PSoC based LSB Stegnography for the Copyright Protection of Images

Swati G. Patil[1] Mr. A. M. Bongale[2]
[1,2]G.H.Raisoni Institute of Engineering and Technology, Wagholi, Pune

Abstract— In recent years, large number of media files are transferred through internet. So it becomes necessary to protect transferred digital data. Stegnography is the technique of hiding secret image in the cover image. In the proposed system secret image is embedded in the cover image by using the technique of LSB Stegnography. Algorithm is implemented on PSoC. Image data is send to hardware through serial communication it applies two third LSB algorithm and send embedded image to PC for display. Performance of the system is monitored through various parameters such as Bit Error Rate, Peak Signal to Noise Ratio and Mean Square Error.

Key words: Copyright Protection; Image Stegnography; LSB; PSOC; MATLAB

I. INTRODUCTION

Steganography is the most powerful techniques to hide secret data inside a cover object. Images are the mostly used cover objects for Steganography .Embedding secret information inside images requires large number of computations, So if Steganography is performed by using hardware it speed up the process of embedding[1]. The image obtained after embedding of message is called a stego image. Message is inserted in the Least Significant Bit (LSB) or Most Significant Bit (MSB) of the image pixels. In the stego image message embedded is invisible to the human eye. This means that there is no difference between the original image and stego image visually [2].

A. Stegnography Types

Data can be hidden in basic formats like image, audio and video. Types of Steganography include [3]

1) Image Steganography

In image Steganography, we embed secret data in an image and there will not be any perceived visible change in the original image.

2) Audio Steganography:

This type of Steganography can be applied to audio files i.e., we can hide information in an audio files. Audio files should be undetectable.

3) Video Steganography

If we hide information in the video file then it is called video Steganography. This video file should be undetectable by attacker.

4) Text files Steganography

Steganography can be performed on text also. If we hide secret information in text file then it is called as text file Steganography[4].

In proposed system, image Steganography is performed. Here, Cover object is image and secret data is also in the image format. Secret image is embedded in cover image by using Least Significant Bit algorithm.

This paper is organized as follows: Section II gives scheme of the proposed system and also explains the least significant bit algorithm. Section III gives the system implementation details such as hardware and software used for the implementation of the system. Results are discussed in Section IV. Finally, the work is concluded in Section V.

II. PROPOSED WORK

A. Block Diagram of Proposed Scheme

Image Steganography consists of two stages:

1) Encryption Stage

The proposed system consists of PC with MATLAB code, PSoC development board as shown in figure 3. Three bytes of cover image data and one byte of secret image data is send from PC to PSoC board through serial communication. In PC some image preprocessing operations are performed on both the images. Secret image is embedded in the cover image by using two third least significant bit algorithms. Embedding of the data is performed in PSoC board. After embedding data is sent back to PC with MATLAB for display.

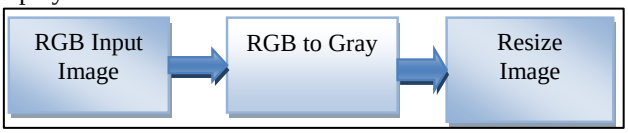

Fig. 1: Image preprocessing steps performed

Figure 1 shows the Image preprocessing steps performed. Image processing is done in MATLAB. First read RGB input image then convert the RGB image to grayscale. Then resize the grayscale image according to the requirement. Cover image should be three times greater in size than the secret image.

2) Decryption Stage

In the decryption stage we separate secret image from the cover image. This is reverse process of encryption. We can retrieve secret data in this stage.

B. System Flow

1) Flow of Encryption

Step 1: Read cover image and secret image of size MXN.
Step 2: RGB to gray conversion of cover image and secret image.
Step 3: Resize cover image and secret image of size MXN into the standard required size
Step4: Convert both secret image and cover image to binary image.
Step5: Send Image data to PSoC development board.
Step6: Apply two third LSB algorithm.
Step7: Get Stego image. Send it back to PC. Convert it back to grayscale and then RGB. Display Stego image.

Flow of Decryption:

Step1: Read stego image.
Step2: Convert image from RGB to gray.
Step3: Convert image from grayscale to binary.
Step4: Extract the encrypted LSB data.
Step5: Get cover image and secret image.
Step6: Display cover image and secret image.

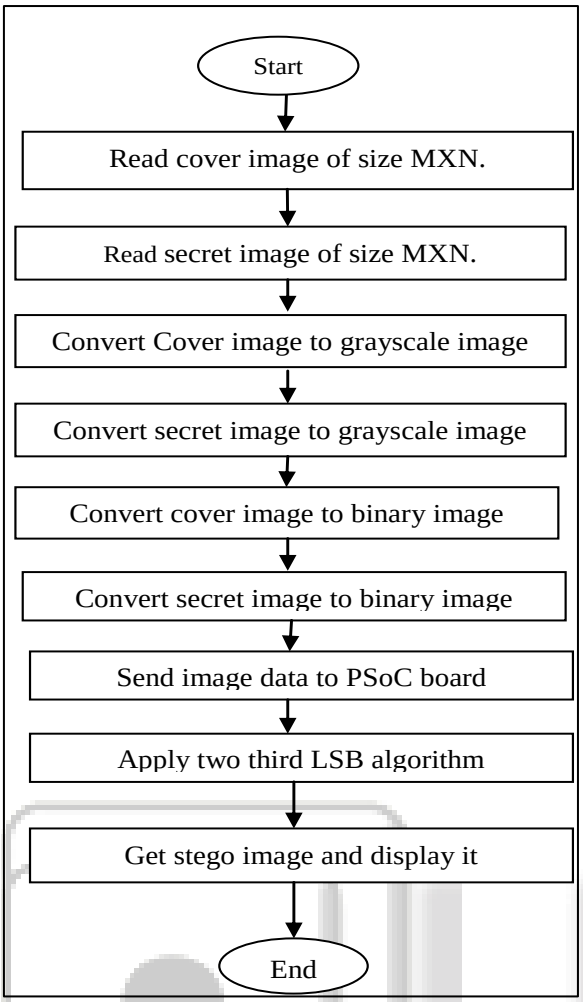

Fig. 2: Image encryption flow

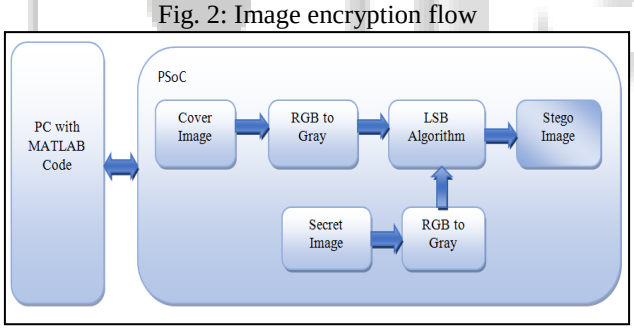

Fig. 3: Block Diagram of the proposed system

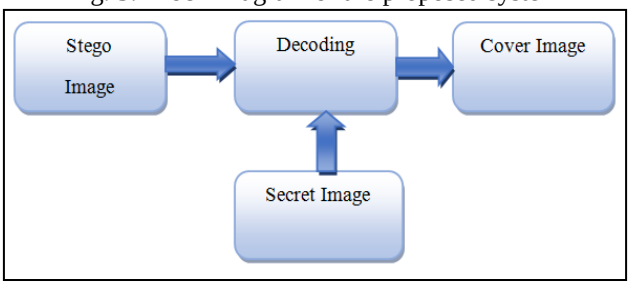

Fig. 4: Block diagram of the Image Decryption

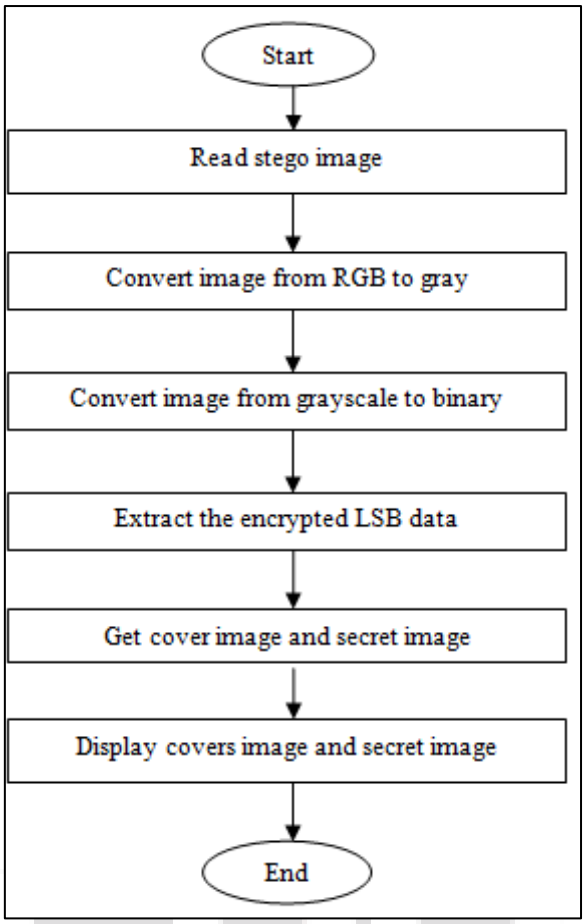

Fig. 5: Flow of Image Decryption

2) LSB Algorithm

LSB stenography embeds the Bits in the least significant bits of the image pixels. Least significant bit insertion varies according to number of bits in an image. Least significant bit insertion varies according to number of bits in an image [1].

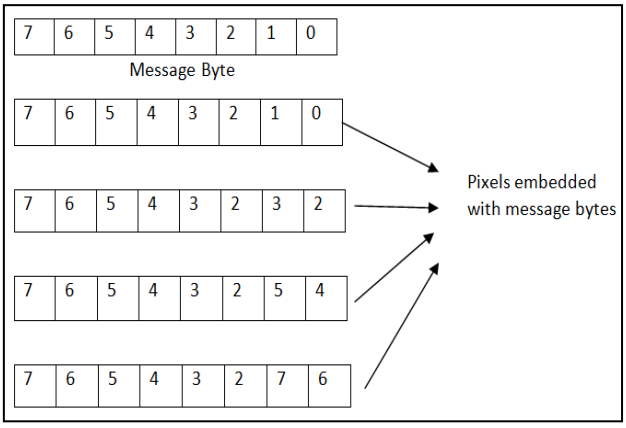

Fig. 6: LSB Algorithm

C. Performance Parameters

1) MSE and PSNR

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics which are used to compare imperceptibility of the stego image [7]. The MSE represents Mean Square Error between the gray levels of the original cover image and stego image, whereas PSNR is a measure of the peak error. If value of MSE is low, then there is less error. To find the PSNR, first calculate mean-squared error using the following equation:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I_{(i,j)} - K_{(i,j)}]^2 \quad \text{.....(1)}$$

Where M and N are the number of rows and columns in the input images, respectively and I(i, j) is the original image, K (i , j) is the Watermarked image. The PSNR is calculated using the following equation:

$$PSNR = \log_{10} \left(\frac{MAX_1^2}{MSE} \right) \quad \text{.....(2)}$$

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255[8].

2) Bit Error Rate

Bit Error Rate is the number of bit errors per unit time. Bit error ratio is the number of error bit divided by the total number of bits transferred during particular time interval [5].

$$BER = \frac{N_{Error}}{N_{Bits}} \quad \text{..... (3)}$$

where N_{Error} is the number of bits received in error and N_{Bits} is the total number of bits received.

III. System Implementation

A. MATLAB

MATLAB is a high-performance language its basic data element is an array that does not require dimensioning. Matrix and vector formulations allows us to solve many technical computing problems. It integrates computation with the programming visualization which gives easy-to-use environment where problems and solutions can be expressed in the mathematical notation. Areas in which MATLAB toolboxes are available include control systems, simulation, signal processing, neural networks, wavelets, fuzzy logic, and many others.

B. Programmable System on Chip

PSoC 4 is used in the proposed system. PSoC integrated circuit consists of a core, configurable analog and digital blocks, programmable routing and interconnect. There is configurable block in PSoC. This differs PSoC from microcontroller. It has three separate memory spaces such flash memory for instructions and fixed data, paged SRAM for data and I/O registers for controlling and accessing configurable blocks. There are various development tools available for the PSoC such as PSoC designer, PSoC Creator etc.

IV. Results and Discussions

Below figures shows the results of the proposed system with original image, Secret image and the steganographed image. Performance parameters are also shown.

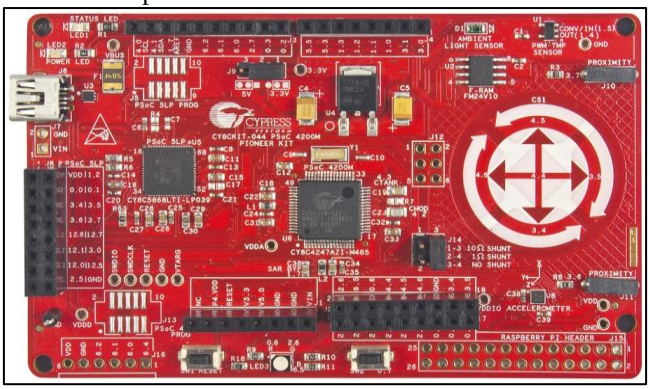

Fig. 7: PSoC Development board

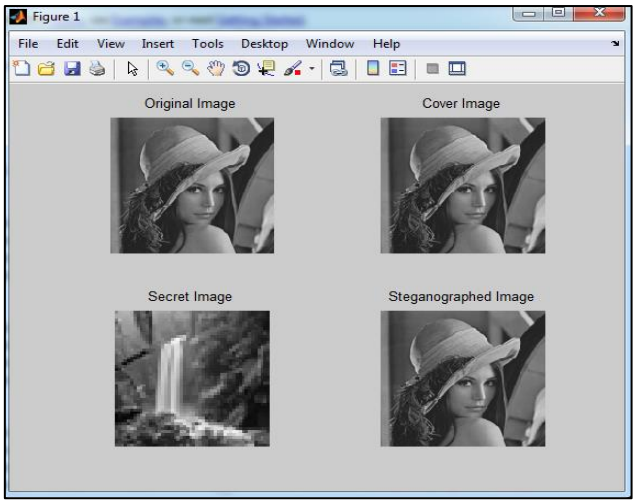

Fig. 8: Results with steganographed image

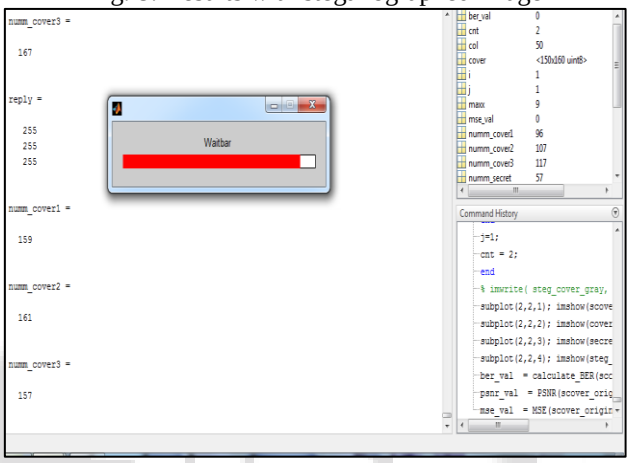

Fig. 9: Results with processing

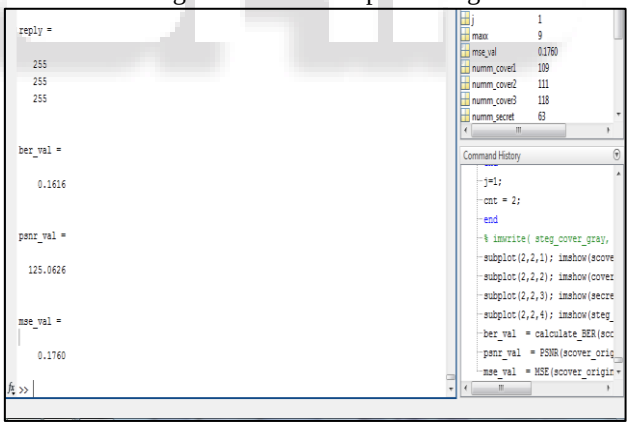

Fig. 10: Results with the performance parameters

V. Conclusion

In this paper PSoC based LSB Steganography algorithm is implemented. It consists of two stages encryption and decryption stage. In the encryption stage we encrypt secret image into cover image. Whole embedding is performed on PSoC development board. Performance of the system is monitored through various parameters such as Bit Error Rate, Peak Signal to Noise Ratio and Mean Square Error. Results shows proposed system gives better security for transferring digital images. The 2/3-LSB has good image metrics compared with 2-bit and 3-bit LSB the 2/3-LSB presentation is in among 2-bit and 3-bit LSB

REFERENCES

[1] Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, "Least Significant Bit Algorithm for Image Steganography", International Journal of Advanced Computer Technology (IJACT), volume 3, number 4.
[2] Anil Khurana, B. Mohit Mehta "Comparison of LSB and MSB based Image Steganography", IJCST Vol. 3, Iss ue 3, July - Sept 2012.
[3] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh ,"Steganography in Images Using LSB Technique", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1 January 2015.
[4] Mr . Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar,"Image steganography using least significant bit with cryptography", Journal of Global Research in Computer Science Volume 3, No. 3, March 2012.
[5] Fariba Ghorbany Beram,"Effective Parameters of Image Steganography Techniques", International Journal of Computer Applications Technology and Research Volume 3– Issue 6, 361 - 363, 2014.
[6] G. Viji and J. Balamurugan, "LSB Steganography in Color and Grayscale Images without using the Transformation", Bonfring International Journal of Advances in Image Processing, Vol. 1, Special Issue, December 2011.
[7] Vijaypal Dhaka, Ramesh C. Poonia ,Yash Veer Singh, "A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.
[8] Naitik P Kamdar, 2Dipesh G. Kamdar 3Dharmesh N.khandhar. ,"Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE", Journal of information, knowledge and research in electronics and communication engineering, issn: 0975 – 6779| nov 12 to oct 13 | volume – 02, issue – 02.
[9] Neha Singla , Raj bhupinder Kaur ,"A Modified Data Hiding Approach for Audio and Video Data", International Journal of Advanced Research in Computer Science, Volume 7, No. 6(Special Issue), November 2016.
[10] Rejani. R , Dr. D. Murugan , Deepu.V.Krishnan ,"Comparative Study of Spatial Domain Image Steganography Techniques", Int. J. Advanced Networking and Applications Volume: 07 Issue: 02 Pages: 2650-2657.

