IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Realization Of Visual Cryptography On Image Steganography For Medical Applications

[1]Chintala Bhavani, [2]Dasari Kishore Babu

[1]Associate Professor, [2]Associate Professor

[1]Electronics and Communications Engineering Department

[2]Mechanical Engineering Department

[1]Srinivasa College of Engineering and Technology, Cheyyuru, India

[1]Aims College of Engineering and Technology, Mummidivaram, India

Abstract: Steganography is a technique of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Medical image steganography requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Many of the exploration systems used for medical diagnosis are based on the medical study images. This paper is mainly focus on Least Significant Bit (LSB) technique where the information is hidden in the LSB of each pixel of the chosen image. This process can be done in 2 ways. At first patient details are converted into QR code using visual cryptographic method than the generated QR code is hide into a cover image. The entire process includes encryption and decryption, where encryption at the sender side and decryption at recipient's end.

Key Terms **– Steganography, Least Significant Bit, QR (Quick Response) Code.**

I. INTRODUCTION

In recent years image steganography has become an important research area in data security, confidentiality and image integrity. The growing use of Internet needs to take attention while we send and receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form.

Digital Steganography has three basic components. (a) Obtain the data to be hidden, i.e., secret message, (b) embed the secret message into the cover medium, i.e., images, sounds or videos, etc., and (c) Obtain the stego-carrier to be sent. In the last decades, many Steganography based data hiding techniques have been proposed.

Visual Cryptography is an image encryption technique used to hide the secure information in images. It allows the encryption of secret image into *n* number of shares and distributed into *n* number of participants. For example in (k, n) secret sharing problem the secret image can be visually recover by stacking together any k or more transparencies of the shares. But cannot reveal any secret information by stacking less thank transparencies together. The Embedded EVCS is constructed by adding random shares of secret image into meaningful covering images.

1.1. Problem Statement:

In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Spies have used it since the time to pass messages undetected The healthcare industry and especially medical imaging systems may benefit from information hiding techniques the use standards such as DICOM (digital imaging and communication in medicine) which separates image data from the caption, such as the name of the picture is lost, thus, embedding the name of the patient in the image could be a useful safety measure.

1.2. Objective:

The main objectives of our project are to product security tool based on steganography techniques to hider message carried by stego-media which should not be sensible to human beings and avoid drawing suspicion to the existence of hidden message in medicinal area.

II. LITERATURE REVIEW

Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography. They demonstrated a visual secret sharing plan, where a picture was separated into n imparts so that just somebody to all n shares could decode the picture, while any n 1 shares uncovered no data about the rst original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. At the point when all n shares were overlaid, the rst picture would show up. There are a few speculations of the fundamental plan including k-out-of-n visual cryptography. Rijimen displayed another 2-out-of-2 VC plot by applying the thought of shading mixture. When two transparencies superimposed on one another with distinctive colours, they lead to raises a third blended shading. In 2002, Nakajima predicted a new method of extended visual cryptography. This method is for regular images which are used to produce meaningful binary shares .This system works by taking three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is recreated by printing the two share pictures onto transparencies and stacking them together. By and large, visual cryptography experiences the deterioration of the image quality. In this also describes the method to improve the quality of the output image. Binary visual cryptography scheme is proposed Houet al. in the year 2004, which is applied to grey level images, that a grey level image is transformed into halftone images.

III. METHODOLOGY

In this proposed system, it is clear that secret message must be in image format. Therefore, a text message converted to a QR code which is in bmp image format. Then the proposed method can be used to conceal QR code image in the same way. The text concealment technique and the retrieval of text message is done in the same way which is shown in the figure1.1.

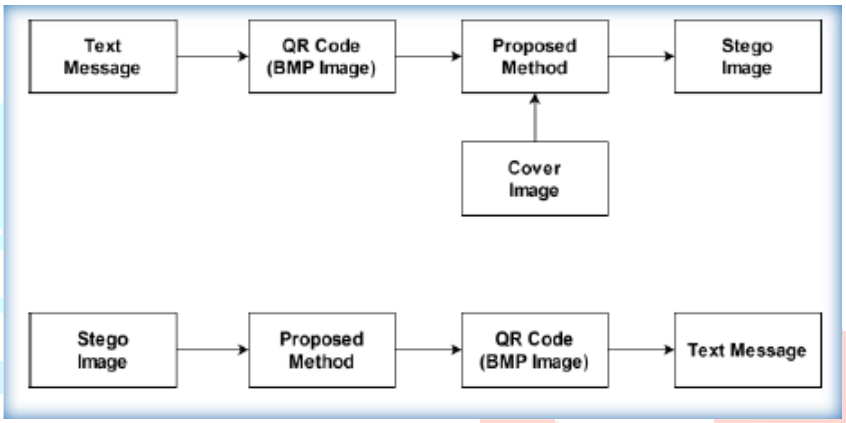

Fig 1.1. Block Diagram

The proposed algorithm employs a key that can be in any length and could contain a mixture of letters, numbers, and symbols. A circular shift function was used to maximize the complexity of the message being covered by moving the coded message bits by several steps at each iteration up to the sum of the password length in an ASCII value. The LSB of the concealment object is replaced in stages up to the appropriate quantity of bits to be substituted. The same method is followed to recover the undisclosed code, but by moving the extracted bits to the left by k steps up to the passwords um in the ASCII value.

IV. WORKING FLOW

The interface is designed keeping the user in mind. There are two buttons on the left panel, with one asking the user to load the file to be encrypted, and the other asking the user to load the image in which the data is to be hidden. Only after the two files are browsed, will the encryption start, or else it'll give an error message asking the user to load both the files. After the user clicks on the encryption button, the status bar at the bottom of the application gives us the state of encryption and after the encryption is complete, we get a message box stating the same. But before encryption is done, it'll ask the user to give the name by which the used would like to save the encrypted image which should also necessarily be filled.

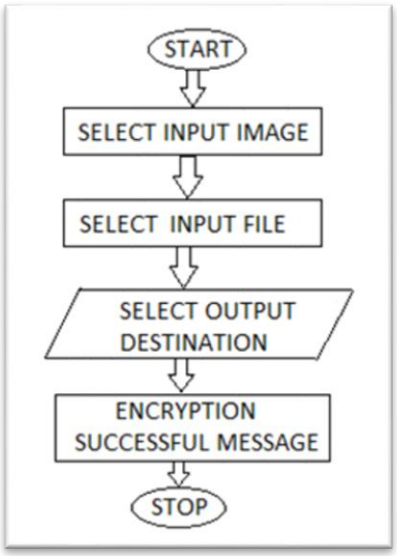

Fig 2 Encryption

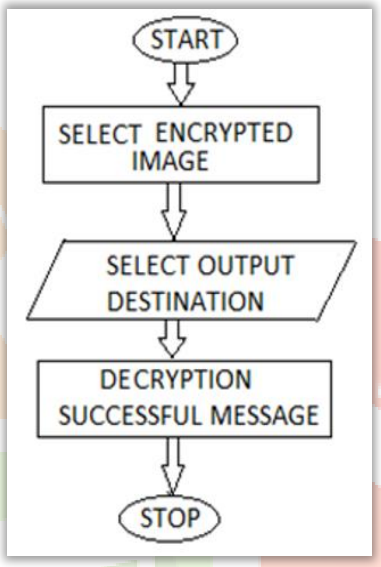

Fig 3 Decryption

V.RESULTS:

The following figures (Fig 4 – Fig 7) shows how the data hide in images. Figure 4 tells that text is converted into QR code and the converted QR code is hide in to a cover image which is shown in figure 5.Figure 6 gives the encrypted message and figure 7 reveals the hidden data.

Fig 4 QR Generator

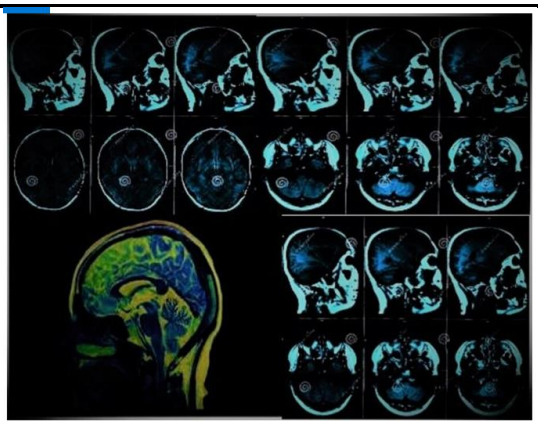

Fig 5 Cover Image

Fig 6 Encrypted message

Fig 7 Decrypted message

VI. CONCLUSION:

The proposed system proved to be a good system used to hide a text in medical digital image by compare value of palette with ASCII of character and if equal we hide position un another Place .In the proposed system transfer the medical image with The Results of Medical Test in high security. The proposed system proved to be easy to use and efficient in terms security and hide every things about the patients. The proposed connect the computer science with medicine by useful a way and help in transfer medical information among the doctors in different country**.**

VII. FUTURE SCOPE:

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

REFERENCES:

1)G. Bhatnagar, Q. M. J. Wu, and Z. Liu, ''Directive contrast based multimodal medical image fusion in NSCT domain,'' IEEE Trans.Multimedia, vol. 15, no. 5, pp. 1014–1024, Aug. 2013.

2)A. Cheddar, J. Condell, K. Curran, and P. M. Levitt, 3, pp. 727–752, 2010.

3] Bere Sachin Sukhadeo, User Aware Image Tag Refinement http://www.ijcsmr.org/eetecme2013/paper19.pdf

[4] Youssef Bassil , A Simulation Model for the Waterfall Software Development Life Cycle, 2011 http://arxiv.org/ftp/arxiv/papers/1205/1205.6904.pdf

[5] ANALYSIS MODEL WATERFALL MODEL

http://www.scribd.com/doc/87322736/Analysis-Model-Waterfall-Model

[6] Data Flow Diagram Symbols
http://www.idi.ntnu.no/~sif8035/pdf/flesn/notation.pdf

[7] Donald S. Le Vie, Jr., Understanding Data Flow Diagrams
http://ratandon.mysite.syr.edu/cis453/notes/DFD_over_Flowcharts.pdf

[8] B. Beizer, Software Testing Techniques. London: International Thompson Computer Press, 1990.

[9] B. Beizer, Black Box Testing. New York: John Wiley & Sons, Inc., 1995.

[10] A. Bertolino, "Chapter 5: Software Testing," in IEEE SWEBOK Trial Version 1.00, May 2001.