International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2,Issue 12,December-2015, Impact Factor: 2.125

FPGA Implementation of Data Hiding in Images

Mr.R.V.Rathod[1],Prof.L.K.Chouthmol[2]

[1]Electronics & Telecommunication, Late.G.N.S.College of Engineering, Nashik
[2] Electronics & Telecommunication, Late.G.N.S.College of Engineering, Nashik

Abstract

In this paper steganography is used to hide the data inside the images. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. 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. This work focuses on the image steganography with an image compression using least significant bit with 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.

Keywords- *Steganography, Data hiding, Embedding Data, LSB,, DWT ,MSE, PSNR, Information Security,.*

I. INTRODUCTION]

Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. In this paper, 8-bit gray scale images are selected as the cove media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. In the digitized world extensive increase of use of extensive data communication the problem of security, authentication of the multimedia data also increases. The solution to this is digital watermarking. Digital watermarking is the process of the modification of original multimedia data to embed a data containing key information such as authentication or copyright codes. The embedded data must leave original data unchanged. Steganography is an art of hiding information in a way that apart from an intended recipient, suspects the existence of secret message. To hide a secret message within an object, Do it such a way that the presence of message is not visible.

II. METHODLOGY

In this paper there are two methodology are used to hide the data inside the image, using LSB & DWT.As shown in following fig.a) the general block diagram of Steganography.

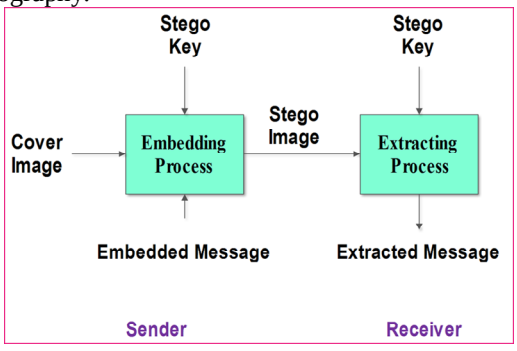


Fig. a) General block Diagram

2.1.Data hiding using LSB.

Data hiding using LSB It is best way to implement Steganography. It embeds the data into the cover so that it cannot be detected by a observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane In a LSB embedding, we lose some information from the cover image. [It is not visible]. Both lossy & lossless image can be used .

2.2. Data hiding using DWT

Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets DWT transforms a discrete time signal to a discrete wavelet representation. In this process image pixel values are divided into even & odd sample, as shown in following fig.b).

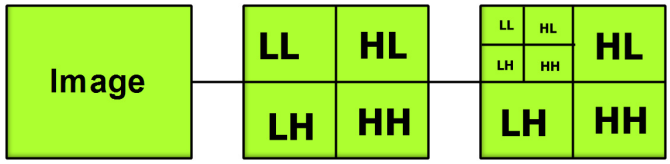


Fig.b] Decomposition of Image using DWT

2.3. Algorithm

The algorithm to hide the data inside the image using DWT along with LSB technique is given below:

- Select the secrete data [or Message]
- Convert the secrete data from decimal to binary.
- Read a cover image
- Resize the cover image by 256 x 256
- Convert the cover image from RBG to gray
- Read the Gray level image [Cover image]
- Create the header file.
- Break the byte of secrete data to be hidden into bits.
- Take first 8 bytes of original data from cover Image.
- Replace the least significant bit by one bit of the data to be hidden.
- Display new pixel valued image [Stego Image] on VB [Using LSB]
- Display new pixel valued image [Stego Image] on VB [Using LSB+DWT]
- Display extracted data using Hyper Terminal Window.
- Display the value of MSE & PSNR using Hyper Terminal window.

III. SIMULATION RESULT

This work is implemented on MatlabR2010a and the Parallel processor Xilinx FPGA Spartan III. The block diagram of hardware implementation is shown in following fig. c).

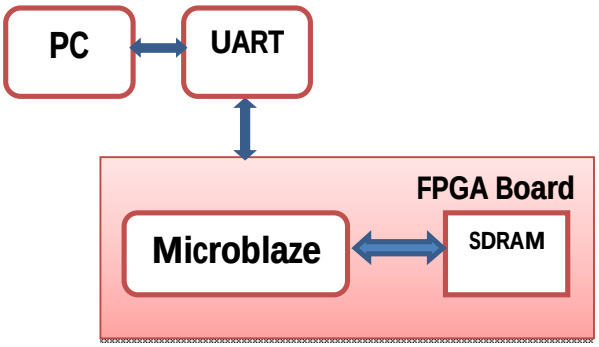


Fig.c) Hardware Implementation Block diagram

This work optimize the processing time of Least Significant Bit replacement image steganography in digital images using Discrete Wavelet Transform. In this research embedded 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 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.

3.1. Matlab Simulation Results

By using Matlab first colour image is resized & converted it into gray level image. And Header file is successfully created using the MatlabR2010a. The simulation processing on MatlabR2010a is shown in following fig .d)

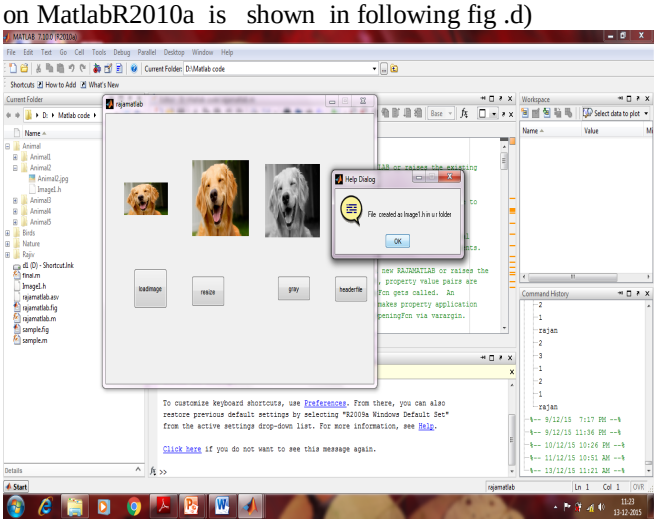


Fig. d) Creation of Header File

3.2. FPGA Implementation Results

The design implementation result using Xilinx Platform Studio (XPS) EDK 10.1 along with Visual Basic Studio and Hyper terminal window is shown in following Fig.e), Fig f) & Fig. g),

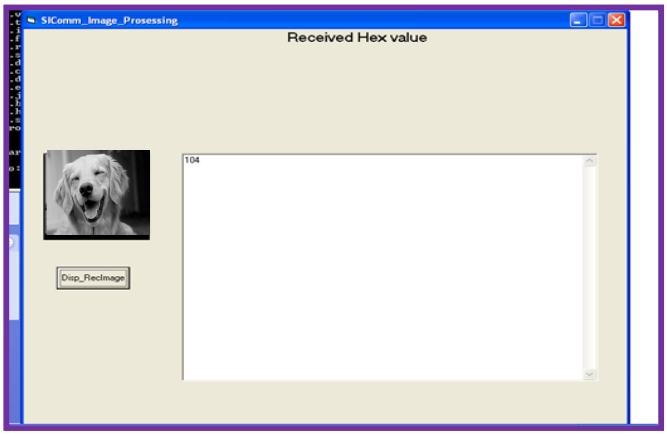


Fig.e) Output Image using LSB

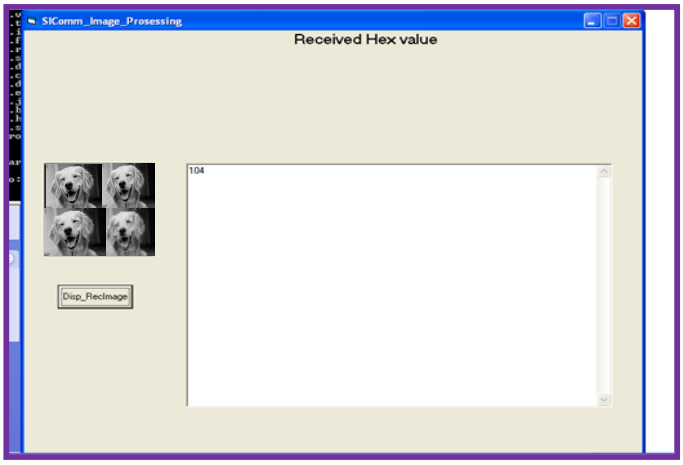


Fig.f) Output Image using DWT

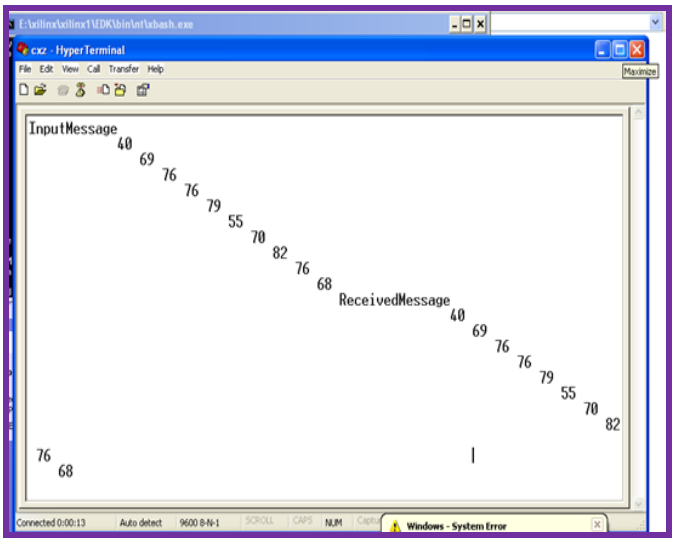


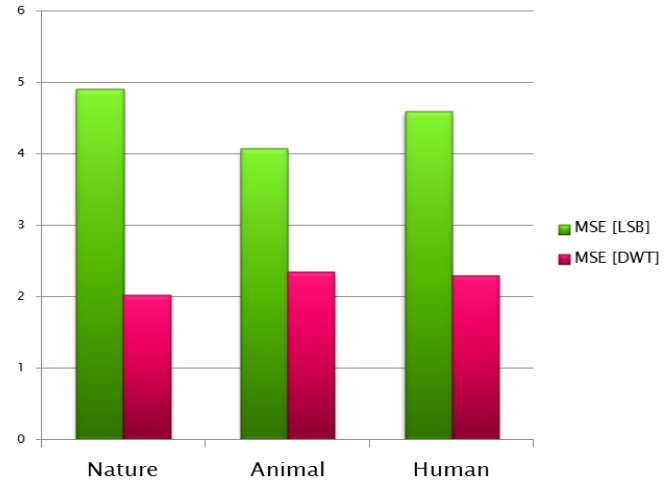
Fig. g) Input & received message

3.3. Comparative analysis using MSE and PSNR

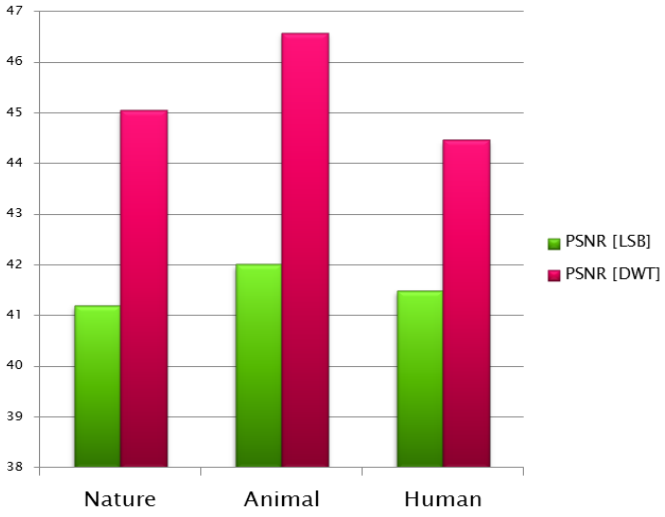
Lower value of MSE gives good quality of image & higher value of PSNR gives good quality of images. As shown in following table & graphs the comparative analysis of MSE and PSNR values .

SR NO.	Images	MSE [Using LSB]	MSE [Using DWT]	PSNR [Using LSB]	PSNR [Using DWT]
1		4.91	2.03	41.21	45.05
2		4.08	2.35	42.02	46.58
2		4.6	2.32	41.50	44.47

Table.a) MSE and PSNR values



Graph.a) MSE [LSB] vs MSE [DWT]



Graph.b) PSNR [LSB] vs PSNR [DWT]

From the above table & graph we can say that the quality of image by using DWT is good as compare to LSB method.

IV. 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. “You never know if a message is hidden”, this is the dilemma that empowers steganography. As more emphasis is placed on the areas of copyright protection & privacy protection. we believe that steganography will continue to grow in importance as a protection mechanism. Steganography can be used along with cryptography to make an highly secure data high way.

IV. ACKNOWLEDGEMENT

My sincere thanks to my paper guide Prof. L.K. Chouthmol mam ,Dept. Electronics & Telecommunication of Late.G.N.Sapkal COE Nashik, for her valuable support and guidance for analyzing and testing the end of the work.

Finally a very Special thanks to my HOD Prof. S. B. Bagal & ME Co-coordinator, Prof. S. B. Borse who showed utmost interest in our endeavor and provided their able guidance and co-operation.

REFERENCES

[1] Ravi Kumar, Kavita Choudhary, Nishant Dubey, “An Introduction of Image Steganographic Techniques and Comparison”, International Journal of Electronics and Computer Science Engineering.

[2] Prashanti .G, Sandhya Rani.K, Deepthi.S “ LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013, pp.788-799.

[3] Namita Tiwari, Dr.Madhu Shandilya,”Evaluation of Various LSB based Methods of Image Steganography on GIF File Format”,International Journal of Computer Applications, Vol. 6– No.2, September 2010 , pp .1-4.

[4] Mr. Rohit Garg, “Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images Vol.1, Issue 8,Oct 2012”.,International Journal of Engineering Research and Technology(IJERT).

[5] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,”Application of LSB Based Steganographic Technique for 8-bit Color Images, World. Academy of Science, Engineering and Technology, 2009.

[6] Shailender Gupta, Ankur Goyal, Bharat Bhushan,” Information Hiding Using Least Significant Bit, Steganography and Cryptography, I.J. Modern Education and Computer Science 2012, Vol .6 pp. 27-34

[7] M.Sivaram B.DurgaDevi J.Anne Steffi, “Steganography of two lsb bits”, International Journal of Communications and Engineering, Vol.1– No.1, Issue: 01, March 2012.

[8] H. Sencar, M. Ramkumar, and A. Akansu, Data Hiding Fundamentalsand Applications: Content Security in Digital Multimedia. Elsevier:Academic, 2004.