Kamala Kumari al./ IJAIR Vol. 2 Issue 7 ISSN: 2278-7844

A NEW ADAPTIVE TECHNIQUE FOR LSB STEGNOGRAPHY

Kamala Kumari Chiluvuru[1], B.Uma Sankar[2]

[1]*Department of electronics and communication engineering, VRS&YRN College of engineering and Technology, Chirala, Prakasam dist, Ap, India.*

[2] *Assistant Professor Department of electronics and communication engineering VRS&YRN College of engineering and Technology, Chirala, Prakasam dist, Ap, India.*

Kamalaece.au@gmail.com[1], umasankar419@gmail.com[2]

Abstract-This paper presents an information hiding technique that utilizes lifting schemes to effectively hide information in color images. A successful information hiding should result in the extraction of the hidden data from the image with high degree of data integrity. Current trends favor using digital image files as the cover file to hide another digital file that contains the secret message or information.

Different streams of digital media can be used as a cover stream for a secret message. Steganography is the art of writing secret messages so that only the sender and the intended recipient are aware of the hidden message. This paper introduces a method of secret message encoding that makes use of wavelets. Wavelets break down the stream into high and low frequency component parts called details and trends.

Keywords : ***FPGA, LSB, Stegnography***

I. Introduction

Steganography is the art of invisible communication by concealing information inside other information. The term steganography is derived from the Greek and literally means "covered writing" [1]. A steganography system consists of three elements: cover-object (which hides the secret message), the secret message and the stego-object (which is the cover object with message embedded inside it.) Given the proliferation of digital images on the internet, and the large redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography [2].

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, whereas 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 [2].

There are several techniques to conceal 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. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. The transform domain techniques embed the message in the frequency domain of the cover image. Typically, spatial domain techniques are easily detectable [3] and have larger capacity [4]. On the other hand, frequency-based steganography has higher peak signal-to-noise ratio (PSNR) and is more secure [2].

Unfortunately, frequency-based techniques are more complex and require much more computations. Several FPGA implementations of spatial-domain stenography designs were proposed, such as the work in [5]. However, in our approach we implemented the spatial technique which balances the secret data size and the imperceptibility of the system.

II. LSB BASED IIMAGE STEGANOGRAPHY

The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR). To illustrate LSB technique, we provide the following example. Suppose the CVR has the following two pixel values:

(0000 1010 0011 0010 0111 0100)
(1111 0101 1100 0011 1100 0111)

Also, assume that the secret bits are: 1011012. After embedding the secret bits, the result pixel values are:

(0000 101**1** 0011 001**0** 0111 010**1**)
(1111 010**1** 1100 001**0** 1100 011**1**)

The underlined bits indicate that the bits were changed from their original value. Only three bits in the cover image were modified. On average about half of the bits in the cover image will be modified when embedding the secret image. The above LSB method limits the size of the secret data to eighth of the size of the CVR. LSB steganography can be extended to embed secret information in the least *n*-bits to increase the capacity of the secret information *n*/8 the size of the CVR. However, increasing *n* distorts stego-image. To illustrate the impact of the value of *n* on the stego-image, we performed several experimental runs on the test image, shown in Figure 1. (a). In each run, we embed random data in the *n* least significant bits, where $1 \leq n \leq 7$. However, we need to introduce the methods to measure the quality and distortion in images.

A. The Discrete Wavelet Transform

The Wavelet Series is just a sampled version of CWT and its computation may consume significant amount of time and resources, depending on the resolution required. The Discrete Wavelet Transform (DWT), which is based on sub-band coding is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required.

The foundations of DWT go back to 1976 when techniques to decompose discrete time signals were devised [5]. Similar work was done in speech signal coding which was named as sub-band coding. In 1983, a technique similar to sub-band coding was developed which was named pyramidal coding. Later many improvements were made to these coding schemes which resulted in efficient multi-resolution analysis schemes.

In CWT, the signals are analyzed using a set of basis functions which relate to each other by simple scaling and translation. In the case of DWT, a time-scale representation of the digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales.

B. Multi-Resolution Analysis using Filter Banks

Filters are one of the most widely used signal processing functions. Wavelets can be realized by iteration of filters with rescaling. The resolution of the signal, which is a measure of the amount of detail information in the signal, is determined by the filtering operations, and the scale is determined by up sampling and down sampling (sub sampling) operations[5].

The DWT is computed by successive low pass and high pass filtering of the discrete time-domain signal as shown in figure 2.2. This is called the Mall at algorithm or Mall at-tree decomposition. Its significance is in the manner it connects the continuous-time multi resolution to discrete-time filters. In the figure, the signal is denoted by the sequence x[n], where n is an integer. The low pass filter is denoted by G_0 while the high pass filter is denoted by H_0. At each level, the high pass filter produces detail information, d[n], while the low pass filter associated with scaling function produces coarse approximations, a[n].

This paper proposes the design of invisible watermarking using LSB algorithm. The work of the project is focused on the design and implementation of watermarking for a FPGA kit. In this project the coding is done in System C & the FPGA synthesis and logic simulation is done using Xilinx ISE Design Suite 10.1.

III. SYSTEM DESCRIPTION

Figure 2. illustrates the main components of the system. It consists of: steganography unit, Micro blaze processor, SRAM and UART interface. The steganography block and Micro blaze processor are implemented in the FPGA chip Spartan 3EDK.

The steganography block implements LSB steganography method by concealing the secret information in the CVR using a combination of 2-bit and 3-bit LSB steganography, referred to as 2/3-LSB. Each CVR pixel is represented by three bytes. A single byte of the secret information is concealed in the three bytes of a CVR pixel as shown in Figure 3. The proposed method has several advantages:

• This implementation significantly simplifies memory access since it maps one secret byte to one CVR pixel. Accessing and manipulating data at the bytes boundary simplifies hardware design and reduces design area and power.

• The secret size is third of the CVR size, which is considerably better than 1-bit LSB.

The LSB block receives the three bytes of CVR and one byte of the secret, combines them and then returns them back to the Nios processor. The steganography block is implemented in System C language.

In this paper first going to create a header file of the

images by using MATLAB. In mat lab we are creating the header files using GUI window. By using that header files as supporting file, fusing the two images by using DWT technique.

IV.RESULTS

This figure shows header file of image created through matlab by GUI

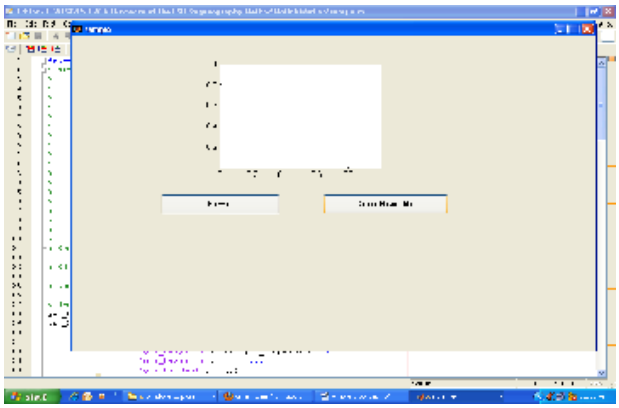

Fig1: GUI window to create header file

Figure shows the hidden data in text format in image at the recevier

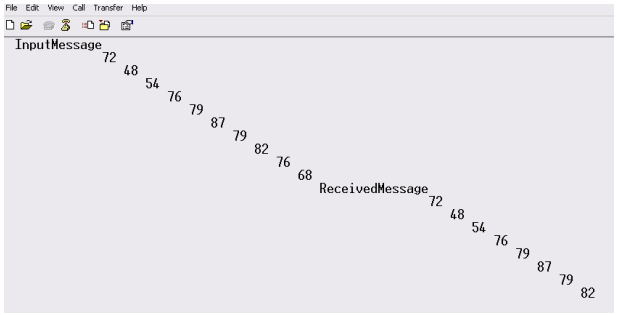

Fig2: Input and output text

This figure represent message is hide with image

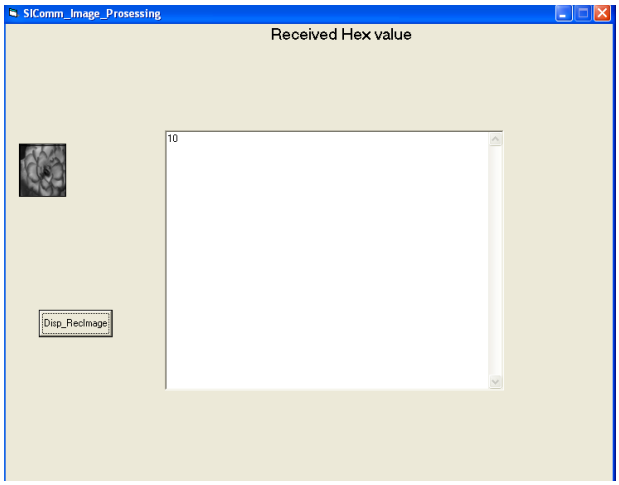

Fig.3. Hide with image

This figure represent image after performing LEAST SIGNIFICANT BIT ALGORITHM which is called as stego image

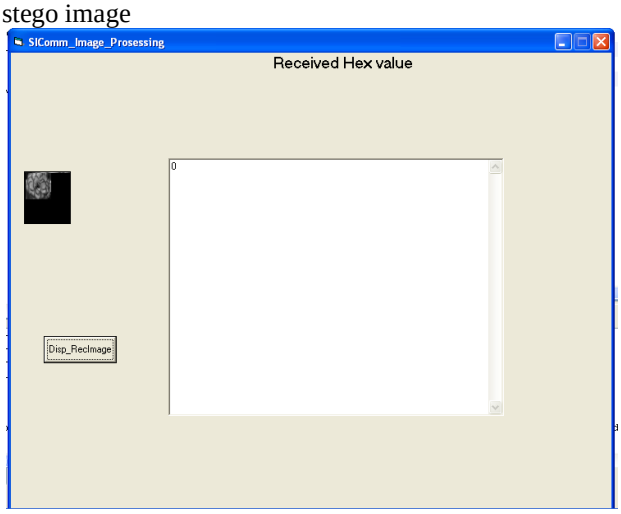

Fig4: Stego image

Figure shows that image which hide the data with little bit modifications which are neglect which appears as original image

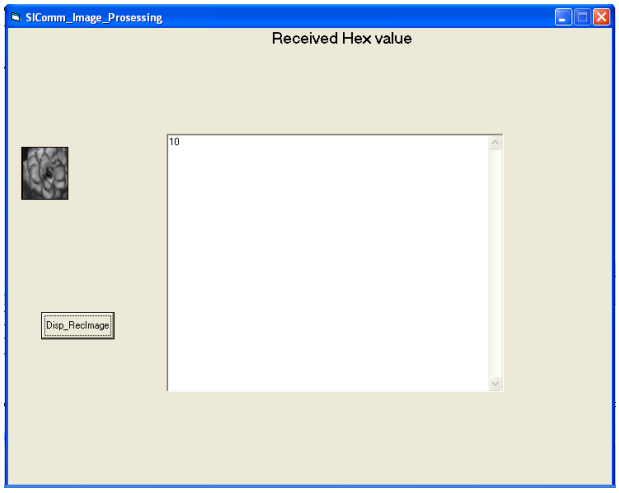

Fig5: Output image

V. CONCLUSION

Here invisible watermarking technique is implemented by using LSB algorithm on FPGA and the outputs are verified by applying discrete wavelet transform technique to the stego image to get the better results.

REFERENCES

[1] Neil F. Johnson, Sushil Jajodia, George Mason University, "Exploring Steganography: Seeing the Unseen", IEEE Computers, February 1998, pp. 26-34

[2] T. Morkel, J. Eloff and M. Olivier, "An Overview of Image Steganography," The Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, July 2005

[3] H. Wang, S. Wang, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, October 2004, Vol. 47, No. 10, pp. 76-82

[4] 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.

[5] E. Hernández, C. Uribe, R. Cumplido . "FPGA Hardware Architecture of the Steganographic ConText Technique", 18th International Conference on Electronics, Communications and Computers, pp. 123-128, Puebla, Mexico, March, 2008.

[6] 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.

[7] "The image database of the signal and imaging processing institute
(USC-SIPI)", The University of Southern California, [online].