High Secured Image by LSB Steganography Technique using Matlab

Ms. Jayashri Gokul Gurav
M.Tech VLSI Design,
Dept of E&TC, SSSIST, Sehore
Email ID:jayu.gurav@gmail.com

Prof. MukeshTiwari
Dept of E&TC, SSSIST, Sehore
Email
ID:mukeshtiwari_79@yahoo.co.in

Prof. Jayakaran Singh
Dept of E&TC, SSSIST, Sehore
Email ID: ec.sssist@gmail.com

***Abstract*:** Steganography is the one type of powerful technique which is science & art in which we have to write hidden messages, or we hide some important images, audio files, videos in this way that no-one, can find a hidden message which exists in cover images. Steganography is most strong techniques to mask the existence of unseen secret data within a cover object. Actually Stego means "Cover" graphy means "writing" that means It is nothing but we are hiding secret objects in cover image in which medium is different types of images. In practical feasible implementation practical approach would be to make the algorithm as strong as possible.

In steganographed images are the most powerful objects that means cover objects, and therefore importance of image steganographed which can Embedding secret information inside images requires systematic computations, and therefore, at the time of designing steganography in hardware which getting high speeds in steganography. Various metrics were used to judge imperceptibility of steganography. The metrics in Matlab indicates how similar or dissimilar the stego-image compares with Cover.

This paper intended to demonstrate LSB steganography, a commanding method for data and image security, its implementation on FPGA and calculate its parameters like SNR, BER for its to analyze its hiding capacity, And also Comparing these parameters of FPGA implementation with that of MATLAB implementation. In this thesis we will demonstrate LSB steganography, which is a powerful method for data and image security.

.

***Keywords*:** - Least Significant Bits(LSB), Steganography, Simulation, MATLAB etc.

*****

I. Introduction:

A steganography method consists of three elements: cover element which hides the secret message, secret element and the stego element which is the cover object with message embedded inside it. There have been different techniques for hiding data in terms of messages either these are in images in such a manner that the alterations made to the image are perceptually indiscernible.

However, the question arises whether they result in images that are statistically indistinguishable from unhampered images has not been easily explored. In this paper we studied & describes LSB Steganography and under what condition can an observer distinguish between Stego images (Images with a secret message) and Cover-images (Images without any secret message).Given the proliferation of digital images on the internet, and the large redundant bits present in the digital representation of an image, images are the most popular & powerful medium as well as cover objects for steganography. A digital image is which is described by using 2-D matrix of the color intestines at each pixel.

Generally, gray images uses 8 bits, whereas colored utilizes 24 bits for describing the color model, which is RGB model. Therefore the steganography system which uses a medium an image as the cover object is referred for image steganography system. Steganography has its place in the protection. On its own, it won't serve much but when used as a layer of cryptography; it would lead to a greater defense.

There are a number of methods to hide some information inside cover-image. There are several techniques in which spatial domain techniques which manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Therefore spatial domain techniques are easy and simple to implement.

The Least Significant Bit is one of the most important techniques in spatial domain image steganography. There is again one type of technique that is transform domain techniques which embed the message in the frequency domain of the cover image. Typically, spatial domain techniques are easily detectable and have larger capacity. On the other hand, frequency-based steganography having higher (PSNR).Main work of this project work, intended to demonstrate LSB steganography, is a powerful technique for data and image security, its implementation on FPGA and calculate its parameters like SNR, BER for its to analyze its hiding capacity, And also Comparing these parameters of FPGA implementation with that of MATLAB implementation.

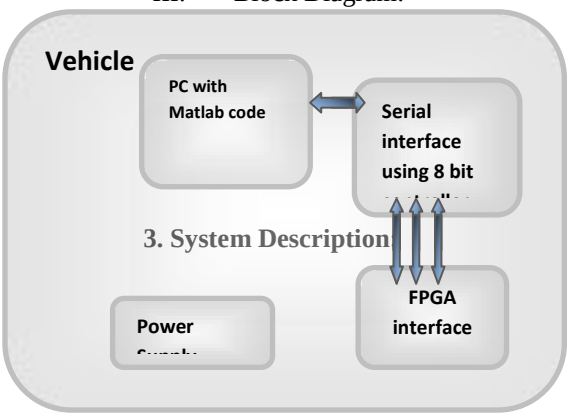
II. Literature survey:

Now a day, application of digital images on the internet increasing rapidly, and this causes redundancy in images,

images are the most powerful cover objects for steganography. A digital image is described by a 2-D matrix of the color intestines at each pixel.Typically, A color model is described by 8 bits for gray images while 24 bits for color images, such as RGB, CMY model. The system which uses an image as the cover object is referred as an image steganography system. There are various methodologies to implant information behind cover-image. The spatial domain techniques operate the cover-image pixel bit values to hide the secret information. The secret bits are engraved directly to the cover image pixel bytes. Therefore, the spatial domain techniques are too simple easy then other domain. The Least Significant Bit (LSB) is one of the techniques in spatial domain image steganography.

Normally spatial domain methods are straight forwardly detectable and have superior capacity. On the other hand, frequency-based steganography has higher peak signal-to-noise ratio (PSNR).

III. Block Diagram:



3.1 Encryption method:

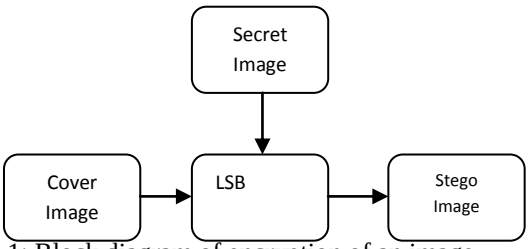


Fig 3.1: Block diagram of encryption of an image

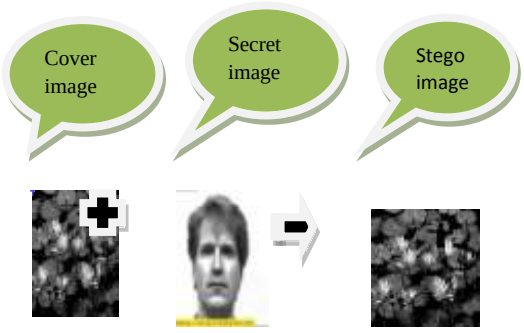


Fig: 3.2: Encryption Process

3.2 Decryption method:

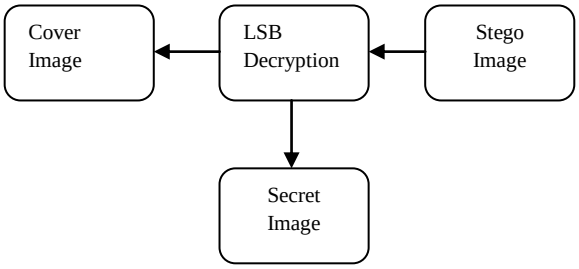


Fig 3.3: Block diagram of decryption of an image.

3.2 Block Diagram Explanation:

Block diagram of steganography is shown in above Fig. Digital images, audio files, video files, text files, executable files and even voice can be used as carrier. How much data can be hidden in the carrier depends on the size of the carrier and the steganography method used to hide the message. 3.2.1

3.2.1 Cover Image

In our project we are using carrier signal as an image ,in which we are hiding an secret data (or image). We are using .bmp format cover image. As a BMP is capable of hiding quite a large message or data. The cover image which we used is of size 300×200.

Fig.3.4: Cover Image (300×200)

3.2.2 Secret Image

The secret image is information which is hide inside an cover image which is also in image format .In our project we are using secret data as an image which is in .jpg format.And secret data is of size 876×634.

Fig.3.5: Secret Image(876×634)

3.2.3 LSB Method

The lowest significant bit in the byte value of the image pixel is called as LSB. The image steganography using this method embeds the secret in the least significant bits of each pixel of the cover image (CVR). To make more understanding of LSB technique, consider the following example. Suppose the CVR has the following three pixel values:

0 1 1 0 0 0 0 1 0 1 1 0 0 0 1 0 0 1 1 0 0 0 1 1

Also assume that secret bytes is : 0 1 0 0 1 1 0 1. After embedding the secret bits, the result pixel values are :

0 1 1 0 0 0 **1 0** 0 1 1 0 0 **1 0 0** 0 1 1 0 0 **1 0 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.

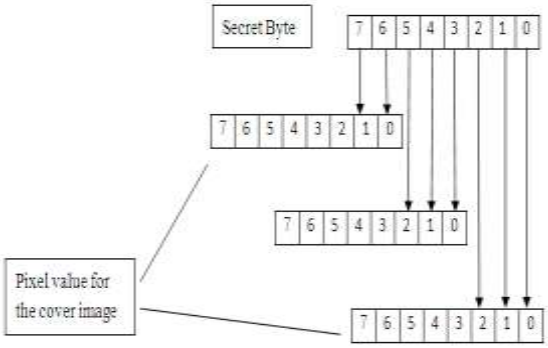


Fig.3.6: Concealing mechanism inside steganography block

The above LSB method has some limitations like, it can hide 8th of the size of the (Cover image) CVR only. LSB steganography technique can be extended to embed secret information in the least n-bits to improve 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 various experiments which run on the test image. In each turns, we embed random data in the n least significant bits, where 1=n=7. However, we need to introduce the techniques to measure the quality and distortion in images.

3.2.4 Stego Image

It is a result image named as stego image. This image is having a same size (i.e 512× 512) as that of cover image, in which we are hiding an secret image.

Fig.3.7: Stego Image(512×512)

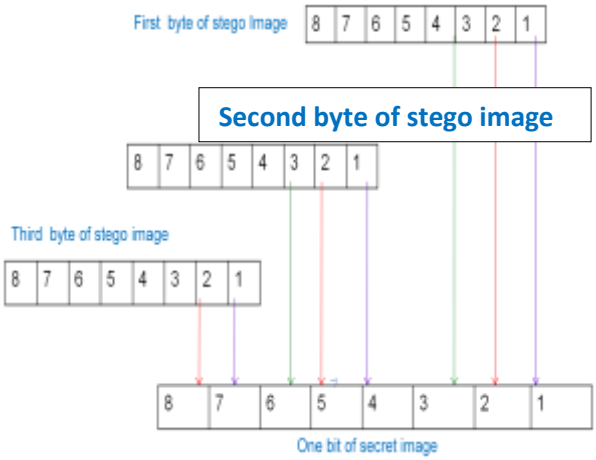


Fig.3.8: Concealing mechanism for retrieve 8 process

IV. RESULTS

Fig.4.1.1 Cover image for encoding

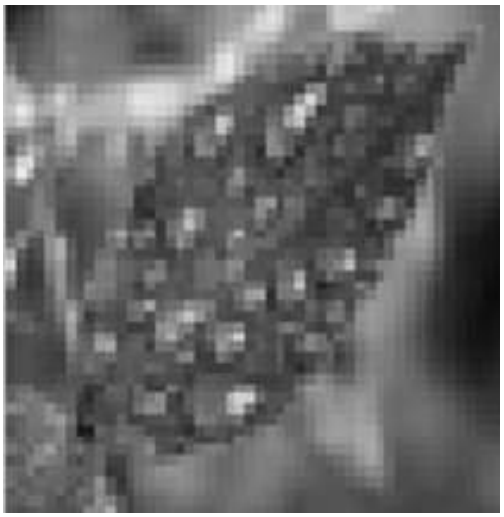


Fig.4.1.2 Secret image for encoding

Fig.4.1.3 Output steganographed image.

Fig.4.1.4 Input of retrieved function (stego image)

Fig.4.1.5 Output retrieved function (secret image)

V. OUTPUT DESCRIPTION:

The proposed work presents a unique technique for Image steganography based on the Least Significant Bits (LSB).From Fig 4.1.1 this is the first input image which we take cover image for encoding as an input image after converting color image to Gray.

Fig 4.1.2 shows secret image for encoding after converting RGB to Gray. This image we are hiding in cover image .Fig 4.1.3. is the Output steganographed image. This is the Encryption. Now we have to retrieved secret image & stego image for that purpose this work needs encryption process with help of Fig.4.1.4 Input of retrieved function (stego image) we get stego image as well as from Fig.4.1.5 Output retrieved function (secret image). Hence the proposed method of Steganography is much efficient to hide the secret data behind an image. Multiple techniques are available to hide the data in steganography. Transformation techniques produce more noise in the image when the information has embedded. To avoid the noise distortion in the image, the LSB insertion method is used to insert the bits in an image by using random number generators.

In this proposed technique before importing the secret information into an image, the secret image has been compressed.

.

VI. 5. Conclusion:

In this paper, we evaluate the performance of different cases of LSB steganography with the help of MATLAB. We then proposed the 2/3-LSB design which provides better quality of image and facilitate simple memory access.

We will be present the results of test image executed on the hardware implementation. Further work must focus on hardware implementation of complex random-based LSB mechanisms, also optimizing the design speed and power. .

.

VII. REFERENCES:

[1] ShouchaoSonga, Jie Zhang, Xin Liao, Jiao Dua, QiaoyanWena, "A Novel Secure Communication Protocol Combining Steganography and Cryptography",Advanced in Control Engineering and Information Science, Procedia Engineering 15 (2011,Published by Elsevier Ltd.doi:10.1016.

[2] Thanikaiselvan V, Arulmozhivarman P, RengarajanAmirtharajan, John BoscoBalaguruRayappan, "Horse Riding & Hiding in Image for Data Guarding", International Conference on Communication Technology and System Design 2011, Published by Elsevier Ltd.doi:10.1016

[3] Mrs. Kavitha, KavitaKadam, AshwiniKoshti, PriyaDunghav, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012, pp. 338-34.

[4] E. Hernández, C. Uribe, R. Cumplido . "FPGA Hardware Architecture of the SteganographicConText Technique", 18th International Conference on Electronics, Communications and Computers, pp. 123-128, Puebla, Mexico, March, 2008.

[5] MamtaJuneja, Parvinder S. Sandhu, and EktaWalia, "Application of LSB Based Steganographic Technique for 8-bit Color Images", World Academy of Science, Engineering and Technology 50 2009.