International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

An Implementation of LSB Steganography Using DWT Technique

G. Raj Kumar, M. Maruthi Prasada Reddy, T. Lalith Kumar

Electronics & Communication Engineering#,JNTU A University
Electronics & Communication Engineering,SVU University*
Electronics & Communication Engineering#,SVU University
Kadapa,A.P,India

[1]rajkumarbalu.2008@gmail.com,
[2]maruthiprasadareddy@gmail.com
[3]lalith.tappeta_cdp2005@yahoo.co.in

Abstract— Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. In steganography, there is a technique in which the least significant bit is modified to hide the secret message, known as the least significant bit (LSB) steganography. Least significant bit matching images are still not well detected, especially, at low embedding rate. In this paper, we have improved the least significant bit steganalyzers by analyzing and manipulating the features of some existing least significant bit matching steganalysis techniques. This paper explains the LSB Embedding technique with lifting based DWT schemes by using Micro blaze Processor implemented in a FPGA using System C coding.

Keywords— *DWT, FPGA, LSB, Micro Blaze, Steganography*.

Introduction

The art or practice of concealing a message, image, or file within another message, image, or fileis called Steganography. The word *steganography* combines *steganos* meaning "co-vered, concealed, or protected", and *graphein* meaning "writing". Generally, the hidden messages will appear to be (or be part of) something else: images, articles or some other *cover text*.

Steganalysis develops theories, methods and techniques that can be used to detect hidden messages in multimedia docu-ments. The documents without any hidden messages are called cover documents and the documents with hidden messages are denoted by stego documents. In steganography, there is a technique in which the least significant bit is modified to hide the secret message, this technique is known as the least significant bit (LSB) steganography or LSB embedding.

A digital image is described using a 2-D matrix of the intestines at each grid point (i.e. pixel). Typically, gray images use 8 bits, whereas coloured utilizes 24 bits to describe the colour model, such as RGB model. The steganography system which uses an image as the cover object is referred to as an image steganography system.

The shift from cryptography to steganography is due to that concealing the image existence as stego-images enable to embed the secret message to cover images. Steganography conceptually implies that the message to be transmitted is not visible to the informal eye. Steganography has been used for thousands of years to transmit data without being intercepted by unwanted viewers. It is an art of hiding information inside other information. The main objective of Steganography is mainly concerned with the protection of contents of the hidden information. Images are ideal for information hiding because of the large amount of redundant space is created in the storing of images. Secret messages are transferred through unknown cover carriers in such a manner that the very existence of the embedded messages is undetectable.Carriers include images,audio,video,text or any other digitally represented code or transmission.The hidden message may be plaintext or another as a bit stream.

2. THE LSB TECHNIQUE

We have implemented the LSB steganography algorithm in gray scale images to reduce the complexity of the system. It is the process of embedding data within the domain of another data, this data can be text, image, audio, or video contents and the scope of the current paper covers only codes (integer values). The embedded data is invisible to the human eye i.e., it is hidden in such a way that it cannot be retrieved without knowing the extraction algorithm. In this paper we evaluated the technique using gray scale images of size

64*64 in which each pixel value was represented with 8 bit representation.

Example:

Take the number 300, and its binary equivalent is 100101100 embedded into the least significant bits of pixel values of the Cover image. If we overlay these 9 bits over the LSB of the 9 bytes cover image pixel values, we get the following (where bits in bold have been changed)

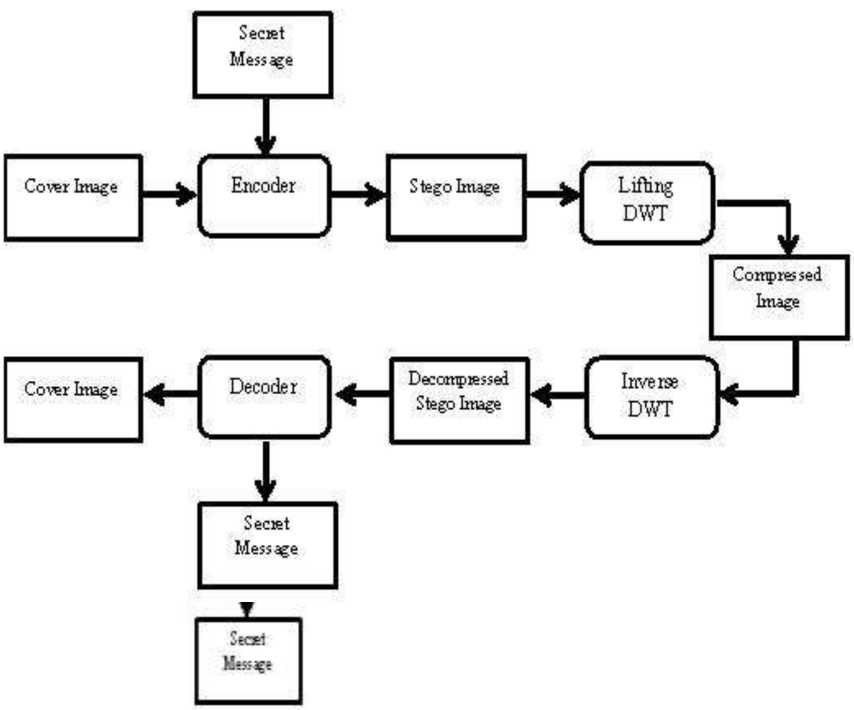
1001010**1** 0000110**0** 1100100**0**

1001011**1** 0000111**0** 1100101**1**

1001111**1** 0001000**0** 1100101**0**

After embedding the message into the cover image, the stego image will be obtained, then this stego image will be transformed with DWT transformation technique so that any hacker can't find where the message was embedded. At the receiver end the inverse DWT is applied, after LSB decryption the original image and message will be obtained.

3. PROPOSED METHODOLOGY



3.1. THE LSB ENCRYPTION AND DECRYPTION PROCESS

LSB encryption process consists of two steps namely masking process and generation of stego image.

Masking process is done by replacing LSB of all pixel values with ‘0’. This is done by performing AND operation with “1111 1110” (254). Now the LSB of all pixels will be zeroes.

Now the binary value of the information is placed in the LSB of the pixel values. This is done by identifying the position of 1s and placing them in the LSB of respective pixel value.

For Example, we have n-bit binary message (binary value of the integer), now AND operation is performed between n-bit binary message and ‘1’ in the nth position, rest all 0s. Then OR operation is performed between the output of the above AND operation and the binary values of nth pixel. This operation is repeated for (n-1), (n-2), (n-3)……till it completes LSB. So for an 8 bit binary message, the above operations start with 8^{th} bit and completes till 1^{st} bit of the message. Now the LSB of pixel values are embedded with message, and now the image is termed as stego image. LSB decryption process contains extraction of the message from LSB of pixel values.

4. DISCRETE WAVELET TRANSFORM

Lifting schemes, also known as integer-based wavelets, differ from wavelet transforms in that they can be calculated in-place. Similar to wavelet transformations, lifting schemes break a signal, the image, into its component parts ‘trends ‘that approximates the original values and ‘details’ which refers to the noise or high frequency data in the image.

A lifting scheme produces integers and this allows the original space to be used to hold the results. Lifting operation requires two steps, one to calculate the trends i.e. low frequency values and another to calculate the details i.e High frequency values. Trends give the original signal values i.e. low frequency components and details give the noise values i.e. High frequency components. In this lifting scheme based discrete wavelet transformation scheme we used the mathematical calculation method to convert the image into frequency domain. In our project we propose a two level transformation in lifting based DWT schemes to convert image pixel values into frequency domain.

The lifting schemes which we have implemented in our project are based on Haar lifting schemes.

lifting calculation of the High and the low frequency values for image pixels are shown below respectively.

High frequency value = odd-even samples

Low frequency values = even + high/2 samples

$$\textbf{High frequency :}\quad s_{i,2j+1} = s_{i,2j+1} - s_{i,2j},\ j = 0,1,\ldots,n/2$$

$$\textbf{Low frequency :}\quad s_{i,2j} = s_{i,2j} + \frac{s_{i,2j+1}}{2},\ j = 0,1,\ldots,n/2$$

Where i, j are the rows and columns of 2D pixel matrix of a stego image.

4.1. 2-D TRANSFORM HEIRARCHY

The 1-D wavelet transform can be extended to a two-dimensional (2-D) wavelet transform using separable wavelet filters. With separable filters the 2-D transform can be computed by applying a 1-D transform to all the rows of the input, and then repeating on all of the columns.

LL	HL
LH	HH

Fig 4.1.1: Sub band Labeling Scheme for a one level, 2-D Wavelet Transform

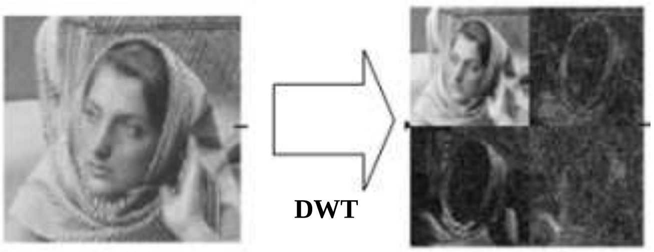


Fig 4.1.2: Pictorial representation of Sub band Labeling Scheme for a one level, 2-D Wavelet Transform

4.2. LIFTING BASED DWT SCHEMES

It is composed of three basic operation stages:

Splitting: Where the signal is split into even and odd pixels.

Predicting: Even samples are added by a prediction factor derived from odd and even pixels to get low frequency values.

Updating : The detailed co-efficients computed by the predict step are multiplied by the update factors and then the results are subtracted to the even samples to get the high frequency values.

Merging/Combining: The reverse process of DWT has done to merge all the LL,LH,HL,HH to reconstruct the original image.In this procedure Image pixels values are divided into even samples and odd samples then for getting high frequency value= odd-even samples and for low frequency values =even + high/2 samples then this procedure is repeated for two phases . The first phase is known as Column Filter that means performing the DWT calculations on columns to get Low and High frequency values and second phase is known as Row filter. That means we are going to apply DWT calculation on rows in order to get the LL, LH, HL, HH.

The Inverse DWT is also fallows the same process in reverse manner to construct original image pixel values from LL, LH, HL, HH values.it is a process converting frequency domain to image pixel values.

5. RESULTS

The Xilinx Platform Studio (XPS) is the development environment or GUI used for designing the hardware portion of your embedded processor system. Visual basic is used to observe the input image, compressed image and decompressed image. Hyper terminal is to see the input and output message.

International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

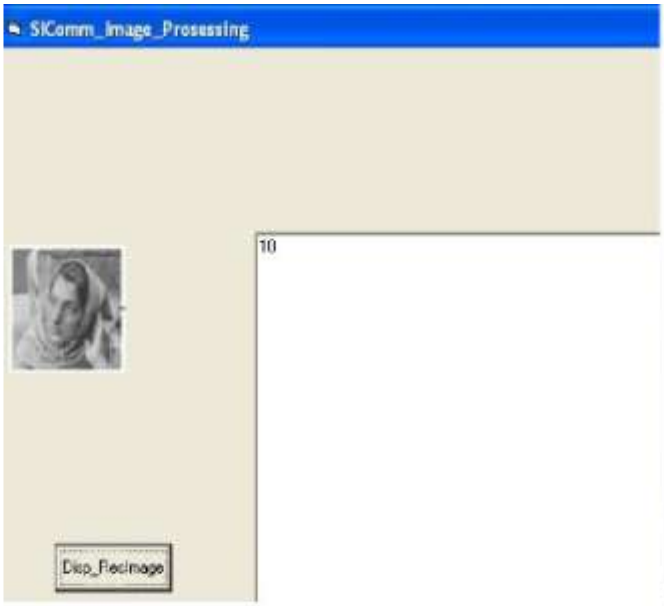


Fig 5.1: Input stego Image

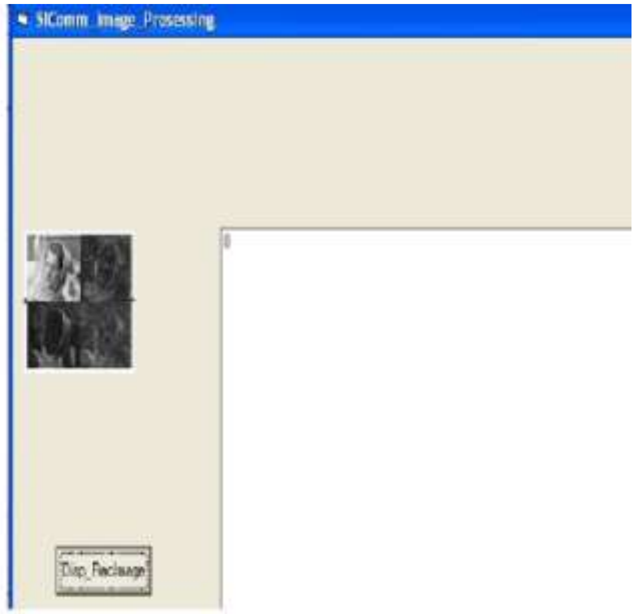


Fig 5.2: Compressed Image using DWT

Fig 5.3: Decompressed Image

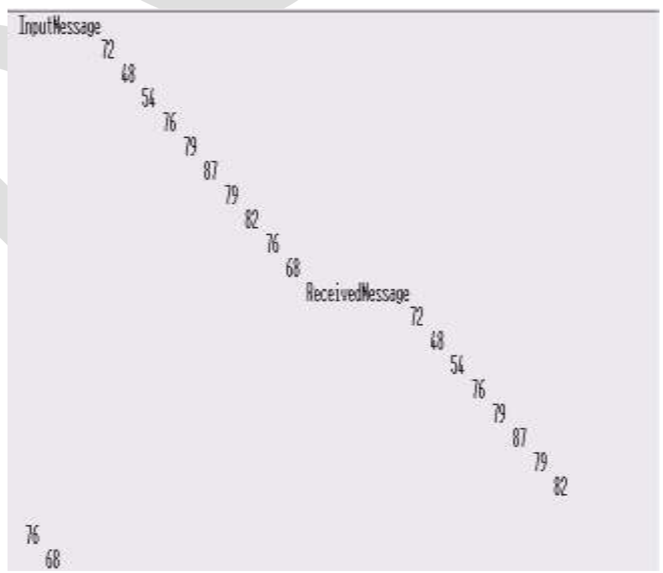


Fig 5.4:Input and Output message

6. CONCLUSION:

In this paper we have presented a new method of LSB Steganography using lifting DWT Process. This process was implemented by developing Micro Blaze processor in FPGA.

Future work can be extended to RGB or color image processing and can be extended to video processing level also.

REFERENCES:

1.G. Xing, J. Li, and Y. Q. Zhang, "Arbitrarily shaped videoobject coding by wavelet," IEEE Trans. Circuits Syst. Video Technol., vol. 11, no. 10,pp. 1135–1139, Oct. 2001.

2.S. C. B. Lo, H. Li, and M. T. Freedman, "Optimization of wavelet decomposition for image compression and feature preservation," IEEE Trans.Med. Imag., vol. 22, no. 9, pp. 1141–1151, Sep. 2003.

3.K. K. Parhi and T. Nishitani, "VLSI architecture for discrete wavelet transforms," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 1, no. 2, pp. 191– 202, Jun. 1993.

4.X. X. Qin and M. Wang, "A review on detection of LSB matching steganography," *Inf. Technol. J.*, vol. 9, pp. 1725–1738, 2010.

5. A. D. Ker, "Locating steganographic payload via WS residuals," in*ACM Proc. 10th Multimed. Secur. Workshop*, 2008, pp. 27–31.

6.A. D. Ker, "A general framework for thestructural steganalysis of LSBreplacement," in *Proc. 7th Inf. Hiding Workshop, ser. Springer LNCS,*

2005, vol. 3727, pp. 296–311.

7..J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, 2001.

8..S. Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, pp.1995–2007, Jun. 2003.

9..A. Ker, "Steganalysis of LSB matching in grayscale images," *Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

10..A. D. Ker, "A fusion of maximum likelihood and structural steganalysis," in

Proc. 9th Inf. Hiding Workshop, ser. Springer LNCS, 2007, vol. 4567, pp. 204– 219.

11..K. Lee, A. Westfeld, and S. Lee, "Generalised category attack—Improving histogram-based attack on JPEG LSB embedding," *Inf.Hiding'07*, pp. 378–391, 2007.

12..J. Fridrich and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain," in *Secur., Steganogr. Watermarkingof Multimed. Contents VI, ser. Proc. SPIE*, 2004, vol. 5306,pp