Image Steganography using 1 Bit LSB Method

Ms.Anuradha S.Pandit[1] Mrs.S.R.Khope[2]
[1]Student [2]Faculty
[1,2]G.H.Raisoni Institute of Engineering and Technology Wagholi-Pune, India

Abstract— This paper presents image steganography method using 1 bit LSB steganography technique. The proposed image steganography secret message is embedded in a cover image so that it is not detected easily. This method also yields improved SNR. There are different types of steganography like image, video or audio. This depends on type of media used for hiding secret message. In proposed method image is used for hiding secret message hence it is image steganography.

Key words: LSB Steganography, Stego Image, Cover Image, FPGA

I. INTRODUCTION

Steganography is the art of concealing information. Main aim of steganography is to secure the information. Steganography word is derived from Greek where "stego" means covered and "Graphia" means writing [6]. So steganography means covered writing. Cryptography is also one method to secure information. But cryptography keeps content of message secret while steganography keeps whole message secret.

Steganography is having different elements like secret message, stego image, and cover image. Secret message is the information which is to be hidden. Cover image is used to hide the secret information. When secret message is embedded in cover image then image we get is called stego image.

There are different types of steganography like text steganography, video steganography and audio steganography. These are classified according to media used to hide the secret message.

- Text steganography: In this method text is used to hide the secret message.
- Image steganography: If image is used as a media to hide the secret message then it is called image steganography.
- Audio steganography: If media used is audio to hide the secret message then it is called audio steganography.
- Video steganography: In this method video is used to hide the secret message.

Rest of paper is organized in following different sections. Section II explains related work, section III describes proposed methodology. Section IV shows result and section V concludes the paper.

II. RELATED WORK

Nedeljko Cvejic and Tapio Seppanen have worked on audio steganography and they have increased number of bits that can be imposed keeping SNR value same.

Shamim Ahmed Laskar and Kattamanchi Hemchandran have brought new concept in steganography i.e. they provided key for encryption and decryption. Juned Ahmed Mazumdar and Kattamanchi Hemchandran used Haar wavelet transform and increased security.

Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh, Sahel Alouneh implemented steganography with LSB method and using FPGA hardware so that maximum speed is achieved. Suraj Baddap, Ketan Khomane, Pratik Dehmukh, Prof. Patharwalkal Shilpa used RSA algorithm for their implementation. Soodeh Ahani, Shahrokh Ghaemmaghami and Z. Jane Wang used discreet wavelet transform for steganography. Deepak Singla and Rupali Sayal combined features of both cryptography and steganography and achieved more security.

III. PROPOSED METHODOLOGY

There are different domain techniques under steganography like spatial domain technique, transform domain technique, distortion technique and masking and filtering.

LSB steganography technique comes under spatial domain technique. Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh, Sahel Alouneh explained hardware design of least significant bit (LSB) steganography technique in a cyclone II FPGA. They used 2/3 LSB method. In this proposed methodology, 1 bit LSB steganography is used. This method provides good SNR, low bit rate. Steganography process is as shown below:

A. Encryption Method

In encryption secret message is embedded inside a cover image using LSB encryption and we get stego image.

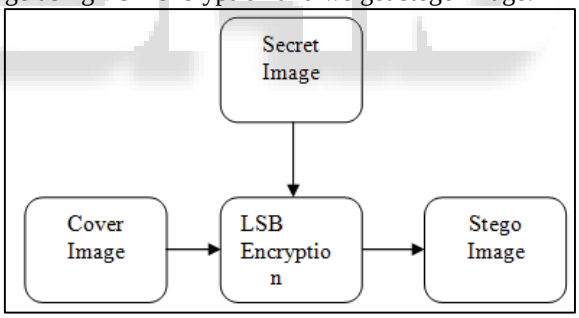

Fig. 1: Encryption of an Image

1) LSB Method

We have proposed LSB based steganography method. Basically in steganography method, secret information is hidden in cover image. And then it is transmitted to the receiver. So that information is secure. In image steganography media used for hiding secret data is image. In our method we are drawing required pixel values of secret image and that are hidden in least significant bit of cover image.

First byte of secret image:

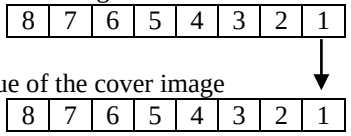

Fig. 2: LSB insertion

Above example shows that in order to embed secret message inside a cover image least significant bit of cover image is changed. In this way we need 8 bits of cover image

to embed the 8 bits of secret image and finally secret message is embedded in cover image.

2) Implementation

For implementing steganography we are using Sparetn III FPGA board. In this system we used MATLAB software for reading images. An aurdinio software is used to dump the code in FPGA.

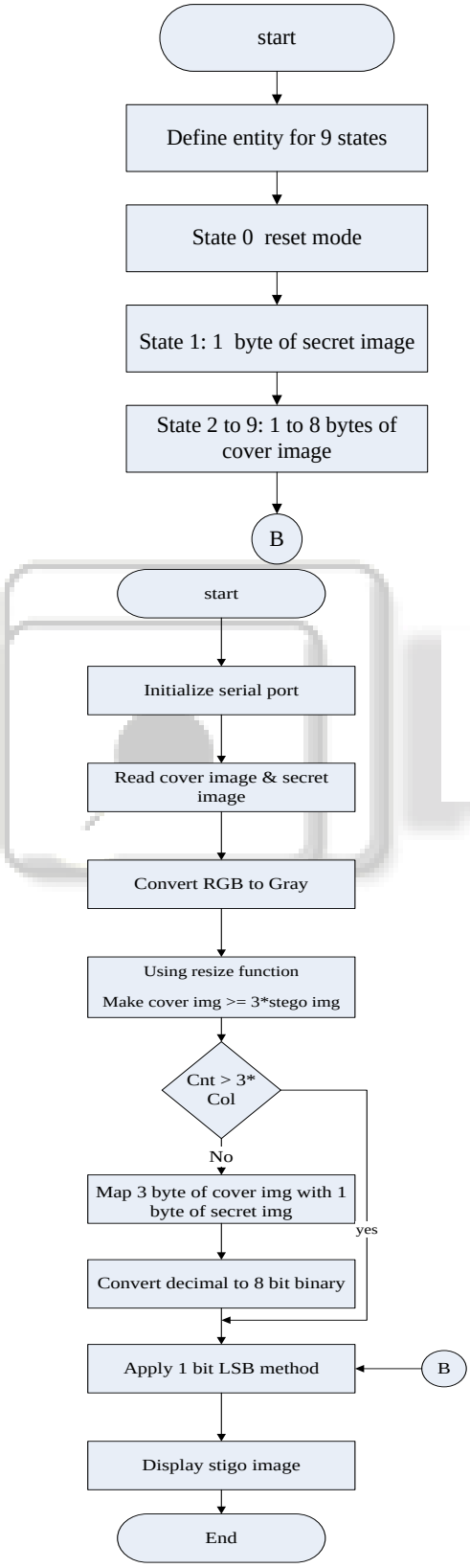

Fig. 3: Flow chart for encoding

IV. RESULT

Following images shows the result of steganography. The secret image is embedded in a cover image and we get the stego image.

Fig. 4: Cover Image

Fig. 5: Secret Image

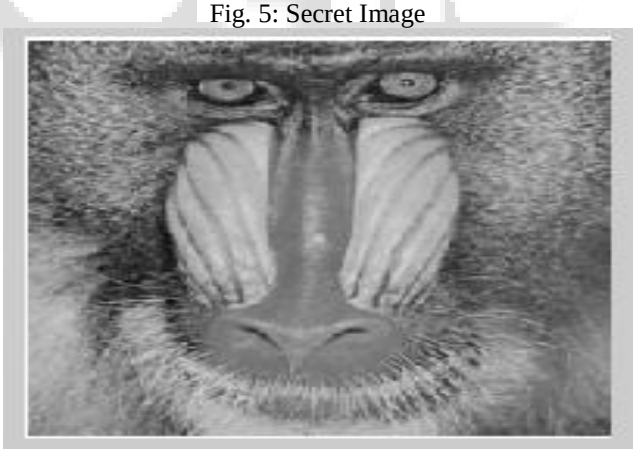

Fig. 6: Stego Image

As only least significant bits are changed, so it does not show any significant change in cover image. Hence the communication is secure. One cannot identify changes.

Parameters	LSB methods			
	3 bits	2 bits	2/3 bits	1 bit
PSNR	37.9	44.1	40.1	145.75
BER	0.19	0.12	0.15	0.0079
MSE	10.5	2.5	5.2	0.0304

Table 1. Comparison Parameters of Different LSB Methods:

V. CONCLUSION

In this paper, we analyzed different techniques of LSB steganography. By analyzing different methods we achieved good SNR and more packing density by 1 bit LSB. Due to use of FPGA i.e. steganography is achieved on hardware, more speed is achieved.

ACKNOWLEDGMENT

Research paper Author is heartily thankful to Guide "Prof. Mrs. Sarika R. Khope", G.H.Raisoni Institute of Engineering and Technology, Pune for guidance, inspiration and her valuable time.

I am also extremely thankful to Principal "Prof. Dr. R.D. Kharadkar" and HOD of Electronics and Telecommunication department "Prof. N. B. Hulle" G.H.Raisoni Institute of Engineering and Technology, Pune. I am also thankful to P.G.Co-ordinator "Prof. Mrs. M. R. Bachute" for valuable guidance.

REFERENCES

[1] Nedeljko Cvejic and Tapio Seppamen, "Increasing the capacity of LSB-based audio steganography", IEEE 2002.
[2] Shamim Ahmen Lasrkar, Kattamanchi Hemachandran, "Steganography Based on Random Pixel Selection for Efficient Data Hiding", International Journal Of Computer Engineering and Technology, Vol.4, issue.2, March-April 2013.
[3] 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.
[4] Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh,Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method", IEEE
[5] Suraj Baddap, Ketan Khomane, Pratik Dehmukh, Prof. Patharwalkal Shilpa, " Hardware Implementation Of LSB Steganography For Data Security", International Journal Of Innovative Research In Advanced Engineering, Vol.2, issue.3, March 2015.
[6] Soodeh Ahani, Shahrokh Ghaemmaghami, and Z. Jane Wang, "A Sparse Representation-Based Wavelet Domain Speech Steganography Method", IEEE/ACM transactions on audio, speech and language processing, Vol.23, No-1, Janury 2015.
[7] 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.
[8] Deepak Singla and Rupali Syal, " Data Security using LSB and DCT steganography in images", International journal of computational Engineering Research, Vol. 2, issue.2, March- April2013.
[9] Linjie Guo, Jiangqun Ni, Wenkang su, Chengpei Tang and Yun-Qing Shi, "Using Stastical Image Model for JPEG Steganography : Uniform Embedding Revisited", IEEE Transaction on Information Forensics and Security, Vol.10, No12, December2015.
[10] Vahid Sedighi, Remi Cograme, Jessica Fridrich, "Content- Adaptive Steganography by Minimizing Statical Delectability", IEEE Transaction on Information Forensics and Security, Vol.11, No.2, feburary 2016.

