Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 6, Issue, 02, pp.5262-5266, February, 2014

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

DATA SECURITY FOR DICOM IMAGES

***Amit Jadhav, Dnyanesh Gaikwad, Gayatri Bhosure**

Department of Computer Engineering, University of Pune, Pimpri Chinchwad College of Engineering, Nigdi, Pune-44, Maharashtra, India

ARTICLE INFO

Article History:
Received 17th November, 2013
Received in revised form
10th December, 2013
Accepted 19th January, 2014
Published online 28th February, 2014

Key words:
DICOM,
Medical Imaging,
Mammography,
CT, MRI

ABSTRACT

Today technology has very much grown in last few years it has been in every aspect of medicine there is a huge development in medical imaging equipment as there are many equipment manufacturers, so a standard for storage and exchange of medical images needed to developed DICOM (Digital Imaging And Communication In Medicine) was created making it more easy and flexible in storage and exchange. DICOM image consist of two parts one is DICOM data and another is Image file we are implementing a security DICOM toolkit which will be able to handle, encrypt and Steganograph the purpose of this tool kit will be providing security for DICOM images and also reducing its size. The main benefit of this DICOM toolkit for avoiding false insurance claim avoid hackers to get the important information and secure exchange over a network. The idea of this paper is to separate the patient information from DICOM file and applying already existing encryption algorithm the encoded data is Steganograph to JPEG file format for secure transfer of image and data over network again the encoded data can be decoded performing reverse for it.

INTRODUCTION

The Dicom files contain both alphanumeric information (the name of the patient, date of birth, diagnosis, the name of the doctor) and one or more images compressed or in raw format. These files cannot be viewed on a computer. In order to do that, the Dicom files must be processed, the information must be extracted and eventually stored in a database. So, the information can be viewed anytime, subjected to some processing or queries. This processing mainly refer to operations that may lead to the improvement of the image quality and clarity, rotations that allow viewing from several angles that provides help for the medical individual. Extracting the information and the images from the DICOM files, to view all the data, brings high benefits to store process of the patient's information. In this way, it is possible to find all the records relevant to a patient, which means all the investigations that have been made along the years using a medical device, which has DICOM, standard. Also, a database allows making statistical situations used on national or international level (Samit Desai and Usha 2011). A DICOM file has the following structure: A preamble of 128 bytes, Prefix (4 bytes) where are stored the letters 'D', 'I', 'C', 'M' which represent the signature of the DICOM file, Data Set, which stores a set of information such as: patient name, type of image, size of the image, etc. Pixels that compose the image (s) included into the DICOM file. Data Set is composed of a number of Data Elements. The Data Set represents a single SOP Instance related to a single SOP Class (and corresponding IOD).A Data Set represents an instance of a real world information object and the Data Elements contain the encoded values of attributes of that object (Samit Desai and Usha 2011).

An IOD (Information Object Definition) is a model of abstract and object-oriented data, which allow specifying information about objects from the real world.

Fig. 2. Dicom File Structure (Samit Desai and Usha 2011)

A Data Element consist of various fields

1. Data Element Tag – which identifies the information in a unique way. The Tag is also composed by Group Number (2 bytes) and Element Number (2 bytes). For example, in (0010, 0020) tag the Group Number is 0010 and the Element Number is 0020. It is important the group with the

***Corresponding author: Amit Jadhav,** Department of Computer Engineering, University of Pune, Pimpri Chinchwad College of Engineering, Nigdi, Pune-44, Maharashtra, India.*

number 0002 and the element with the number 0010 from this group which represent the Transfer Syntax Unique Identifier. The Transfer Syntax UID defines the byte order for raw data. The integer values can be stored using the big endian or the little endian ordering.

2. Value Representation describes the type of data and the size for the value contained in Data Element. It is an array of chars stored in 2 bytes. VR of data Element tag is defined in Data Dictionary. Some of the available value representations are: PN (Person name), TM (Time), AS (Age String), and DA (Date).The VR may or may not be explicitly encoded in the data set. When it is used the Explicit VR function, Data Element is composed by four consecutive fields: Data Element Tag, VR, value length of the tag and the value.
3. Value Length: A 16 or 32-bit unsigned integer containing the Explicit Length of the Value Field as the number of bytes (even) that make up the Value. The length of Data Element Tag is not included, V R, and V L Fields, or a 32-bit Length Field is set to the Undefined Length (FFFFFFFFH).
4. Value Field: An even number of bytes containing the Value(s) of the Data Element. The data type of Values are stored in this field that are specified by the Data Element's VR.
5. The Value Multiplicity specifies how many values with this VR can be placed in the Value Field.ch as would be the case for data type OB, OW, SQ, or UN (Samit Desai and Usha 2011).

Related work and contribution

Today many medical images rely on computer processing. Data obtained from complex imaging devices that use complex methods to store images i.e. images generated from CT scans, MRI's scans. Also CAD (Computer Aided Designs) also use complex data structures to store the images. So for this purpose DICOM standard was made for interchange and to store medical data more easy. As said that DICOM images uses very complex data structures, so the size of images are very large i.e. (30Mb and more...). DICOM Images cannot be viewed in normal viewer, special DICOM viewers are required. DICOM includes data structures that are of importance to the image. Those structures are placed in a header that contains object's description, patient's data, name of the institution and other information such as performed procedures or reports. Information Object Definitions (IODs) are the most important components of data structures. IODs are tables of attributes that define information objects. Information objects are models that are abstracted versions of real-world objects, for example "patient" is an information object that has "patient name" and "patient ID number" as attributes. Some of the DICOM viewers are DICOMWorks, Osiris, Irfan View and these are freeware (Wail *et al.,* 2008). DICOM is one of the most ambitious medical image standards. It is developed to make image data standardized and easy to share between the equipment from different manufacturers. This organization structure is very efficient, because each workgroup is in charge of different areas with as little aliasing between them as possible. DICOM Standard is developed to make possible a further expansion and easy upgrade of some parts that constantly develop. That is a very important possibility, because today imaging standards develop very fast as well as the medical imaging equipment (Wail *et al.,* 2008). There is another approach where, DICOM standard is an image archive system which allows itself to serve as an image manager that controls to take over, retrieve and distribute the medical images within entire picture archiving and communication systems. The DICOM technology is suitable when sending images between different departments within different hospitals, and consultants however some hospitals do not have the DICOM system (Wail *et al.,* 2008).

Where this may also provide an approach for easy and practical MATLAB program that is devised to view medical images stored in the DICOM format and convert them to other common formats consequently the images can be seen using personal computers instead of using the DICOM system software thus patients can have their X-Rays, Computed Tomography (CT's) and other types of medical images in their computers this allows the images to be sent to physicians and consultants anywhere without worrying about the image viewing software they are using. A MATLAB program is developed to extract an image from a given DICOM file and convert it to another format the supported formats are common standard formats as follows (Wail *et al.,* 2008):

1. Portable Network Graphics (PNG).
2. Windows Bitmap (BMP).
3. Tagged Image' File Format (TIFF)
4. Joint Photographic Experts Group (JPEG).

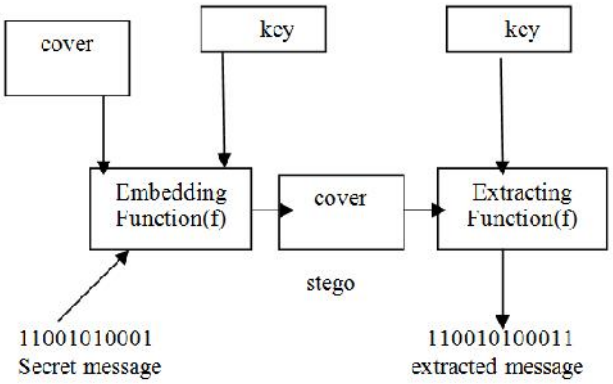
This variety of formats is meant to satisfy different users. Here is the procedure how it deals with DICOM file,read the DICOM file, get the total l0ength of DICOM file, and get the length a side of the square image, extract the pixel data and arrange in the square matrix., select the standard format for storing the image, write the image into the output file (Wail *et al.,* 2008).

Table 1. Comparison between images formats (Wail *et al.,* 2008)

Image Size	Format	BMP	TIFF	PNG	JPEG	DICOM
512 by 512	File size(Kb)	66	51	37	13	521
512 by 512	Word size(Kb)	40	40	100	100	----
256 by 256	File size(Kb)	258	257	144	39	130
256 by 256	Word size(Kb)	160	160	410	410	---

DICOM systems have become important in the medical environment. They ease and speed up the communication between different departments in a hospital and also between hospitals around the globe. Using the simple program presented, other environments will also benefit from the DICOM images. The program can be improved, transferred to other languages, and it can also be transformed into asingle independent executed file. Another approach or work related with DICOM can be explained or taken as example the work is related with JPEG2000. Where universal transcoder reading DICOM images and compressing these using lossy as well as well as lossless schemes such as jpeg, jpeg 2000 the compression technique to be used is either automatically

selected based on image parameters, or as specified by the user it determines results from research conducted in the conversion of images from DICOM format into any other image format, thus reducing the dependency of special DICOM viewer tool for viewing medical images, the aim is to convert DICOM files into JPEG format first and then convert these into other/same common image files in this transcoder the output is best suited and for viewing on wireless handhelds as well as built in viewers on computers, facilitates further analysis and research to be conducted in these images (Samit Desai and Usha 2011). Stegnography is another way to hide the secret message underthe imagefile. Stegnography is another way to hide the message in the data set and to communicate secretly. Thealgorithm used for our system is DCT-LSB.



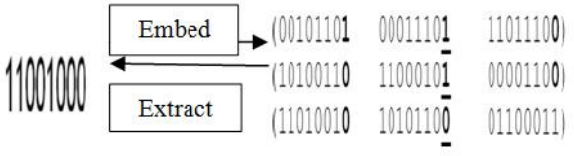
DCT-LSB: (Discrete Cosine Transformation-List Significant Bit Encoding)

It is a stenographic technique. It is a substitution algorithm for hiding the secret message behind the image file. The DCT coefficients D(i, j) of an 8 × 8 block of image pixels p(x, y) is done by formula.

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad 1$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{cases} \quad 2$$

Least Significant Bit (LSB) is a simple Steganographic method that takes the individual pixels of the frame and replaces the least significant bits with the secret message bits. In this technique each bit is been calculated the working of DCT-LSB is as follows



We can commandeer the least significant bit of 8-bit true color image to hold each bit of our secret message by simply overwriting the data that was already there. The effect of changing the least significant bit is almost very small to be seen. This process also includes embedding and extracting the text that is hidden behind the image. Following is the process of embedding the process of DCT-LSB:

Tiny Encryption Algorithm

This is a fiestal cipher encryption network which uses mixed operations like XOR, and operations. In Fiestel cipher network the data is divided into two halves. The F() is used, F() is applied to one the half using a sub-key and output of F() is XORed with other half and two halves are swapped. The main aim of TEA is to minimize memory space and maximize the speed. It is simple to implement and has less execution time takes minimal storage space.

Notations used

x << y: denotes logical left shift of x by y bits
x >> y: denotes logical right shift of x by y bits.
x <<< y: denotes left rotation of x by y bits.
x >>> y: denotes right rotation of x by y bits.

Encryption

It assumes 32 bit word size. The 128 bit keys is split into four parts and is store k(0)-k(3) and data is stored in v(0) and v (1). TEA uses addition and subtraction as the reversible operations instead of XOR. The algorithm has 32 cycles(64 rounds).

Key Size: 128 bit key is split four sub key k={k(0),k(1),k(2), k(3)}
Block Size: 64bits
Structure: Fiesta network
Round: 64rounds

In this the input is divide into two halves and process is done but only last round is not swapped.

Inputs for the Encryption routine

Plaintext P, Key K, The plaintext is split into two halves as P= (Left part(0),Right part(0))

Output for the Encryption routine

The cipher text is C, Where C= (Left part(64), Rightpart(64)).

Decryption

Inputs for the Decryption routine

Cipher text C, Key K, The cipher text is split into two halves as C= (DLeftpart (0), DRightpart (0)) Where Dleftpart(0)= ERightpart (64) and DRightpart(0)=Eleftpart(64)

Output for the Decryption routine

The plain text is P, Where C=(DLeftpart(64), DRightpart(64)). In this way encryption and decryption techniques are been applied to the text data so that this data may not be accessed by unwanted user.In this way data can be kept secured.

Propsed system

The application first separates the text part and image part and stores the image in JPEG format and then encrypts, and uses

the resulted file as the secret message to hide in the harmless message generating a Stego-object. The receiver decrypts, de-embeds and decompresses the Stego-object respectively to get the hidden message. Modules of the Application: The application operates in two modes one is Sender and other is Receiver.

The modules for Sender mode of application are

Encryption: By using a Encryption algorithm the file is encrypted and the output file is used as the secret message.
Compression: The application compresses the document and then it is transferred.
Embedding: The output encrypted file is then hidden in the message(image) using the Steganographic algorithm, which generates the Stego-Object, which is then transferred to actual recipient.

The modules for the Receiver mode of application are

De-Embedding: The Stego Object is de-embedded with the use of encrypted file.
Decryption: The output encrypted file is then decrypted using the encryption algorithm, and the output file is then again given to the compression module.
De-Compression: The application then de-compresses the document and we have the secret message.

Steganography and cryptography are closely related. Cryptography distort messages so they cannot be recognized easily. Whereas, Steganography will hide the message in such a way that there will be no understanding of the hidden message. Even though if we are sending an encrypted message that be become prone to be easily understood where as an invisible message will not do so. The toolkit that is developed

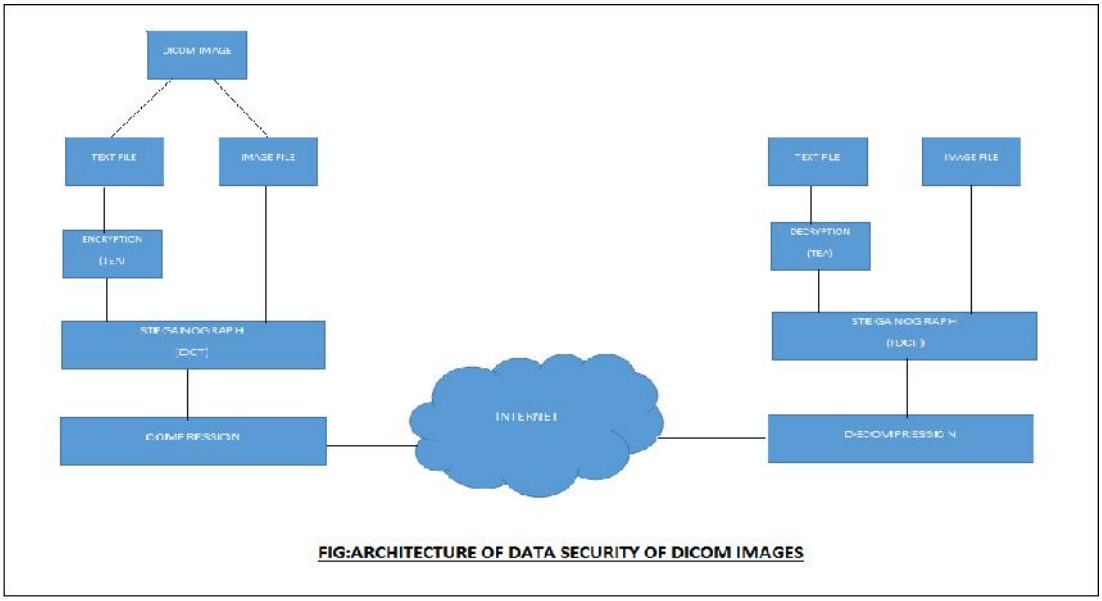
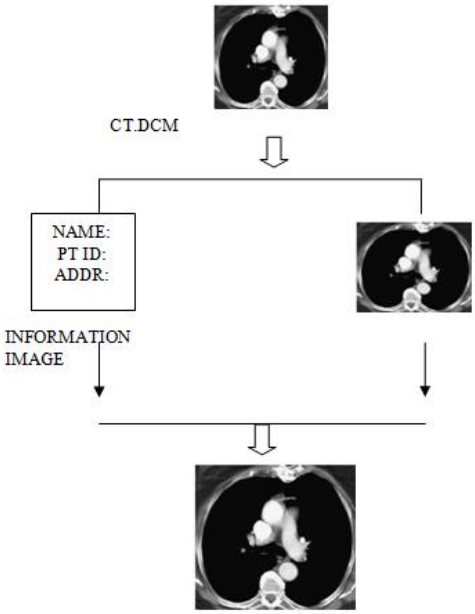


Fig. 3. Architecture for DICOM Toolkit

EXPECTED OUTPUT



in this project combines both sciences that provide better protection method for message/file. Even if the Steganography does not work then, since the message is in encrypted form it is of no use for the others who are actually not the participants, so the total information is secure. This is the process that is to be followed. Firstly we take. DCM image as the input and separate it into two forms that is image and information. Then encryption technique we encrypt the text and apply stegnography to the image. This ultimately results in compressed image. This also holds information behind the image.

Conclusion

In this way we have used different techniques to hide our confidential information behind image without loosing the accuracy of the medical images.

Acknowledgment

We express our sincere thanks to our Guide Prof. Atul Pawar, for his constant encouragement and support throughout our

project, especially for the useful suggestions given during the course of project and having laid down the foundation for the success of this work. We would also like to thank our Project Coordinator Mrs. Deepa Abin, for her assistance, genuine support and guidance from early stages of the project. We would like to thank Prof. Dr. J. S. Umale, Head of Computer Department for his unwavering support during the entire course of this project work. We are very grateful to our Principal Dr.A.M.Fulambarkar for providing us with an environment to complete our project successfully. We also thank all the staff members of our college and technicians for their help in making this project a success. We also thank all the web committees for enriching us with their immense knowledge. Finally, we take this opportunity to extend our deep appreciation for all that they meant to us during the crucial times of the completion of our project.

REFERENCES

Anusudha K., 2013. "An Overview of Digital Watermarking and Data hiding Techniques for Secure Transmission of Medical Images".

Krenn J.R., "Steganography and Steganalysis," Jan 2004

Kyucheol Cho, Jaejoon Kim, Se-Yoon Jung, Kyuhyeon Kim, Hyun-Kook Kuhng, "Development of Medical Imaging Viewer: Role in DICOM Standard", 2005.

Li-Chin Huang, Lin-Yu Tseng, "The Study on Data Hiding In Medical Images", 2012.

Mario Mustra, Kresimir Delac, Mislav Grgic, "Overview of DICOM Standard", 2008.

Rajashekarappa, K M Sanjiv Soyjaudah, Sumithra Devi K.A., "Study of the Tiny Encryption Algorithm", 2013.

Samit Desai & Usha B. S, "Medical Image Transcoder for Telemedicine Based On Wireless Communication Devices", 2011.

Syed Ali Khayam, "The Discrete Cosine Transform (DCT) 2003.

Wail A. Mousa, M. H. Shwehdi and M. A. Abdul-Malek, "Conversion of DICOM System Images to Common Standard Image Format Using Mat lab", 2008.

****