LSB Steganography Based Reversible Data Hiding

Sajna U.A

***Abstract*---** *This paper introduces a new, principled approach to least significant bit (LSB) steganography in digital signals such as images. It is shown that privacy protection of medical images with information using histogram shifting based reversible data hiding.First of all, the patient's privacies need to be preserved.Therefore, embedding secret data into the medical images would be one of the useful methods for protecting the privacies. After data embedding, the output image should be as similar as its original counterpart, and medical doctors may lead to proper treatment by using the images with hidden data. Later on, both the original image and the hidden data can be perfectly recovered with the algorithm corresponding to the embedding scheme.Finally improving the efficiency and speedof calculation by using FPGA pipelined architecture*

***Keywords*---** *Image Steganography, Information Hiding, LSB Technique.*

I. INTRODUCTION

STEGANOGRAPHY is a way of hiding secret messages into innocent looking cover documents, such as digital images.In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages – digital documents, images, video, and audio files. As long as an electronic document contains irrelevant or redundant information, it can be used as a "cover" to hide secret messages.

Steganography is used in just about every walk of life, from the small business to the largest corporations, from the local organization to the huge Government agency. Steganography does provide an extremely strong, safe, and affordable method of data security.

As technology growsneed for encryption increases to protect the rightful ownership of the artist. Steganography is not only limited to images, it can also be used in other forms of digital media such as audio compact discs, DVD's and video. The focus of this project is only on digital images.

II. EXISTING SYSTEMS

A. Image Stenography

Steganography provides a much higher degree of security than anything else. One big area in which security is a concern is on the Internet. With the Internet holding close to an estimated 28 billion images and 2 billion web sites, it is easy to leave embedded messages in a vast number of images as a security precaution. These embedded messages can be used in various different means and methods.

Steganography means to hide secret information into innocent data Digital images are ideal for hiding secret information. An image containing a secret message is called a Stego image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the stego images so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible. "Steganography is the art of hiding information in ways that prevent the detection of hidden messages", Steganography comes from Greek and means "covered writing."

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover- image, a so-called stego-image does not contain any easily detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once this message detection can be reliably achieved, the steganographic tool becomes useless. Obviously, the less information is embedded into the cover-image, the smaller the probability of introducing detectable artifacts by the embedding process.

Another important factor is the choice of the cover-image. The selection is at the discretion of the person who sends the message. The sender should avoid using cover-images that would be easy to analyze for presence of secret messages. For example, one should not use computer art, charts, images with large areas of uniform color, images with only a few colors, and images with a unique semantic content, such as fonts. Although computer-generated fractal images may seem as good covers 6 because of their complexity and irregularity, they are generated by strict deterministic rules that may be easily violated by message embedding.

The medical field is another industry that uses image Steganography. These embedded images hold and store patient information. Rather than having a patient's information in a thick folder of paperwork, the information is embedded into the patient' x-ray image.

Image Steganography not only helps regular civilians but it can also be used for bad intentions. For example, terror groups

Sajna U.A, M.Tech, VLSI design, Department of ECE-PG, MET'S School of Engineering Mala, Kerala, India. E-mail: sajna.u.a@gmail.com

ISBN 978-93-83459-32-2 © 2014 Bonfring

use it to communicate about their criminal intentions without fear of outside intrusion, such as a government agency.

For data streams there are several techniques used. The simplest method of Steganography is the "LSB Algorithm". The principle of this method is embedding a secret message into a data. The procedure for such technique is to convert the desired hidden message into binary form and then embedded each digit into a least significant bit of the data image.

Most Significant Bit (MSB) embedding is a technique much similar of the Least Significant Bit Steganography. Same principle is used for exchanging the most significant bit of the taken image and exchanging it with the digits of the converted to binary form message.

After researching possible approaches to solve this problem we've decided to use Least Significant Bit Embedding for image Steganography. LSB embedding consists of taking the least significant bit (the 0^{th} position bit) of each pixel and changes it to each bit in the encoded message in binary form.

B. Comparison

1. *Cryptography VsSteganography:* Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden. Information to be hidden + cover object = stego object. To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A stego object is one, which looks exactly same as cover object with an hidden information.

2. *Steganography VsWatermarking:* Watermarking is another branch of steganography it is mainly used to restrict the piracy in digital media. In steganography the data to be hidden is not all related to the cover object; here our main intention is secret communication. In watermarking the data to be hidden is related to the cover object it is extended data or attribute of the cover object, here our main intention is to stop piracy of digital data. Steganography is a very powerful tool because, as the stated above, it can be very difficult to detect.

C. Stegosystem

The Stegosystem is conceptually similar to the cryptosystem.

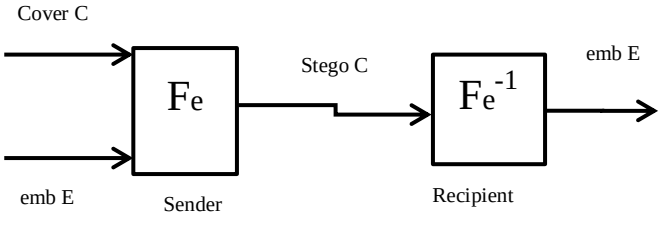

Fig.1.Stego System

Emb: The message to be embedded. It is anything that can be represented as a bit stream (an image or text).

Cover: Data/Medium in which emb will be embedded.

Stego : Modified version of the cover that contains the embedded message.

Fe: Steganographic function that has cover, emb& key as parameters.

Here is a graphical version of the stegosystem

Cover Image

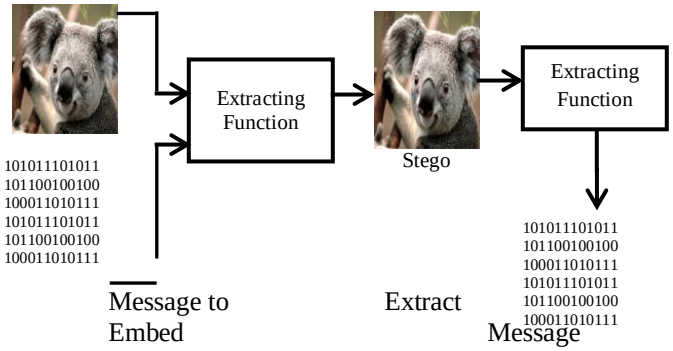

Fig.2. Graphical Representation

This paper introduces a method of secret message encoding that makes use of wavelets. Wavelets break down the stream into high and low frequency component parts called details and trends. As part of the research, an application called Silent Words was developed in Java that makes use of the integer-based wavelet transformation, lifting and a Least Significant Bits (LSB) approach to hide messages in cover images. The lifting technique allows for variation in levels of transformation, selecting region of interest on cover image to be manipulated, type of wavelet transformation to be applied, and how far apart in the image each piece of the message is to be encoded. This method of encoding can be discovered if a bitwise comparison of the cover image is done with the steganographic image, which is the image that contains the secret message. Such a comparison may reveal manipulation but not the message. One way to thwart this discovery is to prevent access to the original image.

D. Block Diagrams

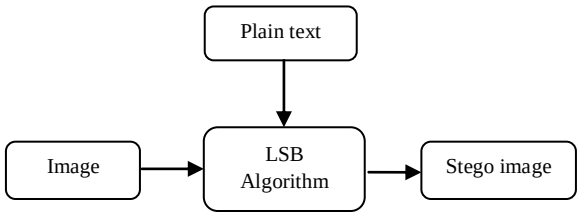

Fig.3. Embedding data

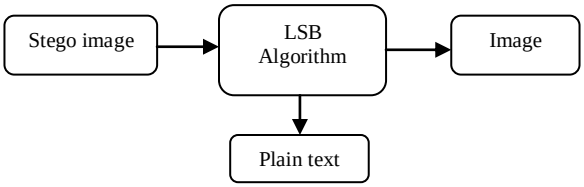

Fig.4. Reverse Data Hiding

E. Block Diagrams Description

Message encoding on a image can be divided in to two parts, one portion is Data Hiding other is Reversible Data Hiding. In Data Hiding part there is a digital image in which we encode secret message by removing LSB of image pixel and add our secret message on corresponding LSB position, then the output image is called stego image. For retrieve the secret message program splits the image into its channels and applies the inverse lifting scheme to each channel to the level specified by the user. When the transformation is completed, the program retrieves the message out of the pixels of the cover image.

Different streams of digital media can be used as a cover stream for a secret message. Steganographyis the art of writing secret message so thatonly the sender and the intended recipient are aware of the hidden message. A successful information hiding should result in the extraction of the hide data from the image with high degree of data integrity. Current trends favor using digital image files as the cover file to hide another digital file that contains the secret message or information.

III. Proposed System

A. *Privacy Protection of Medical Data Using Histogram Shifting*

The project presents privacy protection of medical images with information using histogram shifting based reversible data hiding. An Embedding module involves image encoding and histogram shifting based difference expansion. First of all, the patient's privacies need to be preserved. Therefore, embedding secret data into the medical images would be one of the useful methods for protecting the privacies. Next, because external data are hidden into the original image, some alterations are supposed to be induced. After data embedding, the output image should be as similar as its original counterpart, and medical doctors may lead to proper treatment by using the images with hidden data when necessary. Reversible data hiding is a newly developed branch in data hiding or watermarking researches. Reversibility means that data, including patients' private information and the diagnosis data, can be hidden into the medical image by some means developed by ourselves. Later on, the medical image containing data might be retrieved by medical doctors while necessary, and both the original image and the hidden data can be perfectly recovered with the algorithm corresponding to the embedding scheme. Finally the performance of an algorithm will be evaluated by mean square error, peak signal to noise ratio, entropy and correlation coefficient.

B. *Block Diagrams*

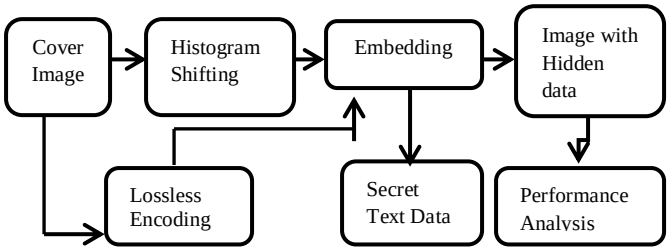

Fig.5. Embedding

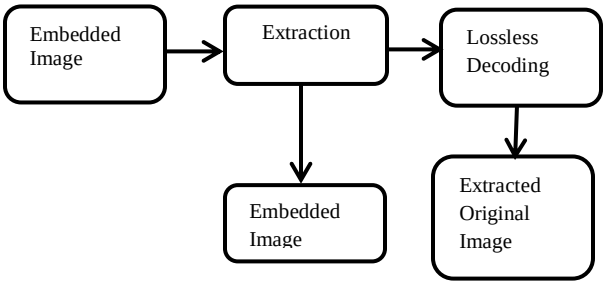

Figure.6. Extraction

C. *Block Diagram Description*

1) *Input Image:* In imaging science, image processing is any form of signal processing is any form of signal processing for which the input is an image, such as a photograph or video frame.

2) *Histogram Shifting:* HS-based algorithm is another important work of RDH, in which the peak of image histogram is utilized to embed data. In this method, each pixel value is modified at most by 1, and thus the visual quality of marked image is guaranteed. IN Lee et al.'s proposed a method by using the histogram of difference image. This method outperforms Ni et al.'s by improving both EC and visual quality. The spatial correlation of natural images is exploited in Lee et al.'s method and thus a more appropriate histogram is obtained. In other words, compared with the ordinary one dimensional histogram, the difference-histogram is better for RDH since it si regular in shape and has a much higher peak point. In, Hong et al. proposed a new HS-based method by modifying the prediction-error histogram. This method can well exploit the image redundancy and thus achieve a more better performance compared with previously introduced DE-based methods such as Recently, Wu and Huang proposed a novel HS- based method where the histogram bins used for expansion embedding are specifically selected such that the embedding distortion is minimized. The experimental results reported in demonstrated that this method is better than some state-of -the-art works including the most recently proposed integer-transform-based method

3) *Encoding Process:* Matrix encoding was proposed by Crandall to enhance the embedding efficiency by decreasing the number of required changed bits. Later,Westfeld implemented the matrix encoding in the famous steganographic scheme. Encoding is generally used in the least significant bits (LSBs) of the coefficients for stenography, e.g., quantized DCT coefficients. High embedding efficiency motivates us to apply matrix encoding to hide secret data into the binary code stream of the VQ indices.

4) *Embedding Process*: The embedding procedure containsseveral steps. Firstafter diving the host image into non –overlapping blocks, then the blocks are further divided into three parts to get I1 I2 and I3. Then, by using shifting and embedding functions, embed the hidden data into ai1 and I3. Next, by using LSB replacement, embed the location map which records the underflow/overflow locations into I1 should be recorded into a LSB sequence. Finally, embed the LSB sequence into I2 using shifting and embedding functions. Herethe partition of three parts is to solve the underflow/ overflow problem by embedding the location map into the host

ISBN 978-93-83459-32-2 © 2014 Bonfring

image. The part I1 is double embedding to embed first the hidden data (using shifting and embedding functions) and then the location map (using LSB replacement).

5) *Extraction Process:* The data extraction procedure also contains several steps. First, the same as the data embedding divide the marked image blocks into three parts to get I1, I2 and I3. Then, determine the location map by reading LSB of I1. Next, according tothe location map and by using shifting and embedding functions, determine the LSB sequence by extracting data from I2, and then replace the LSBs of I1 by the extracted LSB sequence. Finally, extract the embedded data from I1 and I3. Notice that, using shifting and embedding functions, the image restoration can be realized simultaneously with the data extraction.

6) *Reversible Data Hiding (RDH);*In this subsection, as a complement of the proposed embedding mechanism, we discuss how to embed auxiliary information and how to embed required amount of data bits. As is known, a RDH algorithm usually depends on some parameters should be communicated to decoder. To this end, we may slightly modify the embedding and extraction procedures.

Firstly, we divide host image into two parts to get 10 and I 10 contains a fixed number of pixels and I is the rest pixels. Secondly, express the parameters in binary from to get a binary sequence and replace the LSBs of 10 by this sequence. Here, the original LSBs of 10 should be recorded and then embeddedinto host image as a part of hidden data. For example, in the modified version of Ni et al.'s method, we may reserve 8 pixels (i.e., - 10 =8) to embed data into it For decoder, it only needs to read LSBs of 10 to get the parameters, and then hidden data from I. In particular, 10 can be restored by over writing its LSB by a certain part of extracted hidden data.

7) Advantages:

- Lossless recovery of original image
- High hiding capacity
- Low distortion

8) *Applications;*

- Data protection in medical field
- Defines and Research Organization

IV. Software Specification

A. Language Used, MATLAB 7.5

1) Software Description: If you are new to MATLAB, you should start by reading Manipulating Matrices. The most important things to learn are how to enter matrices, how to use the: (colon) operator, and how to invoke functions. After you master the basics, you should read the rest of the sections below and run the demos.

At the heart of MALTAB is a new language you must learn before you can fully exploit its power. You can learn the basis of MATLB quickly, and mastery comes shortly after. You will be rewarded with high productivity, high creativity computing power that will change the way you work.

2) *Introduction:*MATLB is a high performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solution are expressed in familiar mathematical notation. Typical uses include :

- Math and computations
- Algorithm development
- Modeling, simulation, and visualization
- Scientific and engineering graphics
- Application development, including graphics user interface building.

MALTAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you want solve many technical computing problems, especially those with matrix and vector formulations, in especially those with matrix and vector formulation, in a fraction of the time it would take to write a program in a scalar non interactive languages such as C or FORTRAN.

The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects. Today, MATLAB uses software developed by the LAPACK and ARPACK projects, which together represent the state-of- the-art in software for matrix computation.

MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high productivity research, development, and analysis.

MATLAB features a family of application-specific solution called toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and apply specialized technology. Toolboxes are comprehensive collections of MATLABenvironment to solve particular classes of problems. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

3)GUI: A graphical user interface (GUI) is a user interface built with graphical objects, such as buttons, text fields, sliders, and menus. In general, these objects already have meanings to most computer users. For example when you move a slider, a value changes; when you press an OK button, your settings are applied and the dialog box is dismissed. Of course, to leverage this built- in familiarity; you must be consistent in how you use the various GUI building components.

Applications that provide GUIs are generally easier to learn and use since the person using the application does not need to know what commands are available or how they work. The action that results from a particular user action can be made clear by the design of the interface.

The sections that follow describe how to create GUIs with MATLAB. This includes laying out the components, programming them to do specific things in response to user actions, and saving and launching the GUI; in other words, the mechanics of creating GUIs. This documentation does not attempt to cover the "art" of good user interface design, which is an entire field unto itself. Topics covered in this section include:

ISBN 978-93-83459-32-2 © 2014 Bonfring

MATLB implements GUIs as figure windows containing various styles of uicotrol objects. You must program each object to perform the intended action when activated by the user of the GUI. All of these tasks are simplified by GUIDE, MATLABs graphical user interface development environment.

The process of implementing a GUI involves two basic tasks;

- Laying out the GUI components
- Programming the GUI components

GUIDE primarily is a set of layout tools. However, GUIDE also generates an M-file that contains code to handle the initializationand launching your GUI. This M-fileprovides a frame work for the implementation of the callbacks the functions that execute when users activate components in the GUI.

While it is possible to write an M-file that contains all the commands to lay out a GUI, it is easier to use GUIDE to lay out the components interactively and to generate two file that save and launch the GUI:

A FIG-file – contains a complete description of the GUI figure.

M-file- contains functions that launch and control the GUI and theCallbacks, which are defined as sub functions. This M-file is referred to as the application M-file in this documentation.

B. Simulation Result

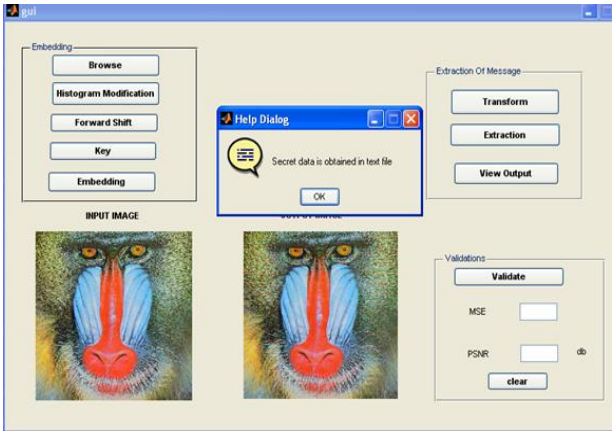

Fig.7.Matlab Simulation Snap

V. FPGA HARDWARE Description

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 objects for steganography, and thus the importance of image steganography. Embedding secret information inside images requires intensive computations, and therefore, designing steganography in hardware speeds up steganography. This work presents a hardware design of Least Significant Bit (LSB) steganography technique in a SPARTAN3 FPGA. The design utilizes the embedded processor as well as specialized logic to perform the steganography steps. Here the core processor Microblaze is design, implement using XILINX ISE 10.1 AND XILI8NX PLATFORM STUDIO. Design suite the algorithm is write in system C Language and test in SPARTAN-3 FPGA kit by interfacing a test circuit with the PC using the RS232 cable.

ADVANTAGES

- This flexibility allows the user to balance the required performance of the target application against the logic area cost.
- The user can tailor the processor with or without advance features, based on the budget of hardware
- it's a pipelined architecture , so can increase speed and reduce processing time

VI. CONCLUSION

In this a data hiding method by LSB substitution process is proposed. Simulation result shows the effectiveness of the proposed method. A good balance between the security and the image quality is achieved. In the proposed algorithm, number of steps less. Thus, the computational complexity is reduced. Algorithm is usage for both 8 bit and 24 bit image of cover and secret image, so it is easy to be implementing in both gray scale and color image. Benefited from the effective optimization, a good balance between the security and the image quality is achieved. Hardware section focus on improving the efficiency and speed of calculation by using pipelined architecture.

VII. ACKNOWLEDGEMENT

The author thanks the Management and the Principal of METS School of Engineering Mala, Thrissur, Kerala for providing excellent computing facilities and encouragement And I would like to thank MsRajy Xavier, MsRintu, Assistant Professors, Department Of ECE, MET'S School Of Engineering for their contributions to this work.

REFERENCES

[1] Neil F.Johnson,SushilJajodia,George Mason University,"Exploring steganography: seeing the unseen", IEEE Computers, February 1998,Pp.26-34.

[2] T.Morkel, J.Eloff And M.Olivier," An overview of image steganography", The Fifth Annual Information security South Africa Conference(Issa2005), Sandton, SouthAfrica, July 2005.

[3] M.U.Celik, G.Sharma, A.M.Tekalp, And E.Saber," Lossless generalized-LSB data embedding", IEEETrans. Image Process,Vol.14,No.2,Pp.253-266,Feb 2005.

[4] L.Kamstra And H.J.A.M.Heijmans," Reversible data embedding into images using wavelet teqniques and sorting", IEEE Trans. Image Process, Vol.14,No.12,Pp.2082-2090,Dec.2005.

[5] Z. Ni, Y.Q.Shi, N.Ansari, And W.Su," Reversibledata hiding", IEEETrans. CircuitsSyst.Video Technol, Vol.16,No.3,Pp.354-362,Mar.2006.

[6] R.Caldelli, F.Filippini, And R. Becarelli," Reversible watermarking techniques: An overview and a classification", Eur. Assoc Signal Process, J.Inf.Security,Vol.2010,No.2,pp.1-19,2010.

[7] Shamimahmedlaskar and kattamanchihemachandran," secure data transmission using steganography and encryption Technique" (ijcis),vol.2, no.3, september 2012

AUTHOR BIOGRAPHY

Sajna.u.a received the bachelor of Engineering degree in Applied Electronics and Instrumentation from KMCT college of Engineering, Mukkam, Calicut, Kerala, India in 2012. Currently pursuing Master of Engineering degree from the department of VLSI Design, at MET'S School of Engineering, Mala, Thrissur, Kerala, India.

ISBN 978-93-83459-32-2 © 2014 Bonfring