio (XPS) EDK 10.1 software platform along with Matlab R2010a & Visual Basic Studio 6 to display images on computer screen. The conversion of true color image into gray scale image as well as resizing of image into (128 * 128) format was carried out using Matlab R2010a Image Processing Toolbox. While coding of our design which include LSB encoding, Forward DWT, LSB decoding & Inverse DWT, was carried out using Impulse C Language in XPS EDK 10.1. For a comparison between a parallel processor and serial processor the work is implemented on MatlabR2010a and the Parallel processor Xilinx FPGA Spartan III. The processing time obtained when implemented the work on Matlab, is 0.446 sec while the processing time obtained from Xilinx FPGA Spartan III is 13.79ns. So this work optimize the processing time of Least Significant Bit replacement image steganography in digital images using Discrete Wavelet Transform. From the device utilization summary, utilization of 4 input LUTs is 76%.

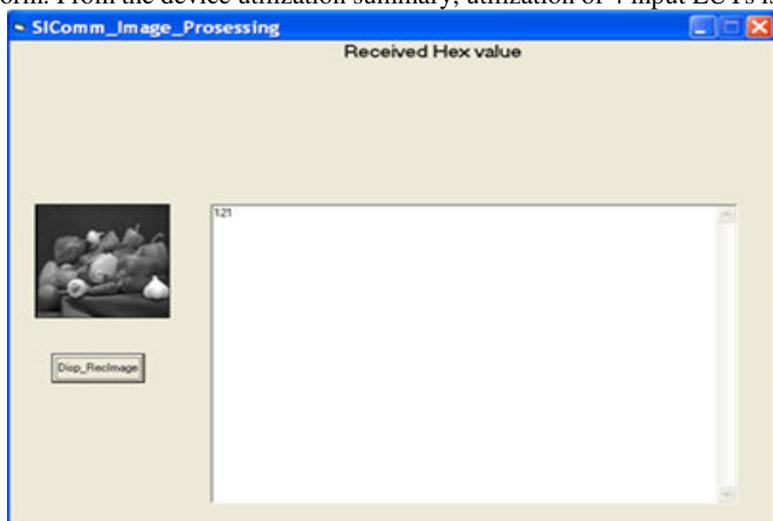


Fig.8 Decrypted image

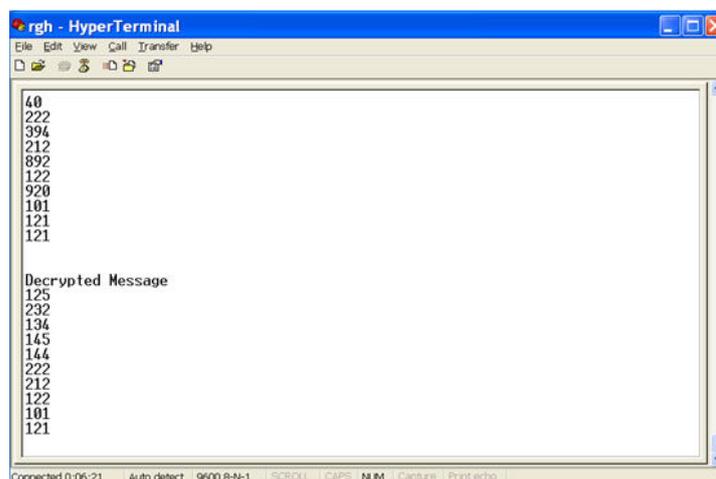


Fig.9 Decrypted message



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

Table.1 Timing information and EDK synthesis report

Post Synthesis Clock Limits		
Modules	CLK Port	MAX FREQ
debug_module	debug_module/update	72.495 MHz
debug_module	SPLB_Clk	72.495 MHz
debug_module	debug_module/drck_i	72.495 MHz
microblaze_0	DCACHE_FSL_OUT_CLK	78.356MHz
microblaze_0	DBG_CLK	78.356MHz
microblaze_0	DBG_UPDATE	78.356MHz
SRAM_256K x 32	MCH_PLB_Clk	83.549MHz
SRAM_256K x 32	RdClk	116.157MHz
RS 232	SPLB_Clk	137.741MHz
mb_plb	PLB_Clk	199.124MHz
proc_sys_reset_0	Slowest_Sync_Clk	294.291MHz
ilmb	LMB_Clk	294.291MHz
dlmb	LMB_Clk	294.291MHz
Clock_generator_0	CLK IN	294.291MHz

Table.2 Device utilization summary

Elements in FPGA	Amount Utilized	Amount Available	% Utilization
Number of Slices	1475	1920	76%
Number of Slice Flip Flops	1569	3840	40%
Number of 4 input LUTs	2330	3840	76%
Number of Bounded IOBs	62	97	63%
Number of BRAMs	4	12	33%
Number of MULT18x18s	3	12	25%
Number of DCMs	1	4	25%

IX. CONCLUSION

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 with a processing time of 13.79ns. At the receiver side by using Inverse Wavelet Transform, both original image and hidden data can be successfully extracted. This work provides a very fast, programmable and cost effective hardware solution in the area of secure communication.

ACKNOWLEDGEMENT

This is the most satisfying, yet the most difficult part of the work to present gratifying words because most often we fail to convey the real influence, others have had on one's life or work. First and foremost, we give thanks to almighty god who gave us the inner strength, resource and ability to complete my work successfully, without which all our efforts would have been in vain. We express my sincere gratitude to our principal, Dr. C. J. Joseph for giving us the provision to do the seminar in the required way. We stand grateful to Prof. Madhukumar S., Head of the Department of Electronics and Communication, and M. Tech coordinator Dr. B Priestly Shan for their valuable advices and motivations. We thank all the lectures and lab assistants who have helped us during the project period with their inspiration and co-operation. We truly admire our parents and friends for their constant encouragement and enduring support which was inevitable for the success of our venture. Once again we convey our gratitude to all those persons who had direct or indirect influence on our work.

REFERENCES

- [1] Lionel Fillatre, "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images," IEEE Transactions on Signal Processing, Vol. 60, No. 2, February 2012. Page(s):556 – 569.
- [2] Bassam Jamil Mohd, Saed Abed and Thayer Al-Hayajneh, Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method", ,Computer, Information and Telecommunication Systems (CITS),International Conference,May 2012, Page(s): 1-4.
- [3] Dr. Ekta Walia , Payal Jain, Navdeep , "An Analysis of LSB & DCT based Steganography",Global Journal of Computer Science and Technology, Page4, Vol. 10 Issue 1 (Ver.1.0), April 2010.
- [4] Jondhale S. R., Ansari A. H. , "A Simultaneous Implementation of Message Encoding using LSB Stegnography & Image Compression using Lifting Scheme on FPGA",InternationalJournal of Computer Applications (pages: 0975 - 8887) Volume 43, No.24, April 2012.



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 1, December 2013

- [5] Shilpa Gupta, Geeta Gujral and Neha Aggarwal "Enhanced Least Significant Bit algorithm For Image Steganography",IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online):2230-7893 .
- [6] T. Morkel , J.H.P. Eloff , M.S. Olivier , "An Overview Of Image Steganography" ,Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, Pretoria, South Africa, 2002.
- [7] Mahendra Kumar, "Steganography And Steganalysis Of Joint Picture Expert Group (JPEG) Images",A Dissertation Presented To The Graduate School Of The University Of Florida In Partial Fulfillment Of The Requirements For The Degree Of Doctor Of Philosophy University Of Florida 2011.
- [8] Jondhale S. R., Ansari A. H. , "A Simultaneous Implementation of Message Encoding using LSB Steganography & Image Compression using Lifting Scheme on FPGA",International Journal of Computer Applications (0975 – 8887) Volume 43– No.24, April 2012.
- [9] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, Sahel Alounch, "FPGA Hardware of the LSB Steganography Method", Page(s): 1-4,Computer, Information and Telecommunication Systems (CITS),International Conference on 14-16,May 2012,978-1-4673-1550 ©2012 IEEE.