A COMPARATIVE REVIEW IN REGARD TO STEGANOGRAPHY AS IN RELATED MEDICAL IMAGE REST ON THE LSB TECHNIQUE

K.Rama[1], S. Punithavathy[2]*

Abstract

In order to escape detection, secret information can be hid using steganography within otherwise unremarkable, non-secret documents or other media. It uses encryption to protect the sender-receiver channel and the message's medical image. In modern digital steganography there are ways to secure digital images in order to meet security objectives, such as availability, confidentiality, and integrity.For eHealth applications, such as storage, retrieval, identity theft, and data management, medical image security is now a crucial necessity. Steganography has thereby improved the security of medical images, and current technology has led to strange intelligent diagnoses and robot surgery. The LSB key advantages it is that it is simple a substantial message payload, is easy to implement, and reduces the likelihood that the original image quality would degrade. In this paper, we focus on LSB-based steganography for medical images for securing image data in storage andtransmission.

Keywords – Steganography, stegokey, digital image, LSB..

I. INTRODUCTION

Digital image processing provides image processing by the use of algorithm. The biggest challenges in the today’s digital world are safe communication, risks and hazards that need to be considered well [1]. Steganography is a method for concealing secret information in a regular, non-secret file or message to escape identification. [2]. It is a method of hiding secret messages in communications over a public channel and is frequently encrypted before it is encompassed in the front portion of the file, and the concealed text is likely treated to make it harder to detect the confidential information.

Today's digital world uses steganography in many different data forms. The most common kind of data drew on PNG, GIF, MKV, FLV, MP4 were mainly because of its uses in internet and ease to employ the steganographic tools that make use of the data formats. The broad scope of the digital health is that, it includes the concepts from an intersection between technology and healthcare. Medical Image deals with numerous technologies that were employed to observe the human body for the purpose to identify, track, or treat medical issues. Medical image processing includes the use and investigation of 3D datasets of the human body, most frequently from a CT or MRI scanner, to identify pathologies, direct medical interventions like surgical planning, or for research.

Furthermore the medical image is presented steganography to add a further layer of security. Steganography uses encryption to protect the sender-receiver channel and the message's medical image. Eight bits constitute each gray scale image pixel, and the eighth bit is referred to as the Least Significant Bit. One such method is known as "least significant bit steganography," which involves replacing the image's least significant bit with data bits.

The structure of this paper's recall is as follows:2 medical image summation, section 3 information hiding techniques, section 4 review in LSB, section 5 conclusion and summary.

[1]Department of Computer Science
PG and Research. Pioneer College of Department of Arts & Science
[2]Department of Information Technology, Pioneer College of Arts & Science

II. MEDICAL IMAGEOVERVIEW

Although recent advances in communication and information technology make data easily and quickly accessible, the installation of secure connection is still the most importantnecessity.

A number of methods for safety communication have been developed. The primary method is steganography.

A. STEGANOGRPAHY

The words "steganography" and "gaphie," which make up the phrase, are Greek words for "hidden data" and "hidden information," respectively. Since ancient times, this method has been used. Data concealing is mostly used to transmit trustworthy data from sender to recipient without interruption by a third party or any data manipulation. With the advancement of steganography technology, various changes have recently been made.

Information concealing is the aggregate name for the methods used in these applications. A user may be directed to the high resolution version of a picture by metadata that is marked on a printed image, for instance. Metadata typically offers further details about an image. In spite of the factthat data about the data can also be put up in an image's file header, this way has significant downside.

The metadata is typically lost when a file is converted to a different format (for example, from TIFF to JPEG or BMP). Similarly, cropping or any other sort of image alteration loses the metadata. Finally, metadata can only be associated with an image while it is still in digital form; once the image is printed, the metadata is lost.

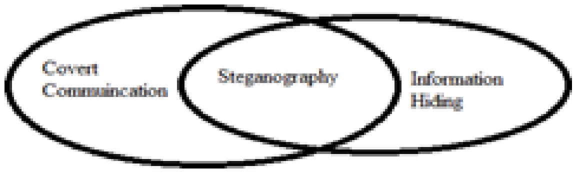

Fig 1. Steganography

B. STEGANOGRPAHYMODEL

As there is no value attached to the process of removing the information hidden in the content, there is no such active opponent in information concealing. Yet, methods for concealing information must be resistant to unexpected distortions.

Suppress message has no knowledge about the secret key that sender uses embedding algorithm and receiver extracting algorithm share, although sender is aware of the algorithm that they could be employing for embedding messages.

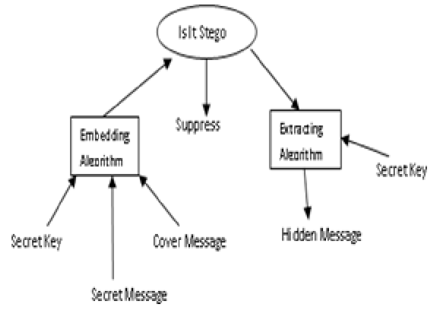

Figure 2. Steganography model

Assuming indeed the theoretically aspect on perfect secret communication (Steganography) entail. send a secret message (M) to create a cover (X) that can be sent unnoticed, then use a stego-key (K) to embed the secret message into the cover (X), converting the cover (X) into a stego-object (S) to demonstrate this concept. The stegoobject (S) should subsequently be able to be sent in the future without being noticed. Because it is aware of the stego-key used to embed the secret message into the cover (X), it will then be able to read the message.

In a perfect system, a normal cover should not be recognizable from a stego-object, neither by a human nor by a machine looking for statistical patterns, as Fabien A.P. Petitcolas points out.

However, this is rarely the case in reality. The cover message must have enough redundant data or noise to allow for the encoding of secret data. This is so that the hidden message can truly take the place of the excess data owing to the embedding technique used in steganography. The forms of information that can be used using steganography are so limited. There are essentially three different steganographic protocols utilized in practice.

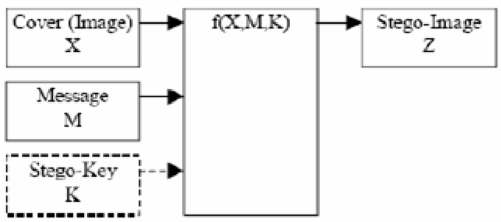

Figure 3. Steganographic Encoding

The usage of medical images, which reflect the human body from the inside using a scan, is quite common in the medical field since it aids in the detection, staging, and treatment of many diseases in the human body's organs. In order to diagnose the sickness a patient is experiencing and choose the best course of therapy based on that diagnosis, it is essential to extract precise and reliable information from medical scans. Medical analysis is done and however, as transactions is done through open communication channels, there is a risk of manipulation and appropriation, and thus the data being transferred needs to besafeguarded.

C. STEGANOGRPAHYSECURITY

Security is needed for both the website where the data will be housed and the transmission link when exchanging medical photographs over the internet. Since web-based and cloud- based medical information systems quickly encroached on the electronic healthcare system, this communication became more and more important in the medical organizations. According to DICOM, a secret data must be implemented as header information in the image file in order to protect the medicalimages

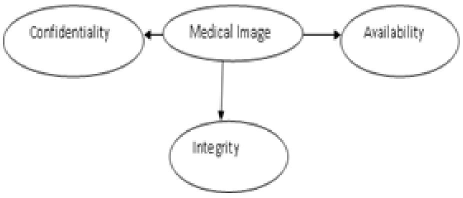

Figure 4. Importance of steganography.

III. INFORMATION HIDINGTECHNIQUES

Image steganography is a sort of steganography that involves hiding data behind an image of another item. The secret to data steganography in images is pixel intensities. Images are frequently used as a cover source in digital steganography behind the computer explanation of an image consists of several bits.

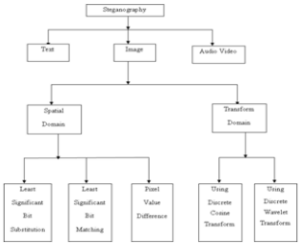
Steganography
Text
Image
Audio Video
Spatial Domain
Transform Domain
Least Significant Bit Substitution
Least Significant Bit Matching
Pixel Value Difference
Using Discrete Cosine Transform
Using Discrete Wavelet Transform

Figure 5. Steganography Technique

I). Spatial domain

When using the spatial domain steganography technique, the information is immediately hidden by changing the image's value of pixels. It suggests that the bits of a secret message are switched out to represent the bits of the pixel values in an image. There are also techniques for classifying data in the spatial domain. Least Significant Bit among those is the most frequently used.

a). Least Significant Bit

The secret message is replaced with the least important elements of an image using this technique For instance, the letter "c",ASCII value is changed to a binary integer in order to be buried within the image. The image binary format's least significant bit is used to store the obtained binary number. A picture is used to store the data. The idea behind this strategy is that if we alter the least significant bits, the image will change slightly but not enough to be noticed by the humaneye.

The key advantages of the least significant bit approach are that itinclude its ease of execution, big message content, and reduces the likelihood that the original image quality would degrade.

b). Pixel ValueDifference

This method uses a gray scale image as the cover image and a lengthy bit-stream as the hidden message. This technique was suggested for concealing sensitive information in 256-gray-Valued photographs. The suggested pixel value differencing method considers the fact that although the eyes of people are capable of recognizing minute changes in gentle parts of an image,they are unable to detect bigger relative changes near the image's edges.

ii) Transformation domain.

This strategy is method to conceal the hidden content in specified sections of picture that serves as an encompass.. By carrying out this procedure, they become more resistant to various image processing processes like cropping, enhancing, and compressing. Several transformation domain approaches exist. The fundamental method for concealing information entails altering the image that serves as the cover, pulling the coefficients, and finally applying the change in form.

a). Discrete Transformation

With the statedtechnique, the photograph is transformed from the spatial to the frequency domain, and depending on its visual quality, it is then divided into sub-bands. To categorize the visual quality of the photographs, high, middle, and low components with frequency will be utilized.

IV. REVIEW IN LSBTECHNIQUE

In this paper Bushra[3], the secret content is used to conceal under a mask bmp image. Initially, the secret message's characters and the cover bmp image's pixels are transformed into binary values. The password must be entered by the user as stego-key which is used to hide secret content in cover file).

The generated stego-picture is delivered to the recipient through the chosen communication channel after the secret message has been included into the cover image file. The user's stego-key is initially obtained while defining the beginning point for embedding LSB. The average of those characters' values is computed after the ASCII value of each stego-key character has been added up, while changing the cover's LSB to reflect the secretmessage.

In the 8-bit-plane, each bit value can be portrayed by 2n- 1, in which n is the plane's order, starting from 1 to 8. [4].

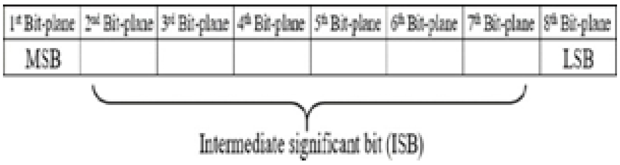

Fig 6 Least Significant Bit

Oluwakemi[2] introduced a novel steganography technique. The approach assumes an improved system over the traditional LSB technique. The main objectives of the work that has been described are to increase the number of documents that can be masked in the convoying image and to increase security through dataencryption.

Our steganography method has the advantage of being able to conceal more data than traditional LSB. The main disadvantage of the process is that the size will increase rather than reduce due to control symbols if the text switches between tiny and capital in each letter, but it can be claimed that such a scenario is uncommon.

In the paper Subhaluxmi[4], author has chosen six patients' X-ray scans and added random text into the photos. Technical elements are actually included in the patient details like patients ID number, patient name a place, an idea, a projection, and rotation Breathing: Airway, pulmonary vasculature, pleural spaces, and lung parenchyma Fig[7]. All of this information can be encrypted and added to the scan's LSB in such a way that it can be recovered and sent over internet with ease. Moreover, Least bit insertion is not harmful to the authenticity or integrity of the scan. [5].

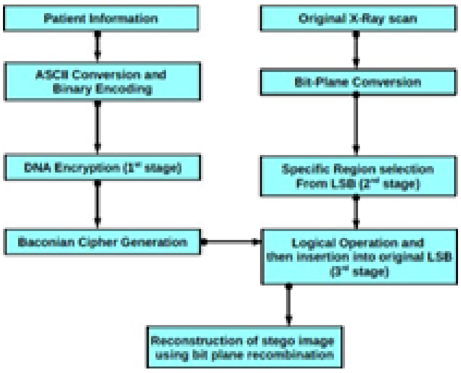
Patient Information
ASCII Conversion and Binary Encoding
DNA Encryption (1st stage)
Baconian Cipher Generation
Original X-Ray scan
Bit-Plane Conversion
Specific Region selection From LSB (2nd stage)
Logical Operation and then insertion into original LSB (3rd stage)
Reconstruction of stego image using bit plane recombination

Fig 7. Encryption

In this research Karawia[6], a new image steganographic algorithm using modified LSB and chaotic map was described. Two piecewise chaotic maps were employed by the author. The first is a chaotic map known as the tent that is used to encrypt private medical images. The second is a piecewise smooth chaotic map in two dimensions that is used to choose host pixel locations at random.

The bits of the cypher pictures are embedded in those pixels. No information from the hidden medical image is lost during this process [7]. According to the experimental findings, the host image's histogram and the stego image's histogram are nearly similar. The comparison between the proposed algorithm and existing algorithms in the literature, based on PSNR and MSE, reveals that the suggested method has the bestresult.

V. CONCLUSION AND SUMMARY

This work provided a background analysis of the LSB used for steganography in digital image. Steganography advises that the medical image be chosen with caution. Also, it is preferable for steganographers to select the right method for protecting digital photos. A high embedding rate is typically difficult to achieve with steganography techniques. The review work on the LSB steganography technology was presented in this study and offers ideas for further research. By minimising distortion, high capacity concealing is regardedas a crucial aspect. Hence, strategies for embedding information without distortions that are effective, high-capacity, and rely on the representational data of 3D models, were evaluated. Despite the fact that the stego model contains a few unnecessary vertices that may not be noticed when the model size is high, these vertices boost the modelsize.

REFERENCES

[1] K. Rama, K. Thilagam, and S. Manjupriya, “Survey and Analysis of 3D Steganography,”, vol. 3, no. 1, pp. 638- 643, Jan2011.

[2] Oluwakemi Christiana Abikoye1 and Roseline Oluwaseun Ogundokun,“Efficiency of LSB steganography on medical information,”, vol. 11 No.5, IJECE, ISSN: 2088-8708, Oct 2021, pp.4157-4164.

[3] Bushra Abdullah Shtayt, “A Comprehensive Review on Medical Image Steganography Based on LSB Technique and Potential Challenges,” Vol: 18, No: 2, Open Access ISSN: 2078-8665,2021.

[4] Subhaluxmi Sahoo, “A new COVID-19 medical image steganography based on dual encrypted data insertion into minimum mean intensity window of LSB of X-ray scans,” (INDICON) |978-1-7281-6916-3.

[5] P. Mohan Kumar and K. L. Shunmugananthan, “A Multilayered architecture for hiding executable files in 3D images”, Indian Journalof Computer Science and Technology, vol.3, No.4.pp-402-407,April2010.

[6] A. A. Karawia, , Medical image steganographic algorithm via modified LSB method and chaotic map, IET Image Processing DOI: 10.1049/ipr2.12246, 14April2021, pp.2580--2590.

[7] Romany F. Mansour, “Steganography-Based Transmission of Medical Images Over Unsecure Network for Telemedicine Applications,” Tech Science Press, DOI:10.32604/cmc.2021.017064.