IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p-ISSN: 2278-8735
PP 10-14
www.iosrjournals.org

FPGA implementation of LSB Steganography method

Pangavhane S.M. [1]&Punde S.S.[2]
[1,2](E&TC Engg. Dept.,S.I.E.RAgaskhind, SPP Univ., Pune(MS), India)

Abstract : *"Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). Steganography is a powerful technique to hide secretes data inside the cover object. We are going to capture image then it is passed to discrete wavelet transform for sub band coding. After that using LSB stenography we are going to embedding secret data using inverse discrete wavelet transform stego image is extracted with secret data and original image is reconstructed. FPGA Spartan 3 kit is used for implementation.*

Keywords: *Steganography, least significant bit, Encryption, FPGA.*

I. Introduction

In this system we are use Steganography method for conceal the existence of hidden secret data inside a cover object. However, in the hiding information the meaning of Steganography is hiding text or secret messages into another media (cover) file such as text,image,video,sound. In this system we are going to capture image then it is passed to discrete wavelet transform. In the DWT sub band coding and then using LSB stenography we are going to embedding secret data and after that using inverse discrete wavelet transform stego image is extracted with secret data and then original image is reconstructed. FPGA Spartan kit is used for implementation.

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

There are several techniques to embedded information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Due to which , the spatial domain techniques are easy to implement. The Least Significant Bit (LSB) is one of the techniques in spatial domain image steganography.

Several FPGA implementations of spatial-domain stenography designs were proposed. The rest of this paper is organized as follows. Section 2 discusses in detail DWT,LSB steganography techniques. Section 3 describes the designed FPGA system. Section 4 summarizes the results. And section 5 and 6 presents concludingremarks.

II. Proposed System

2.1 DWT (Discrete Wavelet Transform)

A DWT is a wavelet transform for which the wavelets are discretely sampled. The DWT of a signal is obtained by passing it through a series of different filters like, lowpass filters and high pass filters to obtain different four sub bands which include one approximation band and three detailed bands belonging to low frequency and high frequency components respectively. The four sub bands of DWT such as approximation band, horizontal band, vertical band and diagonal bands. The significant information is present in the approximation band compared to other three high frequency component bands. Discrete Wavelet Transform (DWT) which is based on sub-band coding yields a fast computation of Wavelet Transform. It is simple and easy to implement and reduces the computation time . Wavelet transform decomposes signal into set of basic functions. These basic functions are called as wavelets. Wavelets are obtained by single prototype wavelet y(t) called mother wavelet.

$$\varphi a, b(t) = \frac{1}{\sqrt{a}} \varphi \left(\frac{t-b}{a}\right) \qquad (1)$$

Where in above equation 'a' is scaling parameter and 'b' is shifting parameter. The parameter 'a' (inverse of frequency) reflects the scale (width) of a particular basis function such that its large value gives low frequencies and small value gives high frequencies. The parameter 'b' specifies its translation along x-axis in time.

The term $1/\sqrt{a}$is used for normalization. The wavelet transform concentrates the energy of the image signals into a small number of wavelet coefficients. The basic idea behind wavelets is to analyze signal according to scale. It can be used as an alternative to the short time Fourier to overcome problems related to its frequency and time resolution properties.

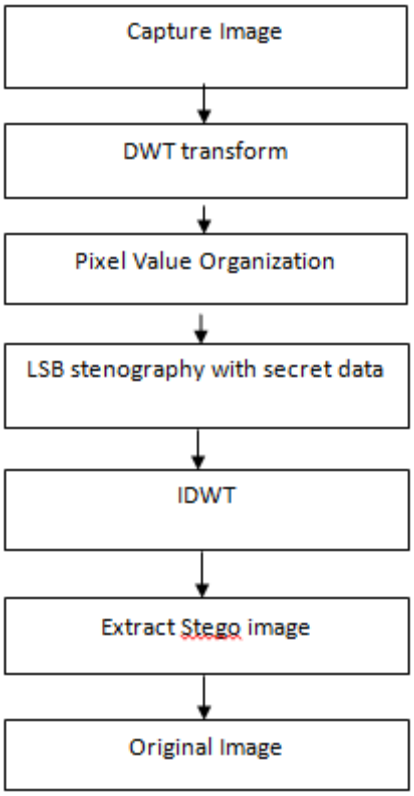

Fig.1.Block Diagram of System

The advantage of DWT over DFT and DCT is that DWT performs a multi-resolution analysis of signal with localization in both time and frequency. Another advantage is that functions with discontinuities and with sharp spikes require fewer wavelet basis vectors in the wavelet domain than sine-cosine basis vectors to achieve a com-parable approximation. The properties of Wavelet Transform is successfully applied to non-stationary signals for analysis and processing, e.g. speech processing, image processing, data compression, and communications. The wavelets can classify into two classes: (1) Orthogonal (2) Biorthogonal. As per application, one of them can be used. Several families of wavelets have proven to be especially useful for signal processing. Some of them are A] DaubachiesB] Haar C] Coiflets D] BiorthogonalE] Symlets.

After DWT sub band coding only LL sub band concentrate on illumination information. Due to which only the LL sub band goes through the process, and which preserves the high-frequency components (i.e., edges). Hence, after inverse DWT (IDWT), the resultant image will be sharper with good contrast.

2.2 Stegonography

Steganography is one of the most powerful techniquesto hidesecret data in an multimedia carrier, e.g., image, audio, and video etc. Because ,if the feature is visible, the point of attack is evident, thus the our aim is always to conceal the very existence of the embed data.Steganographys ultimate objectives are undetectability, robustness and capacity of the hidden data, are the main factors that separate it from that related techniques that was used such as cryptography ,watermarking. And characters in the ASCII code can be represented using 8 bits. The values pixels of original image can be manipulated slightly without being noticed by visual inspection. This research paper is based on the premise that the bits of ASCII characters can be included in each one LSB of pixel of original image without resulting in a visible appearance in the so constructed image. Looking at a bitwise representation of an integer, the leftmost bit is called the most significant bit, or MSB. Conversely, the

rightmost bit is known as the least significant bit or LSB. Because of this property, if the LSB were changed, the number would not be significantly affected.Pixel values in an 8-bit gray-scale image is ranging from zero to 255 including for an 8-bit image. If the Least significant bit of 255 were changed from 0 to 1 , the result would be 254. As pixel values approach zero, the difference becomes larger. A successful insertion of a message into an image is more difficult using color images than that of grayscale images. A information hiding should result in the extraction of the hidden data from the image with high degree of data integrity. We were also aiming to reconstruct the original image after operations of LSB hiding & image compression

2.3 Least significant bit (LSB) algorithm

Based on the premise that the bits of ASCII characters can be included in each one LSB of pixel of original image without resulting in a visible appearance in the so constructed image. Looking at a bitwise representation of an integer, the leftmost bit is called the most significant bit, or MSB. Conversely, the rightmost bit is known as the least significant bit or LSB. Because of this property, if the LSB were changed, the number would not be significantly affected.In LSB technique, we take following example. Suppose the cover image has the following two pixel values

(0101 1010 0011 0001 0001 0100)
(1101 0101 1110 0011 1101 0101)

And, assume that the secret bits are**: 101101**

After embedding the secret bits, the pixel values are as follows:

(0101 101**1** 0011 000**0** 0001 010**1**)
(1101 010**1** 1110 001**0** 1101 010**1**)

The underlined dark bits indicate that the bits were changed from their original value. Out of them only four bits in the cover image were changed. On average about half of the bits in the cover image will be modified when embedding the secret image. If the number was large, 1028 for example, and the Least Significant Bit was changed from 0 to 1, then the number would be changed from 1028 to 1029, which is a change of only 0.0971%. Pixel values in an 8-bit gray-scale image is ranging from zero to 255 including for an 8-bit image. If the Least significant bit of 255 were changed from 0 to 1 , the result would be 254, a change of 0.391 %. As pixel values approach zero, the percent difference becomes larger. On the average only have of the bits would have to be changed in an LSB (Least Significant Bit) encoding scheme. With such a small variation in the colors it would be very difficult for the human eye to discern the difference. Next we will do least bit insertion with an 8 bit value. Since 8 bit values can only have a maximum of 256 colors the image must be chosen much more carefully. Consider a palette with four colors: white, red, blue, and green which have the palette position entries of 0(00), 1(01), 2(10) and 3(11) respectively.

III. System Development

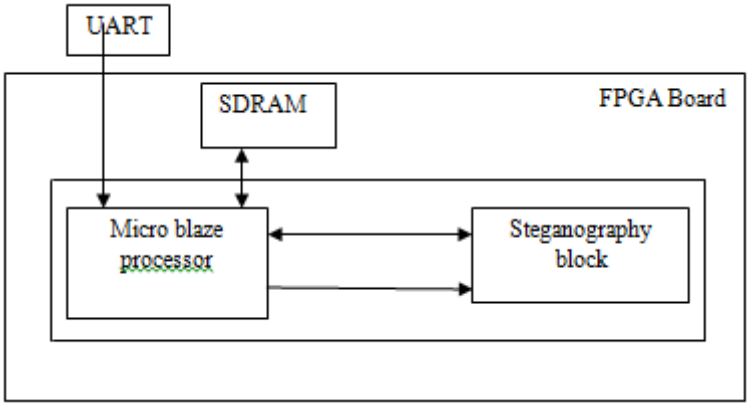

Fig.2 System Overview

3.1 Implementation

This implementation first hides bits of secret message in original test image, followed by Integer WT at single level decomposition. Hiding the bit in the image was accomplished by overwriting the selected bits of a pixel with the value of the bit. This was done by performing a bitwise AND operation of each one LSB of pixels of original image with 0, which effectively set all LSB bits to 0. Then the bit of secret message to be hidden in this pixel was then combined with the pixel by a bitwise OR operator, effectively setting these pixel bits to the message bits. This design implementation required XPS EDK 10.1 software platform along with Mat lab 7.5software. The conversion of true color image into gray color image and resizing of image into (128 * 128) format was carried out using Mat lab 7.5software.While coding of our design which include LSB encoding,Forward Inverse Wavelet Transform , LSB decoding & Reverse Inverse Wavelet Transform, was carried out by using Impulse C Language in XPS EDK 10.1software.The Top-Down Approach followed with the use IP core Micro blaze is 32 bit RISC Processor .Apply Haar Wavelet based Lifting Scheme Wavelet Transform (IWT) onStego image produced in step second to yield single level decomposition of Stego image into different four Bands labeled as LL , LH ,HL & HH .And finally apply decoding process to extract secret message hidden from compressed image obtained .Apply Reverse WT on compressed image obtained in so as to reconstruct the original image.

IV. Results

This design implementation required XPS EDK 10.1 software platform along with Matlab 7.5.The conversion of true color image into gray color image and resizing of image into (128 * 128) format was carried out using Matlab7.5.While coding of our design which include LSB encoding, Forward IWT, LSB decoding & Reverse IWT, was carried out using Impulse C Language in XPS EDK 10.1.And use IP core Micro blaze is 32 bit RISC Processor. Apply Haar Wavelet based Lifting Scheme Wavelet Transform on Stego image produced to yield single level decomposition of Stego image into different four Bands.Subband coding using DWT with different sub bands gives multiresolution analysis compared to other wavelet transforms.LL sub band gives directional information features.DWT with different levels like 3,5level gives more dimensionality reduction.

Fig.3 :stegno image with DWT sub bands

V. Conclusion

Aim is to achieving the purpose ofinformation hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to reduce or completely minimize noise and attacks, making use of redundancy to enhance the sound embed in the way nature to be addressed.A insertion of a message into an cover image is more difficult using color images than that of grayscale images. A information hiding should result in the extraction of the hidden data from the image with high degree of data integrity. We were also aiming to reconstruct the original image after operations of LSB hiding & image compression. This requirement led us to design fully pipelined single chip architecture for a hardware solution for hiding secret message in any given image & compressing it for efficient utilization of network bandwidth.

References

[1] K. Prasad., V. Jyothsna., S. Raju and S. Indraneel, "High Secure Image Steganography in BCBS Using DCT and Fractal Compression," International Journal of Computer Science and Network Security, vol. 10 No.4, April 2010.
[2] E. Walia, P. Jain, Navdeep, "An Analysis of LSB& DCT based Steganography", Global Journal of Computer Science and Technology, April, 2010, Vol. 10, pp. 4-8.
[3] Mohd,B.J., Abed,S., Al-Hayajneh., Alouneh,S "FPGA hardware of the LSB steganography method",Computer ,information and telecommunication system(CITS),2012 International conferenceon,vol., no.,1,4,14-16 May 2012
[4] B. Weaver, Now You See It, Scientific Computing 24.6 (May 2007): 18-39.
[5] B. Glass, Hide in Plain Sight, PC Magazine 21.18 (15 Oct. 2002): 75.
[6] Tucker, Patrick. "Hiding Secrets in Computer Files." Futurist 40.5 (Sep. 2006): 12-12.