International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 3, Volume 2 (March 2015) www.ijirae.com

HARDWARE IMPLEMENTATION OF LSB STEGANOGRAPHY FOR DATA SECURITY

Suraj Baddap[1] ,Ketan Khomane[2], Pratik Deshmukh[3],Prof Patharwalkal Shilpa[4]
Department of Electronics and Telecommunication,PGMCOE
Savitribai Phule Pune University,Maharashtra,India

Abstract— ***Data hiding is the art of hiding data for various purposes such as; to maintain private data, secure confidential data and so on. This work focuses on the image steganography using Least Significant Bit steganography method with encryption of image using RSA algorithm on FPGA Spartan Evaluation Development Kit (EDK). Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover image. The design balances the trade-off such as imperceptibility, quality and capacity.***

Keywords— ***2/3 LSB Steganography; RSA, FPGA, DATA Security***

I. INTRODUCTION

Steganography is the art of invisible communication by concealing information inside other information. The term Steganography is derived from 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.). Steganography is an art of sending secrete message under the camouflage of carrier content. The carrier content appears to have totally different but normal (”innocent”) meanings.

Since the rise of the internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret, but it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. In image Steganography the information is hidden exclusively in images. If these two methods can be combined together to form a hybrid approach, then two levels of security can be achieved.

In this investigation, we developed an alternative approach based on an embedded FPGA system for image processing. Field programmable gate array (FPGA) is widely used in embedded applications such as automotive, communications, industrial automation; medical imaging etc. FPGA is chosen due to its reconfigurable ability. Without requiring hardware change-out, the use of FPGA type devices expands the product life by updating data stream files. FPGA have grown to have the capability to hold an entire system on a single chip meanwhile; it allows in-platform testing and debugging of the system.

Furthermore, it offers the opportunity of utilizing hardware/software co-design to develop a high performance system for different applications by incorporating processors (hardware core processor or software core processor), on-chip busses, memory, and hardware accelerators for specific software functions.

The rest of the paper is organized as follows. Section II deals with system description. Section III introduces literature survey. Section IV introduces LSB steganography technique. Section V deals with RSA Encryption Algorithm. Section VI illustrates algorithm of proposed method. Section VII concluded with simulation results and discussions.

II. SYSTEM DESCRIPTION

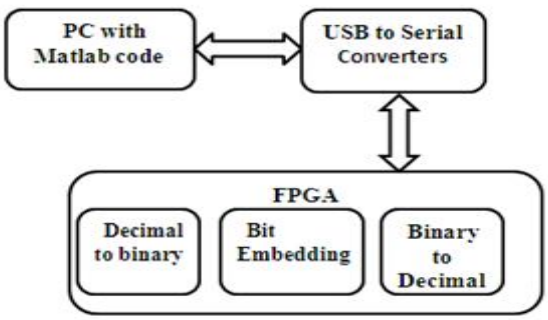

Fig 1: System overview

Figure 1.illustrates the main components of the system. It consists of: PC with MATLAB, Serial to USB converters, Spartan III FPGA. The Bit Embedding block is implemented in FPGA chip. The Bit Embedding block implements LSB steganography method to hide secrete image in cover image using 2/3 LSB method.

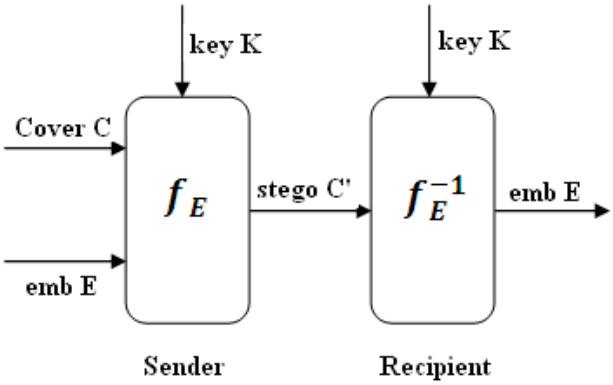

Fig 2: Stegosystem

EMB: The message to be embedded. It is anything that can be represented as a bit stream (an image or text).
COVER: Data/Medium in which EMB will be embedded.
STEGANO: Modified version of the cover that contains the embedded message.
EMB.KEY: Additional data that is needed for embedding & extracting.
F_E: Stegano graphic function that has cover, EMB & key as parameters.

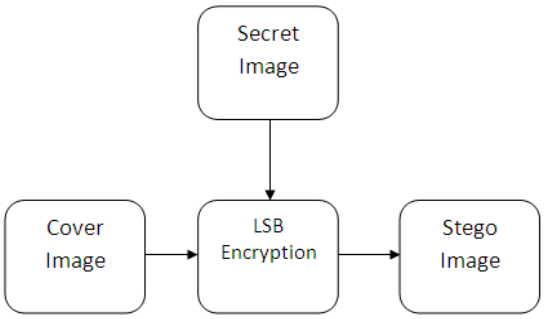

Fig 3: Encryption Algorithm

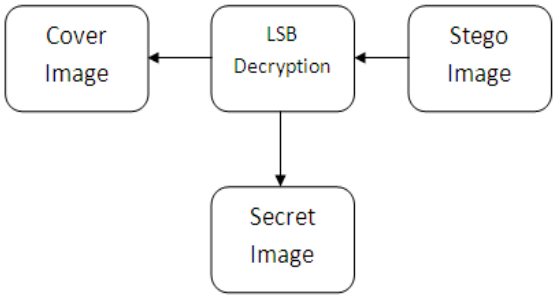

Fig 4: Decryption Algorithm

Image encoding on an image has 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 image on corresponding LSB position, then the output image is called stego image. For retrieve the secret image 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

A lot of Research has been carried out on Steganography because it is important to know how much data can be concealed without image distortion. Their description is as follows:

Bassam Jamil Mohd,Saed Abed ,Thaier Al-Hayajneh, Sahel Alouneh, [1] presents a hardware design of Least Significant Bit (LSB) steganography technique in a cyclone II FPGA of the Altera family. The design utilizes the Nios embedded processor as well as specialized logic to perform the steganography steps. Neil F. Johnson, Sushil Jajodia [2] has discussed image files and how to hide information in them, discuss results obtained from evaluating available

steganographic software. T. Morkel, J. Eloff and M. Olivier [3] this paper intends to give an overview of image steganography, its uses and techniques.

H. Wang, S. Wang [4] has discuss various method and tool being developed to hide information in multimedia data and equal number of clever methods and tools are being developed to detect and reveal its secrets. E. Walia, P. Jain, Navdeep [5] has proposed analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography. Gandharba Swain, Saroj Kumar Lenka [6] has proposed a method for secret communication using cryptography and steganography.

IV. LSB BASED IMAGE 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.
To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar (or different) the stego-image compared with CVR.

•Mean Squared Error (MSE)is computed by performing byte by byte comparisons of the cover image and stego-image. The computation can be expressed as

$$MSE = \frac{1}{MxN} \sum_{1}^{M} \sum_{1}^{N} (fij - gij)^2 \qquad (1)$$

Where M, N are the number of rows and columns in the cover image matrix, f_{ij} is the pixel value from cover image, and g_{ij} is the pixel value from the stego-image. Higher value of MSE indicates dissimilarity between compared images.
• Bit error rate (BER) computes the actual number of bit positions which are changed in the stego-image compared with cover image.
• Peak signal-to-noise ratio (PSNR) measures in decibels the quality of the stego-image compared with the cover image. The higher PSNR better the quality. PSNR is computed using the following equation:

$$PSNR = 10 \log_{10} \frac{255}{MSE} \qquad (2)$$

V. RSA Encryption Algorithm

RSA are the initials of the three creators: “Ron Rivest, Adi Shamir and Leonard Adleman “in 1977, so RSA stands for Rivest, Shamir, and Adleman. It is most widely used public key algorithm. The two main branches of public key cryptography are Public key encryption and Digital signatures. So it supports Encryption and Digital signatures. Get its security from integer factorization problem. Relatively easy to understand and implement and Patent free (since 2000). RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, SSH, SILC, and many more.

3.4.1 Encryption and Decryption Process

- Choose two large distinct primes *p* and *q* and then form the *public modulus n* = *pq*.
- Choose *public exponent e* to be co prime to $(p-1)(q-1)$, with $1 < e < (p-1)(q-1)$.
- The pair (*n, e*) is the *public key*.
- The private key is the unique integer $1 < d < (p-1)(q-1)$ such that

$$ed = 1 \bmod (p-1)(q-1)$$

- **Encryption:** Split a message *M* into a sequence of blocks *M*1, *M*2, . . . , *Mt* where each *Mi* satisfies $0 \leq Mi < n$. Then encrypt these blocks as

$$C = E(M) = M^e mod(n) \quad (1)$$

- **Decryption:** Given the private key d and the cipher text C, the decryption function is:

$$D = C^d (mod\ n) \quad (2)$$

Note that encryption does not increase the size of a message. Both the message and the cipher text are integers in the range 0 to n - 1.

The encryption key is thus the pair of positive integers (e; n). Similarly, the decryption key is the pair of positive integers (d; n). Each user makes his encryption key public, and keeps the corresponding decryption key private.

VI. ALGORITHM OF PROPOSED METHOD

The algorithm for proposed method has two parts, first embedding the secret message into cover image to produced stego image and second retrieve the message from stego image as shown below-

A. Algorithm to embed message

Step 1: Read the cover image and secrete image which is to be hidden in the cover image.
Step 2: Convert secrete image in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret image one by one as per 2/3 LSB steganography method
Step 5: Write stego image

B. Algorithm to retrieve message

Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert it into secrete image.

VIII. SIMULATION RESULTS

In this section we show the result of simulation on a cover image. The algorithm successfully concealed the secret image into cover image to produce stego image shown in Fig 5.

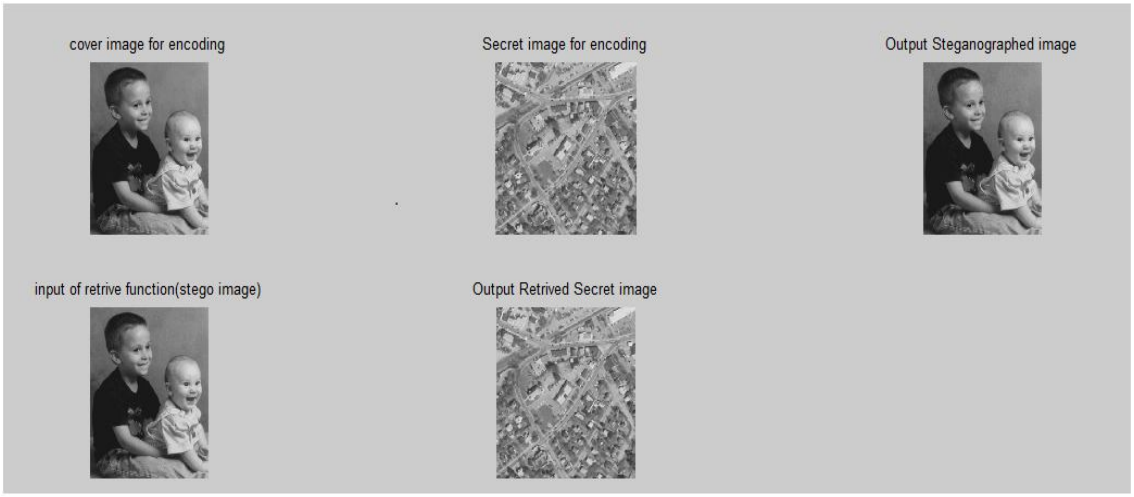

Fig 5: Embedding and Retrieving secret data

The image metrics are computed for produced stego image and original cover image, illustrated in TABLE I.

N-BIT LSB	MSE	BER	PSNR
2/3 LSB	0.89	0.039	109.19
2 LSB	2.97	0.12	97.13
3 LSB	14.61	0.17	81.23

TABLE I

IX. CONCLUSION

In this paper, the 2/3-LSB hardware design which provides good image quality and facilitate simple memory access. We also presented the simulation results of test image executed with 2/3-LSB steganography method. Future work should focus on hardware implementation of more complex random-based LSB mechanisms, as well as optimizing the design speed and power. Here steganography block is implemented in FPGA block so that we can create ASIC for the same.

REFERENCE

[1] Bassam Jamil Mohd, Saed Abed ,Thaier Al-Hayajneh,Sahel Alouneh, “FPGA Hardware of the LSB Steganography Method,” IEEE Transaction on consumer Electronics,vol. 978, no. 1, pp. 4673–1550, 2012.
[2] Neil F. Johnson, Sushil Jajodia, George Mason University, "Exploring Steganography: Seeing the Unseen", IEEE Computers, February 1998, pp. 26-34.
[3] 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
[4] H. Wang, S. Wang, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, October 2004, Vol. 47, No. 10, pp. 76-82
[5] 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
[6] Gandharba Swain Saroj Kumar Lenka, “A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography”, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012 .

