

SECURE AND EFFICIENT TRANSMISSION OF MEDICAL IMAGES OVER WIRELESS NETWORK

Deepika.K¹, Varshini Karthik²

¹Post Graduate Student, Department of BME, SRM University, Tamilnadu, India

²Assistant Professor, Department of BME, SRM University, Tamilnadu, India

Abstract

Advancements in data transmission has allowed radiologists at a given workstation anywhere in the world to send and manipulate any digital information. Wireless networks have been gaining popularity as a result of advancements that has solved security issues that have confined with the use of wireless technology in low-cost applications. This paper discusses an approach for transmission of medical images obtained from various imaging modalities and its remote transmission. The purpose is to study the existing method of medical image transmission over wired network and the proposed method here uses wireless network for the transmission of medical images to remote location. Remote transmission of various imaging modalities like Computed Tomography (CT), Magnetic Resonance Imaging (MRI) and Ultrasound (US) is done. The authentication allows user who are authorized to access the data. Security is provided through the process of encryption and decryption of data. The input is given as a DICOM (Digital Imaging and Communication in Medicine) image from source and is compressed and encrypted at source. The encrypted DICOM file is sent to destination over the network. Once the file reaches its destination, it is decrypted and decompressed. This implementation is done using Java programming language. Medical images are transmitted to doctors Laptop/I pad from source to destination over distributed network. Thus application may be hosted from a single system accessed by many others. A client/server architecture is an example of a distributed network where the server is the producer of a resource and many interconnected remote users are the consumers who access the application from various networks.

Keywords: DICOM, PACS, Compression, Encryption, Data transfer, Decryption and Decompression.

1. INTRODUCTION

The demand for medical image interpretation services in radiology is developing rapidly all over the world. This has highlighted the lack of adequate staff for providing lack of specialty expertise [1]. These problems can be overcome by utilizing robust communication to draw on the expertise of distantly located radiologists. The process whereby images are transferred to distant locations for the purpose of interpretation and diagnosis is defined as Teleradiology [1]. The medical imaging studies include CTs, US's and MRIs for interpretation and diagnosis. It may allow timely interpretation of medical images and give greater access to Physicians. It allows users in various locations to view medical images at the same time and improves patient care by allowing radiologist to provide service without having to be at patient location. The standard technologies such as Telephone line, Internet, Wide Area Network and Local Area Network (LAN) has been utilized for image transmission [1]. Research on teleradiology; have shown that technology such as image compression is often used [1]. The importance of compression has become important in developing standards for protecting medical images. It offers a means to reduce the cost of storage and to increase the speed of medical image transmission [2]. Compressing the data includes high compression ratio and the ability to decode the patient data [2]. In order to provide an efficient means of storing medical data, systems such as PACS and DICOM standards were developed for patient diagnostic purposes. In addition to compression, this requires handling

of security issues when dealing with medical information. The necessity of secure diagnosis is vital in the medical world. The transmission of data is a daily routine and is necessary to find a reliable way to transmit them over wireless networks. The technology is based on data protection through the process called encryption [3]. Encryption and decryption of data requires a passcode value [3]. In proposed work; the input is given as a DICOM image which is compressed and encrypted at source. The encrypted DICOM file is sent to destination over wireless network (Wi-Fi). Once the file reaches its destination, it is decrypted and further decompressed by the receiver.

2. DICOM/PACS STANDARD

2.1 DICOM Standard

The most important standards involved in Teleimaging include DICOM and PACS. DICOM (Digital Imaging and Communications in Medicine) is a standard for storing and transmitting medical images. It uses TCP/IP and allows various components to communicate between each other across multi-vendor environments. DICOM is responsible for the expansion of PACS systems with medical information technologies system. The most commonly used attributes are also listed in the DICOM data Dictionary. An application may add its own private tag and proprietary attributes are therefore possible in DICOM. The main function of a DICOM image reader is to read different tags as per the transfer syntax.

2.2 PACS Standard

The Picture Archiving and Communications System (PACS) refer to a system that is used to capture and store medical images [4]. The components of PACS includes, imaging modalities such as CT, US and MRI, a secure network to transmit information, work station for interpreting images, archives to retrieve and store images [4]. PACS can deliver access to images, interpretations and related patient data. It breaks down the barriers associated with usual film-based image retrieval and display. The software can interface with computers commonly used in hospitals to include the Radiology Information System (RIS) and Hospital Information System (HIS). The radiographic images can be viewed from any workstation within its network. The basic functions carried out by PACS are image retrieval, image transfer, viewing and networking [4].

PACS server is the primary point of entry for digital images. The idea behind imaging data with other medical information is to create Electronic Medical Record (EMR) for every patient that should be capable of being transmitted to any location [4]. The advantage of being able to share PACS files is the possibility to use them remotely and to give access to medical images. Growing number of facilities are available to display image data such as MRI, CT etc. Automation and digitalization are the key features and will help increase the quality of patient care, in case of emergency departments, in which the possibility to receive patient data in a few seconds may be crucial for patient management [4].

3. MATERIALS AND METHODOLOGY

3.1 DICOM Viewer Software

DICOM is a standard that is used in medical imaging. All modern imaging modalities like Ultrasound, CT and MRI supports DICOM [4]. It uses TCP/IP to communicate between the systems. DICOM specifies information objects that include images, whole studies, patients, reports and other digital information [4]. It allows user for the transfer of medical images across multi-vendor environments [4]. An application which does not find a needed attribute name may add its own private tag and proprietary attributes. An image viewer needs to read the attributes like image width, height and bits per pixel.

The viewer used here can be used to view DICOM images with non-compressed transfer syntax. Every patient file holds the patient information (name, ID, sex and birth date) and context of the entire imaging study. All medical imaging applications that are connected to the network use the DICOM protocol to exchange multiple images and patient information between its networks [4]. The network protocol is used to search for imaging studies in the archive and restore in order to display it.

3.2 Existing System – Overview

The images are initially transmitted from one location to another over wired network. It is achieved by using Ethernet

cable as a communicating media between two systems. This technique is followed everywhere in hospitals. Image compression plays a role in saving storage space and saving time while sending images over wireless network. A compression technique proposed to achieve more compression ratio by reducing the number of source codes. It is set up by means of networking using client server architecture. DICOM image from the source is compressed at source. The compressed DICOM file is sent to destination over the network. The images are finally decompressed. The proposed system discusses an approach for transmission of medical images obtained from various imaging modalities (US, CT and MRI) over wireless network to its remote location.

3.3 Discrete Cosine Transform (DCT)

In medical image compression, diagnosis is efficient when compression methods preserve all the information needed without any loss in details or quality [6]. The key to JPEG compression process is based on transformation known as Discrete Cosine Transform. The action used to reduce the number of bits required for storage of the DCT is referred as Quantization. In this system, CT brain and CT-chest images alone are taken for the process of image compression. Medical images obtained from the modality are compressed by using DCT and Wavelet transform techniques [7]. The images have got various compression ratio levels at different SNR. At lower compression ratio, SNR and PSNR are better in the case of DCT coding but as it increases, these factors degrade and become poorer in quality [7].

3.4 Proposed System

The DICOM standard addresses the connectivity between the workflow and various devices in a medical imaging department. Wireless transmission is a secure way to send the data to the remote location. With the use of digital images these networks must support a large number of medical imaging services provided by the hospitals. Healthcare organizations must accommodate the demands for high bandwidth in a cost-effective manner. A source and destination is set up by means of networking using Client server Architecture. Huffman coding is used here for compression and decompression to achieve better image quality for remote patient diagnosis. DICOM images from the source are compressed and encrypted at source. The encrypted DICOM file is sent to destination over wireless network (Wi-Fi). Encryption and Decryption is performed at source and destination for secured transmission of patient data. Once the file reaches its destination, it is decompressed and decrypted by the receiver. Fig-2 shows the block diagram for wireless network.

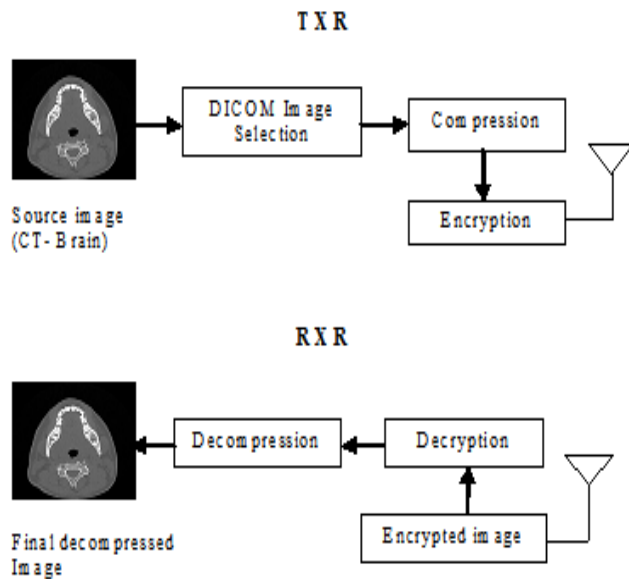


Fig-2: Block diagram for Wireless Network transmission

3.5 Huffman coding

Huffman coding is applied to the original LSB bit plane. It has the following properties: Codes for most commonly used characters are shorter than the ones for less commonly used. Each code can be uniquely decoded. To accomplish this, Huffman coding creates a tree called "Huffman tree". Fig-3 shows the flowchart for image compression and decompression.

Algorithm: Huffman coding based Image Compression

Step1: The code for each symbol is obtained by tracing a path to the symbol from the root of the tree.

Step2: The probability of each symbol has been determined using symbol count and the symbols are sorted.

Step3: Two of the lowest symbols are merged into one subgroup when there is more than one unmerge node.

Step4: A value of 1 is assigned for a branch in left and a 0 is assigned for a branch in the right.

Step5: The code words are generated.

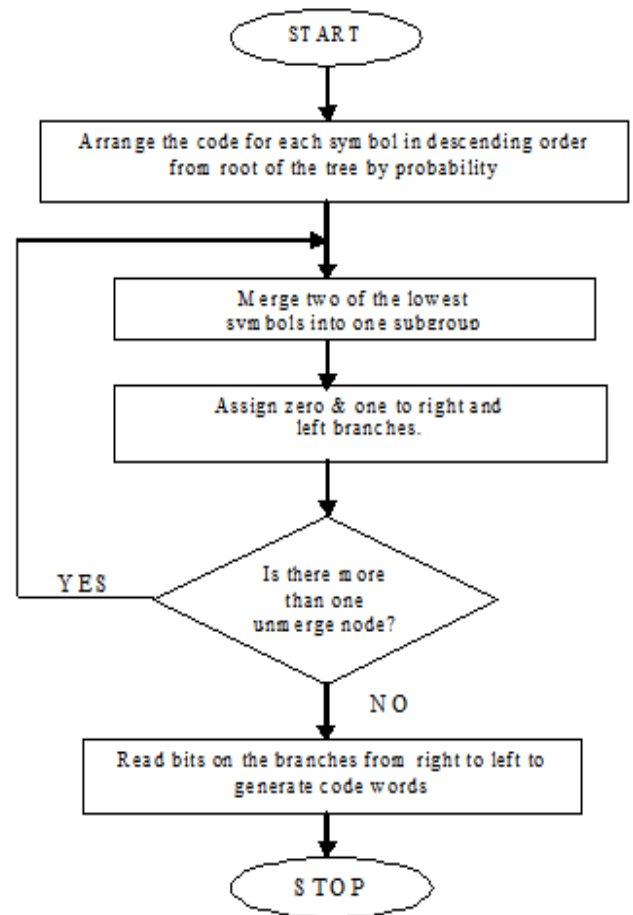


Fig-3: Flowchart for Huffman coding

3.6 Secure Scheme for Image Transmission

Cryptography plays an important role in information security. It is the process of storing and transmitting data in an effective way for protecting the sensitive data transmitted over an unsecured network by encrypting it into an unreadable format. The encrypted information is then processed and decrypted to reveal the original image at the receiving end. This technique reduces the risk of images being accessed by someone other than intended user. This is critical in situations that require the transmission of medical images. The Encryption and Decryption technique uses AES (Advanced Encryption Standard) algorithm for secure transmission of medical images. This standard specifies the Rijndael algorithm, a symmetric cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits [6]. The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences are sometimes determined as blocks and the number of bits they contain is referred to as their length. The AES algorithm's operations are performed on a two-dimensional array of bytes called the State [6]. The length of the input block, the output block and the State is 128 bits. This is represented by $Nb = 4$, which reflects the number of 32-bit words. The proposed system uses 128 bits and is based upon selection of input images [6]. The number of rounds to be performed during

the execution is dependent upon the key size and is represented by Nr , where $Nr = 10$ when $Nk = 4$, $Nr = 12$ when $Nk = 6$, and $Nr = 14$ when $Nk = 8$. The decryption algorithm uses the same key but not identical with the encryption algorithm. AES decryption is implemented with an algorithm that is equivalent to the encryption algorithm (each operation is replaced with its inverse).

4. IMPLEMENTATION

4.1 Input Images

CT and MRI images acquired are transmitted to the remote location over wireless network as shown in Fig-4.1, Fig-4.2 Fig-4.3, Fig-4.4 and Fig-4.5. Multiple frames of images in series cannot be included. Hence, results for only few frames are shown here. Encryption and decryption is performed at source and destination using Advanced Encryption Standard Algorithm (AES).

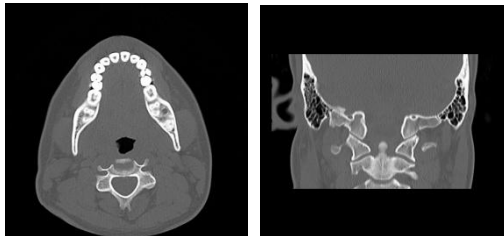


Fig-4.1: CT Brain Fig-4.2: CT Abdomen

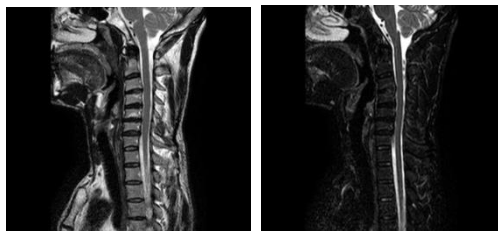


Fig-4.3: MRI Spine1 Fig-4.4: MRI Spine 2

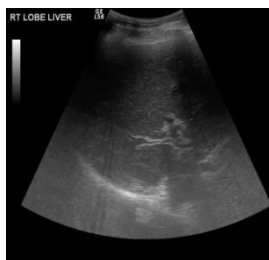


Fig-4.5: US Liver

4.2 DICOM Image Compression

The input image from source is compressed at source as shown in Fig-5. This is done mainly to decrease the file size and to improve bandwidth during medical image transmission over wireless network.

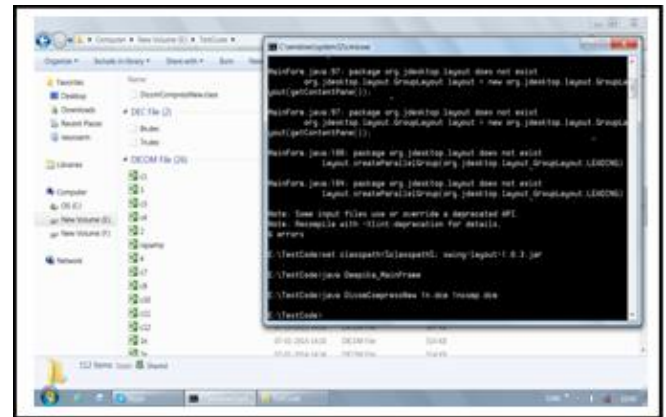


Fig-5: Image compression

4.3 Encryption

The encrypted DICOM image from the source is sent over wireless network securely to remote location as shown in Fig-6.

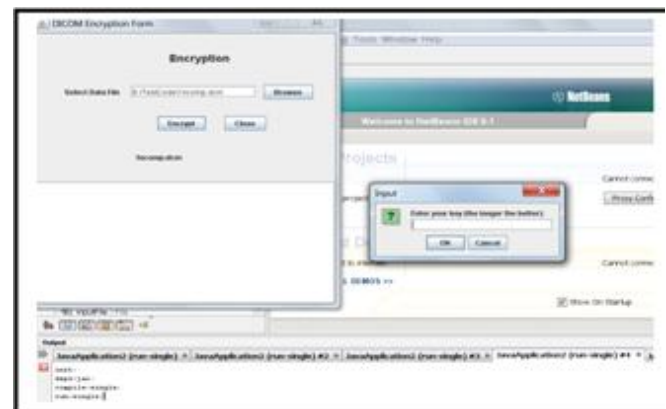


Fig-6: Image encryption

4.4 DICOM Image Transfer

The encrypted file is sent over network to remote location as shown in Fig- 7. This image contains text in unreadable format. Password is required to read an encrypted image file.

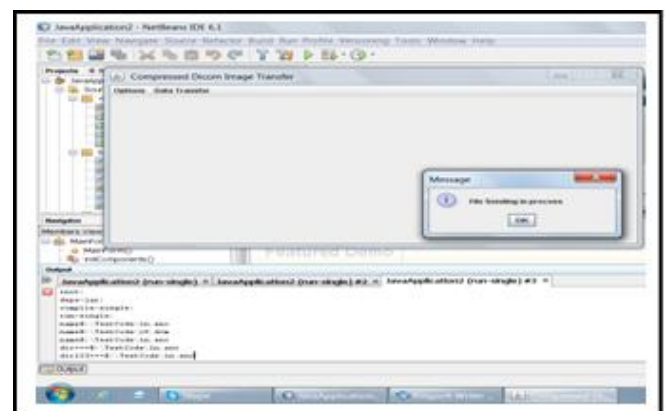


Fig-7: File transfer to remote location

4.5 Decryption

The encrypted image is decrypted and further decompressed by the receiver as shown in Fig-8. Password is required to read a decrypted image file at remote location.

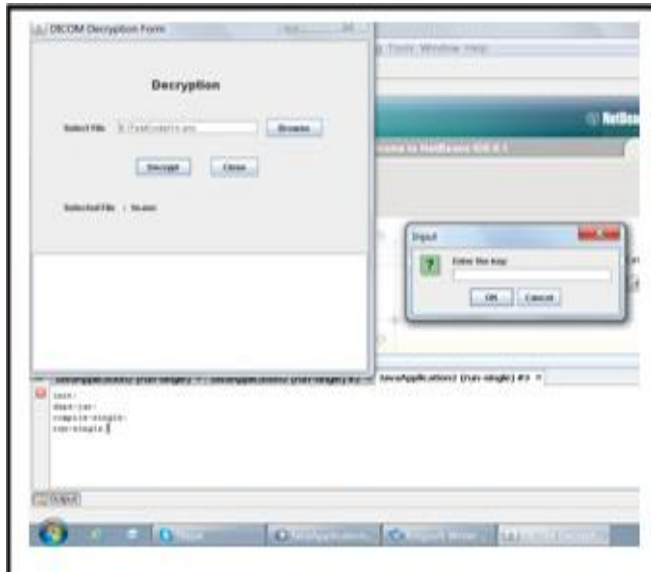


Fig- 8: Image decryption

4.6 DICOM Image Decompression

The decrypted image is further decompressed at receiver. The image can be seen at receiver end without any loss in quality. The image obtained is similar to original image.

5 RESULTS

The DICOM input images are acquired from the medical imaging modalities like CT-Brain, CT-Frontal sinus, MRI-Spine and Ultrasound (US). The images of size include 24.3 Mb, 14.6 Mb and 1538 Kb. The medical images from the source is compressed and encrypted at transmitter end. The encrypted file is sent to destination over wireless network to remote location. Once the file reaches its receiver end, it is decrypted and decompressed. The efficiency and memory space of the images were confirmed by means of image compression measurements which are tabulated below.

Table -1: Comparison of File size

DICOM images	File size before compression	File size after compression
CT-Brain	24.3 MB	18.0 MB
MRI-Spine	12.2 MB	5.69 MB
US-Liver	1538 KB	538 KB

6. CONCLUSIONS & FUTURE WORK

This paper describes an approach for transmission of medical images and its remote transmission to Doctors Laptop/I pad from source to destination over wireless distributed network. Thus application may be hosted and executed from a single system accessed by many people. The input DICOM images are compressed and encrypted at source. The encrypted (cipher text) file is sent to destination over wireless network. Finally the file is decrypted (Plain text) and decompressed by the user at receiver end for further diagnosis.

6.1 Future Work

A network setup will be created in which the patient data will be sent to destination. It may be possible to calculate the time delay, Compression Ratio, Signal to noise ratio (SNR) and PSNR for various DICOM images. Possibility of transmitting medical images from the PC at transmitter end to many PC's at receiver end. The results of the above method will be compared and performance on image quality, SNR and PSNR for various medical images will be seen.

ACKNOWLEDGEMENTS

I am extremely grateful to the Head of the Department for his invaluable guidance, motivation, timely and insightful technical discussions. I am indebted to my Project Co-coordinators for their valuable suggestions and motivation. I am deeply indebted to my Faculties of Department of Biomedical Engineering for extending their warm support and ideas they shared with us.

REFERENCES

- [1]. Bernard Fong, Centre for Prognostics and System Health Management, City University of Hong Kong A.C.M. Fong, C.K. Li, 2011 John Wiley & Sons, Ltd. Telemedicine technologies. "Information technologies in medicine and telehealth and Indian Journal of Radiology and Imaging". Doi: 10.4103/0971-3026.45337 PMID: PMC2747412; 2009 February; 19(1): 16–18.
- [2]. John Retterer, Brian W. Casto, BSEE, CET. "Securing Wireless Technology for Healthcare (AHIMA Practice Brief)".
- [3]. Tam Vu, tamvu@wustl.edu. "Medical Applications of Wireless Networks". April 21, 2008.
- [4]. "Wireless Solutions in Health Care"©, Bridge Wave Communications, Inc. 2011.
- [5]. "Specification for the Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.
- [6]. Asadollah Shahbahrani, Ramin Bahrampour, Mobin Sabbaghi Rostami, Mostafa Ayoubi Mobarhan, "Evaluation of Huffman and Arithmetic Algorithms for Multimedia Compression Standards".
- [7]. M.A. Ansari and R.S. Anand, "Comparative Analysis of Medical Image Compression Techniques and their Performance Evaluation for Telemedicine", Proceedings of the International Conference on Cognition and Recognition.

BIOGRAPHIE

Deepika.K is currently pursuing her master's degree, M.Tech in Biomedical Engineering at SRM University, Chennai. She received her bachelor's degree, B.E in Biomedical Engineering from SRM University in 2012. Her research interest includes Bio- Signal Processing, Teleradiology and Telemedicine.