International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp. 395-401

Steganography based data transmission for disease prediction through image on Optical Networks

Madhumitha Ramamurthy[1], Rajesh Kumar.G[2], Sreeja B.P[3], P. Sherubha[4], S. P. Sasirekha[5]
[1,2]*Associate Professor, Department of Information Technology, Karpagam College of Engineering, madhuperu@gmail.com, grajesh.grk@gmail.com*
[3] *Assistant Professor, Department of Information Technology, Karpagam College of Engineering,* [4,5] *Research Scholar, Karpagam Academy of Higher Education,*

Abstract

Steganography is a data hiding technique where text, image or video data is transmitted in a secure manner. The main aim of this paper is to develop a secure transmission through hiding data in images on optical communication networks. The steganography technique is used to hide the information and to communicate a blowfish algorithm implemented cipher data through histogram enhanced image via optical channel. In this paper, an algorithm called Least Significant Bit (LSB) replacement algorithm is used hide the secret message within the image and the blowfish algorithms are used to encrypt and decrypt the message. The performance of the proposed work is evaluated using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR). This can be applied in various medical applications in predicting diseases like Heart disease, cancer prediction and so on. This may be done by handling huge data as the technology may grows in recent days. Various learning approaches are also having ability to compute disease prediction. These approaches are involved in handling huge healthcare data in healthcare industries.

Keywords— *Cryptography, Optical Communication, Blowfish algorithm.*

1. INTRODUCTION

The advent of technology and wide use of Internet has made digital transmission of informations. Hence there is a need for securing the informations. Steganography is the subfield of network security and information security which enables secured transmission of informations. The informations are secured by hiding the secret messages embedded within another messages. For ecample, the files like text message, image, audio or video can be hidden within another text message, image, audio or video. Steganography is classified as text steganography, image steganography (Parmar Ajit Kumar Maganbhai et.al.2015), audio/video steganography. This paper proposes an image steganography approach to transmission secret information in images using optical networks.

This paper uses the least significant bit technique (Thangadurai, K,et.al, 2014), where the least significant bit is replaced with the data bit. The stegnographic alogorithm uses the 8-bit (gray scale) or 24-bit (color) images. This paper uses the 8bit gray scale image for size reduction. The rate of date transmission is high in 8-bit gray scale image when compared to 24-bit color image. The blowfish algorithm is used to provide more securiy to the message transmiited.

ISSN: 2233-7857 IJFGCN

The main aim of the proposed work is to prevent eavesdropping and ensure secure data transmission with the effect of dispersion on optical steganography by the use of least significant technique along with the blowfish algorithm. This method is also applied in medical applications for disease prediction.

The rest of the paper is organized as follows: Section 2 outlines the related work, Section 3 describes the proposed work, Section 4 shows the results and discussion and Section 5 gives the conclusion.

2. RELATED WORK

Kaur Amanpreet, et.al 2017 proposed an approach for optical steganography to enhance speed of analog transmission with security enhancement through image encryption. This approach uses network bandwidth in terms of twisted pair and coaxial cable.

Siti Dhalila Mohd Satar et.al. 2015 proposed an approach on logical connective model with LSB algorithm is used to result in low secure transmission. This logical connective model with LSB algorithm results in low secure transmission.

Babita Rawat et.al. 2014 proposed an approach using LSB algorithm and transmits over an optical fiber, but noise and dispersion is compensated in this approach.

Obaida M, et.al. 2013 made a research on steganography where AES encryption algorithm is employed. This approach uses data hiding through cryptography technique but this approach results in low secure transmission.

Tyagi Vikas et.al. 2012 proposed an approach of data hiding through cryptography using LSB algorithm. In this approach, the recovery of data is difficult.

3. PROPOSED WORK

The proposed work prevents eavesdropping of the messages and provides secured data transmission by using the proposed architecture shown in Figure 1. This architecture is a modified architecture proposed by Thamilvalluvan et.al., 2016.

ISSN: 2233-7857 IJFGCN

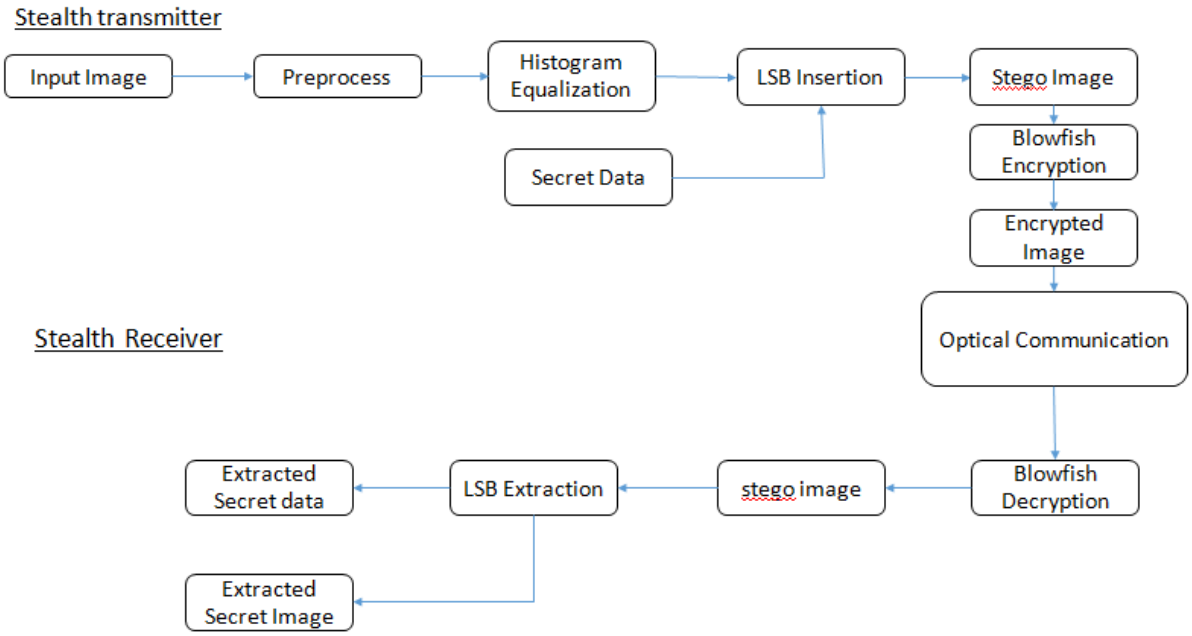

Figure. 1. System Architecture of the Proposed Work

The architecture consists of two parts stealth transmitter and stealth receiver. The stealth transmitter takes 24 - bit Image as an input image and that can be in the form of RGB colors, which represents 3 * 8 bit data. The Figure.2 shows the pixel representation of the RGB image.

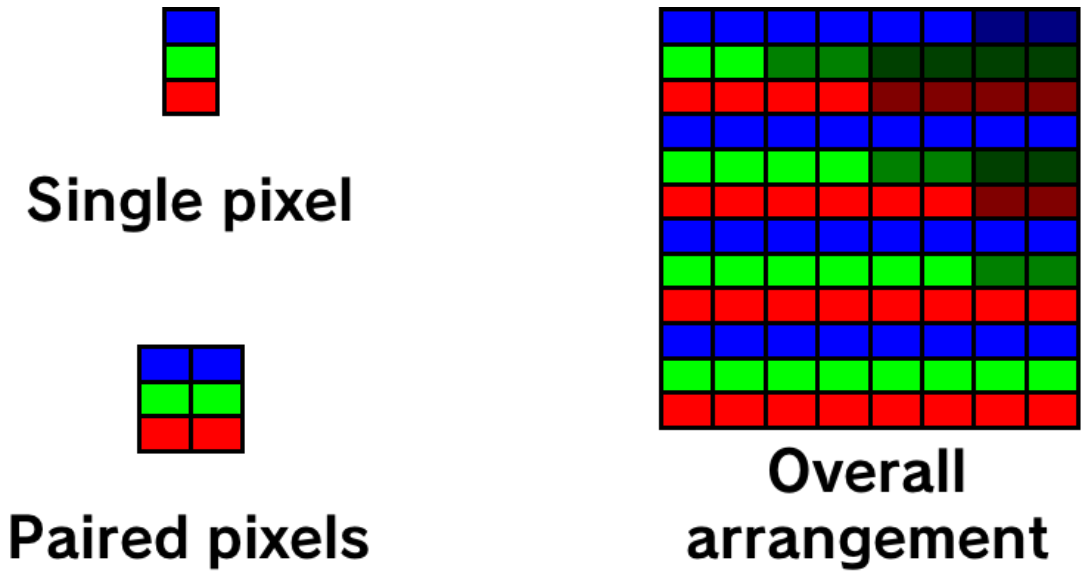

Figure.2 Pixel Representation of RGB Image

The input image take is a 24-bit image that can be in the form of RGB colors which represents 3 * 8 bit data. The Figure 3 shows a sample 24-bit image.

ISSN: 2233-7857 IJFGCN

Figure 3. RGB 24-bit image

Preprocessing:

The 24-bit image consisting mxn pixels which is in the form of RGB. The preprocessing stage converts the RGB image into gray scale image. The grayscale image contains single 8-bit image and the images are in black and white. The RGB encoding for any gray values consists of three equal numbers. i.e.. (x, x, x). Here the value of x is between the range 0 and 255. The gray scale image will be lighter if the numbers are higher in the encoding. The Figure 4 shows a sample grayscale image.

Figure. 4 Grayscale 8-bit Image

Histogram Enhancement:

The Histogram Enhancement improves the image quality by adjusting the contrast of the image. This is performed by modifying the intensity distribution of the histogram. The objective of this technique is to it easier to analyze or improve visual quality of the image. The proposed work changes the cover image RGB to Gray scale with the Histogram enhancement of the cover image. The Figure 5 shows the histogram enhanced 8-bit image.

Figure 5 Histogram Enhanced 8-Bit Image

ISSN: 2233-7857 IJFGCN

Adaptive LSB Embedding

The LSB algorithm ie., the Least Bit of the image is used to replace the secret data.A 8-bit gray scale image matrix consisting mxn pixels and a secret message consisting of k bits. Here the first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixels and so on. The Figure 6 shows the results of applying LSB algorithm on the cover image and obtains a stego image.

Figure 6 LSB algorithm sample conversion of original to stego image.

Blowfish Algorithm for encryption and decryption

The blowfish algorithm is a symmetric algorithm which divides a message into fixed length blocks during encryption and decryption (Kai He et.al,2016). The block length for this algorithm is 64bits. The messages must be padded if it is not in multiples of 8 bytes. The blowfish algorithm encrypts the stego image obtained after applying LSB algorithm. This blowfish algorithm divides the stego image obtained which is 64-bit into 32-bits. After encryption, the encrypted image can be transferred through the optical fiber. The received encrypted image can be decrypted using the blowfish algorithm.

Optical Communication

The communication channel used is the fiber optical transmission line (Ben Wu et.al 2013, Xu Chen,2015). The encrypted image can be transferred through the optical fiber to the trusted person.

Adaptive LSB Extraction

LSB Algorithm with the key can be used to decrypt the data from the image. The decryption is performed as follows: the first bit of message is extracted into the LSB of the first pixel and the second bit of message is extracted into the second some bits of message is extracted from the second reserves coefficients and so on. The encrypted image is first decrypted using the blowfish algorithm and then, the hidden message can be obtained from the stego-image using the adaptive LSB extraction algorithm.

Experimental Results

The first phase of the process is image steganography. Here the input image and the cover image are converted into their binary representations. The bits of the messages are embedded into each pixel's least significant bit and this process continues until all the bits of the message are embedded into the cover image, thus obtaining the stego-image. The step by step algorithm is given below:

ISSN: 2233-7857 IJFGCN

Step-1: Input the message and convert it into its binary equivalent.
Step-2: Input the cover-image and convert the same into it corresponding binary-equivalent.
Step-3: Take the first bit of the message and replace the least significant bit of the first pixel's binary equivalent with the same.
Step- 4: Repeat Step-3, until the whole message is embedded in the cover-image.
Step-5: The final image obtained is the stego - image.
The second phase of the process is done using the Blowfish algorithm. Blowfish is a symmetric block cipher. It has a P-array which has 18 32-bit boxes (P1, P2,… P18). It also has S-boxes, which are 4 32-bit arrays (S1, S2, S3, S4) with 256 entries each. There are 16 rounds for this algorithm. The steps of the blowfish algorithm is given below
Step-1: The 64-bits data element is divided in two halves of 32-bits each (say L and R).
Step-2: L is then XOR with P1 and the obtained 32-bits is passed to a function, say F.
Step-3: The function F, splits the 32-bit data into 4 8-bits and each are changed to 32-bits using the corresponding S boxes.
Step-4: The 4 32-bits obtained are again combined using XOR to finally obtain a 32-bit data.
Step-5: The thus obtained 32-bit data is XOR-ed with R and now L and R are exchanged. The process continues for another 15 rounds before the final encrypted data-element is obtained.
Decryption - Decryption process is always the reverse of the encryption process. Here, the encrypted image must be first decrypted using the Blowfish algorithm and then, the hidden message can be obtained from the stego-image.

The performance of the proposed work interms of the quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The sample images are taken and the proposed algorithms are applied to evaluate the performance. The Table 1 shows the PSNR AND MSE values for the sample images.

Name of the image	PSNR	MSE	Time
Blast	**21.8485**	**424.8404**	**0.624**
Flowers	**21.8943**	**420.3908**	**0.519**
Nature	**21.8133**	**428.3063**	**0.762**
Duck	**21.8919**	**420.6193**	**0.535**
falcon	**21.9907**	**411.1595**	**0.920**

Table 1. PSNR AND MSE VALUES FOR SAMPLE IMAGES

5. CONCLUSION AND FUTURE WORK

Data Transmission through image on optical steganography has been designed in order to transmit the messages in asecured manner. This approach makes use of the LSB and blowfish algorithms are used to encrypt the secret message and decrypt the secret message in the image. The use of blowfish algorithm improves the quality of the reconstructed image and is evaluated by using the PSNR and MSE measures. This method is used for predicting disease in medical applications. This will be used in Machine learning approaches in future.

ISSN: 2233-7857 IJFGCN

REFERENCES:

1. Babita Rawat, Mukesh Kumar Sone , Gaurav Agarwal," Securing Data in Fiber Optics through Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, pp.1351-1356, June 2014.
2. Ben Wu, Zhenxing Wang, Yue Tian, Mable P. Fok, Bhavin J. Shastri, Daniel R. Kanoff, and Paul R. Prucnal, "Optical Steganography based on Amplified Spontaneous Emission Noise", OPTICS EXPRESS, 2013.
3. Kai He, Chuanhe Huang, Hao Zhou, Jiaoli Shi, Xiaomao Wang, Feng Dan, "Public auditing for encrypted data with client-side deduplication in cloud storage, " Wuhan University Journal of Natural Sciences, Volume 20, Issue 4, pp 291– 298,2016.
4. Kaur Amanpreet, Soni Gaurav, "Optical Steganography to Enhance Speed of Analog Transmission with Security Enhancement through Image Encryption", 9th International Conference on Computational Intelligence and Communication Networks (CICN),2017.
5. Obaida M. Al-hazaimeh, "A new approach for complex Encrypting and Decrypting data", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, pp. 95-103, March 2013.
6. Parmar Ajit Kumar Maganbhai, Prof. Krishna Chouhan, "A Study and literature Review on Image Steganography", International Journal of Computer Science and Information Technologies, Vol. 6 (1), pp. 685-688, 2015.
7. Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda, Mustafa Mamat, "A new model for hiding text in an image using logical connective", International Journal of Multimedia and Ubiquitous Engineering, Vol.10 No.6, pp.195-202,2015.
8. Thamilvalluvan B, Lakshmi S, Keerthana S.R and Kalaivani K, "Secured Data Transmission through Image on Optical Steganography based on Noise", International Journal of Recent Scientific Research, Vol. 7, Issue, 4, pp. 9888-9891, April, 2016.
9. Thangadurai, K. and G. Sudha Devi (2014). An analysis of LSB based image steganography techniques. Computer Communication and Informatics (ICCCI), 2014.
10. Vikas Tyagi, Atul kumar "Image steganography using least significant bit with cryptography", Journal of Global Research in Computer Science Vol. 3, No. 3, pp. 53-55,2012.
11. Xu Chen, 'Decentralized Computation Offloading Game for Mobile Optical medium', IEEE Transactions on Parallel and Distributed Systems Vol. 26 No. 4, pp. 974–983, 2015.

ISSN: 2233-7857 IJFGCN