ALTINBAS UNIVERSITY
GRADUATE SCHOOL OF SCIENCES ENGINEERING

Cloud system for Encryption and Authentication Medical Images

Abdulrahman Ahmed Jasim

Master of Electrical and Computer Engineering

Thesis Supervisor:
Asst.Prof Sefer Kurnaz

Istanbul, 2018

Cloud system for Encryption and Authentication Medical Images

By

Abdulrahman Ahmed Jasim
[Master degree, institute of science, 2018]

Submitted to the Graduate School of
Science and Engineering in partial fulfillment
Of the requirements for the degree of
Master of Electrical and Computer Engineering

ISTANBUL ALTINBAS UNİVERSİTY

2018

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asst. Prof. Sefer KURNAZ

Supervisor

Examining Committee Members (first name belongs to the chairperson of the jury and the second name belongs to supervisor)

(Asst. Prof. Dr. Sefer KURNAZ) __________

(Assoc. Prof. Dr. Oğuz BAYAT) __________

(Asst. Prof. Dr. Oğuz KARAN) __________

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Çağatay AYDIN

Head of Department

Approval of [Institution] ____/____/____

Assoc. Prof. Dr. Oğuz BAYAT

Director

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Abdulrahman Ahmed Jasim

ACKNOWLEDGEMENTS

I would first like to thank my thesis advisor Assist Prof. SEFER KURNAZ Their doors office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right the direction whenever he thought I needed it. Secondly, I would like to thank my family especially my dear mother for her support in my studies and my brothers, my friends for them continuous support. Finally, I would like to thanks all my Professors in Istanbul Altinbas University.

ABSTRACT

Cloud system for Encryption and Authentication Medical Images

Abdulrahman Jasim

M.S., Electrical and Computer Engineering, Istanbul Altinbas University

Supervisor: ASST Prof. Sefer Kurnaz

February 2018

Lately, a great number of applications have emerged during the fast and continuous development in the field of telecommunications. One such important application is a tele-medicine where a patient’s digital medical data can be transferred between doctors in order to further diagnosis. Thus, protecting the exchanged medical data is the mission of this study, especially when exchanging those medical data over an insecure channel such as a cloud computing environment. The standard form of medical images is called DICOM (Digital Imaging and Communications in Medicine). When we are outsourcing these medical images containing sensitive information about patients, such as medical status about the patient, there is a need to provide privacy to this information. Where security is considered a valuable issue, this study proposes a novel framework to enhance the protection of DICOM images and the privacy of patient information. In the proposed system, the DICOM file that contain medical images and patient information will encounter a partition process in order to extract medical images and patient information and encrypt the images and upload them with patient information to the cloud, which will store patient information inside an Oracle data base and encrypted image inside a file. The keys of this encrypted image will saved in the database. If a client (doctor) registered in the cloud requests to download any medical image, the cloud will perform the steganography method using least significant bit (LSB) in order to embed the patient medical data inside the encrypted medical image and the key for decrypting the image, and send the encrypted image with the steganography information to the doctor. The proposed system insures provision of a lossless retrieval of the shared image while preserving the resulting images from pixel amplification in addition to guaranteeing a high level of quality of the retrieved images, especially high PSNR values by comparison with other studies on medical images using another encryption algorithm.

Keywords: telemedicine, medical image security, encryption, steganography, cloud system.

ÖZET

Son zamanlarda, telekomünikasyon alanında hızlı ve sürekli gelişme sırasında çok sayıda uygulama karşımıza çıkmıştır. Bunlardan önemli bir uygulama, hastanın dijital tıbbi verisinin daha ileri teşhis için doktorlar arasında aktarılabildiği tele-tıbbi bir uygulamadır. Bu nedenle, aktarılan tıbbi verilerin korunması, özellikle bu tıbbi verileri bilgi bulutu işleme ortamı gibi güvensiz bir kanal üzerinden aktarılırken, bu çalışmanın hedefidir. Tıbbi görüntülerin standart formuna DICOM (Tıpda Dijital Görüntüleme ve İletişim) adı verilir. Hastalar hakkındaki tıbbi durum gibi, hastalarla ilgili hassas bilgileri içeren bu tıbbi görüntüleri dışa aktarıldığında, bu bilgilerin gizliliğinin saklanmasına ihtiyaç duyulur. Güvenlik, değerli bir mesele olarak kabul edilmesiyle birlikte, bu çalışma, DICOM görüntülerinin korunmasını ve hasta bilgilerinin gizliliğini artırmak için yeni bir çerçeve ve çalışma sistemi öneriyor. Önerilen sistemde, tıbbi görüntüler ve hasta bilgileri içeren DICOM dosyası, tıbbi görüntüleri ve hasta bilgilerini almak ve sonra görüntüleri şifrelemek ve bunları hasta bilgileriyle buluta yüklemek için bir bölüntülemek işlemi ile geçirilir; tıbbi görüntüleri ve hasta bilgilerini içeren şifreli dosya bir Oracle veri tabanı içinde saklanır. Bu şifreli görüntünün anahtarı merkezi veritabanına kaydedilecektir. Bulutta kayıtlı bir müşteri (doktor) herhangi bir medikal görüntüyü indirmek isterse, bulut, şifreli medikal görüntü içine yerleştirilen hasta tıbbi veriyi şifresini çözmek için anahtarı üretmek için en az anlamlı bit (LSB) kullanarak steganografi yöntemini uygulayıp şifrelenmiş görüntüyü steganografi bilgileri ile birlikte doktora gönderilecektir. Önerilen sistem paylaşılan görüntünün kayıpsız alınabilmesi ve paylaşabilmesi sağlarken elde edilen görüntüleri piksel yükseltmeden korur; alınan görüntülerin yüksek kalitesinin, özellikle de başka bir şifreleme algoritması kullanan tıbbi görüntülerle ilgili diğer çalışmalarla karşılaştırıldığında yüksek PSNR değerlerinin korunmasını garanti etmektedir.

Anahtar kelimeler: teletıp, tıbbi görüntü güvenliği, şifreleme, steganografi, bulut sistemi.

Table of Contents

List of figure

List of table

1. Introduction

In recent years the need to apply security techniques for medical images has increased with the utilization of tele-communications technologies for medical diagnosis and patient care when the supplier and customer are separated by distance. A system known as telemedicine is used in such cases. Tele-medicine is of high importance due to the fact that it provides the ability for consultations by remote specialists, loss-free and immediately available individual patient data, and improved communication between partners in medical systems (O. S. Pianykh, 2008). This leads to enhancement in the quality of medical care, and simplifies accessing to medical files, from which medical images can be either transmitted through a channel to a particular destination or stored and then given to the specialist. Transmitting medical information like the radiological results from a medical data base center to another center or to a remote radiologist spicily over cloud computing without applying security methods a limited degree of privacy for patients. Cloud computing, the environment offering encapsulating resources on the Internet as dynamic, scalable, and virtualized services (Borko Furht, 2010), offers many different on demand services to people, like the tele-medicine services. Over this environment, the user may benefit from many advantages presented by this computing model, such as transmission, storage, and more processing requirements on the user data. In spite of the cloud computing benefits, it has some drawbacks like the security which considered a significant issue facing the users of this technology due to the fact that they outsource their data to distributed storage systems and not local ones (Yanjun, September 2010). Thus, when transmitting user's data via the cloud environment, especially medical data, this type of data containing highly important information about the patients, requires a high degree of protection of the integrity and confidentiality (Mustafa Ulutas G. U., 2011) this data has to have the guarantee to avoid attacks it may face.

1.1 Problem statement

The security of medical information, obtained from strict ethics and legislation laws, gives rights to the patient and responsibilities to the health ethics (H. Nyeem, 2013). The need to secure medical images and other data on the patient is not only for privacy purposes but also to deter the manipulation that might occur by a malicious person during the transmission from one medical center to another. If a medical image is tampered with and sent to a specialist or a radiologist, this could lead to a wrong diagnosis that might cause severe problems or death.

In Canada, personal health information (names, provincial health card numbers, ages, billing codes and diagnostic codes) of 620,000 residents of Alberta, was stolen in September 2013. Later it was revealed that the personal health information stored in a laptop was unencrypted (News, Laptop stolen with health information of 620,000 Albertans, 2014). In the last decade, hundreds of thousands of Canadians have been affected by at least four similar incidents (News, 4 other cases of stolen health data in alberta, 2014). However, the biggest incident in medical history so far is in the US. Medical records were stolen that belong to 4.5 million American patients of 206 hospitals across 29 states during April and June 2014 (Sullivan, 2014). Stealing medical records is not a North American problem; it happens everywhere in the world; for example, in 2012 ransom hackers encrypted the entire database of an Australian medical Centre (Dunn, 2012).

Generally, the major types of network attacks that have been taking place can be classified into the following categories:

- Interruption which is an attack on availability. The purpose of this attack is to damage the information or the computer system using a small code such as viruses or worms.
- Interception is an attack on confidentiality. Capturing data is the aim of this attack using a code known as a Trojan horse hidden in some free software.
- Modification is an attack on integrity, for example altering the content of messages that are transferred via a network.
- Fabrication is an attack on authenticity, such as the inserting spurious messages in a network.

Therefore, there is a need of using methods to ensure the security of the transferred data.

A solution for achieving the needed trust management between the cloud computing ends is using Image encryption (Yanjun, September 2010) and Steganography method to hide related information inside image. Image encryption is referred to as image scrambling as well. It performs converting the input image to a meaningless version, and ensures protection due to users not being able to extract any meaningful information from those meaningless images. It has been commonly implemented in the protection of image content, in addition to image authentication (Borko Furht, 2010). Even though a wide range of encryption algorithms have been modeled, there is still a set of issues in practical applications. For example, a real-time system needs a high speed of encryption and decryption of images and a high quality of decrypted image while keeping efficient degree of security. Some techniques may process small sized images fast, but aren't proper for high-resolution images, like medical images and family photos. Thus, choosing image encryption algorithm with high speed processing to be suitable for high-resolution image is a very important task. Steganography can be put into words as the art and science of writing hidden messages in a way that nobody but the intended receiver is aware of the presence of the message (Memon, 2011). Because of the growing demand for security of images, steganography is gaining popularity (R.J. Anderson, 1998). The main aim of steganography is to communicate in a secure and entirely undetectable manner (N.F. Johnson, 1998) in addition to avoiding drawing suspicions to the transfer of hidden data.

1.2 Thesis statement

My study is to build secure telemedicine system to transfer medical images from medical devise clinic to the doctors clinics, this system will contain three applications, in the first application DICOM file that contain medical images and the patient information will face partition process in order to extract medical image and patient information, and store medical image in PNG file and patient information inside txt file, and encrypt medical image by using Chaos-based medical image encryption algorithm based on the traditional chaos-based image cryptography architecture that produced by Fridrich (FRIDRICH, 1998) which include two main steps. The used algorithm will applying on the resulted PNG medical image from the DICOM file partition and the two steps will perform in pixel by pixel mode on medical image pixels, after that encrypted image with patient info will upload to the cloud over TCP IP, cloud will store patient info inside oracle data base and encrypted image inside file, the keys of this encrypted image will saved in database with patent information, if client (doctor application or second application) that registered in cloud request to download any medical image, the cloud will perform steganography method using least significant bit (LSB) algorithm (Petitcolas, 1998) (third application) in order to embed the patient medical information inside the encrypted medical image and the key for decrypt the image, this encrypted image with steganography information will sent to the client over TCP IP. Now second application (doctor application) will decrypt stego image in order to extract patent information and after that decrypt the encrypted image and display the result to the doctor.

1.3 Literature survey

In the review of literature a great deal of studies have improved medical images security. Some of the suitable methods are listed in this section.

Zhou et al. (2001) proposed an approach for authenticity and integrity of digital mammography for the sake of encountering the requirements of authenticity and integrity, which is done via replacing the LSB of a random pixel of the mammogram by a single bit of the digital envelope bit sequence and repeating this operation for each bit in the sequence (Zhou X.Q, 2001). Timothy et al. (2006) suggested a health dialog model that has been properly estimated in clinical approaches and showed to be precise. This research gives an overview of the theories, techniques and methods utilized in constructing and evaluating those systems, in addition to describing several of the systems that have been developed and tested. (Giorgino, 2006). Mor Peleg Et Al. (2008) had the aim to state cases of request for patient's data access for preserving the privacy of patients (Mor Peleg, 2008). Stallings (2010) emphasized on security problems in his book (Stallings W. , 2010). K. Faraoun (2010) presented an image encryption method based on chaos maps for providing security, he proposed an “n-ary” key sequence generation technique, based on hierarchical combining of three chaos maps. In addition, he demonstrated that the production of key sequences are of good statistic features, like the uniform distribution. (Faraoun). Chao-Tung et.al. (2010), proposed a system known as MIFAS (short for “Medical Image File Accessing System”) for solving the exchange, storing and sharing on Medical Images of crossing various hospitals problems. Through this system it is possible to improve the productiveness of data sharing between patients and their doctors (Chao-Tung, 2010). Rajendra Acharya et al. (2011) proposed an approach to enclose patient information like texts and physical signals with medical images for efficient storage, this approach has been adapted in this research to interleave patient data with medical images for reducing the overhead of storage and transferring. The texts are enciphered prior to interleaving with images for ensuring higher degree of security. The graphic signals are compressed and then interleaved with the image (Rajendra Acharya U, 2011). T. Neubauer et al. (2011) presented safeguarding medical files from illegal access where patient data is stored, and determine the certified people (Heurixb, 2011). M. Ulutas et al. (2011) presented a (k, n) secret distribution system that performs a segmentation of the medical images amongst a health team of 'n' healthcare specialists in a way minimum 'k' of them have to collect for disclosing the medical image for being analyzed (Mustafa Ulutas G. U., 2011). G.Kanagaraji, et.al. (2011) presented a system that used the Cloud computing for the Hospital Information System. The proposed system was based on cloud computing idea. The medical image data sharing, exchange and high-end processing is available in the "Cloud". The information (i.e. the Medical Images) that are in the cloud are capable of providing the required details to the health professionals and the patient can get treatment in another branch of the hospital, and that reduces the informational and computational resource maintenance (G.Kanagaraji, 2011). D. Bouslimi et al. (2012) suggested an integrated encryption watermark approach for the resolution of keeping medical images combining the Quantization index modulation and an encryption method (Dalel Bouslimi, 2012). M. Ahmad et.al. (2012) suggested a paradigm for protecting the patients’ medical images for secure telediagnosis. The permutation and diffusion procedures of the model offer high security for encrypted information (Ahmad, 2012). H. Jian et al. (2012) proposed a security hidden danger of hospital and the existence of medical disputes issues timely (Hao Jianl, 2012). M. Ahmad et.al. (2012) suggested a model for providing visual protecting in order to withstand statistical attacks that may face the medical images (Ahmed, 2012). Sandra V. B. Jardim (2013) presented a paper which included a study has been made on E-Health files and proposed a group of overall guide-lines to build them (Jardim, 2013). M. Milutinovic et al (2013) presented privacy preserving protocols based on an innovative e-health system model, to ensure protecting user data (Decker, 2013). C. Huangc et al. (2013) proposed a histogram shifting approach for reaching high bit depth medical images (Li-Chin Huangc, 2013). Narendra et al. (2013) presented an encryption process for grey images with the use of a private 128-bit key. In this study, the image has been split to active blocks and afterwards, those blocks are accepted via diffusion and substitution approaches (Narendra K. Pareek, 2013). J. Luis et al. (2013) proposed an e-health record, and that allowed organized medical images to be united between approved medical fellows for developing the worth of medical images (Jose Luis Fernandez-Aleman, 2013). C. Fu et al. (2013) presented a chaos-based medical image encryption model, for indicating the efficacy issue, this paper offers a substitution appliance in the permutation procedure via a bit-level shuffle process (Chong Fu, 2013). A. Mahmood et al. (2013) attained full security against different types of attacks for a prolonged period. The result has been established as lossless (Ahmed Mahmood, 2013). R. Pakshwar et al. (2013) proposed an image encryption process for increasing the safety degree by offering chaotic outline for image encryption (Rinki Pakshwar, 2013). J. Cooley and S. Smith (2013) presented a keyboard video mouse, capable of capturing automatic text redaction for producing exact official content which is capable of recovering participant infrastructures and develop end-user influence on it (Smith, 2013). Fatma E., et al. (2013) introduced two security methods guaranteeing the ability for secure sharing of health images via the cloud computing media by offering the mean of trust managing between the authorized ends of this data, moreover, it permits the privacy sharing of the Electronic Patients' Records sequence data between these ends, at the same time keeping the shared image from distortions. The first method applies spatial water-marking method, the second one applies a hybrid spatial and transforming methods (Fatma E.-Z. A. Elgamal, 2013). Maria .S et al. (2015) introduced an interpolation method with lower degree of complexity, less blurring and higher resolution (Muneeswaran.K, 2015). J. Anbarasi et al. (2015) introduced a multi secret image sharing approach for sharing multiple images based on the interpolation polynomial (Jani Anbarasi.L, 2015). Akila et al. (2015) proposed an approach performance of which is measured with the use of enhancement and PSNR (Akilaa.K, 2015). A. Al-Haj. (2015) proposed a cryptography based algorithm providing confidentially, authentication, and integrity for the pixel data, and the header data as well, which is achieved with the implementation of a strong cryptography primitives using internally produced security data, like digital signature encryption keys and hash codes. The security data is produced internally from the header data and the pixel data, therefore, a strong connection is established between the DICOM and its corresponding security data (Al-Haj, 2015).

Z. Tang et al (2015) proposed a sufficient encryption algorithm for images with block shuffle and chaos map. The introduced approach splits an input image to overlapping blocks, shuffles those blocks for making initial encryption, makes use of a chaos map and Arnold transformation for generating secret matrices, and makes final encryption via conducting XOR operation between corresponding objects of every block and an arbitrary secret matrix (Lan, 2015). Prema T. Akkasaligar et al. (2016) approach is proposed using Chao's theories and DNA encoding to provide the security for digital medical images. In the presented approach, firstly the input medical image is revamped into two DNA encoded matrices based on intensity levels. Later, for odd pixel value based DNA encoded matrix Chen's hyper chaotic map and for even pixel value based DNA encoded matrix Lorenz chaotic map are used to produce the chaotic sequences separately (Prema T. Akkasaligar, 2016). Syifak Izhar Hisham et al. (2016) they use water-marking approach for grey-scale images. The method is implemented for achieving efficient numbering pattern, precise detecting and image recovery. The presented method utilized a unique spiral pattern numbering prior to the implementation of the block-based approach in hiding (Syifak Izhar Hisham, 2017). Narendra K. Pareek et al (2016) proposed an encryption approach for grayscale medical images based on genetic algorithms characteristics. Performance analysis shows that the presented model is of efficient statistical features, key sensitivity and is capable of efficiently resisting brute force attacks, differential attacks, plaintext attacks and entropy attacks (Patidar, 2016). P. Mantos1 et al. (2016) presented a method that has been introduced for Digital Imaging and Communications in Medicine (DICOM) medical images, applying secret-sharing steganographic approaches to make certain the integrity of private patient data in addition to the important portions of the image. In the presented method, images are segmented to two areas: the region of interest (ROI) and the region of non interest (RONI). Patient data and integrity hashes are placed within the region of interest while the information (map) required for recovering the region of interest prior to inserting is placed in the region of non interest (Maglogiannis, 2016). K. Anusudha et al. (2016) introduced a hybrid water-marking and encryption method for copy-right protection and authentication of health images. The image is water-marked in wavelet domain where in the Electronic Health Record (EHR) is utilized as a water-mark and the logo of the hospital as the reference image. Inserting EHR data is based on selecting the energy band and in reference to the bit index in the reference image. A combined algorithm for enhance image security is presented by benefiting from DNA-based image encryption and genetic algorithms (GA). Several deoxyribo-nucleic acid (DNA) masks are produced with the use of a logistical map function and DNA converting rules (Valarmathi, 2016). Philomina Jees, Diya Thomas (2016) they proposes a framework to strengthen the protection of DICOM images and privacy of personal data. In the proposed system metadata and image is extracted from DICOM image and encrypted separately using user defined key. The metadata is encrypted using modified AES algorithm and this encrypted data is again encrypted to enhance the security. When a doctor from remote location wants to access a medical image for diagnosis objective, he can access the encrypted metadata and identical encrypted medical image from the database in cloud and decrypt it (Philomina Jees, 2016). Ali Al-Haj et al. (2017) described a region based, crypto-watermarking approach which can provide authenticity, integrity and confidentiality for health images of various modalities. The presented method offers authenticity via embedding robust watermarks in images' area of non-interest with the use of a SVD in the discrete wavelet transform domain. Integrity is ensured in a couple of levels: strict integrity implemented by a cryptography hash water-mark, and content-based integrity provided by a symmetrical encryption-based tamper localizing model (Amer, 2017). M. Y. Mohamed Parvees et al. (2017) the pseudo random number generators (PRNGs), namely, the linear congruential generator (LCG) and exclusive OR shifting generator (XSG) are developed and paired with developed logistic two dimensional coupled chaos map for providing improved chaotic-based encryption. The presented model enciphers the Digital Imaging and Communication in Medicine (DICOM) images for protecting the patient confidentiality throughout storing and transferring in radiological information system (RIS) (Bose, 2017). Arda Ustubioglu et al (2017) proposed an innovative health image water-marking approach for the detection of tampered areas on health images with better precision by the authentication of 4x4 blocks and without the restriction of (ROI) size. The presented approach may mark a 4x4 pixel block if it has even a single tampered pixel, while similar approaches (having no region of interest size restriction) mark 8x8, 16x16, and 40x40 pixel blocks. Modified difference expansion (MDE) and LSB hiding approaches are utilized together first (Ulutas, 2017).

1.4 Thesis objective

The overall objective of this study is to build secure telemedicine system that can protect transferring medical images between medical center and doctors over cloud and assure providing a lossless retrieval of the shared image while preserving the resulting images from pixels amplification and guaranteed high level of quality of the retrieved images.

2. Background

In this chapter, background material describing medical imaging security techniques, and the environment that used in this study (cloud computing) and network protocol that we are used (TCP) is introduced. Achieving the security of a medical imaging system requires confidentiality data integrity, and authenticity (J. Franco-Contreras, 2014).

Confidentiality can be defined as keeping the content of the transmitted data secret from all others except authorized receivers. Transmitted medical images should be invulnerable to eavesdropping (R. Norcen, 2003). The major technique used to pledge confidentiality of data is cryptography and also steganography. Therefore, it is used to provide the required security for medical images. Obtaining a secure communication channel during data transmission by validating the communicating parties can be recognized as authenticity and that's provide by TCP\IP protocol. Validation can be obtained by applying entity authentication and digital signatures to enhance the security of the communication channel, figure 1 Show the General security problems and solutions.

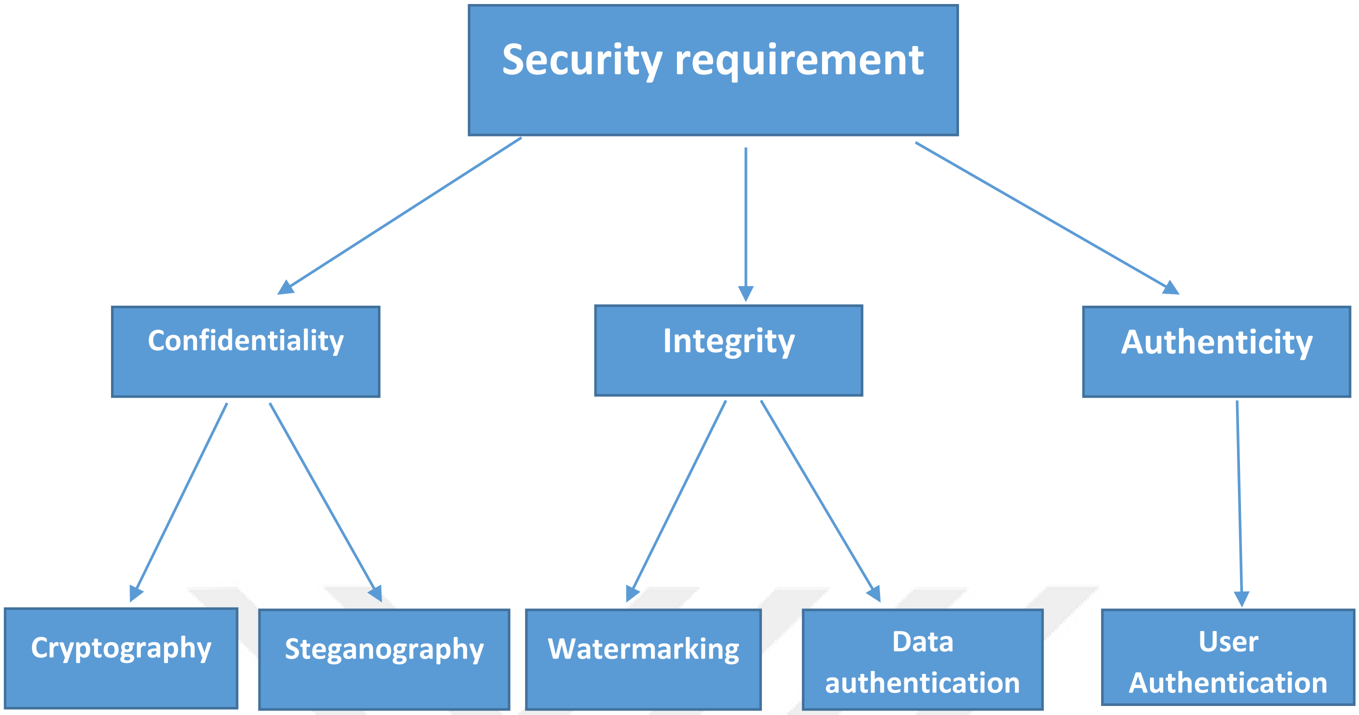


Figure 1 General diagram of security problems and solutions

2.1 Overview of the Medical Imaging System

Picture archiving and communication systems (PACS) are medical systems that consist of the required hardware and software modeled and utilized for running digital medical imaging applications. PACS includes three components: acquiring, storing, and viewing; digital image capturing devices (like computed tomography (CT) scanners, or ultra-sound), digital image archives (in which the captured images are stored), and workstations (in which radiologists display images) (Pianykh, 2008). Digital imaging and communications in medicine (DICOM), and health level 7 (HL7) represent the main standards for PACS (H. Huang, 2014). Health level 7 is a standard that includes only text files, while medical Digital imaging and communications includes both data format and communication protocols. The DICOM standard established by the National Electrical Manufacturers Association (NEMA) is used in the radiology and cardiology imaging industry for exchanging images and image-related data (Manufacturers, The DICOM standard, n.d.) (Lymberopoulos, 2009). It is supported by the majority of devices that allow data exchanging, without taking under consideration the type of equipment or examination. DICOM v3.0 is a unified format to store and transmit medical images. A single DICOM file includes each of a header, storing patient data, such as name, type of scan, image dimensions, and so on, and all the image data. DICOM images use 16 bits instead of 8 bits to represent a pixel to provide better image quality: image quality and size increase with the increment of number of bits. Therefore, there’s a trade-off between processing time versus image sizing and quality that affects network bandwidth requirements.

2.2 DICOM file

Digital Imaging and Communications in Medicine (DICOM) is a standard to handle, store, and transmit data in medical images. Files of this type may be transferred between a couple of parties able to receive image and patient data in DICOM format. The National Electrical Manufacturers Association (NEMA) owns the Copy-right to DICOM (Mario Mustra, 2008) and is the international standard for medical images and related information (ISO 12052). This standard determines medical images formats which may be transferred with the data and quality required for medical utilization and is applied in the majority of radiology, cardiology imaging, and radio-therapy devices (MRI, Ultra-sound, X-ray and CT, etc.), and, increasingly, in devices in other medical areas like ophthalmology and dentistry (Manufacturers, About DICOM, n.d.). This standard was proposed in the year of 1993 after decades of standards evolvement from the beginning of 80’s when only producers of CT or MR imaging devices were capable of decoding images which the early machines produced. It is different from some, but not all, formats in the fact that it collects information into Data groups. Therefore, for instance, a file of an X-Ray image actually includes the patient ID, Name, and so on, in the file, in a way that the image cannot be mistakenly split from this data.

This is identical to the way image formats like JPEG is also capable of having inserted tags for identifying and describing the image. DICOM has a data model differentiating it from other standards utilized in the medical industry field. The model depends on information items including definitions on the information for exchanges. Every type of image, and thus data object, has certain characteristics. For instance, a CT image needs various descriptors in the image header in comparison with an ultra-sound or ophthalmology images. Those templates are recognized with distinct identifiers registered by the National Electrical Manufacturers Association (NEMA), the DICOM standard facilitator. Information objects are considered as part of the Service Object Pair (SOP) Classes as well. An example of a SOP Class is the CT Storage SOP Class, allowing CT images to be exchanged (J. M. Blackledge, 2012).

Figure 2 show an example of DICOM file and how its look like when viewing it using a special viewer.

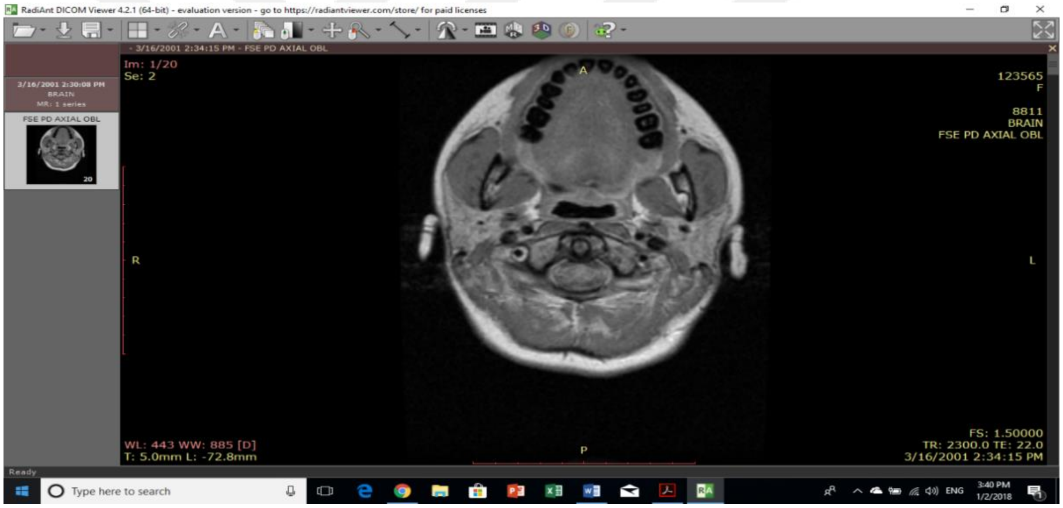


Figure 2 : An example of the DICOM file

2.3 Cloud computing

2.3.1 Essential Characteristics of Cloud Computing

There are 5 main properties of Cloud Computing explaining their relations and variation from the conventional computing.

· On-demand-self-service

Consumers may provide or un-provide services whenever required, with no human interactions with the provider.

· Broad Net-work Accessing

It has abilities over the net-work and accessed via standard mechanism.

· Resource Pooling

The computation resources of the supplier are gathered for serving several customers with the use of a multi-tenant framework, with different physical and virtual sources granted in a dynamic way, according to the demands of the consumer.

· Fast Elasticity

Services may fast and elastically be provided.

· Measured Service

Cloud Computing systems are in an automatic control and are capable of improving resource utilization via ensuring a metering capability to the type of services (such as storing, processing, bandwidth, or active user accounts) (Alliance, 2009)

2.3.2 Cloud Service Models

There are 3 Cloud Services Models and those three basic classifications are typically known as “SPI model” i.e. software, platform or infrastructure as a service.

- Cloud Software as Service

It is a capability where the customer is capable of using the provider’s applications that work on the cloud.

- Cloud Platform as Service

In this kind of service, the consumer is capable of deploying consumer generated or acquired applications produced with the use of programming languages or tools granted by the server, on the cloud structure.

- Cloud Infrastructure as Service

It is an ability granted to the customer by which, it may provide processing, storage, net-works and other fundamental computational sources in which the customer is capable of deploying and running the software (such as operating systems and applications) (Alliance, 2009).

2.3.3 Cloud Deployment Models

- Public Clouds

In which the cloud structure is publicly available.

- Private Clouds

The kind of the clouds, available only for single organizations.

- Community Clouds

In this kind of clouds, the cloud infrastructure is shared via a number of organizations and supports a specified community with shared concerns.

- Hybrid Clouds

A cloud structure which is composed of two or more clouds such as private, community or public (Alliance, 2009).

2.3.4 Cloud Computing Benefits

The previously mentioned properties may indicate different advantages for the possible consumers. The most significant advantages of Cloud Computing are listed below:

Cost reduction is reached by the avoidance of big initial investments for software and hardware acquisitions. The costs to maintain and train are minimized as well. The firm may give sources for other types of activities (such as integrating services, R&D) (Hamid R Motahari-Nezhad, 2009), (Mahmood, 2011)

Business agility and **scalability** are performed via the implementation of Cloud-based solutions, which results in innovating and changing ability for the firm (Mahmood, 2011).

Accessing to new IT services which in the other case would not be possible for a small organization to get. In that way the rules of competition don't remain the same (Mahmood, 2011).

The on premise IT systems are improved for supporting peak capacity, having an implication that the majority of the computational power sits idle. In a statistical view, 85% of the computational capacity remains idle while the rates of deployment lie in a range between 12% and 18%. Cloud-based solutions give **efficient capacity utilization** resulting again in reducing costs (Hamid R Motahari-Nezhad, 2009).

Cloud Eco-systems offer **disaster recovery** and **business continuity** (Mahmood, 2011)**.**

The Cloud services are of **high availability** due to the actuality that users are capable of ubiquitously accessing their resources. They are eligible of accessing data or applications anywhere that they are capable of finding Internet connections (Duipmans, 2012).

2.4 TCP IP

The TCP/IP protocol suite, known as the Internet protocol suite as well, is the collection of communication protocols implementing the protocol stack which the Internet and the plurality of commercial net-works operate on. It took its name from the two most important protocols in the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP) (Fujitsu Network Communications, 2006). This protocol just as the OSI reference model is outlined as a group of layers, the upper ones are logically closer to the user and are dealing with more abstract data, and they depend on protocols of the lower layers for translating data into forms transferred in a physical way via the network.

2.4.1 TCP/IP and the OSI Reference Models

This protocol has been developed prior to developing the OSI model. Therefore, it doesn’t map to the 7-layer OSI model directly. This protocol stack has only layers which may be loosely mapped to the OSI protocol.

Application Layer

This layer is corresponding to the application layer of the OSI model. Some popular examples of the application level structure within the TCP/IP domain are:

- SNMP
- FTP/Telnet/SSH
- POP3/SMTP
- HTTP/Secure HTTP (SHTTP)

Transport Layer

This layer corresponds to the OSI transport layer. Two widely implemented transport layer elements are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

Internet Layer

This layer is corresponding to the OSI net-work layer. Also, this layer is often known as the net-work layer. The main element of this layer is the Internet Protocol (IP). Several TCP/IP routing protocols are also categorized as part of this layer.

Net-work Access Layer

This is the bottom layer of the TCP/IP protocol. It includes a couple of sub-layers, namely, the media access control (MAC) and the physical sub-layers. The first one is closely aligned with the OSI’s data link layer, and is often known by that term (Fujitsu Network Communications, 2006).

2.5 Medical Imaging Security

2.5.1 Cryptography

Cryptography consists of encryption and decryption processes, so that only the destination can recognize the data. The original data, known as plain-text, is encrypted with the use of a key for creating disguised data called ciphertext. The encryption process can be implemented using either software algorithms or hardware devices. Some software applications of encryption methods are not efficiently fast for processing the huge amounts of data produced using medical imaging equipment. At the same time, hardware applications can add additional expenses to each of the transmitters and receivers (M. Yang, 2004). The cipher text in this application is a ciphered image transmitted from one medical center to another through a network over cloud, as shown in Figure 3 if an attacker makes a copy of the cipher text, it is still difficult to decrypt it without the decryption key. On the receiver side, a decryption process is required to recover the plaintext. The real security lies in the nature and length of the encryption key, which is a main design subject. Stream and block ciphers are the most important components of symmetrical encryption approaches. For algorithms of stream ciphers, a single bit of the plain-text is encrypted at a time, whereas block ciphers encrypt several bits as a whole unit. Stream ciphers usually process faster than block ciphers and are less complex. Nevertheless, stream cipher may be vulnerable to nontrivial security issues if they get used incorrectly (Stallings W. , 2014). The encryption scheme is considered to have a high degree of computational security when it follows the following criteria: (1) the expenses to break the ciphertext is more than the true value of the ciphered data. (2) The time that is needed for breaking the cipher is more than the useful information lifetime.

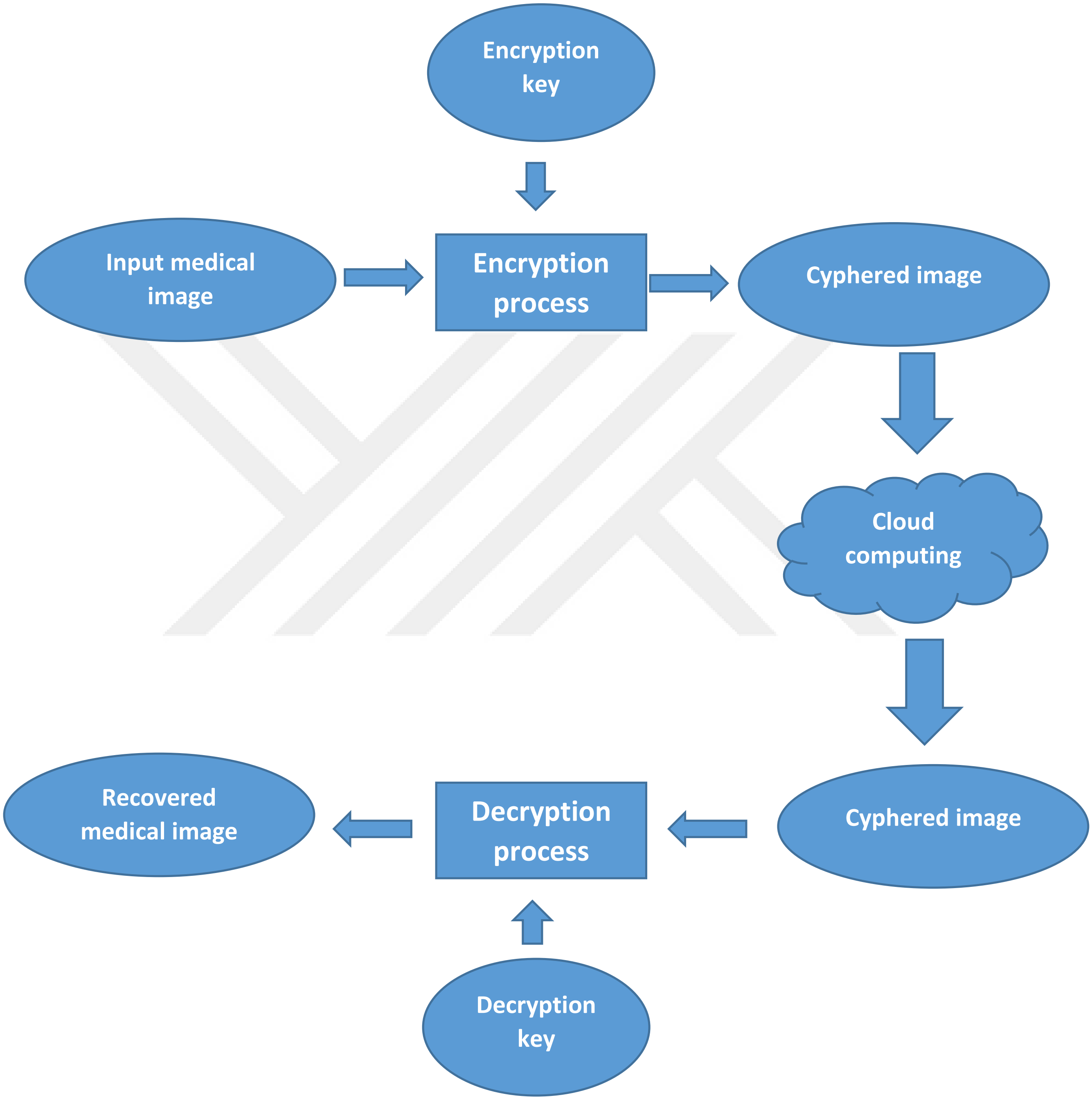


Figure 3: General block diagram of cryptography process

2.5.2 Encryption Algorithms

The following paragraphs provide a brief background on some of the encryption algorithms that are used in the medical imaging security field.

2.5.2.1 Triple Data Encryption Standard (3DES)

In 1998, 3DES replaced the data encryption standard (DES) via applying the DES algorithm three times on every one of the data blocks (Stallings W. , 2014). The 3DES is a closed key system used as an encryption algorithm and adopted for many practical applications. The basic operations in the 3DES algorithm are XOR, substitution, and permutation (M. Yang, 2004). These simple operations lead to adequate speed and a low cost encryption algorithm. The 3DES can be obtained via encryption using key1, decrypting using key2, and encrypting using key3. The receiver side performs the opposite steps to obtain the original information by decrypting with key 3, encrypting with key 2, and decrypting with key 1 (Samie, 2013).

2.5.2.2 Advanced Encryption Standard (AES)

In 2001, AES was invented by Daemen and Rijmen, and became the official encryption standard for the US government (M. Yang, 2004). AES is a block-structured approach with different length keys of 128, 192, and 256 bits. The objective of the AES is replacing the 3DES, due to having keys of a smaller length and the slower hardware implementation of the DES. This approach depends on the round function, and various combinations of the algorithm are structured via the repetition of the round function several times. Every one of the round functions includes four uniform and parallel stages: Sub Bytes, Shift Rows, Mix Column, and Add Round Key Transformation with every stage having its own specific functionality.

2.5.2.3 Encryption with the Use of the Chinese remainder theorem (CRT)

Chinese remainder theorem (CRT) is based on prime factorization (Stallings W. , 2014) Consider that n _ 2, andm1, m2... MN are positive relatively prime integers. Considering that the integer bi denotes the remainder of x modulo mi for 1 _ I _ n. The CRT resolves a number x that when divided by given divisors results in certain remainders. X is the lowest number that when divided by m1 has a remainder of b1, when divided by m2 leaves a remainder of b2, and when divided by MN leaves a remainder of bn. The CRT is represented by the following system that has a unique solution x.

2.5.2.4 Chaotic Maps Used For Image Encryption

Arnold cat map: This map was proven by Vladimir Arnold in 1960s by means of consuming an image of a cat. Arnold cat map utilizes the theory of linear algebra to bring a variation in the position of pixels of original image. Original image is allocated into blocks and then Arnold transformation is completed (Nasim, 2012).

Let X is a vector, X=, then Arnold cat map transformation is,

$$\boldsymbol{T}\colon \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{bmatrix} \to \begin{bmatrix} \mathbf{1} & \boldsymbol{p} \\ \boldsymbol{q} & \mathbf{1}+\boldsymbol{q} \end{bmatrix}$$

About conditions such as p and q are positive integers and

$$\begin{vmatrix} \mathbf{1} & \boldsymbol{p} \\ \boldsymbol{q} & \mathbf{1}+\boldsymbol{q} \end{vmatrix} = \mathbf{1}$$

This sort it as area-preserving. Original image can be shuffled through spread over the Arnold map operation repeatedly. But shuffled image can make a reappearance to original form after numerous repetitions (Nasim, 2012).

Sine map: sine map is defined as in formula (1):

$$Xn+1 = aXn^2 \sin(\pi Xn) \qquad (1)$$

When x0 = 0.7 and a=2.3, equation 3 has the simplified form. For the interval (0, 1) it produces chaotic sequence.

Tent map: it is similar to the logistical map. It produces chaotic sequences in (0, 1) assuming the subsequent equation (2):

$$Xn+1 = \begin{Bmatrix} \mu Xn & Xn < 1/2 \\ \mu(1 - Xn) & Xn \geq 1/2 \end{Bmatrix} \qquad (2)$$

Where µ is a positive number and reliant on its value which is found from tent map exhibiting dynamic behavior ranging from predictable to chaotic.

Circle map: it is defined as formula (3):

$$Xn + 1 = Xn + d - (c \;/\; 2\pi)\sin(2\pi Xn) mod1 \qquad (3)$$

Where d = 0.2, c = 0.5, and x0 € [0, 1] produces Chaotic sequence in [0, 1] (Nasim, 2012).

Logistic Map

The word chaos means randomness in the system. It is the measurement of disorder into a system. In case of data encryption it can be considered as how much cipher block has sensitivity to the initial conditions of the chaos maps (RAGHAVA, 2014). Chaotic map, which is mathematically represented by the formula (4) given:

$$\mathrm{F(Xn) = aXn(1 - Xn)} \qquad (4)$$

Here Xn denotes the chaotic sequence (Qiu Run-he, 2011), which value is between 0 and 1, as depicted in. The preliminary condition in case of the logistic map is for n=0, X0∈ [0, 1]. The parameter „a‟ is a real number whose value is between 0 and 4, i.e. a ∈ [0, 4]. After a lot of research, researchers have found that system is chaotic for „an‟ in the range from 3.56994 < a ≤ 4. For the value of „a‟ beyond 4, the value of X leaves ranges [0, 1]. And Xn diverges for the majority of initial values of X0. According to the values of „a‟, X has various nature figure 4 and 5 shows the Bifurcation for Logistic Map and Variation of Chaotic Logistic Map with Iteration (RAGHAVA, 2014).

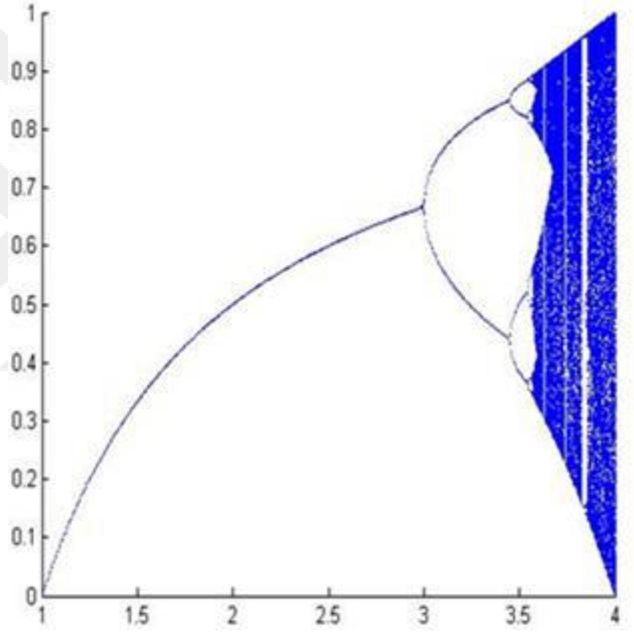


Figure 4: Bifurcation Diagram for Logistic Map

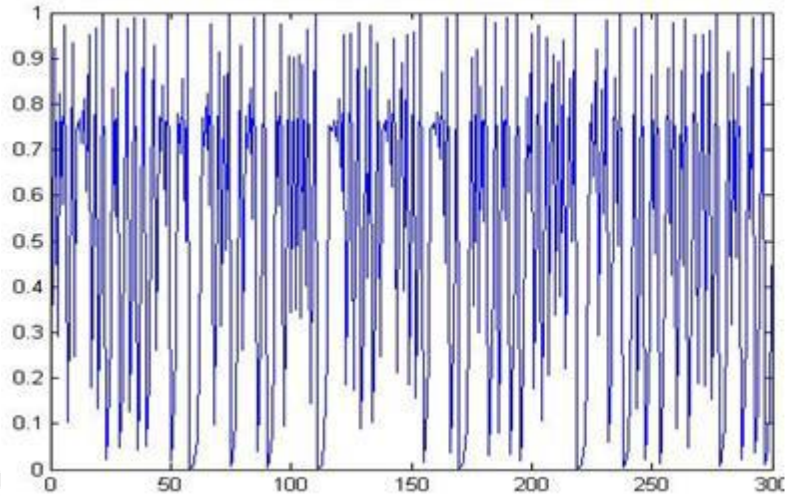


Figure 5: Variation of Chaotic Logistic Map with Iteration

We will use the chaotic logistic map, in this encryption process, because even if we know the initial condition, we can’t predict what will be the value of Xn at a given iteration n, since there is no direct relation between them. One of the major advantages of using chaotic system is its low cost in the signal generation process. Image encryption using chaotic systems divided into two broad categories, block cipher based encryption and stream cipher based encryption. In our proposed method we have used block cipher based technique for multimedia encryption (RAGHAVA, 2014).

2.5.3 Cryptanalysis

Cryptanalysis is the science of decrypting a message completely or partially, when the deciphering key is not known. Attacks may be categorized into a couple of main class. In the first kind, the attacker is aware of the method and/or a sample of a plain text-cipher text pair. In the second kind, the attacker is not aware of the ciphering method; this is referred to as a brute-force attack when each potential key on a portion of cipher text is tried, to the point where its plain-text is extracted (T. Lo, 2008).

The various kinds of cryptanalytic attacks are listed in the upcoming sections.

- Cipher text - Only Attacks.

In this type of attacks, a portion of the cipher text can be derived when the attacker is in possession of some medical data encrypted using the same encryption approach. The job of the attacker is recovering the plaintext of as many images as possible, or deducing the key(s) deployed for recovering the images (T. Lo, 2008). An example of this type of attacks is the jigsaw puzzle attacks, in which the attacker splits the encrypted image to several smaller parts, after that attempts breaking those parts simultaneously.

- Chosen - Cipher text Attacks.

In this type of attacks, the attacker is capable of to getting many encrypted and original images (Stallings W. , 2014).

- Known – Plain text Attacks.

This type of attacks happens when the attacker can have the access to a number of encrypted images and their original versions, which can be helpful in the determination of the key or part of it (T. Lo, 2008).

- Chosen- Plain text Attacks.

In this type of attacks, the attacker is capable of selecting some medical images, obtaining the corresponding encrypted images. This arrack happens when the attacker can have the access to the encrypted images and the original ones, in addition to the fact that the attacker is capable of choosing the interesting parts of the image, which makes it of more effectiveness than the known-plain text attacks (Stallings W. , 2014).

2.5.4 Encrypted Image Evaluation Metrics

For verifying the security and performance of an algorithm, the algorithm has to be tested and evaluated based on the encrypted image properties. A good encryption algorithm should result in an encrypted image meeting the requirements of the following evaluation metrics (Samie, 2013). The metrics may be classified into a couple of categories. The first class evaluates the efficiency of the substitution process, which includes the histogram, entropy and correlation coefficients. The second group is responsible for evaluating the ability of the approach to diffuse the original image. This group includes the mean absolute error (MAE), the number of pixels change rate (NPCR), and the unified average changing intensity (UACI).

2.5.4.1 Histogram

The cipher image histogram has to have a uniform distribution for the sake of avoiding the statistical attack (Wong, 2009). The image histogram illustrates the redundancy of every gray level value in the image. From a mathematical perspective, the histogram is a discrete function and its gray level values are between 0 and L - 1 as in the following formula (5):

$$hist(rk) = \frac{nk}{N} \qquad (5)$$

Here rk represents the kth graylevel, and nk represents the number of pixels in that image with that graylevel value. N is the overall number of the image's pixels, and k = 0, 1. . . L - 1. The histogram provides an overall image description, where a narrow histogram refers to the fact that the image's visibility is poor due to the lack of contrast in the gray levels that exist in the image. Similarly, a widely distributed histogram refers to the fact that the majority of gray levels exist in the image, and therefore, the general contrast and visibility are better.

2.5.4.2 Entropy

This is a statistic measurement of disorder and randomness. In the application of encryption the bigger is the value, the better are the results. The entropy H (d) of data d is calculated using the equation (6) bellow (El-Latif, 2012):

$$H(d) = \sum_{i=1}^{N} p(di) \log \frac{1}{p(di)} \qquad (6)$$

Where N indicates the overall number of pixel values and p (di) denotes the possibility of occurrence of a pixel of value di.

2.5.4.3 Correlation Coefficients

The encryption algorithm of a medical image has to resist the statistical attacks, when the pixel's correlation coefficients in the cipher image are as small as possible. Horizontal, vertical, and diagonal correlation coefficients of two neighboring pixels may be computed with the use of the formulas (7, 8, and 9) bellow (Mohammad, 2009):

$$cor\ xy = \frac{cov(x.y)}{\sqrt{D(X)}\sqrt{D(Y)}} \qquad (7)$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N}\left(Xi - \frac{1}{N}\sum_{i=1}^{N} Xi\right) \qquad (8)$$

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}(Xi - {}^{-}x)(Yi - {}^{-}y) \qquad (9)$$

Where x and y represent the grayscale values of two neighboring pixels, and N represents the overall number of pixels in the image, ¯x and ¯y denote the mean value depicted in.

$${}^{-}x = \frac{1}{N}\sum_{i=1}^{N} Xi$$

His directions of many pairs of neighboring (vertical, horizontal, and diagonal) pixels are arbitrarily chosen from the cipher image, and the correlation coefficients are computed.

2.5.5 Steganography

This term has Greek origins, derived from the words stegos which translate as cover and grafia which translate as writing (R.J. Anderson, 1998) which defines it as the covered writing. In image steganography the data is embedded merely within images. Steganography can be defined as the art and science of secret communications. It is also the practice of encoding/embedding private data in a way in which the existence of the data is not visible. The original files are known as cover text, cover image, or cover audio. Following the insertion of the private message it is known as stego-medium. A stego key is utilized in the operation of hiding/encoding for the restriction of detecting or extracting the embedded message (Niels Provos, 2003).

2.5.5.1 Steganography and cryptography

Steganography is different from cryptography (Chi-Kwong Chan, 2002)

- Analyzing the steganography is referred to as Steganalysis.
- Breaking cryptography is referred to as Cryptanalysis.
- Cryptography encrypts the data prior to sending to the recipient, without needing a carrier or cover.
- Steganography hides the data within the Cover, Many Carrier formats.

Watermarks and fingerprints related to steganography are mainly utilized to protect the intellectual property. A digital water-mark is a type of marker secretly inserted in a noise-tolerant signal like audio or images. It’s usually utilized for identifying the ownership of the copy-right of those signals. The inserted data in a water-marked item is a signature means data ownership for ensuring the protection of copy-right. In finger-printing, various and particular marks are inserted within the copies of the work which various customers are supposed to gain. In this case, it becomes easier for the property owner discovering customers giving themselves the right of violating the license agreement when they transfer the rights to other groups illegally (R.J. Anderson, 1998) (Ran-Zan Wang, 2000).

2.5.5.2 Approaches of Image Steganography

There is a number of Steganography methods for image files depicted bellow (Ran-Zan Wang, 2000):

2.5.5.2.1 Spatial Domain Method

There is a big number of spatial Steganography versions, all of them directly alter a group of bits in the image pixel values in embedding data. LSB's-based steganography is one of the most trivial methods of hiding a private message in the least significant bits of pixel values with no noticeable distortions. To the observers, the alteration of the value of the least significant bits are not perceptible. Inserting message bits may be performed either simply or arbitrarily. (T. Morkel, 2000) LSB replacement method and Matrix embedding, are some spatial domain methods.

2.5.5.2.2 Masking and Filtering

This is a steganography approach used on grayscale images. This approach is identical to placing a watermark on a printed image. Those approaches insert the data within the more important regions than merely embedding it to the noise signal. Water-marking methods may be implemented without being afraid of image destructions because of lossy compression due to the fact that they're more integrated with the image (Johnson, 1998)

2.5.5.2.3 Transform Domain Method

The Frequency domain the message is hidden within the image's transformed coefficients offering more data hiding capacity and higher degree of robustness against the attacks. The embedding of transform domain may be referred to as a domain of embedding methods for which several algorithms were proposed [3]. The majority of the strong steganography systems nowadays work in the transform domain transform domain approaches have a benefit compared to the least significant bit methods as they embed data in regions of the image which are less exposed to compression, cropping, and image processing. A number of transform domain methods seem independent of the format and they may be more advantageous than lossless and lossy format conversions. This type of methods are of various kinds (K B Raja):

1. Discrete cosine transformation method (DCT).
2. Discrete Wavelet transformation method (DWT).
3. Discrete Fourier transformation method (DFT).

2.5.5.2.4 Distortion Methods

This type of techniques, stores data by signal distortion and asses the deviation from the original cover image in the procedure of decoding. Those methods require being aware of the original cover throughout the process of decoding in which the decoder function checks for distinct features between the original cover and the distorted one for restoring the private data. In this method, a steganography image is produced via implementing a set of modifications on the cover. This set of is used for matching the private data needed for transmission. The data is encoded at pseudo randomly selected pixels. In the case where the steganography image differs from the cover at the specific message pixel, the message bit is a 1. On the opposite case, the message bit is a zero. The encoder is capable of modifying the 1 value pixels in a way which does not affect the image's statistic feature. In the case where the attacker attempts to interfere with the steganography image via cropping, scaling or rotating, the recipient is capable of easily detecting it (P. Kruus, 2003)

2.5.5.2.5 Least significant bit (LSB)

The LSB i.e. the 8th bit within an image is altered to a bit of the private message. When deploying a 24- bit image, the sender is capable of storing three bits in every one of the pixels via changing a bit of every one of the red, green and blue color elements, due to the fact that every one of them is denoted by a byte. An 800x600 pixel image, is therefore capable of storing an overall amount of 1,440,000 Bits or 180,000 bytes of inserted data. Which means that some of the bytes or all of them bytes within an image is changes to private data bit. Digital images are basically of two kinds (a) 24-bit images and (b) 8-bit images. In the first type of images it is possible to embed 3 bits of data in every one of the pixels, one in every one of the least significant bit positions of the three 8-bit values. Raising or lowering the value via altering the least significant bit doesn't vary the image appearance; therefore, the resulted steganography image looks approximately identical to the cover. In 8-bit images, a single bit of data may be embedded.

The secret image is obtained from the steganography image via applying the inverse procedures. If the least significant bit of the pixel of the cover C (i,j) is equal to the message bit m of the private data to be inserted, C(i,j) stays unaltered; otherwise, group of the least significant bit of C (i, j) to m. The data inserting process is depicted below:

$$S\ (i, j) = C\ (i, j) - 1, \text{ if } LSB(C\ (i, j)) = 1 \text{ and } m = 0$$

$$S\ (i.j) = C\ (i, j), \text{ if } LSB(C\ (i, j)) = m$$

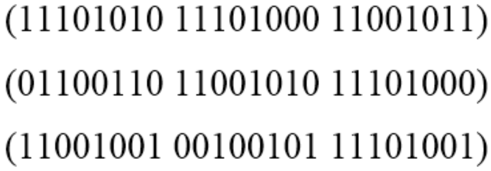
$$S\ (i, j) = C\ (i, j) + 1, \text{ if } LSB(C\ (i, j)) = 0 \text{ and } m = 1$$

In which LSB(C (i, j)) denotes LSB of the cover C (i,j) and m denotes the following bit to be embedded.

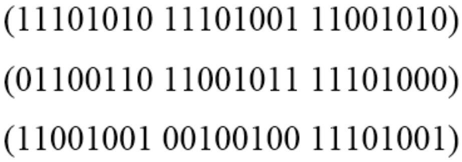
S (i,j) is the steganography image

As it is known, every one of the pixels consists of 3 bytes made up of either a 1 or a zero.

For instance, assuming one may embed data in 3 pixels of a 24-bit color image. Supposing that the original three pixels are: (January, 2004)

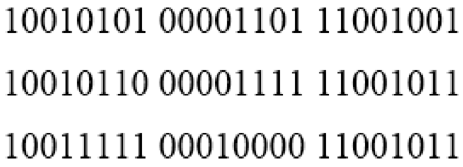

(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

Assuming that the steganography program hides the letter "J" which has the code 74 in the ASCII character set and has a binary representation "01001010", via updating the channel bits of pixels.

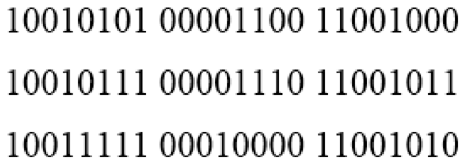

(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

In this case, only 4 bits had to be altered to successfully embed the character. The resulted changes applied on the LSBs are too little to be seen by an observer, so the data is efficiently embedded.

Another example, supposing to have 3 neighboring pixels (9 bytes) with the RGB encoding.


10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, may have the binary representation of 100101100 inserted into the LSBs of this portion of the image. When overlaying those nine bits over the least significant bit of the nine bytes above, the result is the following (where bits in bold are changed).


10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

Here the number 300 has been inserted into the grid, only the five bits required to be altered with respect to the inserted data. Generally, only 50% of the bits in an image will have to be altered to hide the data with the use of the maximum cover size. Due to the fact that there are 256 possible intensities of every one of the main colors, altering the least significant bit of a pixel produces little alterations in the color intensities. The human eye is not capable of perceiving those alterations, therefore data is successfully embedded. With an efficiently chosen image, the sender may even embed the data in the least significant bits without perceiving the difference (Deshpande Neeta, 2006). The benefit of the least significant bit hiding is that it is simple and several methods implement those approaches (Mandal). The least significant bit hiding also permits a high degree of perceptual transparency.

2.5.5.3 Image Steganalysis

Steganalysis is defined as breaking steganography and it is the science that detects embedded data (W Bender). The basic aim of this operation is breaking steganography and detecting the steganography image. The majority of the steganalysis algorithms are dependent on steganography methods that introduce statistical variations between the cover and the stego images. Steganalysis are of 3 various kinds:

- Visual attacks it detected the embedded data, and that helps separating the image to bit planes for extensive analysis. Statistical attacks can be either passive or active.
- Passive attacks are involved with the identification of the presence of the private data or hiding algorithm implemented. Active attacks are utilized for investigating the length of the hidden message or its location or the private key implemented in the process of hiding.
- Structural attacks the data format changes as the data to be embedded is hidden, the identification of this property structure variations may be helpful in finding the existence of image/text file.

3. Methodology

3.1 Introduction

IN this research a secure tele-medicine system has been developed, which has the aim of transferring medical images from medical devise clinic to the doctor's clinic, the developed system is made up of a set of three applications, in the first one (i.e. the Specialist application) DICOM file containing medical images and the patient information faced partition procedure for the sake of extracting medical images and patient data, and storing that image as a PNG file and the patient data as a text file, MATLAB 2016 has been utilized for the extraction of medical images from DICOM file and JAVA programming language for constructing first application for the extraction of patient data and execute MATLAB code to obtain medical images from DICOM file and encrypted medical image with the use of Chaos-based medical image encryption algorithm based on the traditional chaos-based image cryptography architecture developed by Fridrich (FRIDRICH, 1998) which includes a couple of basic operations. The utilized algorithm applied on the produced PNG medical image from the DICOM file partition and the two stages will be performed in a pixel by pixel manner on the medical image pixels, then, the encrypted image including patient information will be uploaded to the cloud over TCP/IP, cloud will store patient information in oracle database 10G and the encrypted image inside a file, the keys of this encrypted image will be saved in a data-base with patient information, if client (doctor application or second application that has been used JAVA programming language to build this application) which is registered in cloud request for downloading any medical image, the cloud will perform steganography operation using least significant bit (LSB) algorithm produced by R.J. Anderson (Petitcolas, 1998) (the third application that has also been used is JAVA programming language to construct this application) for hiding the patient medical information stored in the oracle database within the encrypted medical image and the key for decrypting the image, this encrypted image with steganography data will be transferred to the client via TCP/IP. Now, the second application (i.e. the doctor application) will decrypt the steganography image (LSB) for the extraction of patent data and after that, it will decrypt the encrypted image (chaos logistic map) and show the result to the doctor figure 7 show the main system steps.

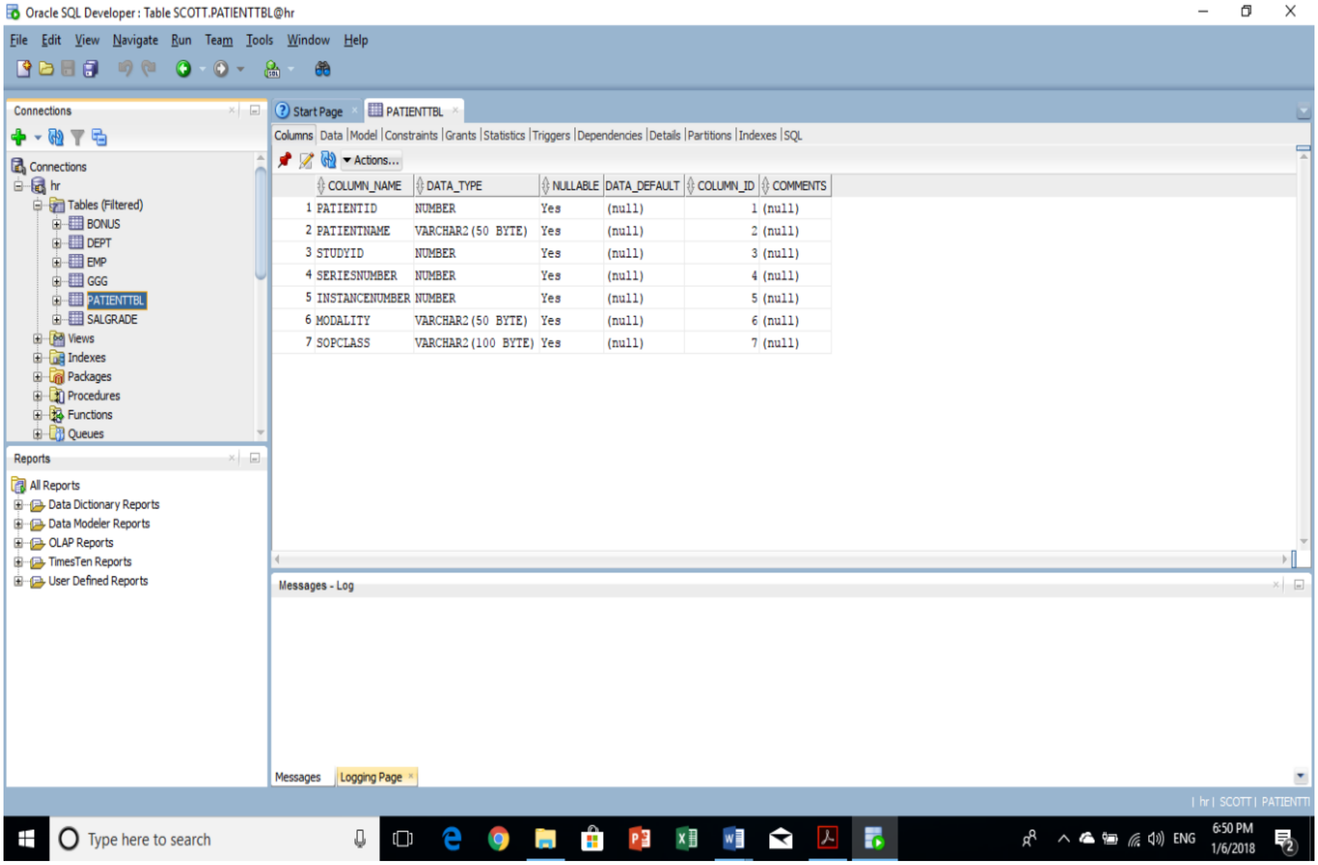
3.2 Tools of Implantation

Programing languages: JAVA 8 & MATLAB 2016

Environment: NetBeans IDE 8.0.2

Data base: ORACEL 10G

In the database a table was created, containing seven columns: (PATIENTID, PATIENTNAME, STUDYID, SERIESNUMBER, INSTANCENUMBER, MODALITY, and SOPCLASS) for saving patient information as shown in figure 6.



	COLUMN_NAME	DATA_TYPE	NULLABLE	DATA_DEFAULT	COLUMN_ID	COMMENTS
1	PATIENTID	NUMBER	Yes	(null)	1	(null)
2	PATIENTNAME	VARCHAR2 (50 BYTE)	Yes	(null)	2	(null)
3	STUDYID	NUMBER	Yes	(null)	3	(null)
4	SERIESNUMBER	NUMBER	Yes	(null)	4	(null)
5	INSTANCENUMBER	NUMBER	Yes	(null)	5	(null)
6	MODALITY	VARCHAR2 (50 BYTE)	Yes	(null)	6	(null)
7	SOPCLASS	VARCHAR2 (100 BYTE)	Yes	(null)	7	(null)

Figure 6: Oracle database table and attributes

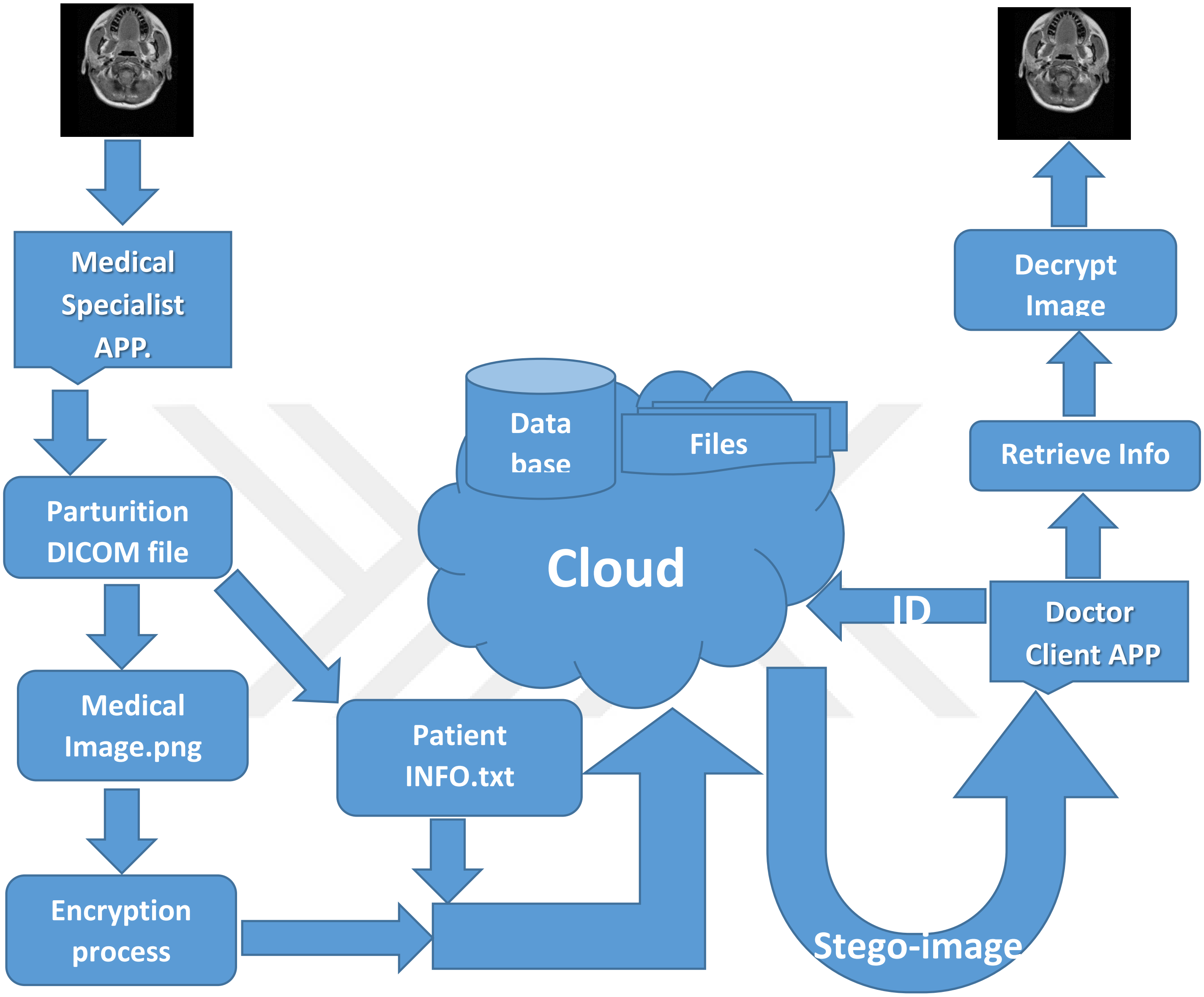


Figure 7: Main system diagram

3.3 DICOM file partitioning

As it has been stated in chapter (2) the term DICOM is short for (digital imaging communication in medicine) which is the current standard medical images file format the medical imaging devices produce and store; due to the fact that the DICOM file is difficult to handle because it does not merely store image data like the ordinary image files, it also stores the medical data concernig the image and the patient like the hospital logo, type of medical imaging device, some data concerning the medical image and information releted to the patient’s health like the name,ID, gender, age, and soon, known as mentioned in chapter two as the electronic patient record (EPR), figure 8 illustrates an example of DICOM file and the way it looks like when observing it with the use of a spatial viewer.

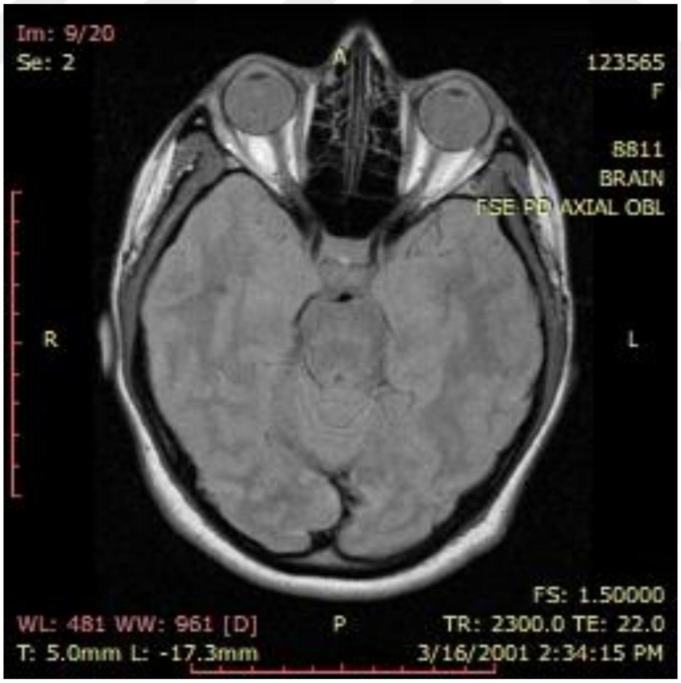


Figure 8: An example of the DICOM file

the proposed system splits the image from the medical meta information as shown in **table 1** and handle each one in a separate way in the forwarded steps of the system.

Table 1: DICOM file partition steps

1st step	**Partition DICOM File**
Input	DICOM FILE
Output	PNG medical image and medical meta information
	Begin
Step 1	Read DICOM file
Step 2	Split the medical image pixels data from its relatedmedical meta information.
Step 3	Store the medical meta information into text file
Step 4	Store medical image pixels in PNG file formate with 24-bit depth.
	End

As it has been depicted above, the medical image will be saved in PNG format in orderto ease handling the pixels in the encryption process which comes later and the medical related information stored in text file to use later as a stegongraphy data.

3.4 Encryption processes

3.4.1 Medical Image Encryption

Encryption means concealing information by altering its form according to specific algorithmic steps with a key in order to make it comprehensible only by the desired recipient, the person who possesses the key that has been used in the encryption process, The protection of medical images during transmission from a place to another in both private and public networks is the main goal of this thesis, which makes the attention towards the encryption increased lately, since the encryption operation has the aim of providing some security level to those medical images during transfer or even when storing it into computers and a good encryption algorithm must be able to maintain the main security goals to these digital medical images as show in Figure 9 which include : confidentiality, integrity and availability.

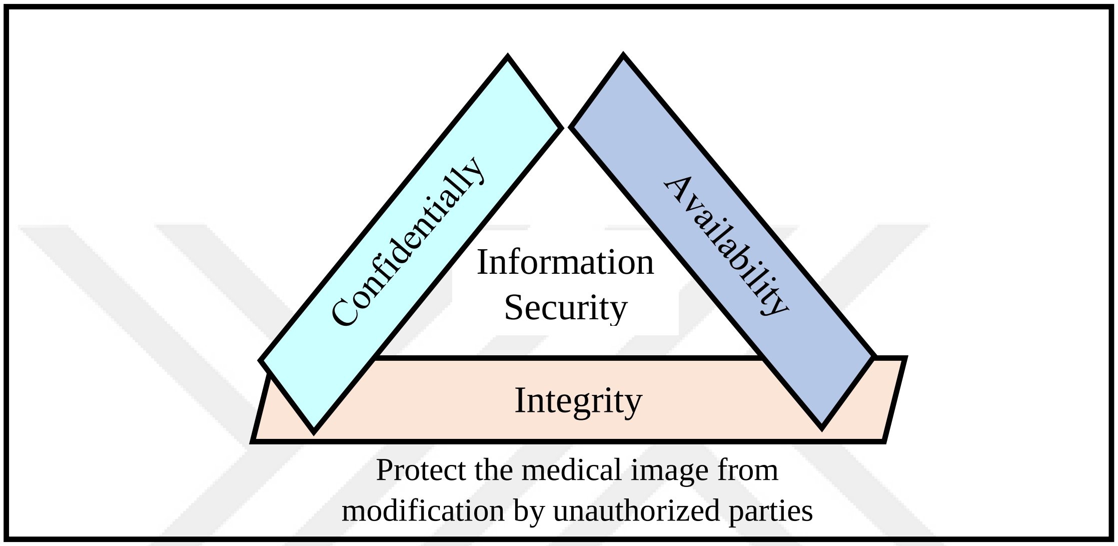

Confidentially
Availability
Information Security
Integrity
Protect the medical image from modification by unauthorized parties

Figure 9: General security goals

Chaos theory and its behavior have been used in medical image encryption in this thesis, due to the powerful features of the chaos systems which makes it give a significantly improved performance since it met the requirements of digital images like the strong correlation between its pixels, redundancy, having a big size and a bulk of data capacity; especially the medical images that the deformation or loss not allowed in its content that the standard encryption algorithm could result in it; Some of those features play an important role in the encryption procedure is its randomness, high sensitivity to initial conditions and parameters, aperiodicity, etc.

This study includes a proposal of chaos-based medical image encryption algorithm based on the traditional chaos-based image cryptography architecture produced by Fridrich (FRIDRICH, 1998) which include a couple of main steps. The utilized algorithm is applied on the resulted PNG medical image from the DICOM file splitting and the two steps is performed in pixel by pixel mode on medical image pixels, Figure 10 illustrates an example of the input image into the encryption operation.

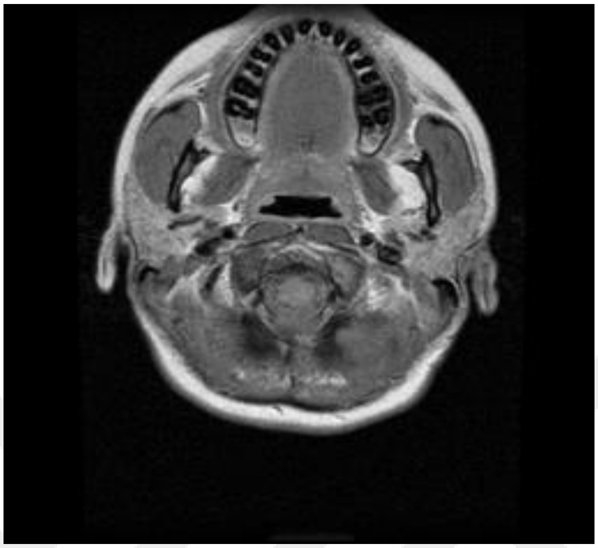


Figure 10: medical image entered to the encryption process

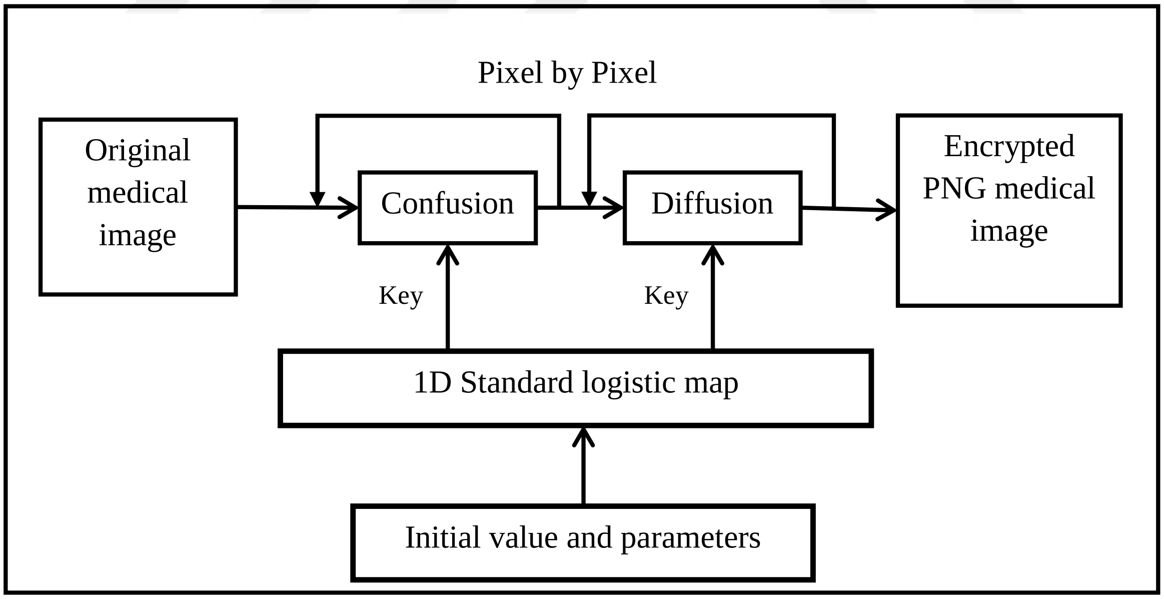
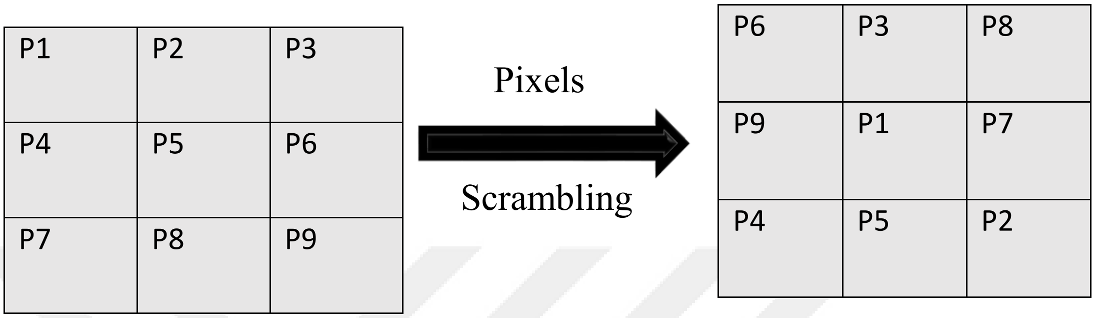


Figure 11: Block diagram of medical image encryption process

Pixels confusion means re-arranging the original medical image pixels locations; this step has the aim of reducing the high degree of correlation between the neighboring pixels, Figure 12 illustrates an example of an array of pixels to describe the way image scrambling is accomplish.



P1	P2	P3
P4	P5	P6
P7	P8	P9

P6	P3	P8
P9	P1	P7
P4	P5	P2

Figure 12: description of the elements scrambling in a matrix

On the other hand, diffusion refers to changing the values of pixels of the medical image by performing some transformations on the pixels values due to the fact that sole confusion will not be enough and any inverse process that will return the pixels to their original locations will declare the original image, therefore, giving the pixels new values will strengthen the encryption operation and cancel the correlation between pixel resulting in an encrypted image with a uniform histogram. As depicted in Figure 11 (Nasim, 2012), the key generator in this process is one of the widely known one dimensional chaos maps known as the "1D standard logistic map" (SLM)

that has only x variable as output and a single initial condition x_0 and one control parameter µ which give varying results and properties when altering its value as inputs, generally this map can be described as formula (1

$$\boldsymbol{Xn + 1 = \mu Xn(1 - Xn)\ for\ n = 0, 1, 2,}\ 3 \qquad (10)$$

The experimental results of this map shows that it is chaos when $x_0 \in [0,1]$ and its control parameter µ∈ [0, 4] and for more accuracy the logistic map is always chaotic and have appositive Lyapunov exponent when 3.58≤µ≤4 (Hua Xue, 2013), as show in Figure 13.

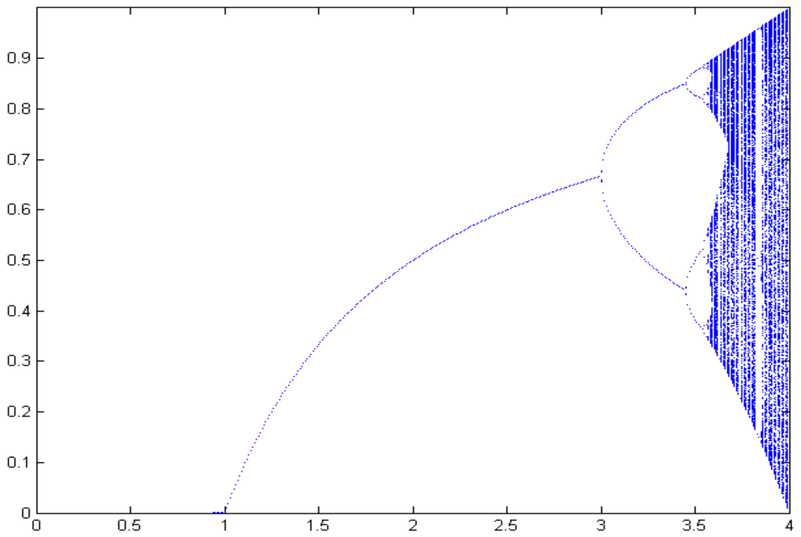


Figure 13: Bifurcation diagram of the standard logistic map

This research utilizes the SLM as key generator for confusion and diffusion of medical image pixels in spatial domain, where the SLM is iterated for all image pixels in order to give arbitrary values to be utilized to encrypt the pixel, each value of the control parameter and initial condition of the SLM in utilized as the private key of enciphering and deciphering of the medical image so it can be considered a symmetrical key encryption algorithm and as soon as the recipient possesses them he can generate all the random keys utilized for encrypting the image, the SLM in this research uses $x_0 = 0.4$ and the control parameter μ=3.87 as its starting inputs.

2nd step shows the encryption algorithm steps as in the Table 2 and input medical image and output encrypted medical image as shown in the figure 14 in this thesis.

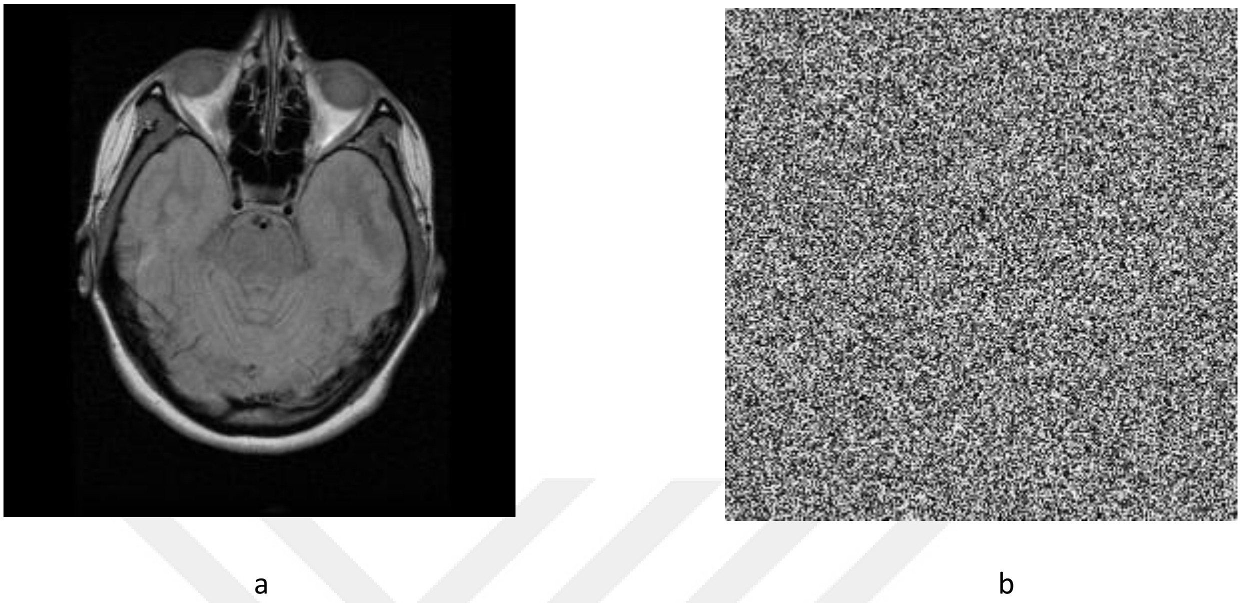


Figure 14: (a) input medical image, (b) output encryption image

Table 2: Medical image encryption steps

2nd step	**Medical Image Encryption**
Input	PNG medical image
Output	PNG encrypted medical image
	Begin
Step 1	Read medical image and store it into 2D array of pixels
Step 2	Use1D standard logistic map as random key generator and its intial condition and its control parameter as image encryption secret key
Step 3	Confuse the image pixels (rearrangment pixels positions) depending on the generated values from the (SLM)

Step 4	Diffuse the image pixels by changing their values depending on the key generated by the (SLM)
Step 5	Store the secret key values in the same text file that store the medical meta information that result from DICOM partition.
	End

3.4.2 Steganography Encrypted medical image

The methods and approaches of steganography can be defined as a form of data hiding in some digital files like videos, images and audio where the embedded data is associated with the digital media data content; utilized for providing authentication, copying control, owner identification, etc., which makes it gain a great deal of interest during the past years and may be considered one of the most widely known protection strategies for digital data while transmission.

The focus of this study is on the Steganography operations for hiding data within the encrypted medical image and it isn't a simple task and has some limitations especially in medical application that the need of full reconstruction for both of the medical image and the Steganography data is an important aspect and any distortion or loss isn't permitted, therefore, it has to be treated with caution, some of those limitations which should be mentioned:

- The conventional watermarking or Steganography methods make some alterations on the cover for placing the embedded data, which distorts the cover and referred to as "embedding distortions" and cannot be entirely recovered and this isn't proper in medical application.
- There's a challenging problem during inserting a water-mark within the encrypted image due to the fact that the entropy of the encrypted image is high and the water-mark inserting will be considered as noise, therefore, a conclusion has been obtained, that

whenever the lower “embedding distortion” is, the more powerful and proper to the medical application it is, which makes the focus on the Steganography approaches increase rapidly, which is utilized when each of the cover and the watermark have equal importance such as medical application, due to the fact that it provides a no distortion retrieval for each of the medical image and Steganography data.

In this research, the LSB method has been applied on encrypted medical image and each of the medical image encryption key and medical related data resulting from separating the DICOM file are utilized as steganography data as depicted in Figure 15.

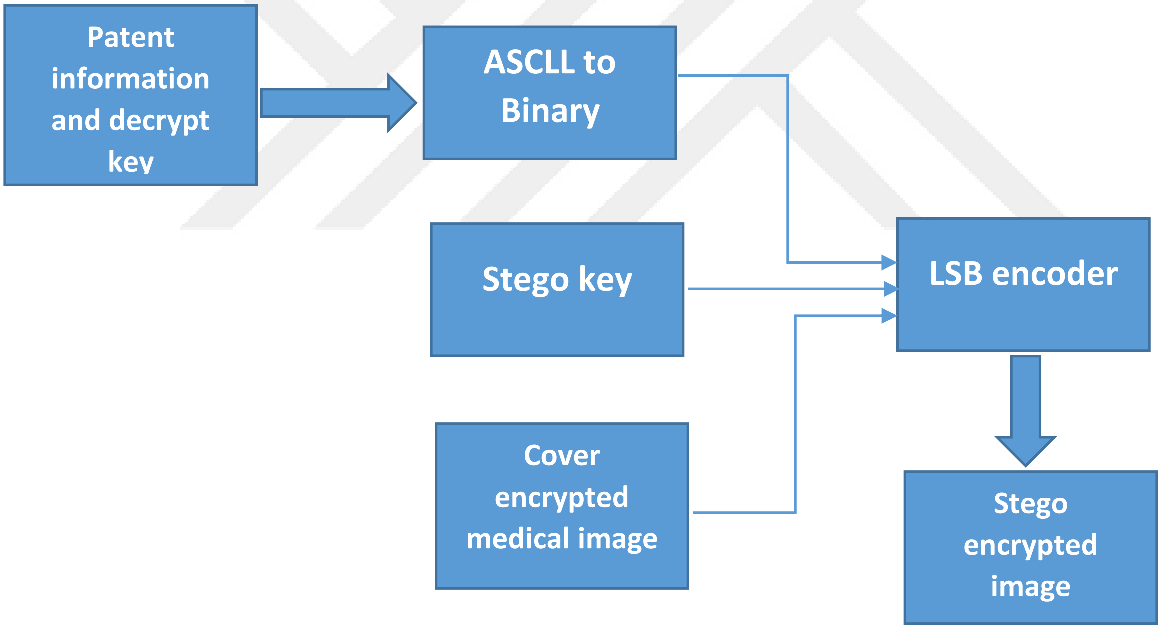

Patent information and decrypt key
ASCLL to Binary
Stego key
LSB encoder
Cover encrypted medical image
Stego encrypted image

Figure 15: The block diagram of LSB embedding in encrypted medical image

This operation increases the power in securing the medical content and its benefits are illustrated as follows:

- Medical image encryption before steganography is an important aspect in protection patient privacy and gives the doctor option to decide, whether he wants to open the medical image or just wants to read the medical record without seeing the image
- Steganography widely used in Providing security goals and image authenticity is one of the importance one, by extraction of the steganography by the reception in successful manner
- Instead of sending the cryptography key separately and make it vulnerable to be lost or objected by adversary when sending it to the reception, the sender embed it into the encrypted medical image.
- Provide safe transfer for the medical related information that describe the patient health state when hiding it in the medical image as steganography data.

3rd step illustrate the propose system steps of embedding steganography data in the encrypted medical image as shown in the Table 3. Figure 16 show the input encrypted image and output stego-encrypted image.

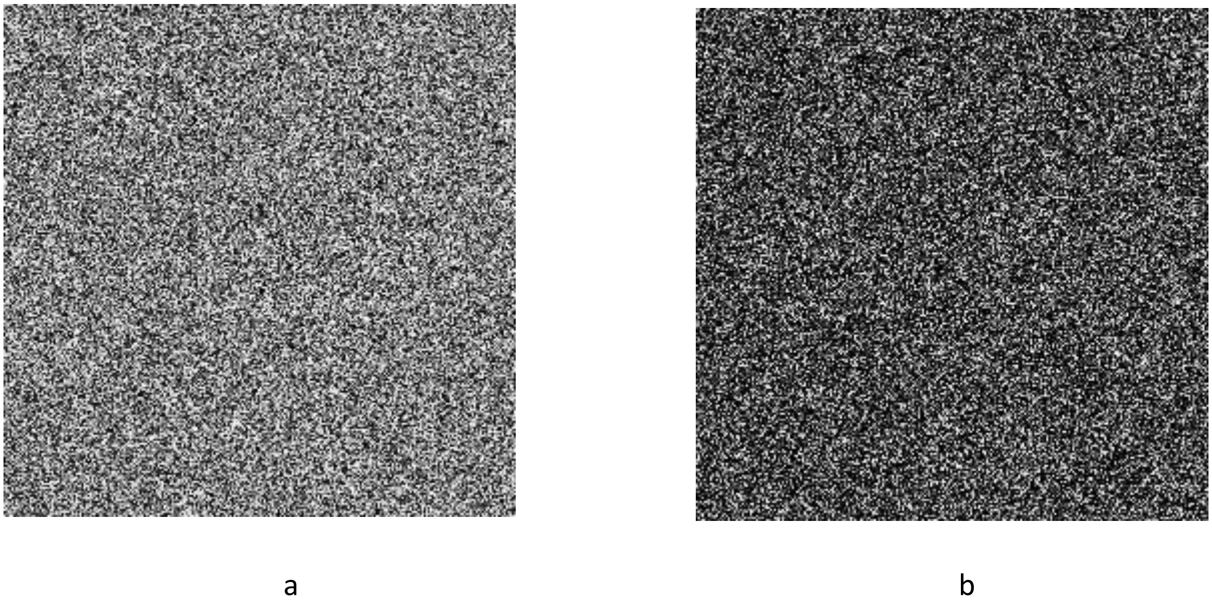


Figure 16: (a) input encrypted image, (b) output stego decrypted image

Table 3: Patient info hiding steps

3rd step	The embedding process for Medical informaition
Input	PNG encrypted medical image
Output	Encrypted Medical image, steganography data, steganography key
	Bedin
Step 1	Read the encrypted medical image and store it into 2D array of pixels
Step 2	Read the text file that contain the related medical meta information and the encryption secret key
Step 3	Convert the text data into binary form to use it as stegongraphy data
Step 4	Select the first pixel, then take a characters from the Stego- key and put it in the first Pixel Component.
Step 5	Put a termination symbol to signify they key ending. Here the symbol used is “0” as a termination symbol.
Step 6	Enter the text file characters in each first component of the following pixels by replacing it.
Step 7	The previous step is repeated until embedding is completed for all characters.
Step 8	Repeatedly put termination character to signify the end of data.
Step 9	Write the stego encrypted image into PNG file format.
	End

3.5 The processes of Retrieval

Typically, any information transferred from a place to another, there is a recipient for them on the other side that recipient can be a person or a device and generally, the recipient expects to receive clear and lossless information so they can process it and obtain the desired goal from it. Medical images and related medical information transfer is the point of focus of this thesis; there are a few steps the reception has to perform prior to being able to use them or find out their content and will be illustrated as follow:

3.5.1 Steganography extraction

Steganography extraction is the first step done by the recipient and by utilizing the same key that has been utilized for hiding data in encrypted medical image. In general, the procedure of image decryption is not possible without steganography extraction due to the fact that steganography data is made up of the image decryption key and is completely dependent on it. This step is performed with the use of the same steganography key, Figure 17 illustrates the block diagram of the extraction at the recipient end.

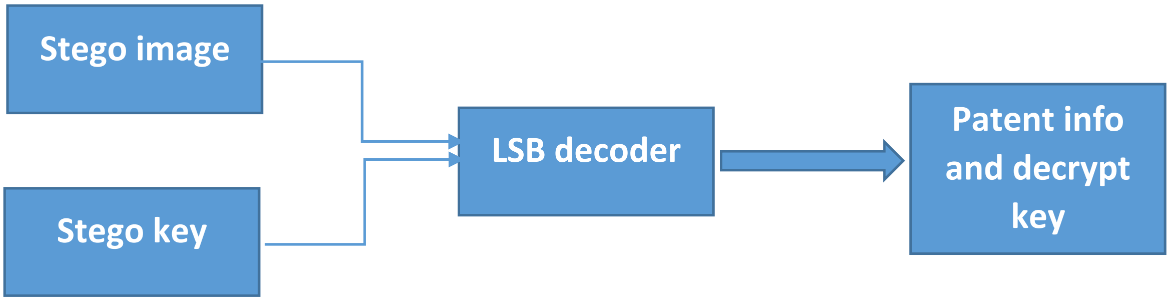


Figure 17: LSB extraction Mechanism

4th step illustrate the steganography extraction steps from the encrypted medical image as shown in the Table 4.

Table 4: Patient info extraction steps

4th step	Meta data extraction
Input	PNG stego encrypted medical image
Output	steganography Data (Medical information, encryption secret key)
	Bgin
Step 1	Read the stego encrypted medical image and store it into 2D array of pixels
Step 2	Extract stego-image pixels.
Step 3	Staring with the first pixel and extracting stego-key characters from the pixel's first Component. Follow the Step 3 up to terminating symbol, or else go to the Step 4.
Step 4	If there was a match between the extracted key and the other key which was inserted by the receiver, then go to the upcoming step, or else the program is terminated.
Step 5	Provided that the key was acceptable, then move to the next pixels and the characters of the secret message will be extracted from the first component of the next pixels. Move to Step 5 until up to the terminating Symbol, or else move to the next step.
Step 6	Save the retrieved steganography data into text file
	End

3.5.2 Medical image decryption and retrieval

It is a very important operation and has to be done carefully and retrieved in the best manner as possible, due to the fact that any loss in the medical image content resulted from this procedure will make some distorting impacts or erasure to some important details in the medical image which lead to misjudgment by the doctor and he will have difficulty determining patient's health state.

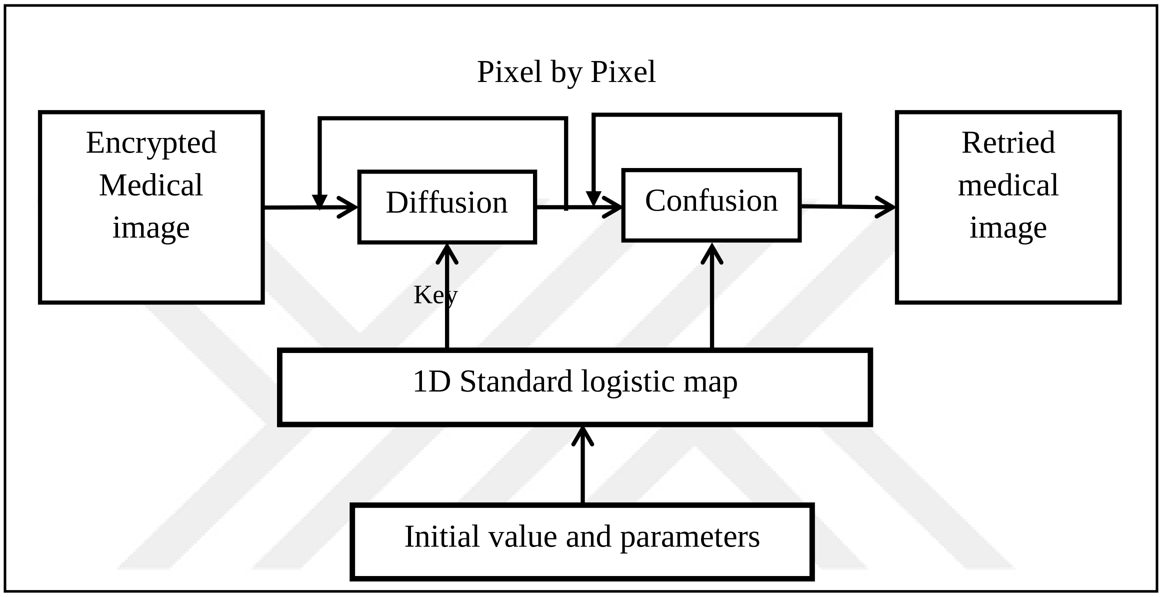


Figure 18: Block diagram of medical image decryption process

The process of decryption of medical images in this study is shown in Figure 18, it is nothing more than retracing the processes of encryption, but backwards; afterwards, the recipient obtains the private key of the encryption which has been embedded as steganography in the encrypted image and can easily be used in the SLM for the generation of the random values used in the encryption, where the pixel value back to its original value prior to the encryption by performing the diffusion step first and then the confusion and restore pixels to their initial locations that were presented in the image prior to encryption, decryption procedure illustrated in **5th** step, figure 19 show input encrypted image and output decrypted image, Table 5 show the steps for **5th** step.

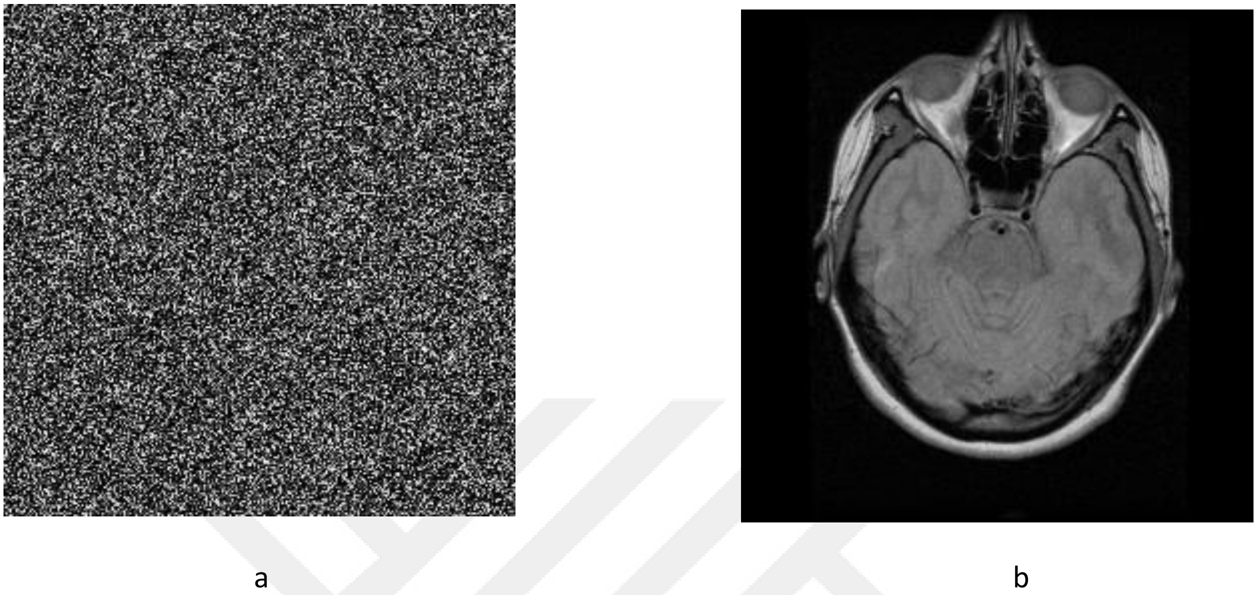


Figure 19: (a) input encrypted image, (b) output decrypted image

Table 5: Medical image decryption steps

5th step	**Medical Image Decryption**
Input	Encrypted PNG medical image
Output	Original PNG medical image
	Begin
Step 1	Read encrypted medical image and store it into 2D array of pixels
Step 2	Search in the text file that contain the extracted steganography data about the used encryption secret key
Step 3	Enter the secret key into the 1D SLM

Step 4	Itrate the 1D SLM for all image pixels
Step 5	Diffuse the image pixels depending on the generated values from the (SLM) and perform inverse transformation to return the pixels to their original values
Step 6	Conffuse the image pixels in which bring them back to their original locations before encryption depending on the values generated by the (SLM)
Step 7	Write and store resulted image pixels into PNG file formate
	End

Results

4.1 Introduction

In this chapter, we will show the results of our system steps that lead to building a cloud system able to extract medical images and patient information from DICOM files, and encrypt any medical images and hide the patient info inside it in order to secure data during transmission, and provide secure access to doctors using an authentication application which can access the cloud and retrieve patient information and decrypt the medical images.

The results of the proposed system were carried out inside:

1. MATLAB 2016: A high-level language and interactive environment used by millions of engineers and scientists worldwide. We use it to extract medical image pixel data from DICOM files and store them as PNG image files.
2. Oracle 10g is an object-relational database management system to store data and secure them by creating a backup for medical information data. We use Oracle 10g to store patient information produced from a partitioned DICOM file. Oracle 10g is the best database management software that one can use.
3. The overall system is built using Java SE version 8, graphic user interfaces and an encryption process in addition to steganography and a decryption process. The Java programming language is one of the top preferences for software developers struggling for sovereign with C and C-based languages. Its features are used on most common electronic devices, such as PCs, mobile terminals or media players.
4. NetBeans IDE 8.0.2 is known for the Java Integrated Development Environment (IDE) with its easily merging of language backing and other features into any of the default packages. NetBeans Marketplace allows for practically unbounded customization and extension.

4.2 System design

The main system consists of two main parts, the first being three applications (Clint, cloud, Clint), as shown in Figures 20 and 21. And the second of which is a part of an Oracle database:

1. First application (medical device clinic application) that can extract medical images and patient information from a DICOM file and encrypt images and upload them with patient information to the cloud over TCP/IP.
2. Second application (doctor application) that can access the cloud and decrypt steganography to retrieve patient information, decrypt medical images and display the results to the doctor.
3. Third application that is inside the cloud and performs the steganography method to conceal patient information inside an encrypted image base at the request of the doctor.

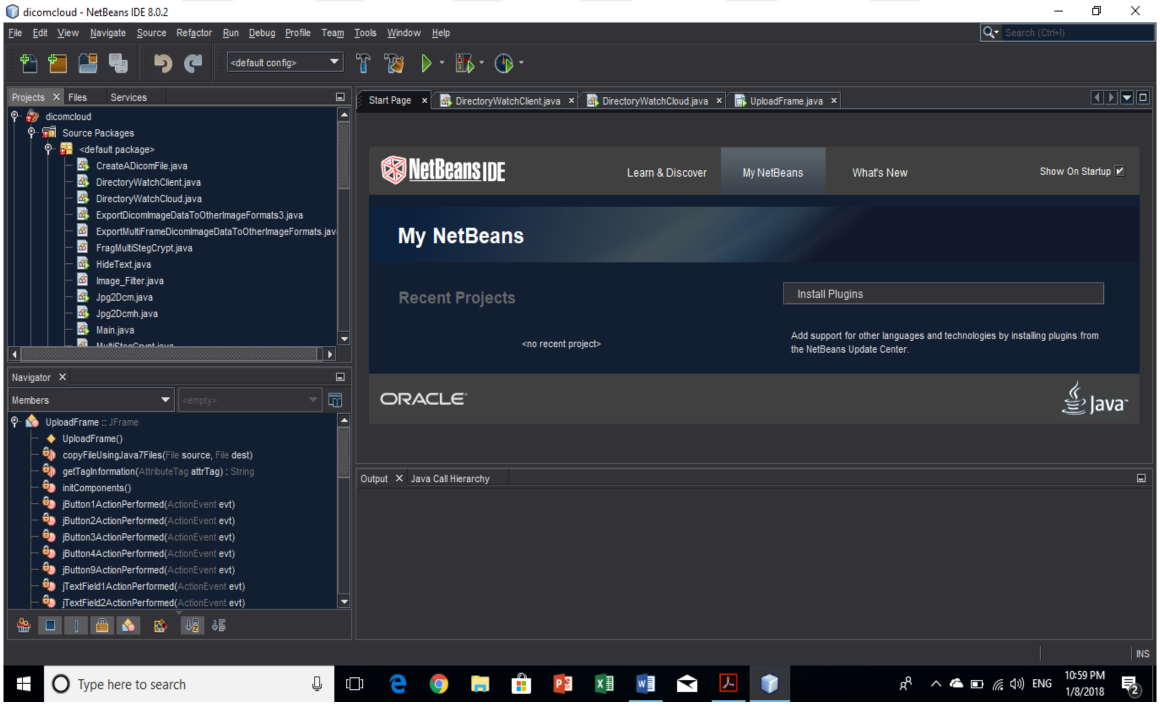
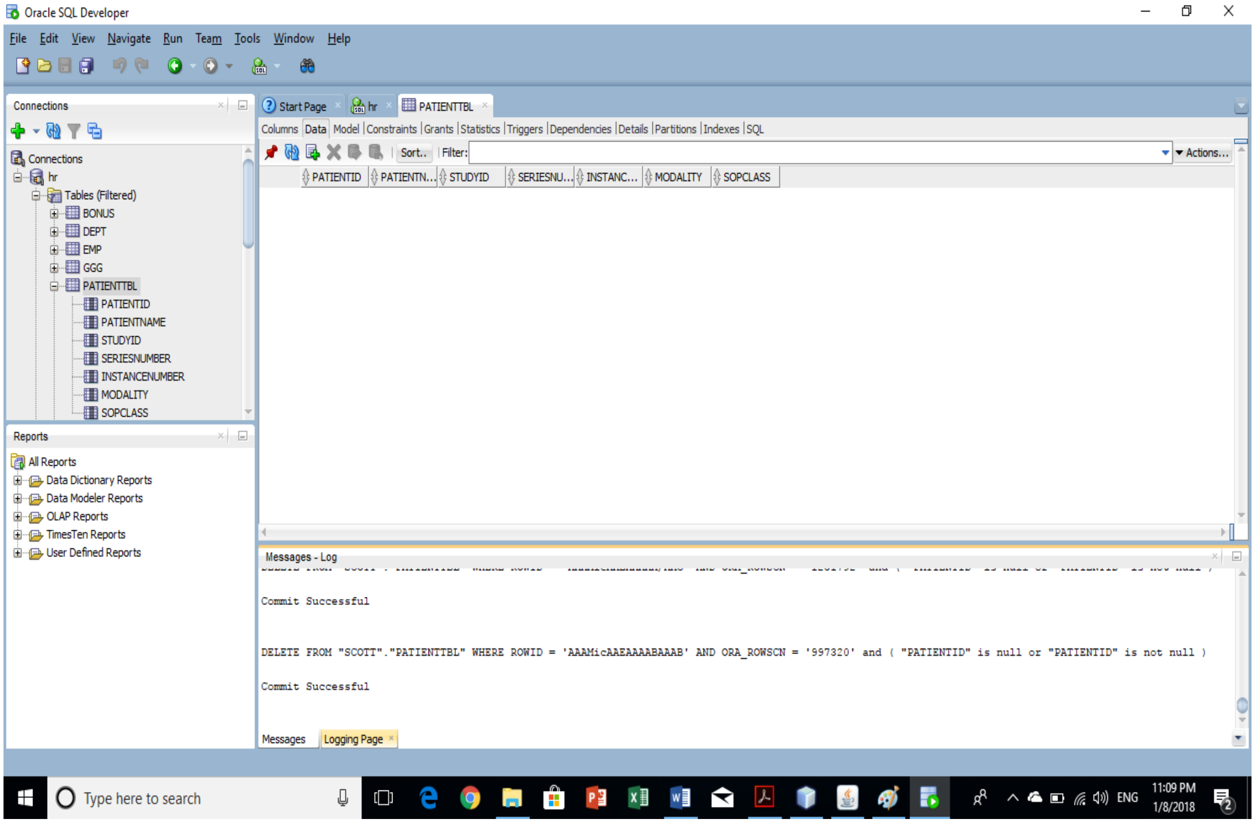

dicomcloud - NetBeans IDE 8.0.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
<default config>
Projects Files Services
dicomcloud
Source Packages
<default package>
CreateADicomFile.java
DirectoryWatchClient.java
DirectoryWatchCloud.java
ExportDicomImageDataToOtherImageFormats3.java
ExportMultiFrameDicomImageDataToOtherImageFormats.jav
FragMultiStegCrypt.java
HideText.java
Image_Filter.java
Jpg2Dcm.java
Jpg2Dcmh.java
Main.java
Start Page
DirectoryWatchClient.java
DirectoryWatchCloud.java
UploadFrame.java
NetBeans IDE
Learn & Discover
My NetBeans
What's New
Show On Startup
My NetBeans
Recent Projects
<no recent project>
Install Plugins
Add support for other languages and technologies by installing plugins from the NetBeans Update Center.
ORACLE
Java
Navigator
Members
<empty>
UploadFrame :: JFrame
UploadFrame()
copyFileUsingJava7Files(File source, File dest)
getTagInformation(AttributeTag attrTag) : String
initComponents()
jButton1ActionPerformed(ActionEvent evt)
jButton2ActionPerformed(ActionEvent evt)
jButton3ActionPerformed(ActionEvent evt)
jButton4ActionPerformed(ActionEvent evt)
jButton9ActionPerformed(ActionEvent evt)
jTextField1ActionPerformed(ActionEvent evt)
jTextField2ActionPerformed(ActionEvent evt)
Output
Java Call Hierarchy
INS
Type here to search
ENG
10:59 PM
1/8/2018

Figure 20: First part of the main system (three apps)

4. The second main part of our system is the Oracle database containing seven attributes, namely PATIENTID, PATIENTNAME, STUDYID, SERIESNUMBER, INSTANCENUMBER, MODALITY, and SOPCLASS to store patient information produced from the DICOM from the partition.

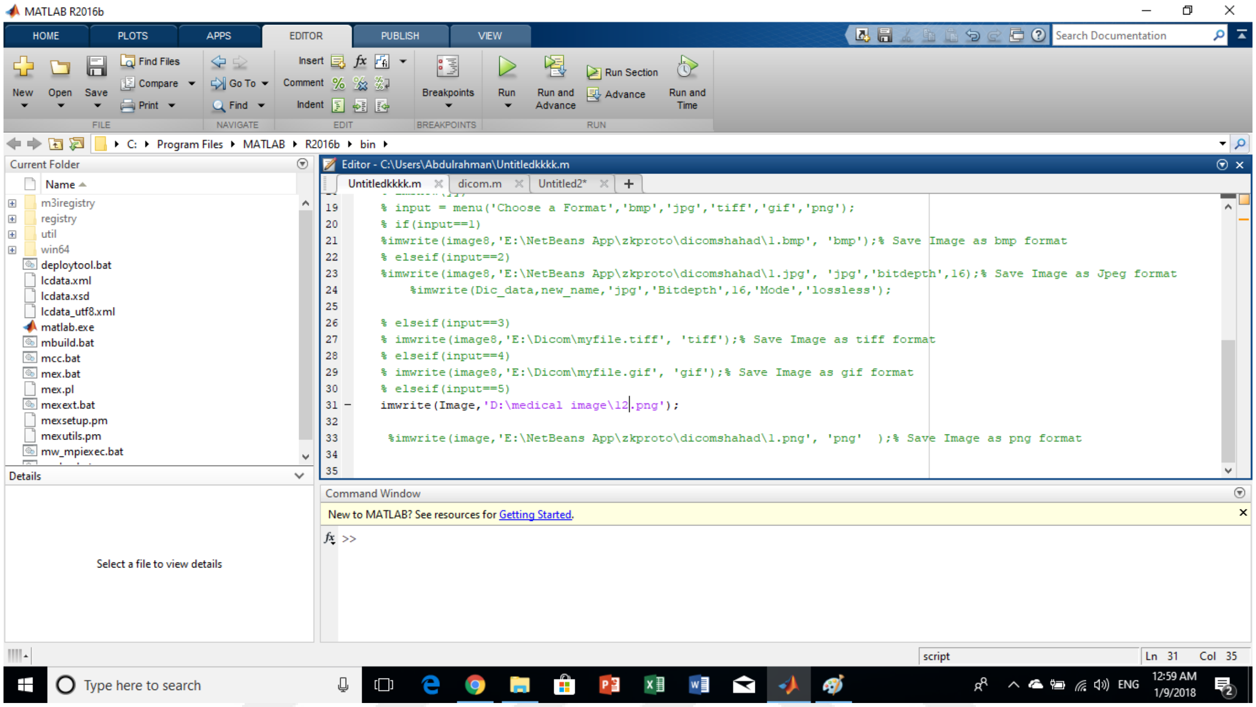


```
Commit Successful

DELETE FROM "SCOTT"."PATIENTTBL" WHERE ROWID = 'AAAMicAAEAAAABAAAB' AND ORA_ROWSCN = '997320' and ( "PATIENTID" is null or "PATIENTID" is not null )

Commit Successful
```

Figure 21: Second part of the main system (oracle database)

4.2.1 DICOM file partition

The first step of our system was the DICOM file partition to extract medical image pixels from the DICOM file data and store it in a PNG file using MATLAB in order to prepare the medical image for encryption, as shown in Figures 22 and 23.



```
% input = menu('Choose a Format','bmp','jpg','tiff','gif','png');
% if(input==1)
%imwrite(image8,'E:\NetBeans App\zkproto\dicomshahad\1.bmp', 'bmp');% Save Image as bmp format
% elseif(input==2)
%imwrite(image8,'E:\NetBeans App\zkproto\dicomshahad\1.jpg', 'jpg','bitdepth',16);% Save Image as Jpeg format
    %imwrite(Dic_data,new_name,'jpg','Bitdepth',16,'Mode','lossless');

% elseif(input==3)
% imwrite(image8,'E:\Dicom\myfile.tiff', 'tiff');% Save Image as tiff format
% elseif(input==4)
% imwrite(image8,'E:\Dicom\myfile.gif', 'gif');% Save Image as gif format
% elseif(input==5)
imwrite(Image,'D:\medical image\12.png');

 %imwrite(image,'E:\NetBeans App\zkproto\dicomshahad\1.png', 'png'  );% Save Image as png format
```

New to MATLAB? See resources for Getting Started.

```
>>
```

Figure 22: MATLAB code for extract medical image

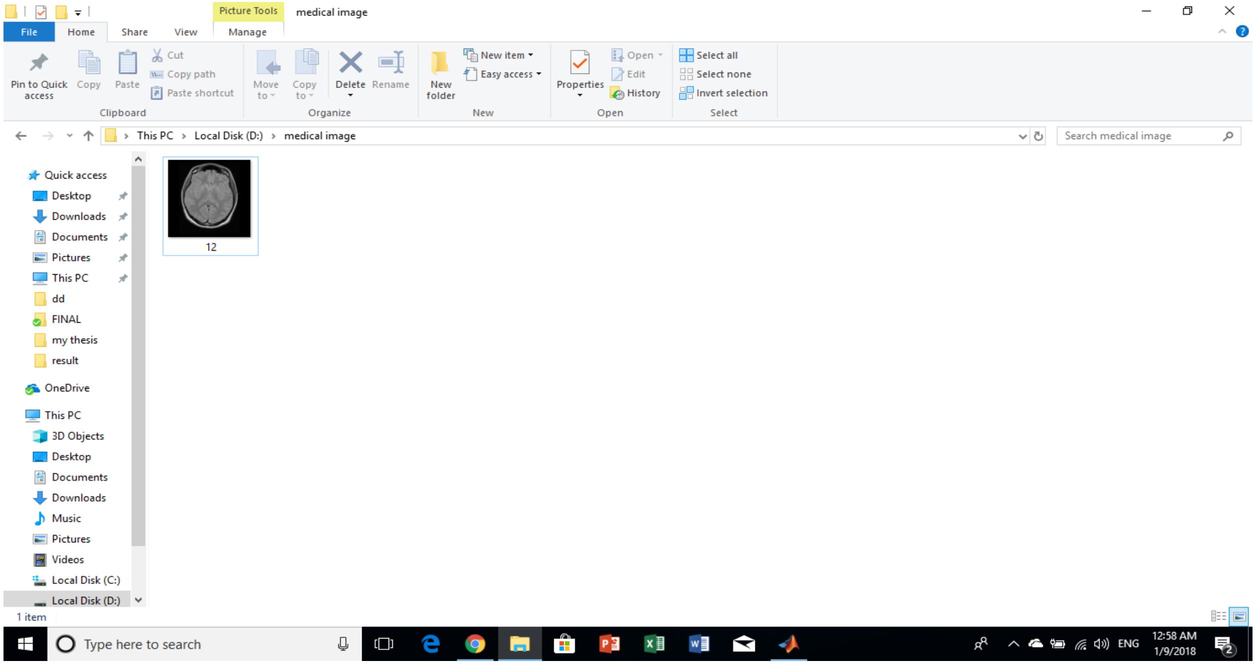


Figure 23: Medical image extracted

4.2.2 First application

In this application, three main steps are performed, the first of which is to partition the DICOM file. The second step is image encryption followed by uploading data to the cloud over TCP/IP as the third step.

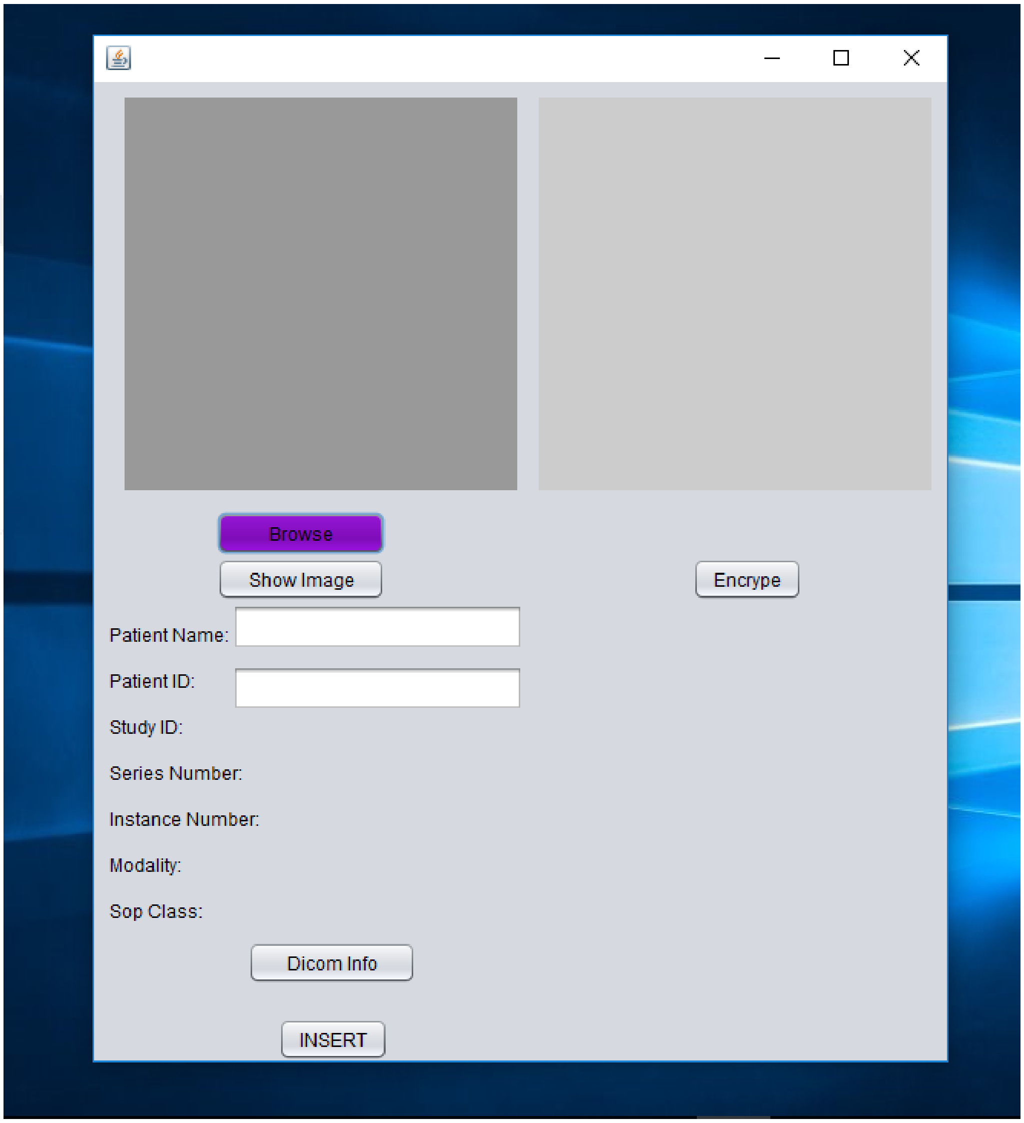
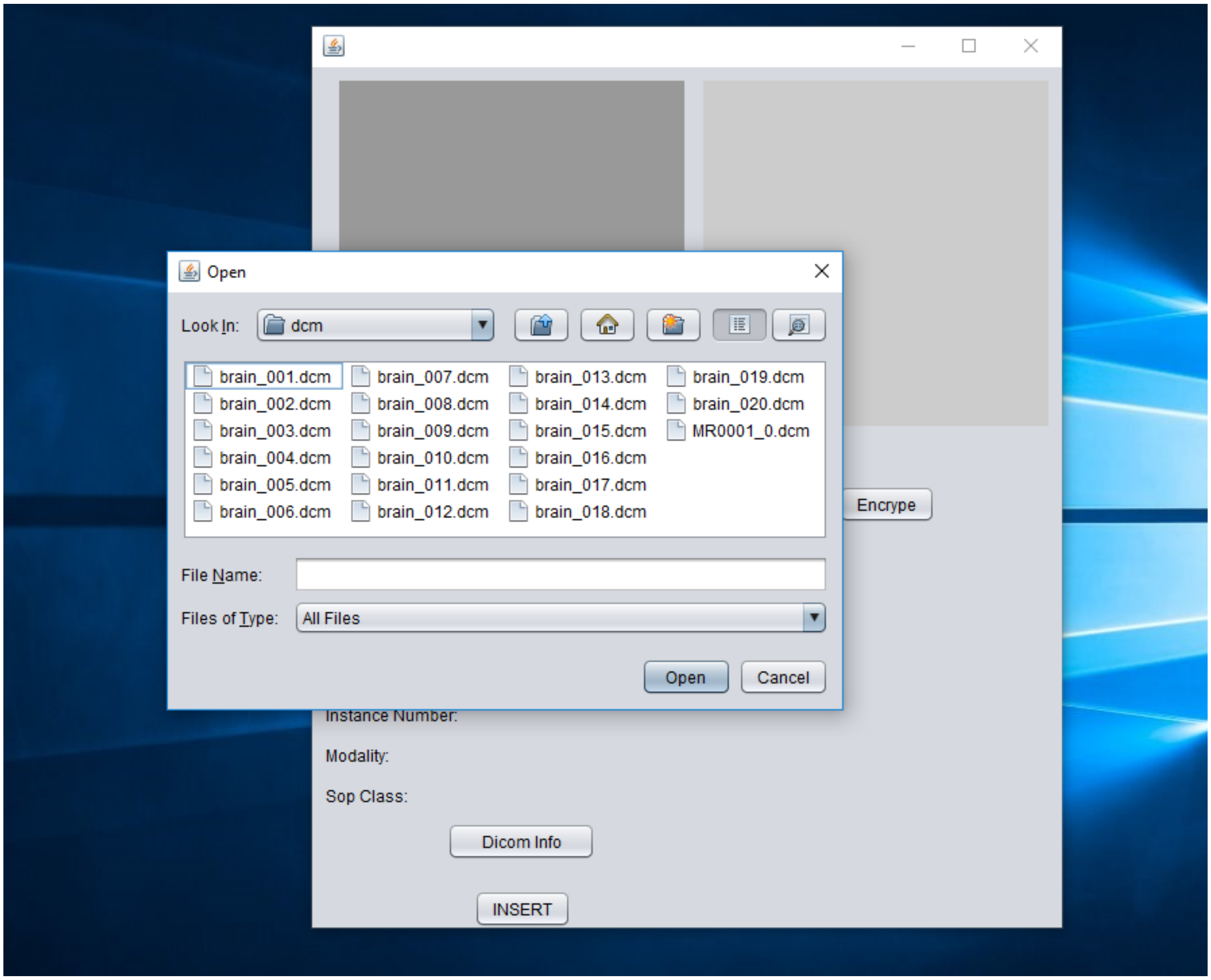


Figure 24: First application

This application includes five buttons, as shown in Figure 24, showing browse, show image, DICOM info, encrypt and insert. Clicking the browse button opens the navigate window in order to select a DICOM. The file on which we want to work is shown in Figure 25.


Look In: dcm

File Name:

Files of Type: All Files

Figure 25: First application (browse button)

After selecting the DICOM file using the browse button, partitioning of the DICOM file is performed to split the medical image and patient information by clicking on the show image button. The medical image will display in the specific label in the application, as shown in Figure 26.

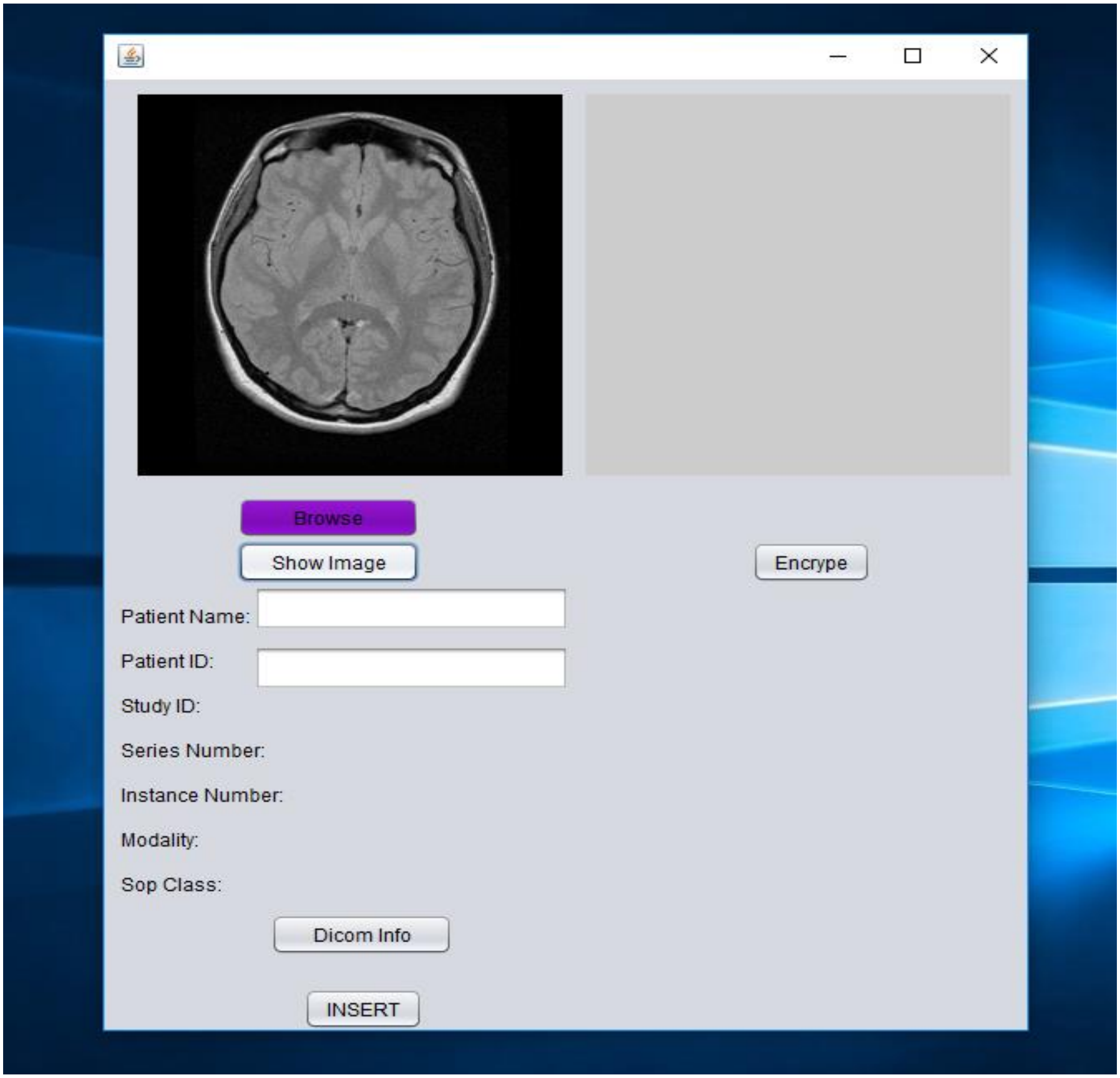
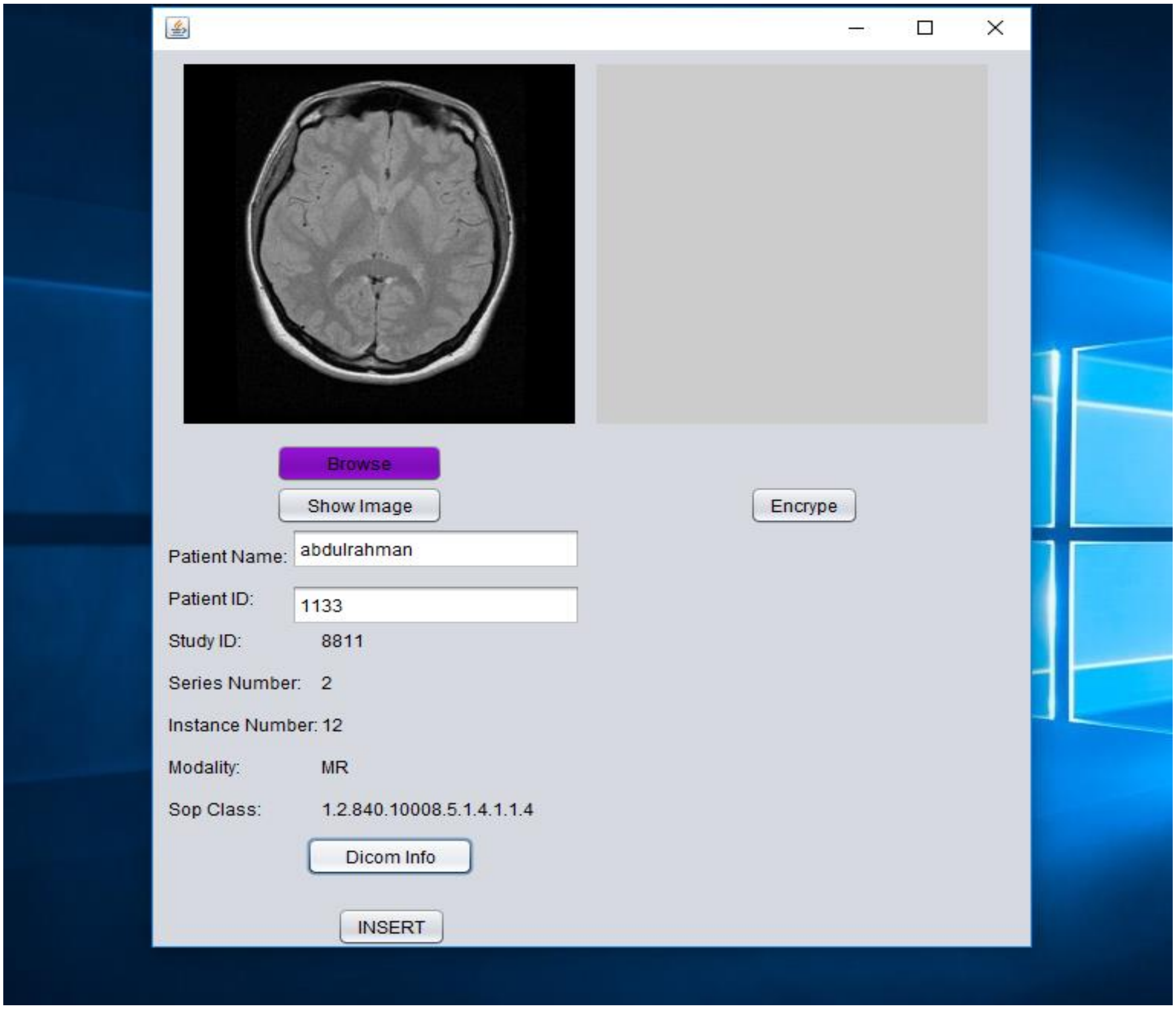


Figure 26: First application (show image button)

The second step of partitioning the DICOM file is to obtain patient information, after showing the image, by clicking on the DICOM information button, patient information will appear in its specific section inside the application, as shown in Figure 27. The application user also should write the patient ID and patient name in the specific section before uploading information to the cloud.



Patient Name: abdulrahman

Patient ID: 1133

Study ID: 8811

Series Number: 2

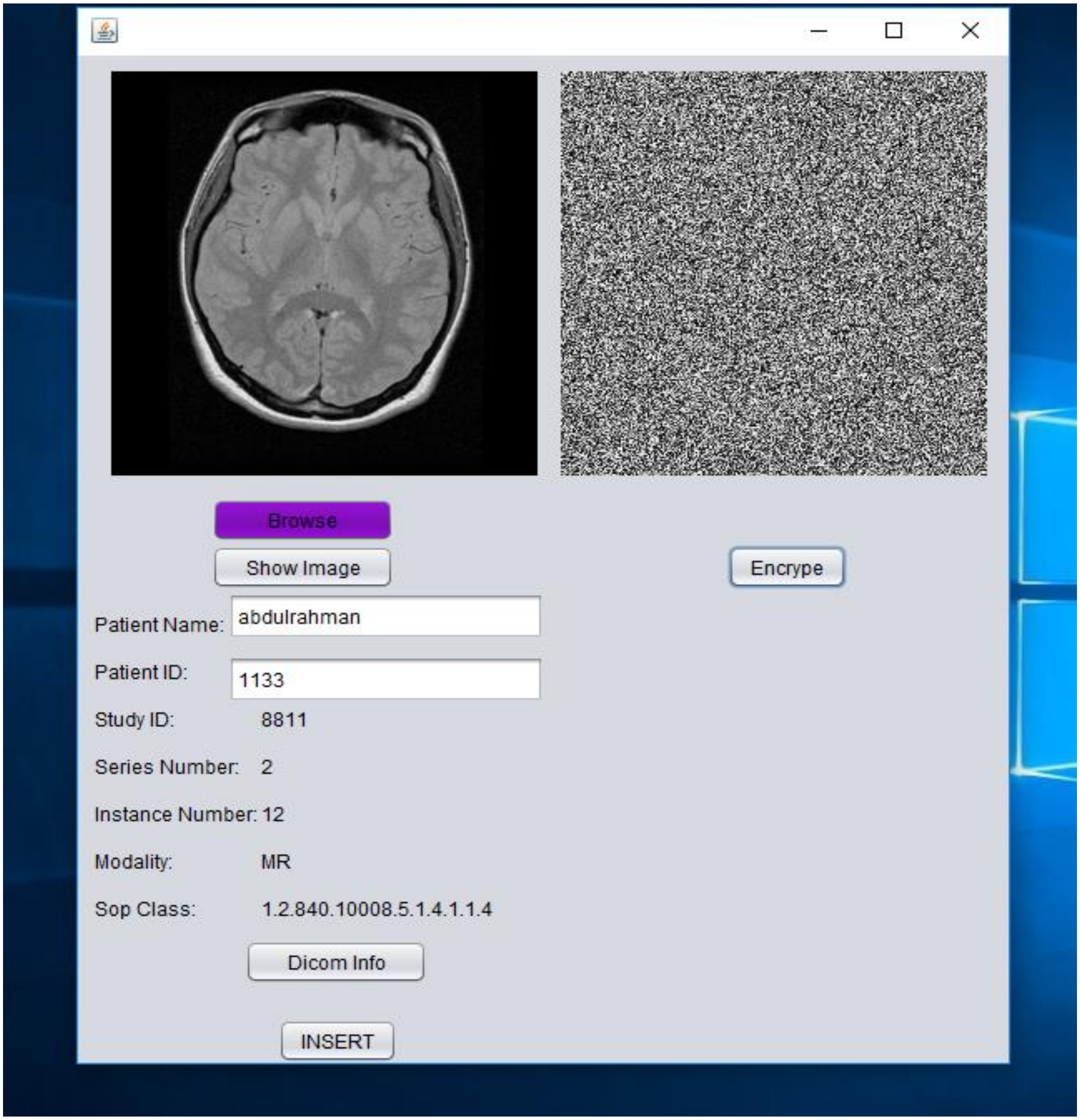
Instance Number: 12

Modality: MR

Sop Class: 1.2.840.10008.5.1.4.1.1.4

Figure 27: First application (DICOM info button)

After DICOM partition is done, the encryption process for the extracted medical image is performed by clicking on the encrypt button, as shown in Figure 28.



Patient Name: abdulrahman

Patient ID: 1133

Study ID: 8811

Series Number: 2

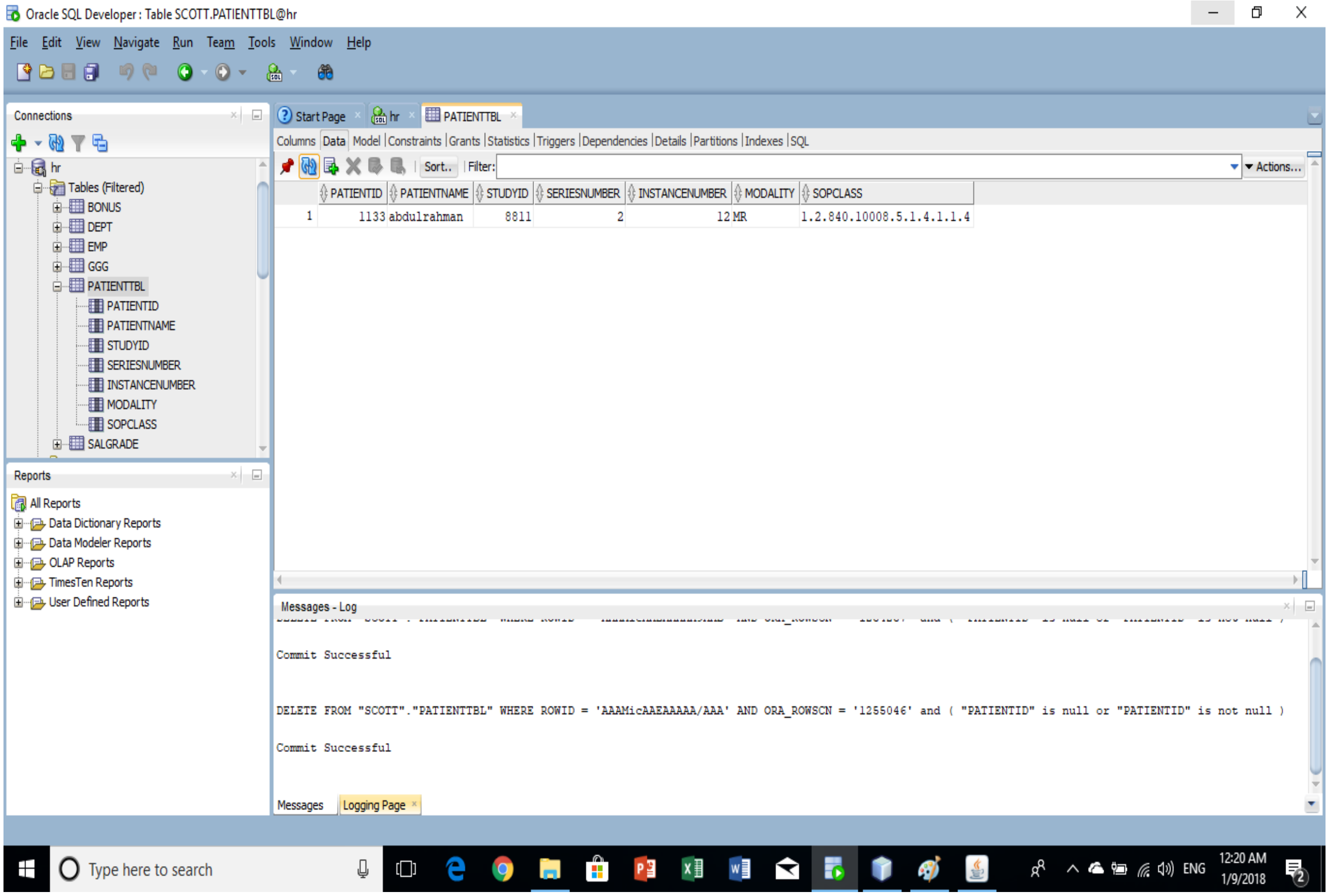
Instance Number: 12

Modality: MR

Sop Class: 1.2.840.10008.5.1.4.1.1.4

Figure 28: First application (encrype button)

After clicking on the INSERT button, the encrypted image with Meta information is uploaded to the cloud. The Meta information is stored inside an Oracle database, as shown in Figure 29.



	PATIENTID	PATIENTNAME	STUDYID	SERIESNUMBER	INSTANCENUMBER	MODALITY	SOPCLASS
1	1133	abdulrahman	8811	2	12	MR	1.2.840.10008.5.1.4.1.1.4

```
Commit Successful


DELETE FROM "SCOTT"."PATIENTTBL" WHERE ROWID = 'AAAMicAAEAAAAA/AAA' AND ORA_ROWSCN = '1255046' and ( "PATIENTID" is null or "PATIENTID" is not null )

Commit Successful
```

Figure 29: Meta info stored inside oracle database

4.2.3 Second and third applications

In the second application, three main steps are performed, the first of which is to request a medical image using the patient ID, as shown in Figure 30.

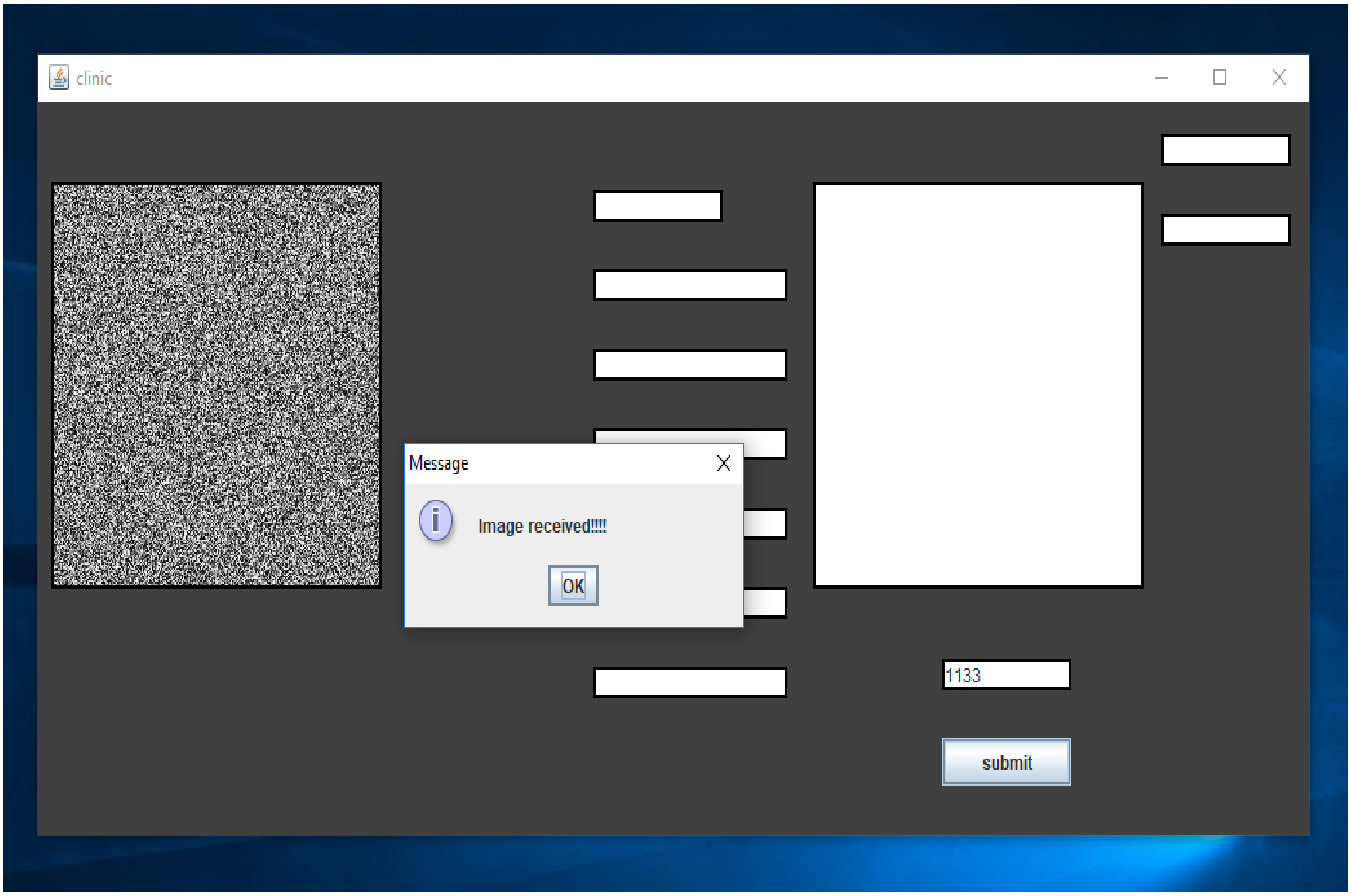
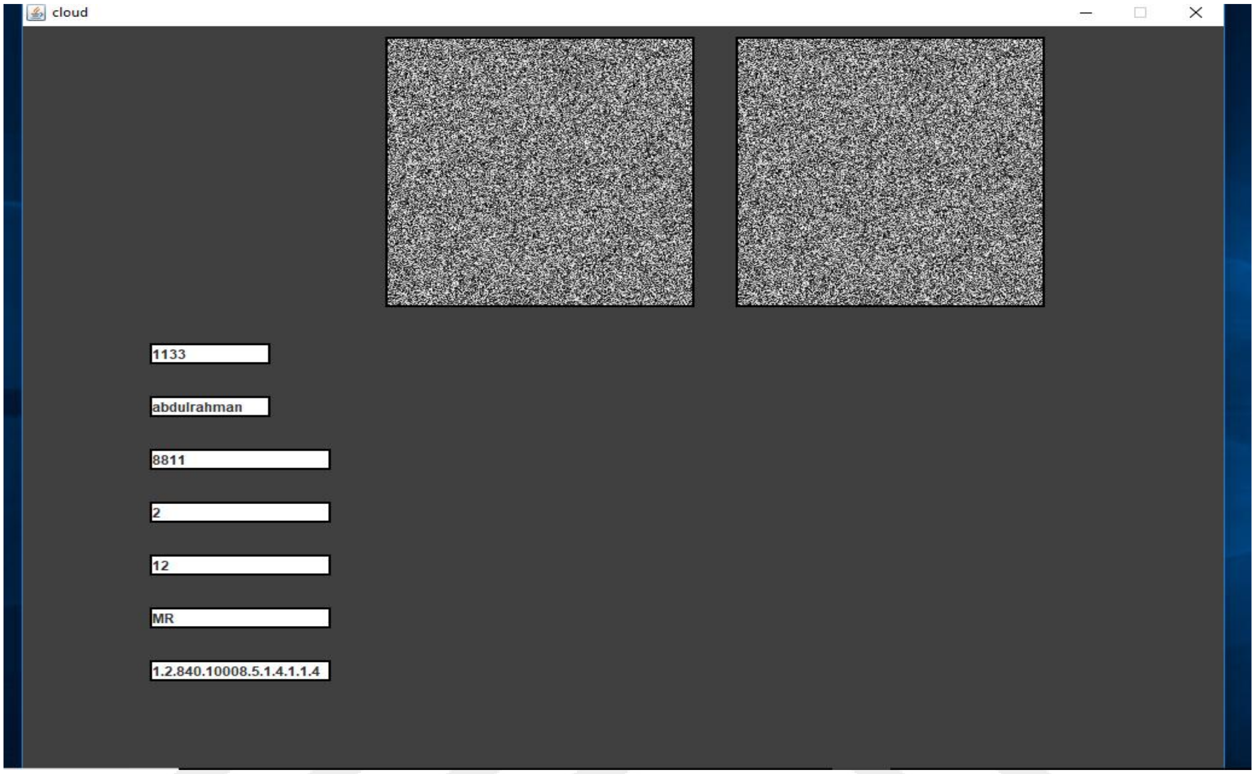


Figure 30: Second application (used ID to request image)

Depending on this request, the third application inside cloud performs the steganography method to hide Meta information inside the encrypted image and send it to the doctor application, as shown in Figure 31.



1133

abdulrahman

8811

2

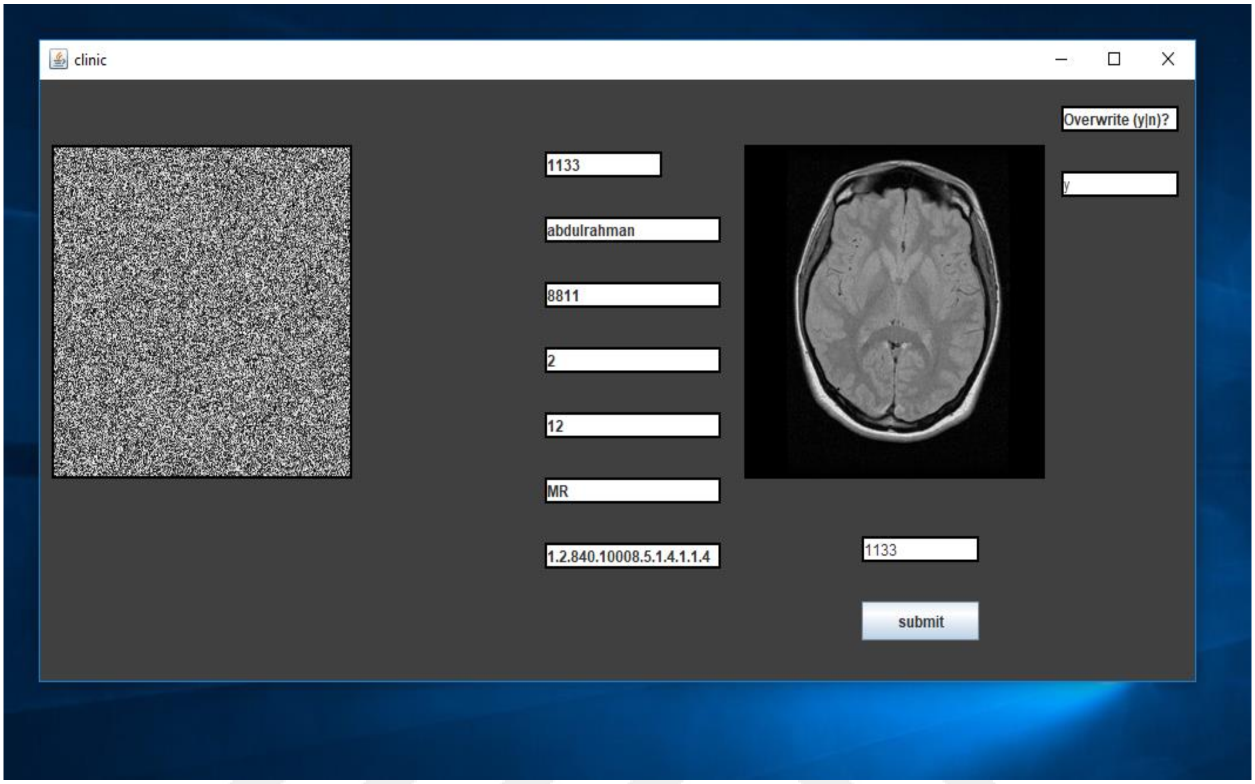
12

MR

1.2.840.10008.5.1.4.1.1.4

Figure 31: Third application (hide Meta info inside encrypted image)

After sending a stero-encrypt image from the cloud, the doctor application performs the second step in order to retrieve Meta information from the encrypted image the final step is to decrypt the encrypted image and display the results, as shown in Figure 32.



clinic

Overwrite (y|n)?

y

1133

abdulrahman

8811

2

12

MR

1.2.840.10008.5.1.4.1.1.4

1133

Figure 32: Second application (retrieve Meta info and decrypt medical image)

5. System Performance Analyzing

Performance analysis was applied by the Python programming language using the Anaconda environment with a set of 26 DICOM files (CR, CT, MR, and OT). Moreover, medical images have been utilized for more extensive research of the presented system efficiency. Therefore, to check the efficiency of the system, numbers of quality measures have been applied. Those measures comprise the MSE and the PSNR which have been computed via formulas (1) and (2). The structural similarity (SSIM) index address has been utilized for measuring the similarities of the local images as well, which were measured through formula (3). The number of the changing pixel rate (NPCP) and the unified averaged changed intensity (UACI) measurements for checking the number of altered pixels and the number of averaged altered intensity respectively between encrypted images and decrypted ones were also calculated using formulas (4), (5) and (6) respectively (Yue Wu, 2011). Moreover, histogram analysis shows the allocation of pixel values based on density. For encrypted images based on the scatter of pixel values, the cryptanalysis arbitrate for the strength of image encryption algorithm.

$$MES = \frac{1}{MP}\sum_{i=0}^{M-1}\sum_{j=0}^{P-1}[OMI(i,j) - RMI(i,j)]^2 \qquad (11)$$

$$PSNR = 10\log 10\left(\frac{R^2}{MES}\right) \qquad (12)$$

Where R represents the maximal fluctuation in the input image data type, and M and P represent the sizes of the original medical image (OMI) and the retrieved medical image (RMI) (Rabbani, 2011). The attributes of PSNR are under 30 dB, meaning that the quality is low, For example, the distortion caused by embedding is high. A PSNR of over 40 dB means there will be high quality image encryption (Jessica Fridrich).

$$\begin{aligned} SSMI(OMI, RMI) = {} & LC(OMI, RMI)^{\alpha} \\ & xCC(OMI, RMI)^{\beta} \qquad (13) \\ & xSC(OMI, RMI)^{\lambda} \end{aligned}$$

Where OMI are RMI represent the initial and the reconstructed medical images, LC represents the luminance, CC represents the contrast and SC represents the structure of OMI and RMI α, β and λ are greater or equal to 1 and are utilized for weighing the value of each one of the three elements (Rabbani, 2011).

$$D(i,j) = \begin{cases} 0, if\ OMI(i,j) = RMI(i,j) \\ 1, if\ OMI(i,j) = RMI(i,j) \end{cases} \qquad 14$$

$$NPCR: N(OMI, RMI) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \qquad 15$$

$$UACI: U(OMI, RMI) = \sum_{ij} \frac{|OMI(i,j) - RMI(i,j)|}{F.T} \times 100\% \qquad 16$$

Where F represents the largest value of the supported pixel of the image format and T denotes the OMI and RMI size (Yue Wu, 2011).

Prior to going through those metrics, the process of the overall system was depicted in Figures 1, 2 and 3. Those results have been calculated on a PC of an Intel (R) Core (TM) i7-2640M, 2.80 GHz CPU and (RAM) 4.00 GB (3.89 GB usable) of installed memory running Windows 10 (64 bit).

5.1 Quality analysis

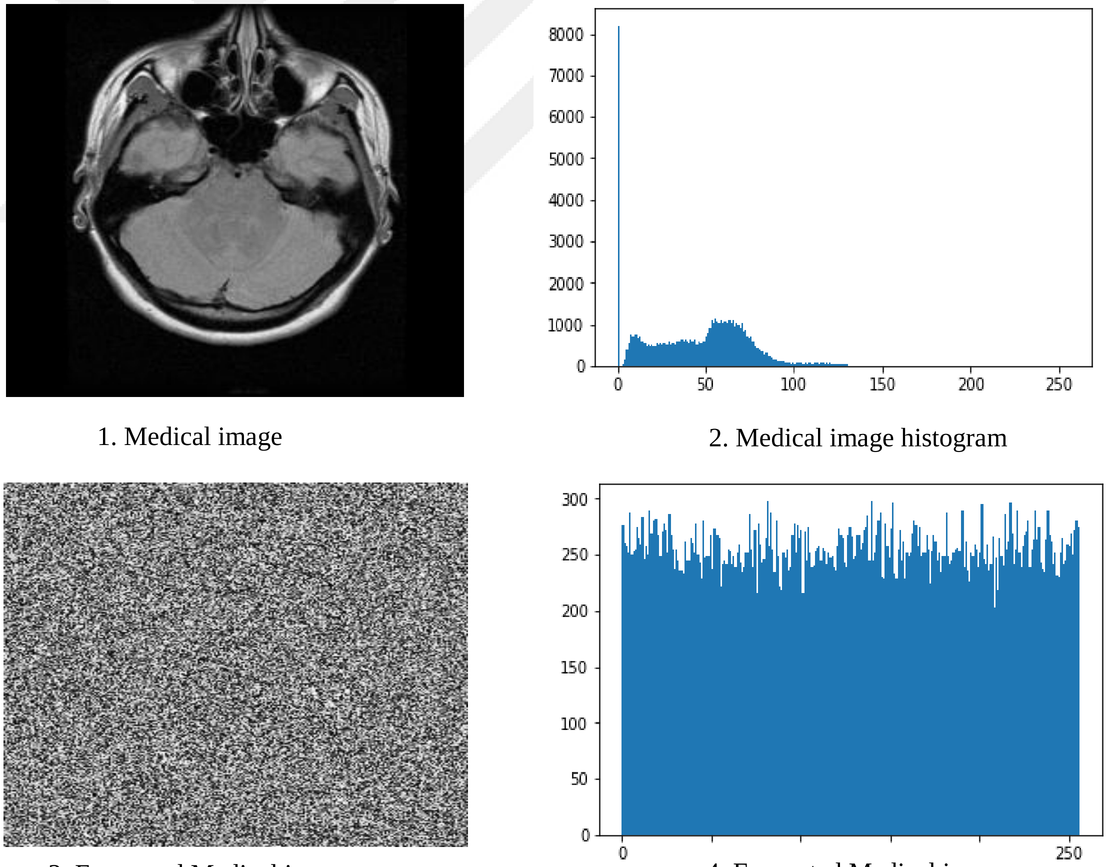
Now, to evaluate the image quality, we selected a sample from the set of used images. Table 6 was constructed to prove that the proposed system offers a guarantee for lossless regeneration of the transmitted images. Moreover, the table indicates to a degree of distortion due to the encryption and steganography processes held throughout system stages. Nevertheless, it ensures very acceptable high-quality outputs, as depicted especially for the SSIM which is considered as an optimal measurement to test similarity in medical images because of the focus on the local instead of the global image similarity and focusing more on the Human Visual System than on peak signal to noise ratio (Rabbani, 2011). Generally, the good performance of the system performance were achieved due to the usage of the chaos logistic map and least significant bit insertion algorithm.

Table 6: Quality evaluation of system

Image	MSE	PSNR(dB)	SSIM	NPCR	UACI
Image1	0.0013427734375	76.95	0.999989256797444	0.131225585938	0.000514610140931371
Image2	0.00131225585938	77.05	0.999988884460064	0.128173828125	0.000502642463235293
Image3	0.00103759765625	77.6	0.99999109275437	0.112915039063	0.000442804074754901
Image4	0.00103759765625	77.97	0.999990162412045	0.103759765625	0.000406901041666665
Image5	0.00128173828125	77.16	0.999989291524351	0.125122070313	0.000490674785539214
Image6	0.00115966796875	77.49	0.999988506418613	0.115966796875	0.000454771752450979
Image7	0.001220703125	77.37	0.999988018665477	0.119018554688	0.000466739430147057
Image8	0.00149536132813	76.30	0.999984424536379	0.152587890625	0.00059838388480392
Image9	0.00143432617188	76.66	0.999985968801158	0.140380859375	0.000550513174019606
Image10	0.000175619834711	75.69	0.999997790332674	0.0175619834711	0.0000688705234159779
Image11	0.000091552734375	88.51	0.99999899415064	0.0091552734375	0.0000359030330882352
Image12	0.000114440917969	87.54	0.999998344114482	0.0114440917969	0.0000448787913602941
Image13	0.00048828125	81.24	0.999996150248731	0.048828125	0.000191482843137254

5.2 Histogram analysis

Image pixel distribution is denoted as a graph known as histogram. Due to the fact that the presented system completely licenses and diffuses pixels of the image, the distribution of the encrypted pixels becomes more symmetrical, and that will supply no valuable information to the attacker, Figure (33), (34), and (35) three sample images and histogram for original images and encrypted CR CT MR images shows whether an attacker attempts to analyze the statistic characteristic of the cipher image from the histogram and attempts for inferring pixel data. This style of attacks is called as a cipher only attack, to which this system is resistant.



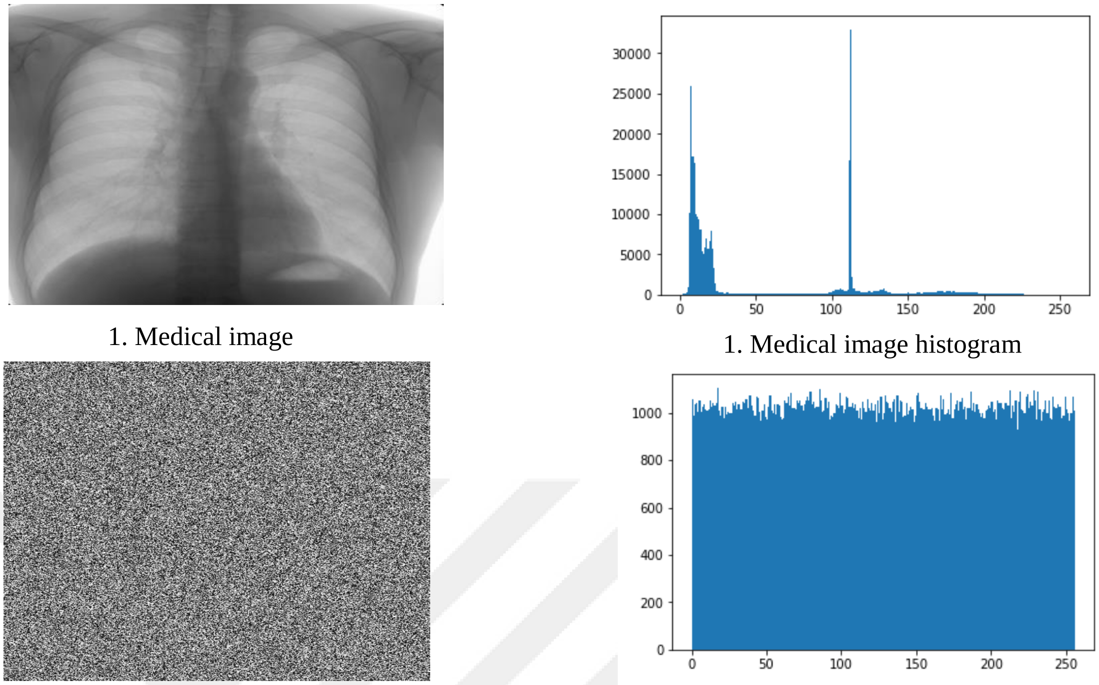
1. Medical image

2. Medical image histogram

3. Encrypted Medical image

4. Encrypted Medical image

Figure 33: histogram analysis MR image



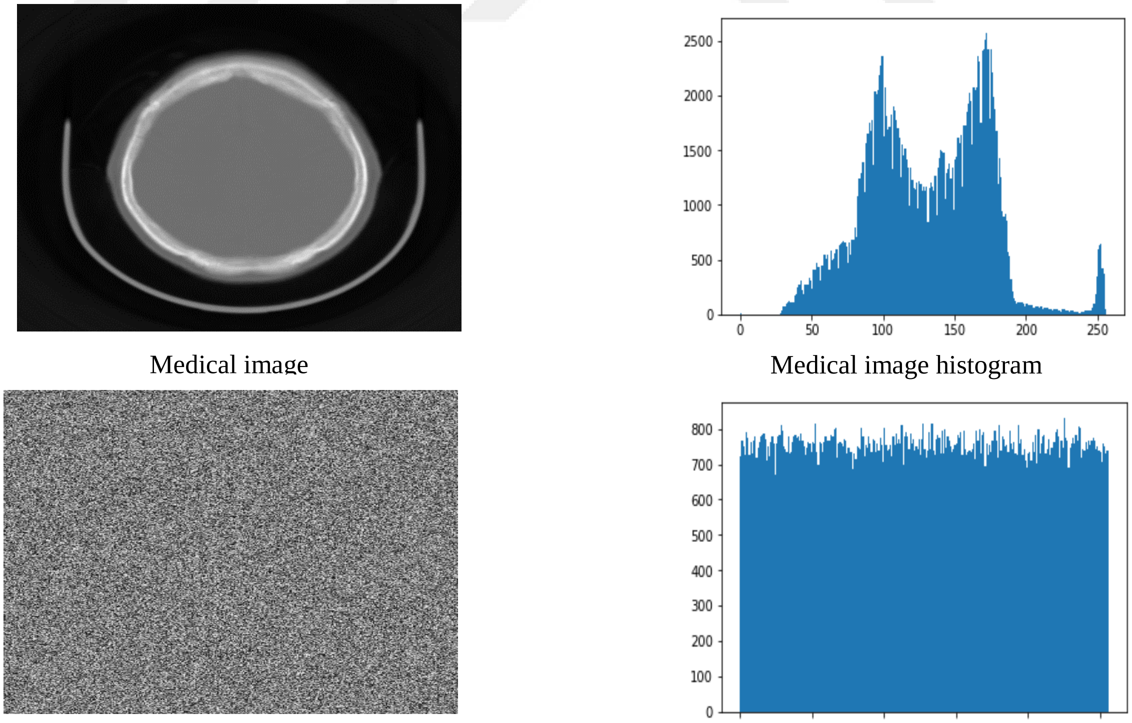
1. Medical image

1. Medical image histogram

3. Encrypted Medical image

4. Encrypted Medical image histogram

Figure 34: Histogram analysis CR image



Medical image

Medical image histogram

3. Encrypted Medical image

4. Encrypted Medical image histogram

Figure 35: Histogram analysis CT image

5.3 Comparison

The scheme presented in (Fatma E.-Z. A. Elgamal, 2013), (Digvijay Singh Chauhan, 2017) and (A.Umamageswari, 2013) also guarantees lossless retrieving of the shared image at the same time maintaining the resulting images from pixels amplification. However, the presented system here preserves the images from pixel expansion; it guarantees very good quality of the obtained images and simultaneously provides high levels of security for the shared data.

Tables (7, 8, and 9) and figure (36) show that our proposed system provides a higher degree of robustness in comparison to (Fatma E.-Z. A. Elgamal, 2013) (Digvijay Singh Chauhan, 2017) And (A.Umamageswari, 2013). This means that our system helps delivering the shared information to the other party with a very good degree of quality.

Table 7: Comparison table with using other algorithms for medical images security

Reference	Used algorithm	PSNR Average
(Fatma E.-Z. A. Elgamal, 2013)	Hybrid spatial and transform techniques	57.4735714
(Digvijay Singh Chauhan, 2017)	DCT and DWT	38.71335
(A.Umamageswari, 2013)	AHF and ACC	60.848
Proposed system	Chaos logistic map & LSB	80.4728571

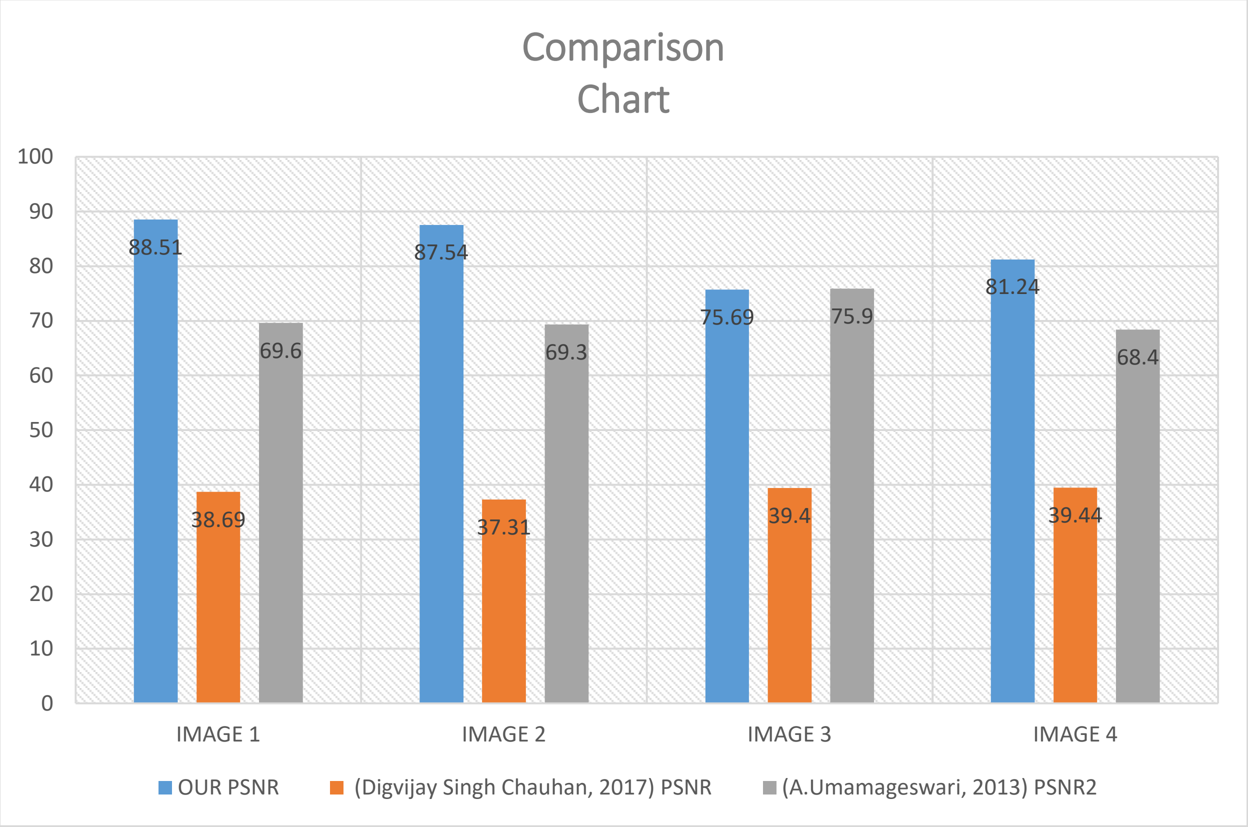
Table 8: Quality evaluation of (Fatma E.-Z. A. Elgamal, 2013)

Image	MSE	PSNR (dB)	SSIM	NPCR	UACI
Image 1	0.0940	58.3988	0.9997	0.3461	0.0031
Image 2	0.0239	64.3420	1.000	0.3306	0.0014
Image 3	0.4962	51.1744	0.9987	0.6604	0.0140
Image 4	0.1408	56.6460	0.9999	0.3412	0.0036
Image 5	0.1337	56.8688	0.9999	0.3861	0.0035
Image 6	0.1017	58.0587	0.9997	0.2612	0.0029
Image 7	0.1350	56.8263	0.9998	0.2718	0.0034

Table 9: Quality evaluation of our system

Image	MSE	PSNR(dB)	SSIM	NPCR	UACI
Image 1	0.00149536132	76.30	0.99998442453637	0.152587890	0.00059838388480392
Image 2	0.00143432617	76.66	0.99998596880115	0.140380859	0.00055051317401960
Image 3	0.00017561983	75.69	0.99999779033267	0.017561983	0.00006887052341597
Image 4	0.00009155273	88.51	0.99999899415064	0.009155273	0.00003590303308823
Image 5	0.00011444091	87.54	0.99999834411448	0.011444091	0.00004487879136029
Image 6	0.00048828125	81.24	0.99999615024873	0.048828125	0.00019148284313725
Image7	0.001220703125	77.37	0.999988018665477	0.119018554688	0.000466739430147057

Figure 36: PSNR Comparison between our system and (Digvijay Singh Chauhan, 2017) (A.Umamageswari, 2013)



5.4 Conclusion

The system established by this research has been able to accomplish the goals stated. With this framework, authenticated and secure communications can be established between three components. The first is an application for a medical image clinic, the second a cloud and the third being a doctor or clinic application with the goal to provide the means of trust managing between the ends of the cloud computing environment taken under consideration as an unsecure environment with which to deal. The system uses well established and common methods to create a system which can authorize, authenticate and secure communications between client and cloud and clinic. Two main algorithms are used in this system: the chaos logistic map algorithm to encrypt medical images that extracted from DICOM file and least significant bit (LSB) for steganography patient information inside the encrypted image. The proposed model assures provision of a lossless retrieving of the shared data, at the same time maintaining the resultant images from pixel amplification while guaranteed a good degree of quality of the obtained images, especially high PSNR values by comparison with other study uses of another algorithm in (Fatma E.-Z. A. Elgamal, 2013) (using a spatial watermarking technique in addition to hybrid spatial and transform techniques), in (Digvijay Singh Chauhan, 2017) (using two-step watermarking such that the first step uses DCT and the other step uses DWT coefficients for embedding), and in (A.Umamageswari, 2013) (using AHF and ACC algorithms). Moreover, the distribution of encrypted pixels has become more symmetrical in our system, thereby providing no meaningful information to an attacker, which means the system can resist cipher only attacks.

5.5 Future work

For future work, we can aim to implement the proposed system using other encryption techniques such as the Advanced Encryption Standard (AES) algorithm with the least significant bit algorithm or the close logistic map with the watermarking method, such the reversible watermark or Discrete Cosine Transform (DCT) and evaluating the results for maximizing the robustness against attacks. Moreover, we may aim to apply the presented methods in different types of medical data and test the corresponding efficiency. Alternatively, we could use the Android application for phones or pads or the iOS application for the iPhone or iPad instead of the doctor’s application to add more flexibility to the system.

6. References

A.Umamageswari, G. (2013). Novel Algorithms for Secure Medical Image Communication Using Digital Signature with Various Attacks . *2013 Fifth International Conference on Advanced Computing (ICoAC).*

Ahmad, M. A. (2012). A Framework to Protect Patient Digital Medical Imagery for Secure Telediognosis. *Procedia Engineering, 28*, 1055 - 1066.

Ahmed Mahmood, C. O. (2013). Improving the Security of Medical Images. *Int Journal of Advanced Computer Science and Applications, 4*.

Ahmed, M. a. (2012). Framework to Protect Patient Digital Imagery for Secure Telediognosis. *Procedia Engineering, 28*, 1055 - 1066.

Akilaa.K, J. a. (2015). Mammographic image enhancement using indirect contrast enhancement techniques. *Procedia Computer Science, 47*, 255 - 261.

Al-Haj, A. (2015). Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. *J Digit Imaging*. doi:0.1007/s10278-014-9734-8

Alliance, C. S. (2009). *Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing.*

Amer, A. A.-H. (2017). Crypto-Watermarking of Transmitted Medical Images. *J Digit Imaging*. doi:10.1007/s10278-016-9901-1

Borko Furht, A. E. (2010). *HandBook of Cloud computing.* Springer Science + business Media, LLC.

Bose, M. Y. (2017). Medical Images are Safe – an Enhanced Chaotic Scrambling Approach. *J Med Syst*. doi:10.1007/s10916-017-0809-1

Chao-Tung, Y. L.-T.-L.-C. (2010). Implementation of a Medical Image File Accessing System on Cloud Computing. *IEEE 13th International Conference on Computational Science and Engineering (CSE).*

Chi-Kwong Chan, L. (2002). *Hiding data in images by simple LSB substitution.* University of Hong Kong, Cheng Department of Computer Engineering and Information Technology, Hong Kong.

Chong Fu, W.-h. M.-f.-l. (2013). An efficient and secure medical image protection scheme based on chaotic maps. *Computers in Biology and Medicine, 43*, 1000-1010.

Dalel Bouslimi, G. C. (2012). A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. *IEEE Transaction on Information Tech in Biomedicine, 5*.

Decker, M. M. (2013). Privacy-preserving data management in eHealth systems. *Int. Conf. on Health and Social Care Information Systems and Technologies, 9*, 1085-1092.

Deshpande Neeta, K. S. (2006). Implementation of LSB Steganography and Its Evaluation for Various Bits. *1st International conference.*

Digvijay Singh Chauhan, A. A. (2017). Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment. *2017 40th International Conference on Telecommunications and Signal Processing (TSP).*

Duipmans, E. F. (2012). *BUSINESS PROCESS MANAGEMENT IN THE CLOUD WITH DATA AND ACTIVITY DISTRIBUTION.* FACULTY OF ELECTRICAL ENGINEERING, MATHEMATICS AND COMPUTER SCIENCE SOFTWARE ENGINEERING.

Dunn, T. T. (2012). *The TECH WORLD*. Retrieved from http://news.techworld.com/security/3415635/ransom-hackers-encrypt-medical-centres-entire-database/

El-Latif, A. (2012). Digital image encryption scheme based on multiple chaotic systems. *Sensing and Imaging, 13*, 67–88.

Faraoun, K. (n.d.). Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption. *Int Journal ofInformation Technology, 7*.

Fatma E.-Z. A. Elgamal, N. A.-C. (2013). Secure Medical Images Sharing over Cloud Computing environment. *(IJACSA) International Journal of Advanced Computer Science and Applications,, 4*, 130-138.

FRIDRICH, J. (1998). SYMMETRIC CIPHERS BASED ON TWO-DIMENSIONAL CHAOTIC MAPS. *International Journal of Bifurcation and Chaos, 6*(8).

Fujitsu Network Communications, I. (. (2006). The TCP/IP Protocol Suite. Fujitsu Network Communications, Inc. (FNC).

G.Kanagaraji, A. (2011). Proposal of an Open-Source Cloud Computing System for Exchanging Medical Images of a Hospital Information System. *3rd International Conference on Trendz in Information Sciences and Computing (TISC).*

Giorgino, T. B. (2006). Health dialog systems for patients and consumers. *Journal of Biomedical Informatics, 39*, 556--57.

H. Huang, R. D. (2014). Medical imaging informatics simulators: a tutorial. *International Journal of Computer Assisted Radiology and Surgery, 9*, 433 – 447.

H. Nyeem, W. B. (2013). review of medical image watermarking requirements for teleradiology. *Journal of Digital Imaging, 26*, 326 – 343.

Hamid R Motahari-Nezhad, B. S. (2009). Outsourcing Business to Cloud Computing Services: Opportunities and Challenges. *IEEE Internet Computing*.

Hao Jianl, Z. F.-n.-w.-j. (2012). The Research of Medical Safety Information Engineering in Hospital Application Study. *Int. Conf on Solid State Devices and Materials Science, 25*, 982-988.

Heurixb, T. N. (2011). A methodology for the pseudonymization of medical data. *International Journal of medical informatics, 80*, 190-204.

Hua Xue, S. W. (2013). Study on One Modified Chaotic System Based on Logistic Map. *Research Journal of Applied Sciences, Engineering and Technology*.

J. Franco-Contreras, G. C.-B. (2014). Robust lossless watermarking of relational databases based on circular C. Roux. *Information Forensics and Security, IEEE Transactions, 9*, 397–410,.

J. M. Blackledge, M. D. (2012). Non-Gaussian Anisotropic Diffusion for Medical Image Processing using the OsiriX DICOM. *International Society for Advanced Science and Technology (ISAST), 4*(1), 24 - 31.

Jani Anbarasi.L, A. M. (2015). DNA based Multi-Secret Image Sharing. *Int. Conf. on Information and Communication Technologies, 46*, 1794-1801.

January, J. K. (2004). Steganography and Steganalysis.

Jardim, S. V. (2013). The Electronic Health Record and its Contribution to Healthcare Information Systems Interoperability. *Procedia Technology, 9*, 940 - 948.

Jessica Fridrich, M. G. (n.d.). *Detecting LSB Steganography in Color and Gray-Scale Images.* State University of New York, Binghamton.

Johnson, N. J. (1998). Exploring Steganography: Seeing the Unseen. *Computer Journal*.

Jose Luis Fernandez-Aleman, I. C. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*, 541-562.

K B Raja, V. K. (n.d.). *"A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images.* University Visvesvaraya, Department of Computer Science and Engineering,, 2004.

Lan, Z. T. (2015). Efficient image encryption with block shuffling. *Multimed Tools Appl*.

Li-Chin Huangc, L.-Y. T.-S. (2013). A reversible data hiding method by histogram shifting in high quality medical images. *The Journals of systems and software, 86*, 716-727.

Lymberopoulos, G. K. (2009). WADA service: an extension of DICOM WADO service. *IEEE Transactions on Information Technology in Biomedicine, 13*, 121 – 130.

M. Yang, N. B. (2004). Data-image-video encryption. *IEEE potentials, 23*, 28–34.

Maglogiannis, P. L. (2016). Sensitive Patient Data Hiding using a ROI Reversible Steganography Scheme for DICOM Images. *J Med Syst*. doi:10.1007/s10916-016-0514-5

Mahmood, Z. H. (2011). Cloud Computing for Enterprise Architectures. *Computer Communications and Networks*.

Mandal, P. C. (n.d.). Modern Steganographic technique: A Survey. *International Journal of Computer Science Engineering Technology*.

Manufacturers, T. A. (n.d.). *http://medical.nema.org*. Retrieved from http://medical.nema.org/Dicom/about-DICOM.html

Manufacturers, T. A. (n.d.). *(NEMA)*. Retrieved from http://medical.nema.org: http://medical.nema.org/Dicom/about-DICOM.html

Mario Mustra, K. D. (2008). Overview of the DICOM Standard. *International Symposium ELMAR-*.

Memon, R. C. (2011). Analysis of LSB based Image Steganography. *IEEE ICIP*, 1022-1022.

Mohammad, E. S. (2009). Chaotic image encryption design using tompkins-paige algorithm. *Mathematical Problems in Engineering*, 1–22.

Mor Peleg, D. B. (2008). ituationBased Access Control: Privacy management via modeling of patient data access scenarios. *Journal of Biomedical Informatics, 41*, I 028-1040.

Muneeswaran.K, M. C. (2015). Hiding of Confidential Data in Spatial Domain Images using Image Interpolation. *Int.I Journal of Network Security, 17*, 722-727.

Mustafa Ulutas, G. U. (2011). Medical image security and EPR hiding using Shamir' s secret sharing scheme. *The Journals of systems and software, 84*, 341-353.

Mustafa Ulutas, G. U. (2011). Medical image security and EPR hiding using Shamir’s secret sharing scheme. *The Journal of Systems and Software*.

N.F. Johnson, S. J. (1998). Staganalysis: The Investigation of Hiding Information. *IEEE*, 113-116.

Narendra K. Pareek, V. P. (2013). Diffusion substitution based gray image encryption scheme. *Digital siginal processing, 23*, 894-991.

Nasim, A. S. (2012). *CHAOS BASED CRYPTOGRPHY AND IMAGE ENCRYPTION.* University of Applied Sciences, Luebeck.

News, C. (2014, 11 03). 4 other cases of stolen health data in alberta. Retrieved from http://www.cbc.ca/news/canada/edmonton/4-other-cases-of-stolen-health-data-in-alberta-

News, C. (2014). *CBC*. Retrieved from http://www.cbc.ca/news/canada/edmonton/laptop-stolen-with-health-information-of-620-000-albertans-1.2507161

Niels Provos, P. H. (2003). Hide and Seek: An Introduction to Steganography. *IEEE computer society*.

O. S. Pianykh. (2008). Digital Imaging and Communications in Medicine (DICOM) APractical Introduction and Survival Guide. *Springer*.

P. Kruus, C. S. (2003). A survey of steganography techniques for image files. *Advanced Security Research Journal.*

Patidar, N. K. (2016). Medical image protection using genetic algorithm operations. *Soft Comput*. doi:DOI 10.1007/s00500-014-1539-7

Petitcolas, R. a. (1998). On the limits of steganography. *IEEE Journal of Selected Areas in Communications, 16*.

Philomina Jees, D. T. (2016). MEDICAL IMAGE PROTECTION IN CLOUD SYSTEM. *INTERNATIONAL JOURNAL OF CURRENT ENGINEERING AND SCIENTIFIC RESEARCH (IJCESR)*. doi:10.21276/ijcesr

Pianykh, O. S. (2008). Digital Imaging and Communications in Medicine (DICOM) A Practical Introduction and Survival Guide. *Springer*.

Prema T. Akkasaligar, S. B. (2016). Secure Medical Image Encryption based on Intensity level using Chao’s theory and DNA Cryptography. *IEEE International Conference on Computational Intelligence and Computing Research*.

Qiu Run-he, C. Y.-Z. (2011). Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption. *4th International Congress on Image and Signal Processing*, 629- 632.

R. Norcen, M. P. (2003). Confidential storage and transmission of medical image data. *Computers in Biology andMedicine, 33*, 277–292.

R.J. Anderson, F. P. (1998). On The Limits of Steganography. *IEEE Journal ofSelected Area in Communicafions*, 474-481.

Rabbani, F. R. (2011). A dual adaptive watermarking scheme in contourlet domain for DICOM images. *BioMedical Engineering*.

RAGHAVA, B. K. (2014). A NOVEL APPROACH FOR MULTIMEDIA ENCRYPTION BASED ON CONFUSION AND CHAOTIC LOGISTIC MAP. *International Journal of Computer Science Engineering, 4*(4), 47-58.

Rajendra Acharya U, D. A. (2011). Compact Storage of Medical Images with Patient Information. *IEEE Transaction on information technology in biomedicine, 5*.

Ran-Zan Wang, C.-F. L.-C. (2000). Hiding data in images by optimal moderately signicant bit replacement. *IEE Electron.*

Rinki Pakshwar, V. K. (2013). A Survey On Different Image Encryption and Decryption Techniques. *Int Journal of Computer Science and Information Technologies, 4*, 113-116.

Samie, F. E. (2013). *Image Encryption: A Communication Perspective.* Boca Raton,FL: CRC Press.

Smith, J. C. (2013). Privacy-preserving screen capture Towards closing the loop for health IT usability. *Journal ofBiomedical Informatics, 46*, 721- 733.

Stallings, W. (2010). *Cryptography and network Security.*

Stallings, W. (2014). *Cryptography and Network Security: principles and practice.* Boston: Prentice Hall,.

Sullivan, T. W. (2014, 08 31). *The Washington Post*. Retrieved from http://www.washingtonpost.com/news/morning-mix/wp/2014/08/19/chinese-hackers-may-have-stolen-your-medical-records/

Syifak Izhar Hisham, A. N. (2017). Numbering with spiral pattern to prove authenticity and integrity in medical images. *Pattern Anal Applic*. doi:0.1007/s10044-016-0552-0

T. Lo, a. G. (2008). Cryptanalysis of an image scrambling scheme without bandwidth expansion. *IEEE Transactions on Circuits and Systems for Video Technology, 18*, 338–349.

T. Morkel, J. E. (2000). *An overview of image steganography.* University of Pretoria, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science .

Ulutas, A. U. (2017). A New Medical Image Watermarking Technique with Finer Tamper Localization. *J Digit Imaging*. doi:10.1007/s10278-017-9960-y

Valarmathi, K. A. (2016). Secured medical image watermarking with DNA codec. *Multimed Tools Appl*. doi:10.1007/s11042-015-3213-1

W Bender, D. G. (n.d.). "Techniques for data hiding,. *IBM Systems Journal,, 35*.

Wong, K. (2009). Image Encryption Using Chaotic Maps. *Springer*, 333–354.

Yanjun, D. C. (September 2010). A Study on Secure Data Storage Strategy in Cloud Computing. *ournal of Convergence Information Technology, Volume 5*.

Yue Wu, J. P. (2011). NPCR and UACI Randomness Tests for Image Encryption. *Journal of Selected Areas in Telecommunications (JSAT)*.

Zhou X.Q, H. H. (2001). Authentici ty and Integrity of Digital Mammography Images. *IEEE Transaction on medical imaging, 20*.