I J C T A, 10(9), 2017, pp. 49-55
© International Science Press

ISSN: 0974-5572

LSBI Steganography on Real Time Embedded System

M.S. Chelva* and S.V. Halse**

ABSTRACT

Information security is one of the major concern in this age of digital world. As the society is at large towards digital domain security becomes a paramount issue. Many applications like confidential communication, secret data storage & transmission, digital signature etc, need to be highly protected from hackers or persons with ill intention. Though there exist several techniques for information security such as encryption still people with evil mind snoop into to cause damage. Steganography though not a new technique but still has a lot of promise in the digital world for information security. This is a way to communicate secret messages through images. This technique helps to hide data such a way that even if the image is examined, no secret message can be retrieved. In this paper, we discuss about multiple images Steganography techniques and focuses in detail on the Least Significant Bit Insertion (LSBI) based image Steganography. We implement LSBI on embedded platform with real time constraints and found that results are encouraging.

Keywords: Image Steganography (IS), Least Significant Bit Insertion (LSBI), Message Hiding (MS), ARM Embedded System.

1. INTRODUCTION

The important factor of technology called internet is essentially required a security for information needs because of its waste rise. Various techniques being originated in order to encode as encrypt and decode as decrypt the data for keeping secret messages and a new technique called Cryptology is developed for securing communication secrecy. All the time, it is not necessary to keep message secret, so the technique called as Steganography. It is a art and science of communication made invisible. It is the way of hiding the secret data in a communicated channel. Steganography is a Greek word “stegano” means cover , “grafia” means writing Obiously, it is “cover writing”. It is a method by which we can hide a data in a cover media of image in such manner that unplanned observer will not be aware of the message is hidden.

Covered media should be chosen in such a way that it should have good capacity [2] to achieve good results. There are different types in steganography i.e. image, audio, video steganography. These are segregated depending on the medium to embed the secret information. If inside the image secret information is embedded then it is image steganography or if inside the audio secret data is embedded then audio steganography. Concealing the content of message is called cryptography whereas concealing their existence is called steganography. Whenever there is a requirement to hide data, steganography can be used. Whether the image is suspected or not, no one can prove about the involvement of image caring secret information is the advantage of this technique.

Useful applications of Steganography are as follows:

- It provides confidential communication and secretes storing of data
- provides protection for data alternation so that people can send and recieve their digital certificate information or important document or anything information to anywhere in the world.

* Research Scholar, SVMV, SRTM University, Nanded, Maharashtra, India, *Email: mschelva@gmail.com*

** Karnataka States Women’s University Vijaypur, Karnataka, India, *Email: drsvhalse@rediffmail.com*

- It is very useful in TV broadcasting for copyright control of materials.
- A unique identification ID can be embedded in to image.
- For analyzing network traffic of a particular user [3] .
- Network Steganography method is used in telecommunication network which is applied to IP Telephony. It works more accurately if it is applied to encrypted form of secrete data.
- Terrorist are also using Steganography for their secrete communication.

The most likely used image formats in Steganography are:

- Graphics Interchange Format (GPF).
- Joint Photographic expert Group (JPG).
- Portable Network Groups (PNG).

The general process of Steganography is to enveloped image and then secret message is merged in to envelope image and so called newly image is stegno image. Obviously, the sender must have merging algorithm and the receiver must have retrieving algorithm with same secret key.

A diagram shown above in a Figure 1 is a generic image Steganography complete system. Through this algorithmic logic, the data message is embedded in binary image with the help of secret unique key. Resulted stego image transmitted through a channel to a receiver, where the same key is used by retrieving algorithm. A stego image: the unauthorized viewers who can notice only communication of an image not the content of hidden data in a image during transmission time.

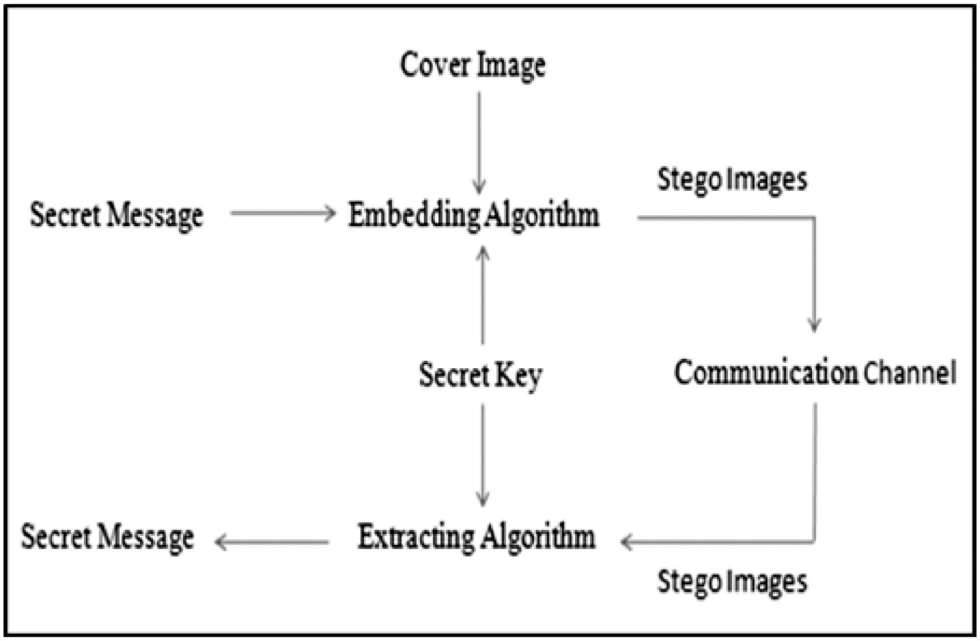


Figure 1: Generic image Steganography system

2. LITERATURE REVIEWS

There are various methods of steganography to hide the secret data. Common methods are Least Significant Bit Insertion (LSBI) which uses least bits of pixels to embed secret data [4]. This method is substitution to increase security [5]. Dynamic programming strategy is an ancient method Proposed by Chang et al [6]. In human visual system characteristics, the sizes of variables LSBs are Embedded is given in [7]. Few samples of halftone images hiding way shows that maintaining quality of image visual, embeds a huge amount of secret message in [8]. The quality Stego image embedded data in to digital image with good capacity of hiding ,ensuring high security is presented [9][10]. Wu and Tsai [11] have presented the two consecutive pixels between deference's in envelop image to find out the message of secret to be hide. Certainly, the way provides imperceptible quality of stego image.

A new technique in the year of 2010 was derived for enhancing the picture quality as well as addresses the steganalysis problem [12]. They used Quantisation based image steganography. For proper modification of pixel value and its coefficient close loop computing framework system is designed. This method is particularly suitable where the secrete message information is spread to multiple pixel and coefficient to optimizes the pictorial looking quality of the stego image.

Another technique was suggested to minimize detectable distortion in data hiding. By considering Quantisation step, Magnitude of quantized Discrete Cosine Transform (DCT) coefficient (MQ), Perturbation error (PE) a new channel selection rule was introduced by author for JPEG image [5]. This technique provide higher security performance, minimize distortion and it is easy to conduct.

The one third of embedding technique in the year 2013, which decreases changing probability pixel value of each pixel. Thus 1/3 of embedding data will be enable, without scarifying embedding capacity is suggested by Saeed Sarreshtedari et.al [13]. The LSB-detector gives a 1bit/pixel, with good imperceptibility and more robustness for capacity of embedding is described in above said technique. Envelop image and stego images are all most look same in such a way that detection of embedding is less. Stego-image provides high embedding capacity & preserves the histogram maximum extent.

The data hiding scheme is proposed by wang el al, recently[14], Genetic algorithms and Least Significant Bit(LSB) substitution optimal . By using proposed algorithms in above said method the envelop image and sego image half of the obtained by the Worst Mean Square Error(WMSE).

For secure banking application one technique was proposed: where we use eight more around the Neighbour Pixels(NP) focussing with target pixel (TP), the code of customer (password) is encoded and then dividing into shared manner. Some shares are given to banks while the customer is authenticated by examining these shares [15]. Here, this technique provides customer authentication as well as both cryptography and steganography is used through image processing for better imperceptibility and security.

Another technique used Haar wavelet transform [16]. The image of cover ie. cover image is divided into two parts i.e. high frequency and low frequency. The information is inserted in all color components to increase security. Speed of this method is slow which makes it unfit to be used for real time embedded system.

For improving the , hide ability of hidden message of secret and to give an invisible stego good image : a method of novel used for steganography for the replacement of least significant bit and pixel value differencing [11]. The PVD method is used for Obtaining the value of difference between two successive or continues pixels. A difference small value situated on flat or plane surface & big value can be situated on border or boundary area. By using of LSB method, the flat area concerned secret message data is hidenin to envelop image at the same time pixel value difference or PVD methodology is used for the data is hiding in edge area. It is very hard to guess in either methods: least significant-bit or pixel value - difference. Where the assurance of security is same in either case.

Image steganography based a novel technique: Discrete Cosine Transform is used for transforming of envelop image from spatial to frequency domain conversion [18]. First, we divide image of gray MXN matrix length in to block 8X8 then 2D (Two Dimensional) DCT is made. The Huffman code performed before the secret message. In frequency domain each bit is embedded by changing LSB of each DCT coefficients of the image cover blocks. Comparing with existing approaches of steganography, PSNR gives good results of cover image with image of stego.

In view of improving the quality of image and achieving good capacity & speed, a LSB image steganography is implemented on hardware using FPGA[17]. Due to use of FPGA good speed is achieved but the signal to noise ratio (SNR) is low.

3. METHODOLOGY

The image steganography is a methodology to send information in a secret manner and this can be used to communicate any type of information may it be text or symbols or numbers or special characters. We have used the Least Significant Bit Insertion (LSBI) steganography algorithm hiding of data and its inverse to retrieve the information. This algorithm is implemented on the ARMv9 board embedded system. Consider a random Image being using in application to hide and transmit the data. The information that can be hidden in an image directly depends on size of the image used to transmit data and also on the number of bytes representing one pixel. For example a 32-bit image hides more data than an 8-bit image. Get the text to hide from a file and get size of the text in bytes. Now, consider a byte from the text string and convert it to binary string and OR each bit with the pixel bits and assign the modified pixel to output image. This process of hiding requires a very less time as it involves only logical operations.

Encoding Algorithm:

```
  i. Get Input image (RGB image)
 ii. Get the text to be hidden
iii. Get Encode pattern
 iv. For each text k in string
        For each row i
        For each column j
        currPixel = img(i, j)
        currTxt = string[k]
        if any of the 0th 1st or 2nd bit in currTxt is set
            OR it with corresponding 3 LSB of Red pxl
        End
        if any of the 3rd, 4th or 5th bit in currTxt is set
            OR it with corresponding 3 LSB of Green
        End
        if any of the 6th or 7th bit in currTxt is set
            OR it with corresponding 2 LSB of Blue pxl
        End
        End Column
        End Row
  v. End String
 vi. Assign size and width of text to one of the pixel value
vii. Construct image with hidden data
```

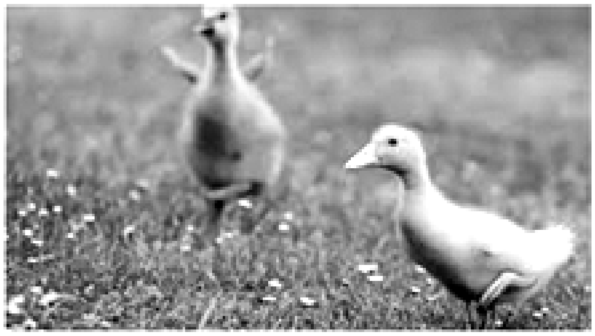
The message hidden will be retrieved using exactly the reversal method of that used for hiding message. The algorithm to retrieve data is described below.

Decoding Algorithm:

```
  i. Get image with hidden text (RGB image)
 ii. Get Encode Pattern
iii. Get size and width of text from image
 iv. For k = 1 to sizeo(text)
     For each row i
     For each column j
     currPixel = img(i, j)
     currTxt = string[k]
     if any of the 0th 1st or 2nd bit in RedPxl is set
         OR it with corresponding 3 LSB of kth byte of text
     End
     if any of the 0th 1st or 2nd bit in Green Pxl is set
         OR it with 3rd, 4th or 5th bit of kth byte of text
     End
     if any of the 0th 1st or 2nd bit in Blue Pxl is set
         OR it with 6th or 7th bit of kth byte of text
     End
     End Column
     End Row
     DecodedText = Concat(DecodedText,Curr_Char)
     End k loop
  v. Write decoded text to a file
```

4. RESULTS

The LSB insertion algorithm for steganography is implemented on the ARMv9 processor based embedded system. The results shown are shown in the Figure 2. Fig. 2a is the input image used to hide the message in the



(a)

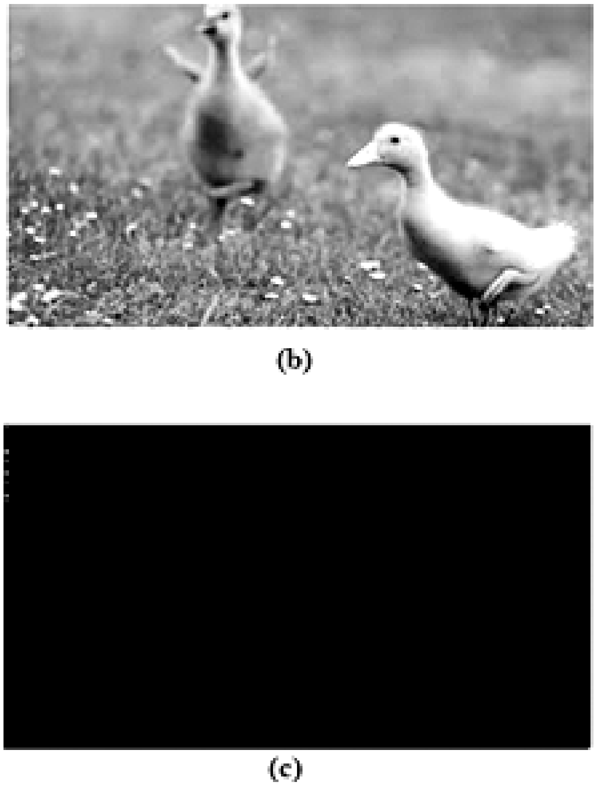
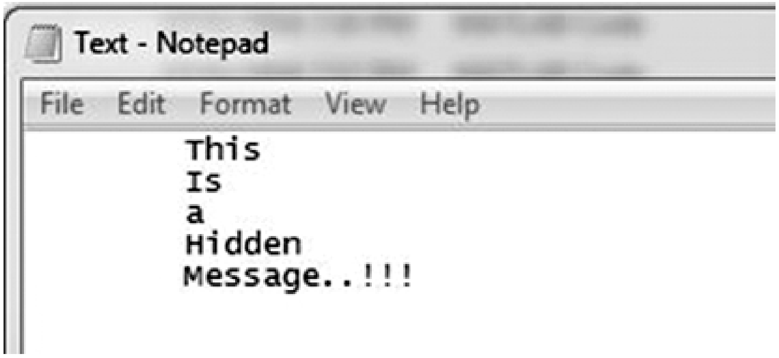


Figure 2: (a) Input image used in Steganography (b) Image with Hidden Message (c) Difference Image



```
This
Is
a
Hidden
Message..!!!
```

Figure 3: Message Hidden in the Image

algorithm; Fig. 2b is the image with a hidden message to be conveyed to the other end. The both Fig. 2a and Fig. 2b seems to be identical, with no visible change in the nature design. The hidden message has certainly change the pixel values of image, but as the algorithm alters maximum three LSB of image, it make a minor difference and hence difference is not visibly reflected in the output image in Figure 2b. The Figure 2c showing the difference image that is the white pixel denote the pixels that have modified pixel values.

5. CONCLUSION

The image steganography is widely used in exchanging secret information between two end base stations. The Least Significant Bit Insertion algorithm implemented here takes few hundreds of milliseconds to execute on the ARM based embedded system. The complete system produces faithful results for both, information hiding and retrieving, on embedded platform. The execution time of algorithm directly varies Quantity of data to conceal in a image. As the algorithm involves majorly the logical operation, the execution time remains small enough making algorithm feasible for real time embedded system.

REFERENCES

[1] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science,

[2] Rahki, Suresh Gawande, “A Review On Steganography Methods”, International Journal Of Advanced Research in Electrical, Electronics and Insrumentation Engineering, Vol.2, issue 10, October 2013.

[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevit, Digital image steganography: Survey and analysis of current methods, Elsevier Signal processing 90(2010) 727-752.

[4] S. Walton, “Image authentication for a slippery new age,” Dr. Dobb’s Journal, vol. 20, no. 4, pp. 18–26, 1995.

[5] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognition, vol. 34, no. 3, pp. 671–683, 2001.

[6] C. C. Chang, J. Y. Hsiao, and C. S. Chan, “Finding optimal least signiûcant-bit subsuitution in image hiding by dynamic programming strategy,” Pattern Recognition, vol. 36, no. 7, pp. 1583–1595, 2003

[7] Y. K. Lee and L. H. Chen, “High capacity steganographic model,” IEEE Proceedings Vision, Image and Signal Processing, vol. 147, no. 3, pp. 288–294, 2000.

[8] M. S. Fu and Oscar C. Au, “Data hiding watermarking for halftone images,” IEEE Transactions on Image Processing, vol. 11, no. 4, pp. 477–484, 2002.

[9] Y. C. Tseng, Y. Y. Chen, and H. K. Pan, “A secure data hiding scheme for binary images,” IEEE Transactions on Communications, vol. 50,pp. 1227–1231, Aug. 2002

[10] Y. C. Tseng and H. K. Pan, “Data hiding in 2-color imgages,” IEEE Transactions on Computers, vol. 51 Issue: 7, pp. 873–878, Jul. 2002.

[11] D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24, no. 9-10,pp. 1613–1626, 2003

[12] Qian Mao, “A fast algorithm for matrix embedding steganography”, ELSEVIER Digital signal processing 25(2014)248-254.

[13] Saeed Sarreshtedari, Mohammad Ali Akhaee, One third probability embedding: A new +-1 histogram compensating image least significant bit steganography scheme, IET image processing(2013)78-89

[14] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683.

[15] S.Premkumar, A.E. Narayana, New visual steganography scheme for secure banking application, International conference on computing, electronics and electrical Technologies[ICCEET]IEEE(2012)1013-1016

[16]]Juned Ahmed Mazumdar and Kattamanchi Hemchandran “Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method”, International Journal Of Computer Science and Engineering, Vol-2,issue-7, Jully 2014.

[17] 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

[18] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar “A novel technique for image steganography based on Block-DCT and Huffman Encoding “ International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010