Achieving Securityin Medical Scanned Images using Extended Image Steganography

Nitin Arora* , Ahatsham , Kamal Preet Singh

*Assistant Professor(SS), Department of Informatics, School of Computer Science, University of Petroleum and Energy Studies, Bidholi.

**Assistant Professor, Department of Informatics, School of Computer Science, UPES, Dehradun

Received: May 31, 2018 Accepted: July 16, 2018

ABSTRACT *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. It is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. Traditionally this was achieved with visible ink, microfilm or taking the first letter from each word of a message. This security is now achieved by hiding the message within a graphics or sound file. For hiding secret information, there exists a large variety of steganography techniques. This paper proposed a new technology called extendedimage Steganography. It not only changed the meaning of data but also hides the presence of data from the hackers.The growth in medical field has led to the advancement of the paper data to the digital data. As the medical field is moving towards the digital world the security has become a major issue. The patient detail, patient disease, diagnosis etc. are being represented through the digital images. This paper aims to how the data is embedded in the medical scanned images using steganography. The patient information and diagnosis both serves as the secret data. The algorithm keeps the diagnosis and the patient information which helps to make the patient treatment accurate and fast.*

Keywords: *Security, Steganography, Hacking, Sender, Receiver, medical images*

I. INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media [1]. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.Steganography has become more important as more people join the World Wide Web revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages [2]. Steganography include an array of secret communication methods that hide the message from being seen or discovered.Due to advances in Information and Communications Technology, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown [3]. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user.Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

Now a day, all the hospitals are transforming from papers to the digital images, it contains information of patients and helps in treatment. The diagnosis by the doctor is based on these medical digital images. If the medical scanned images are tempered, the doctor diagnose can be reflect and results in poor treatment. In hospitals the treatment of the patients is delayed due to the patient data is scattered to various

departments in the hospitals. So the problem formulates, by which a system is to be made using steganography approaches on a single platform. This process will secure the patient's information and doctors diagnose which results in the right treatment of the patients. With all the information of the patient on one digital image reduces, the treatment time and it fasten the process of the treatment.This paperprimarily concentrated on the data security issues when sending the data over the network using steganography techniques. Secondly, to hide the patient profile and diagnosis in the medical scanned images and also proposed and analyzed the application of combined approach to the steganography in medical field.

II. LITERATURE REVIEW

G.Prashantiet al. [4] provides a review of current accomplishments of LSB centered spatial domain steganography that have an enhanced steganography's vital purposes, which are unnoticeable, forcefulness and bulk of unseen data.This paper also discussed two new steganography techniques.

S.Goel et al.[5] proposed a new technique that use LSB method with changed progression. Experimental outcome shows that proposed technique is fast and vastly efficient as compared to traditional LSB technique.

Della Baby et al. [6]proposed a new technique in which numerous RGB images are embedded into single RGB image using DWT. This system has high embedding capacity and security with minimal changes in stego image

Amitava Nag et al. [7] provides a new steganography technique based on Huffman coding and the least significant bit substitution in order to provide high embedding capacity, a strong security and imperceptible visual quality to secret message. This works on high security and embedding capacity and acceptable level of visual quality of stego image.

E.Dagar et al. [8] presented the steganography technique for color RGB images to improve the security level of data transfer through the internet. 24 bit RGB image is utilized as cover image to embed secret data in red, green and blue pixels. X-Box mapping is used and several boxes contain 16 different values. Here "X" represent any integer number from 0 to 9. After this values saved in X-Boxes are mapped with LSBs of carrier image. It is very difficult for the attacker to extract the secret informationbecause they make use of mapping. Thus this mapping provides high level of security to hidden information. PSNR value is also calculated and it has high PSNR value which leads to greater stego image quality.

M. R. Modi et al. [9] proposed a novel steganography technique to embed secret information of LSBs of cover image. In their method least two significant bits of edges are utilized to store secret message as edge regions are very good areas to embed the secret information than other smooth regions of cover image. In this method edge region are detected on basis of amount of secret information, which means it does adaptive edge detection. Experimental results analysis shows that their method performs better than traditional LSB image steganographicmethods and has greater security against visual attacks.

S. Sachdeva at al. [10] uses the vector quantization table to embed the secret information. They present new method of steganography named as JMQT based on modified Quantization Table. They also compare their proposed approach with JPEG-JSteg steganography method. Embedding capacity and stego image size are used as performance analysis parameters and experimental results are also compared with JPEG-JSteg method. Experimental results show that the hidden capacity andstego size has been increased.

III. METHODOLOGY

Methodology is divided into four major parts namely User login, Encode, Decode and Database Connectivity.

A. User Login

In this, user can login to the system using his Username and Password which would be already allocated. While login it will validate whether the username and password matched or not, if it has been matched then user will be able to use the service otherwise user have to check the username and password is correct or not.

B. Encode

In this, Sender encode the text in an image. Creating an array of integers which will hold the entire message in the form of bit format. A message is made up of characters, each character is of the size of one byte that is 8 bits. Each byte here is divided into 4 parts of 2 bits, and stored in the two Bit Message array. Thus, the size of two Bit Message is 4 times the length of the actual message. While doing this, it encodes 2 bits of message in 1 pixel. Basically, 4 pixels carrying 8 bits of encoded bits. In total carry one character.

C. Decode

In this, Receiver decode the text from an image. Grab a RGB value at specific position and then extract 2 least significant bits (LSB) from encoded data and add the data in a queue for later processing. As soon, it gets 8 bit of data combines it and makes a byte and stores it as a character.

D. Database Connectivity

In this, connecting to Mysql database. It stored Usernames and password in Mysql server. During login, the user enters the given username and password and then database will check whether it has any match in database. If it matched, then has it will access otherwise it won't.

IV. PROPOSED ALGORITHM

Step 1: *Ask User for either Encryption or Decryption.*
Step 2: *If user have to decrypt, go to step 7.*
Step 3: *If user wants to Encryption then go to step 4, Otherwise go to step 10.*
Step 4: *Ask the user for image and text.*
Step 5: *In encryption, message would be divided in 4 parts of 2 bits and store it.*
Step 6: *Image pixels would be add(OR) with the 2 bits of every char in a message. Go to step 10.*
Step 7: *In decoding, select image.*
Step 8: *Image selected, then choose RGB and extract 2 LSB from encoded data.*
Step 9: *Combine them, and create a character.*
Step 10*: End*

V. CONCLUSION AND FUTURE WORK

Successfully created a medical application on steganography, in which doctor can send an encoded image to another doctor, so that another doctor would be able to decode and read the text file. Hence, this application is providing data security to doctors, so that data can't be leaked. Encoded image here are the medical records or reports of a patient. In future more effective techniques can be implemented to secure medical images from the third user.

REFERENCES

1. Pallavi Das, Satish Chandra Kushwaha, Madhuparna Chakraborty, "Data hiding using randomization and multiple encrypted secret images", Communications and Signal Processing (ICCSP) 2015 International Conference on, pp. 0298-0302, 2015.
2. R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, Springer-Verlag Berlin Heidelberg, 2004, pp. 35-49.
3. Bhoomika Modi, Vinitkumar Gupta, Progress in Intelligent Computing Techniques: Theory, Practice, and Applications, vol. 519, pp. 195, 2018.
4. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI*, vol. 2, 2015.
5. Goel, S., Gupta, S., Kaushik, N.: Image steganography – least significant bit with multiple progressions. In: Satapathy, S.C., Biswal, B.N., Udgata, S.K., Mandal, J.K. (eds.) Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing (FICTA) 2014. AISC, vol. 328, pp. 105–112. Springer, Heidelberg, 2015
6. Baby, J. Thomas, G. Augustine, E. George, and N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, vol. 46, 2015.
7. Nag A, Singh JP, Biswas S, Sarkar D, Sarkar PP: A Huffman code based image steganography technique. In: International Conference on Applied Algorithms. Springer International Publishing, pp 257–265, 2014
8. Dagar, Ekta, and Sunny Dagar. "LSB based image steganography using x-box mapping. "Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.
9. R. Modi, S. Islam and P. Gupta, "Edge Based Steganography on Colored Images", 9th International Conference on Intelligent Computing (ICIC), (2013) July 28-31, Nanning, China.
10. Sachdeva, S and Kumar, A., "Colour Image Steganography Based on Modified Quantization Table", Second International Conference on Advanced Computing and Communication Technologies (ACCT), (Rohtak, Haryana, India, 7-8 January 2012), IEEE Conference Publications, 309-313.