International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5S, May 2019

Image Steganography Technique based on Canny Edge Detection and Hamming Code for Medical Data

Sheelavathy, Hamsavani.R, Disha J, Bhavana C, Bhoomika Rathod

Abstract: ***Image steganography has major role in enhancing the confidentiality of sensitive information related to business information, research data, and health record data and so on. Here the sensitive data considered is Medical data. When the medical image is transmitted through in secure public network, there are chances for medical images to be tampered. To avoid intruders in viewing the sensitive data i.e. Medical information the need of hiding it becomes the foremost criteria. This project mainly aims at enhancing medical integrity. To achieve medical integrity, it is required to hide the medical information within a cover image which is the medical image here. The proposed system aims at providing high security of data integrity by using cryptography along with steganography. The method of digital steganography is involved in the transfer of high imperceptible method that enhances the hiding of Electronic patients record (EPR) into medical images without major modification in the data transfer. It is predominantly required to protect and enhance the security methods ensures that the eavesdroppers will not have any suspicion that medical image or sensitive medical data is hidden in that image***

Keywords: Digital steganography, Electronic Patients Record (EPR), edge-detection, XOR, Medical Data

I. INTRODUCTION

In today's world there is very much need to protect the medical data from being exploited for various other purpose. Digitization of data has emerged with serious issues, with regards to privacy and security of sensitive data. In order to protect the confidential data Encryption is the foremost step. In this paper, data considered is related to biomedical system, where the security and privacy of digital medical images needs to be increased. The complete integral security of images cannot be achieved by Encryption alone since it is detrimental for not being applied on low bandwidth channel. The fundamental standard for data security is been provided by DICOM which ensures storing, handling, printing and transmitting information of medical images and related information.

Manuscript published on 30 May 2019.
***** Correspondence Author (s)
Sheelavathy, School of C & IT, REVA University, India.
Hamsavani.R, School of C & IT, REVA University, India.
Disha J, School of C & IT, REVA University, India.
Bhavana C, School of C & IT, REVA University, India.
Bhoomika Rathod, School of C & IT, REVA University, India.

It mainly characterizes the format of exchange of medical images and related secret data which is necessary for clinical use, but then it was introduced without considering network security or data protection required to conceal the secret information. Further, a DICOM encoding technique has been the data protection for almost 20 years. The main condition for transfer of suspicious data is the secured transfer and reliability thereby enhancing the security of medical images. There have been numerous applications put forward to enhance protection and confidentiality of medical images and patient records. Most of these applications depend on cryptography where in the contents of the message is protected and treated as a secret message by changing its structure. But this algorithm has its failure, as certain cryptographic algorithms are vulnerable to certain type of attacks, which would enable intruders to gain access to the encrypted information. Steganographic algorithm along with cryptography encapsulates the contents of the data and considers it as secret message by concealing the data under some digital cover. The digital cover used here is an image i.e. cover image. The secret information is transferred in such a manner that it avoids bringing the suspicion to the existence of secret information. One of the prominent methods in hiding the secret data within non-overlapping blocks of 2×2 pixels is Tri-way Pixel Value Differencing (TPVD) a well-known steganography method. The data hiding is a crucial method where in it depends on quality, imperceptibility and robustness. The embedding process is a kind of trick which is been played, considering the visual limitation of human eye.

The main aim of this paper is to recommend an efficient biomedical image steganography which aims at achieving better capacity and imperceptibility through the method of

1. edge-detection of original medical image,
2. Applying Hamming code algorithm and
3. Optimization function is required to balance the embedding capacity and the bits consumed for detecting the edge locations.

The technique of edge-detection mechanism is achieved by Canny Edge detection algorithm where the reference parameters considered are the Gaussian Filter Variance and threshold value.

The data hiding technique can be applied to colored images using Canny Edge Detection algorithm and LSB matching being applied to one channel of the color image making embedding capacity relatively low and is unable to achieve same edge pattern in all the three channels of color image.

II. EMBEDDING TECHNIQUE

Least Significant Bit Algorithm

1. Initially select an input as cover image of size M*N.
2. The message to be embedded is implanted in RGB segment of a picture into the RONI.
3. The pixel determination channel is implemented to get the best regions to conceal data in the spread picture to acquire a superior rate. The channel is subjected to Least Significant Bit (LSB) algorithm to each pixel in order to conceal data, leaving most critical bits (MSB).
4. After that Message is shrouded utilizing Bit Replacement technique

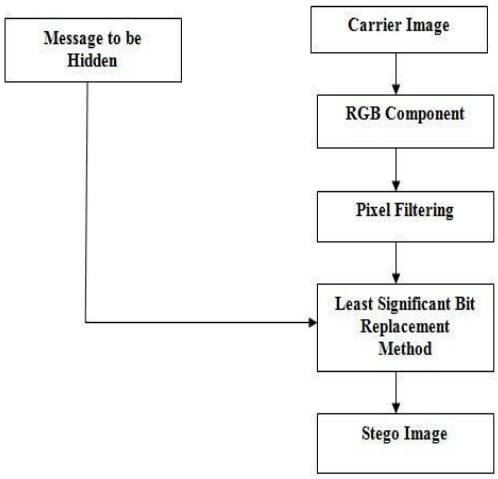

Figure 1. LSB Algorithm

Enhanced Least Significant Bit Algorithm

1. Select a spread picture of size M*N to embed the information.
2. The message to be hidden is embedded within the Blue segment just of a picture.
3. Utilize a pixel choice channel to acquire the best territories to conceal data in the spread picture to get a superior rate. The channel is connected to Enhanced Least Significant Bit (ELSB) of each pixel to conceal data, leaving most huge bits (MSB).
4. After that Message is concealed utilizing Bit Replacement

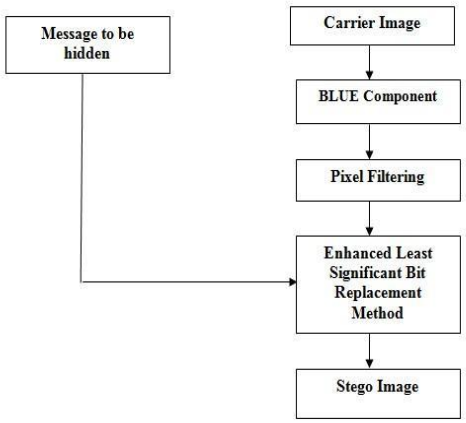

Figure 2. Enhanced LSB Algorithm

Example for modification of three adjacent pixels (9 bytes) along with RGB encoding: -
10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011
When a value of 300 with binary representation 100101100 is embedded into least significant part of the image. On overlaying 9 bits over LSB of 9 bytes we get the encoded output as:
10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010
Here in this example 300 is being embedded into the grid and the number of bits needed to change is 5 bits depending on the embedding message. On an average calculation it is observed that only half number of bits in an image needs to be modified to hide a secret message by utilizing the maximum size of the cover image.

A. Figures and Tables

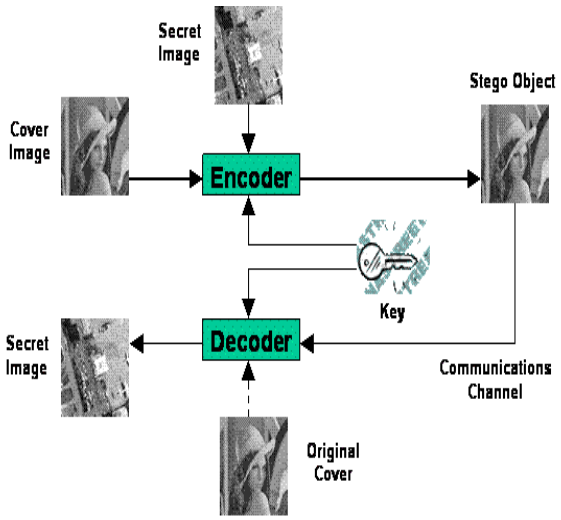

Figure 1. Steganograhy process implemented in our project.

B. *Abbreviations and Acronyms*

EPR – Electronic patient's data

XOR – Hybrid exclusive OR

TPVD – Tri Pixel Value Differencing

DICOM- Digital Imaging and Communications in Medicine

C. Equations

$$PSNR = 10\log_{10}\left[\frac{255^2 \times W \times H}{\sum_{i=1}^{W}\sum_{j=1}^{H}(c_{ij}-s_{ij})^2}\right](dB) \quad (4) \quad (1)$$

A. *W and H are the width and stature of the spread picture separately,*

B. *cij and sij are the dark estimations of pixel (I, j) of the spread and stego pictures separately.*

$$wPSNR = 10\log_{10}\left[\frac{max(C)^2}{\|NVF(S-C)\|^2}\right](dB) \quad (5)$$

(2)

where *NV F* is the Noise Visibility function

III. CONCLUSION

This paper carries the information of various methodologies that can be used to enhance the efficiency of medical image steganography which is precisely based on hiding patient's confidential information. The approach of edge detection using Canny Edge and the Hamming Code algorithm is used as an efficient supplement to cryptography methods. The computation of edge detection is mainly incorporated to identify and embed the secret data into high contrast areas of the image hence, gain less attraction from intruders. The edge region detection is identified based on non-overlapping blocks of the adjacent pixels. The secret message is embedded into the cover image using XOR technique and the threshold value determines the message embedding capacity and is flexible to make any changes. The entire process is based on the concept of visual capacity of humans. The distortion introduced by the embedding of the secret message data is minimized by using a Hamming code, that controls the number of bits to embed in each block based on its edge strength. The embedding procedure does not consider ROI pixels because altering of these pixels reduces the clarity of original image and can also lead to distortion. The exploratory outcomes exhibit that the proposed method offer both high payload and great nature of stego pictures.

IV. ACKNOWLEDGMENT

We extend our gratitude towards REVA University for giving us the opportunity to take up this project. We are thankful to our department lecturers who have guided us through our project. We extend our heartful gratitude toward our guide Prof. Sheelavathy for guiding us by providing all the ideas required for this project. Above all I thank my team mates for working cordially in completing this project.

REFERENCES

1. Shuliang Sun, "Image Steganography based on Hamming Code and Edge Detection", 2018, Research gate publications
2. Kumar Gaurav, Umesh Ghanekar, "Image Steganography algorithm based on Edge-region detection and Hybrid Coding", 2018
3. Hayat Al-Dmour, Ahemd Al-Ani, "Quality Optimized Medical Image Steganography based on Edge-Detection and Hamming Code", International Conference on IEEE, 2015
4. Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.
5. Tayana Morkel, Jan HP Eloff, and Martin S Olivier, "An overview of image steganography." in ISSA, 2005.
6. Bremnavas, B Poorna, and GR Kanagachidambaresan, "Medical image security using lsb and chaotic logistic map," 2011.

AUTHORS PROFILE

I am Hamsavani.R pursuing 4th year B. Tech CSE in REVA University. I am presenting the paper under IJEAT format. I have done a research on Image Processing and an internship in the same. And have knowledge on Artificial Intelligence and done internship related to Chatbot and their working.

I am Bhavana C, pursuing 4th year B. Tech CSE in REVA University. I am presenting the paper under IJEAT format.

I am Bhoomika, pursuing 4th year B. Tech CSE in REVA University. I am presenting the paper under IJEAT format.

I am Disha J, pursuing 4th year B. Tech CSE in REVA University. I am presenting the paper under IJEAT format.