ISSN 2321 – 2004
ISSN 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 3, June 2013

Releaving the Hidden Secret with LSB Steganography

Ankita Ganorkar[1], Sujata Agrawal[2]

E & TC Dept, Smt.Kashibai Navale college of Engineering, pune, Maharashtra, India [1]

Assistant Professor, E&TC Dept, Smt.Kashibai Navale college of Engineering, pune , Maharashtra, India [2]

Abstract: Data hiding is the art of hiding data for various purposes such as; to maintain private data, secure confidential data and so on. There are lots of techniques used for data hiding and the well known technique is the Steganography. Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover medium used in steganography. Embedding secret information inside images requires intensive computations, and therefore, designing steganography in hardware speeds up steganography. This paper provides a hardware design of Least Significant Bit (LSB) steganography technique. The design utilizes the Spartan III FPGA kit of the Altera family and 2/3-LSB steganography algorithm to perform the steganography steps. The design balances the tradeoffs such as imperceptibility, quality and capacity.

Keywords: 2/3-LSB steganography, Security, FPGA

I. INTRODUCTION

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. The technique used to implement this, is called steganography. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret Steganography is the art and science of invisible communication [4]. This is accomplished through hiding information in other information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing"[3]. 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. Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages, steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file.

A proposed algorithm for steganography is in digital image. There are many methods to hide information in images. Any text, image, or anything that can be embedded in a bit stream can be hidden in an image. Image steganography has come quite far in recent years with the development of fast, powerful graphical computers. An image in a computer is an array of numbers that represent light intensities at various points. These pixels make up the image's raster data. Digital images are stored in either 24-bit (true colour images) or 8-bit per pixel files. A common image size is 640 × 480 pixels and 256 colours (or 8 bits per pixel). Such an image could contain about 300 Kb of data. Such large size images should be avoided since the attention when sending over a network or the Internet. Hence 8-bit colour images, like GIF files, can be used to hide information. Here, each pixel is represented as a single byte, and the pixel's value is between 0 and 255. Grey-scale images are preferred because the shades are changed very gradually between palette entries. This increases the image's ability to hide information [1].

II. 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

ISSN 2321 – 2004
ISSN 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 3, June 2013

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] have 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. The cryptographic algorithm is a block cipher with a block length of 128 bits and key length of 256 bits. The secret message is encrypted by this block cipher. As the embedding locations are decided at the run time of the algorithm, so it is called as dynamic steganography. The technique is experimented and results are discussed. V.Sharma,V. Shrivastava [7] has present a new steganographic algorithm for 8bit (grayscale) or 24 bit (colour image) based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. in this n LSB of cover image ,from a byte is replaced by n MSB of secret image.A.E.Mustafa,A.M.F.ElGamal , M.E.ElAlmi,Ahmed.BD [8] have proposed a novel method based on the spatial domain for encoding extra information in an image by making small modifications to its pixels. R.Ibrahim, Teoh Suk Kuan, [9] have proposed a new image steganography method called Steganography Imaging System (SIS) ,which uses binary codes and pixels inside an image. The zipped file is used before it is converted to binary codes to maximize the storage of data inside the image. M.Umamaheswari, S.Sivasubramanian, S.Pandiarajan [10] proposed a method to compress the secret message and encrypt it by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm. Aneesh Jain and Indranil Sengupta [11] have proposed new image steganography that make use of Least Significant Bit (LSB) algorithm for hidding the data into image which is implemented through the Microsoft .NET framework.

III. LSB BASED IMAGE STEGANOGRAPHY

Least significant bit (LSB) steganography is a common, simple approach to embedding information in a cover file to hide an image in the LSBs of each byte of a 24-bit image; you can store 3 bits in each pixel. A 1,024 x 768 image has the potential to hide a total of 2,359,296 bits (294,912 bytes) of information. If you compress the message to be hidden before you embed it, you can hide a large amount of information. To the human eye, the resulting stego-image will look identical to the cover image.

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is **10000011**. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits or only 50% of bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to distinguish it [8].

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar or different the stego-image compared with cover image. The following metrics are used

- 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, fij is the pixel value from cover image, and gij 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:

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

The results of the image metrics are summarized in Table I.

IV. 2/3 LSB STEGANOGRAPHY METHOD

2/3 LSB steganography implemented 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 cover image pixel is represented by three bytes. A single byte of the secret information is concealed in the three bytes of a cover image pixel as shown in Fig 1.

ISSN 2321 – 2004
ISSN 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 3, June 2013

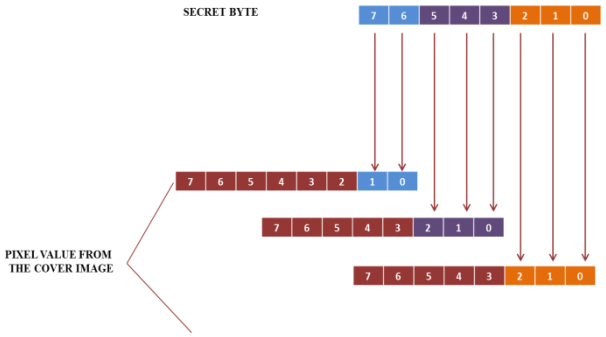

Fig. 1 Mechanism of 2/3 LSB steganography

The 2/3 LSB has advantages over traditional 1-bit LSB method such as it simplifies memory access and reducing design area and power requirement. It also simplifies the hardware design. It has good image metrics compared to 2-bit LSB or 3-bit LSB [1].

V. 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 message which is to be hidden in the cover image.
Step 2: Convert message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
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 each 8 bit into character

VI. SYSTEM DESCRIPTION

This algorithm is using two layers of security to maintain the privacy, confidentiality and accuracy of the data. Fig. 2 shows the block diagram for the overall process of the system. The system is able to hide the data inside the image as well as to retrieve the data from the image. From Fig. 1, for hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. Using 2/3 LSB steganography algorithm, these data will be embedded and hided inside the image with almost zero distortion of the original image and send to the receiver side.

For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data.

The secret key in this proposed steganography algorithm is playing an essential role where the key is acts as a locker that used to lock or unlock the secret message In order to retrieve a correct message from the image, a secret key is needed for the purpose of verification. Once the key is matched, the process continues to retrieve the secret message.

VII. SIMULATION RESULTS

In this section we demonstrate the result of simulation on a test cover image. The cover image is as shown in Fig.3. The secret message is shown in Fig.5. The algorithm successfully concealed the secret image into cover image to produce stego image shown in Fig 4.

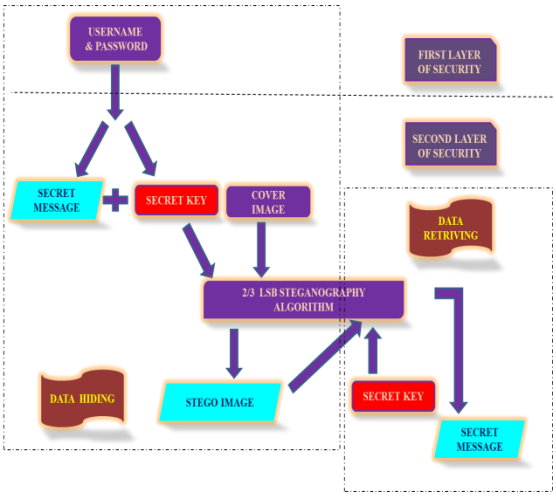

Fig. 1 The block diagram for the system

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

The result shows that produced stego image has good PSNR and small error results to that LENA image for the 2/3-LSB case.

TABLE I
IMAGE METRICS FOR PROPOSED LSB METHOD

n-bit LSB	MSE	BER	PSNR(dB)
2/3-bit	2.7	0.051	48.52
2-bit	2.5	0.032	42.31
3-bit	9.5	0.085	37.31

ISSN 2321 – 2004
ISSN 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 3, June 2013

Fig. 3 The cover image

Fig. 4 The stegno image (after embedding secret image)

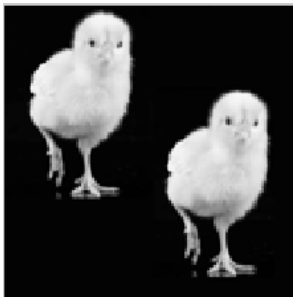

Fig. 5 the Secret image

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.

REFERENCES

[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 .

[7] V. Sharma ,v. Shrivastava,"a steganography algorithm for hiding image in Image by improved LSB substitution by minimize" Detection",Journal of Theoretical and Applied Information and Applied Information Technology,15th February 2012.Vol.36 No.1

[8] A. E.Mustafa , A.M.F.ElGamal , M.E.ElAlmi , Ahmed.BD ,"A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit",Research Journal Specific EducationFaculty of Specific Education Mansoura University Issue No. 21, April. 2011

[9] R.Ibrahim,Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application 2 (2011) 102-108

[10] M.Umamaheswari,S.Sivasubramanian, S. Pandiarajan, "Analysis of Different Steganographic Algorithms for Secured Data Hiding", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010

[11] Kavitha, K.Kadam ,A.Koshti, P. Dunghav, "Steganography Using Least Signicant Bit Algorithm",International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012.

[12] 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

[13] "Peak Noise to Signal Ratio". [online]. Available: http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[14] "The image database of the signal and imaging processing institute (USC-SIPI)", The University of Southern California, [online]. Available: http://sipi.usc.edu/database