SECURING MEDICAL DIAGNOSIS REPORT USING IMAGE STEGANOGRAPHY

Ankita Patel [1],Rahul Joshi [2]

[1]M.E. 4th (SEM) I.T., PIET, Wagodiya,Vadodara, Gujarat, India ankita19291@gmail.com
[2]Professor, I.T., PIET, Wagodiya,Vadodara, Gujarat, India,rah1985@gmail.com

Abstract: The amounts of digital medical images have increased rapidly today so fast and secure transmission of medical diagnosis has become prime importance. Efficient transmission of images over the internet is required. So, this paper is on medical diagnosis image steganography methods which are used for enhancing security of medical data for further diagnosis and reference. For securing the medical diagnosis report as an image using modified LSB data hiding method is used. In receiver direction when the stego image is received then the inverse methods in reverse order is applied to get the original medical diagnosis report as an image. Then, receiver sent the expert opinion as any file format using the modified LSB data hiding method. In sender side when image is arriving apply the reverse order to get the expert opinion as any file format.

Keywords: LSB, Image Steganography, Medical Image

I. INTRODUCTION

Steganography, coming from the Greek words segos, meaning roof or covered and graphic which means writing. It is the art and science of hiding the fact that communication is taking place. With literally millions of images moving on the internet each year it is safe to say that digital image Steganography is of real concern to many in the IT security field. Digital images could be used for a number of different types of security threats.

The use of digital images for Steganography makes use of the weaknesses in the human visual system, which has a low sensitivity in random pattern changes and luminance. The human eye is incapable of discerning small changes in color or patterns and because of this weakness text or graphic files can be inserted into the carrier image without being detected. Each graphic image is made up of what is called pixel elements (pixels). Each elements color is determined by the numerical value that it is assigned, ranging from 0 to 255. For example, a typical elements value could be seen as 00000000 or 00000001. The typical digital image is made up of either 8 bit (256 color) or 24 bit (true color) pixels. In a 24 bit graphic file each pixel would be represented by 3 bytes, each being 8 bits long. [15] A white pixel would look like this:

Red byte	Green byte	Blue byte
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1

An 8-bit colour image could hold around 300 kilobits of hidden data and a 24-bit colour image around 2 megabytes.[15]Other factors will also influence the type of image that would be used as the carrier file. Items such as compression type and colour variance will need to be considered. The more gray scale that the hidden image has the

Now a day, the necessity of rapid and secure diagnosis is important in the medical world. There are many digital medical images have increased hurriedly in the internet. In the medical field it is common to processing and handling medical information by computer and sharing them over the internet. Protection of the integrity and confidentiality of medical images and diagnosis reports are an issue in the management of patients' medical records. Confidentiality states that unauthorized parties should not be granted to access medical images during transmission. Integrity implies that images should not be modified in any way during transmission.

II. LEAST SIGNIFICANT BIT TECHNIQUE

A common, simple and easy approach to embedding information in a cover image infusion is Least Significant Bit (LSB). Image was converted from JPEG to GIF or BMP format, which reconstructs original message exactly (lossless compression), which does not lossy compression and then back destroy the information hidden in the LSB. [3]

A common, simple and easy approach to embedding information in a cover image infusion is Least Significant Bit (LSB). The Least Significant Bit is changed to a bit of secret massage of some or all of bites inside an icon. It means one can store 3 bits in each pixel. An 800 x 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

For example a grid for 3 pixels of a 24-bit image can be as follow:
(11101110 11011101 11010100)
(01101110 00010100 10101100)
(00010110 01101100 11101011)

Here the number 180, which binary representation is 10110100, is fixed into the Least Significant Bits (LSB) of this part of icon, the result grid as follows:
(11101111 11011100 11010101)
(01101011 00010100 10101101)
(00010110 01101100 11101011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an icon will need to be modified to hide a secret message using the maximum cover size. [8]

III. PROPOSED METHODS

3.1 Data Embedding Process

The data embedding process happens two times in proposed approach, once it happens when a medical diagnosis report, as an image, is sent to the receiver. And another is when an expert opinion, as a text file, is sent to the first person.

(1) In the data embedding process, two images are available. One of them is the color image which is a cover image. The cover image is divided into three matrices R (RED), G (GREEN) and B (BLUE). Get LSB of the R, G and B and create 1D array for these R, G and B LSB bits. Another one is hidden image. Now Convert hidden image into the binary form and create 1D array.

Inputs: Hidden image, a cover image (size m × n)
Outputs: Embedded image which carried hidden information (size m × n)

(2) In the data embedding process, two different files are available. One of them is the color image which is a cover image. The cover image is divided into three matrices R (RED), G (GREEN) and B (BLUE). Get LSB of the R, G and B and create 1D array for these R, G and B LSB bits. Another one is expert opinion which is in text file form. Now Convert text file into the binary form and create 1D array.

Inputs: A text file, a cover image (size m × n)
Outputs: Embedded image which carried a text file (size m × n)

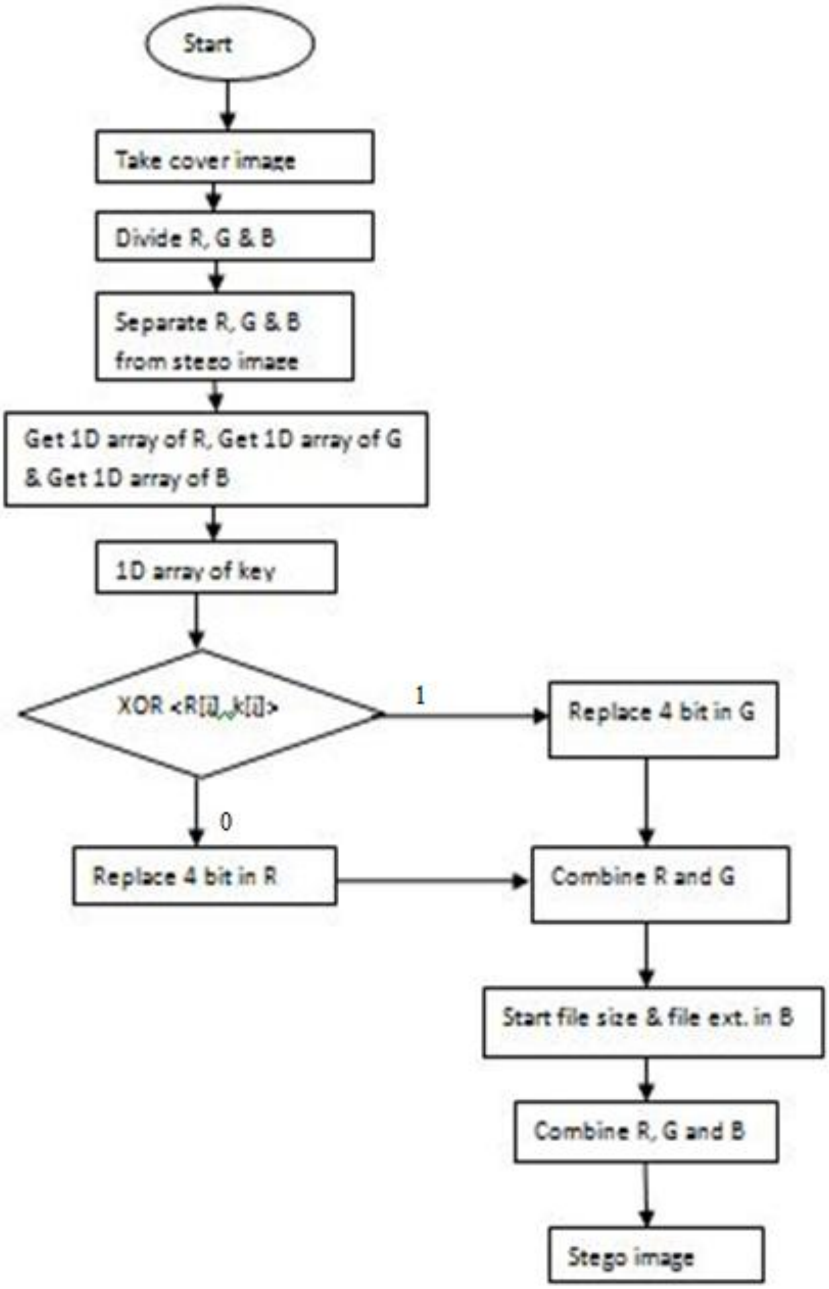


Figure 3.1 Flow Chart for Proposed Embedding method

3.2 Data Extraction Process

Data extraction process is depended on data embedding process. So, the data extraction process also happens two times in proposed approach. Once it happens when a medical diagnosis report, as an image, is received by the receiver. And another is when an expert opinion, as a text file, is received by the first person.

In data extraction process, read stego image and divide R, G and B from it. Then get LSB from R, G and B. now, reconstruct the hidden information which is in the form of hidden image or text file, from LSB of R, G and B. then read the hidden image or text file. And finally reconstruct the original hidden image or text file.

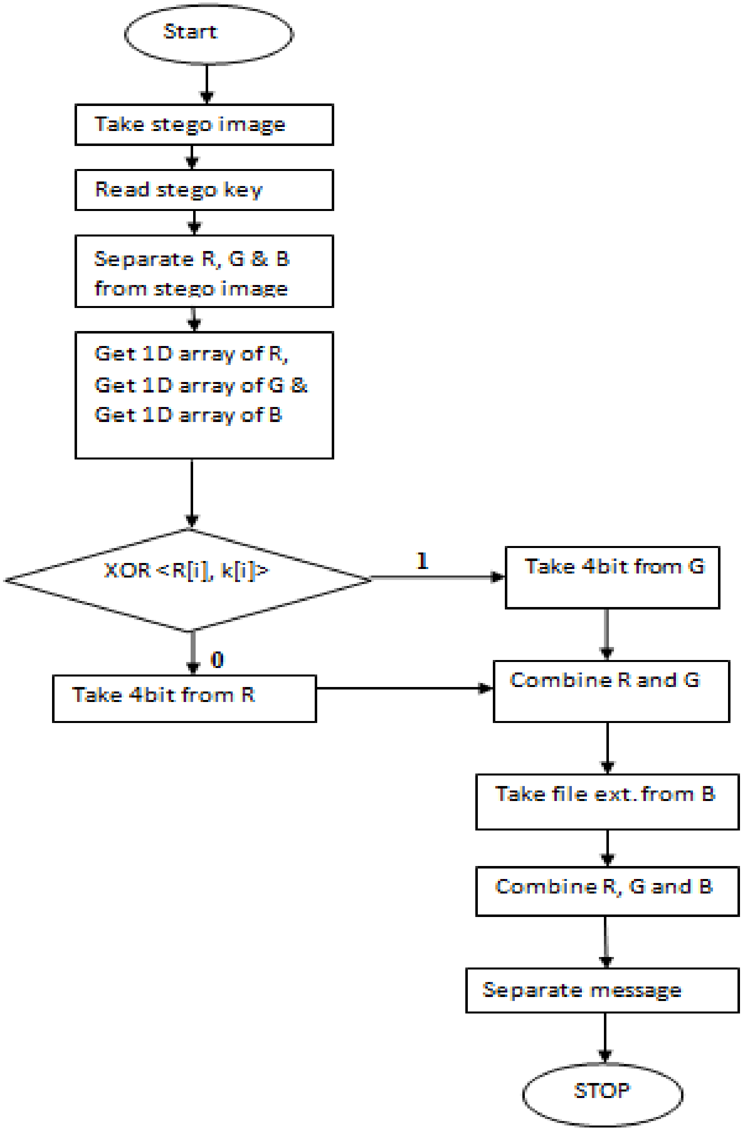
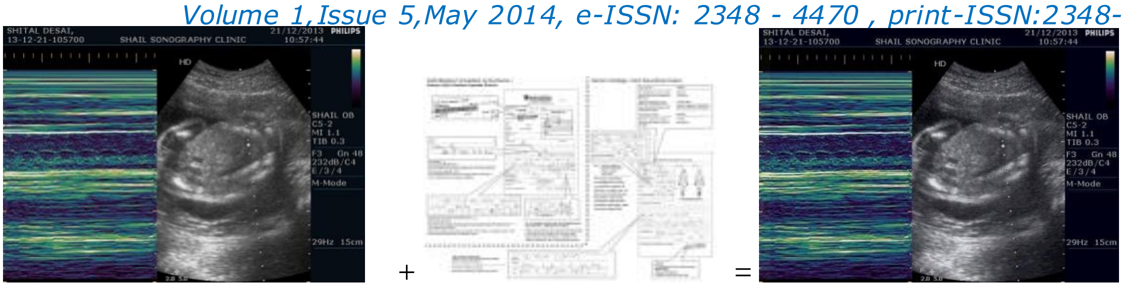


Figure 3.2 Flow Chart for Proposed Extraction Method

IV. RESULTS AND ANALYSIS

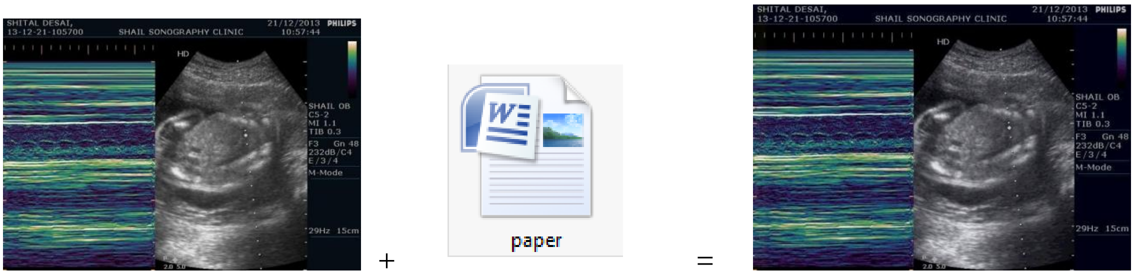
Experimental results are given in this section to demonstrate the performance of our proposed method. Medical images with different types of hidden files can be applied in my proposed system such as .doc file, .ppt file, .jpg file, .pdf file.
Figure 5.3 shows the cover image (.jpg), hidden file image (.jpg) and then resulting image which is stego image (.jpg).



. Cover image: jpg file hidden file:Jpg File Stego Image: Jpg file

Figure 5.3 Cover Image, Hidden Image and Stego Image of .jpg File

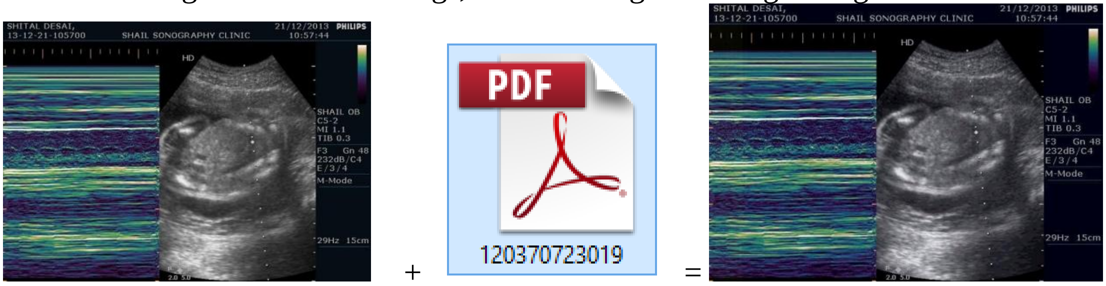
Figure 5.4 shows the cover image (.jpg), hidden file image (.doc) and then resulting image which is stego image (.jpg).



Cover image: jpg file hidden file:Doc file stego image: Jpg file

Figure 5.5 shows the cover image (.jpg), hidden file image (.pdf) and then resulting image which is stego image (.jpg).

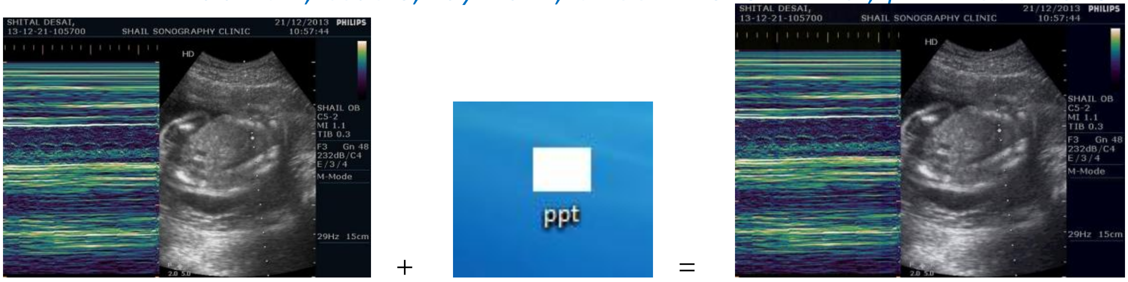
Figure 5.4 Cover Image, Hidden Image and Stego Image of .doc File



Cover image: Jpg file hidden file: Pdf file stego image: Jpg file

Figure 5.5 Cover Image, Hidden Image and Stego Image of .pdf File

Figure 5.6 shows the cover image (.jpg), hidden file image (.ppt) and then resulting image which is stego image (.jpg).



Cover image: jpg file   hidden file: ppt file   stego image: jpg file

Figure 5.6 Cover Image, Hidden Image and Stego Image of .ppt File

Medical images with different types of hidden files can be applied in my proposed system such as .doc file, .ppt file, .jpg file, .pdf file.

Parameters have been performed to test the proposed system. The system is simulated in Matlab 8.1.0.604.

Table 5.1: Results of proposed system

Size of cover image	Size of hidden image	MSE	PSNR (dB)	Time (second)
60KB (752 X 530)	4KB (143 X 100) (.jpg file)	1.40014e	85.9367	31.320193
60KB	16KB (.doc file)	2.09273e	86.7929	27.525694
60KB	40KB (.pdf file)	2.0294e	86.9263	25.299380
60KB	29KB (.ppt file)	2.05658e	86.8685	30.025536

V. CONCLUSION

Security of medical diagnosis report as an image and information has become a primary concern for covert communication across several fields in today's world. Thus information security is obligatory and worthy. Data hiding provides an innovative way to hide the secret data into any digital cover. In my dissertation work several data hiding techniques are discussed based on research papers studied. From which it is found that each tactic has its own pros and pitfalls. In the base method used a secret key to hide hidden information into cover image. This process provides a new dimension for image steganography. My proposed approach provides better PSNR value where larger PSNR indicates better quality of the image or in other terms lower distortion in embedded process. And it also reduces time consumption.

REFERENCES

[1] Vinay Pandey, Manish Shrivastava, "Secure Medical Image Transmission using Combined Approach" International Journal of Advanced Research in Computer Science and Software Engineering, Dec-2012

[2] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key" IEEE,DEC-2011

[3] Agniswar Dutta, Sankar Das, Asoke Nath, Abhirup Kumar Sen, Shalabh Agarwal, "New Data Hiding Algorithm in MATLAB using Encrypted secret message"IEEE-2011

[4] Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, "A CHALLENGE IN HIDING ENCRYPTED MESSAGE IN LSB AND LSB+1 BIT POSITIONS IN VARIOUS Cover Files", Journal of Global Research in Computer Science, April-2011

[5] Dr. V. Vijayalakshmi, Dr. G. Zayaraz, and V. Nagaraj, "A Modulo Based LSB Steganography Method" INTERNATIONAL CONFERENCE ,june-2009

[6] Rig Das and Themrichon Tuithung, "A Novel Steganography Method for Image Based on Huffman Encoding", IEEE, 2012

[7] Jagvinder Kaur and Sanjeev Kumar, "Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011

[8] Johnson, N.F and Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 2008.

[9] Vinay pandey , Angad Singh, Manish Shrivastava," Medical Image Protection by Using Cryptography Data-Hiding and Steganography" International Journal of Emerging Technology and Advanced Engineering

[10] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science

[11] Bret Dunbar "Steganographic Techniques and their use in an Open-Systems Environment" SANS Institute,2002

[12] T. morkel , J.h.p. eloff , M.s. olivier "An overview of image Steganography" information and computer security architecture (icsa) research group

[13] Krenn, R., "steganography and steganalysis" , http://www.krenn.nl/univ/city/steg/article.pdf

[14] Fixmar, Robert, "Terrorists and steganography", Zdnet News, 09/23/2001, http://zdnet.com.com/2100-1107-530751.html

[15] Mendall, Ronald, "Steganography-Electronic Spycraft", Earthweb Networking and Communications, 09/20/2000 http://www.earthweb.com/article/0,,10456_624101,00.html

[16] MATLAB, from Wikipedia, the free encyclopaedia http://en.wikipedia.org/wiki/MATLAB

[17] MATLAB GUI - Math Works http://www.mathworks.in/discovery/matlab-gui.html

[18] T. morkel , J.h.p. eloff , M.s. olivier "An overview of image Steganography" information and computer security architec Piyush Goel, C.E, "Data Hiding in Digital Images: A Steganographic Paradigm", Indian Institute of Technology–Kharagpur, MAY-2008