IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. II (Jan.- Feb. 2018), PP 65-75
www.iosrjournals.org

Cloud System For Encryption And Authentication Medical Images

Sefer kurnaz, Abdulrahman Ahmed jasim
(Electrical and computer engineering department, College of engineering / Istanbul Altinbas University, turkey)

Abstract : *Lately, a great number of applications has emerged during the fast and continuous development in telecommunications area. One of those important applications is a tele-medicine where the patient digital medical data can be transferred between doctors in order to farther diagnosis. Thus, protecting the exchanged medical data is the mission of this study, especially when exchanging that medical data over an insecure channel like the cloud computing environment, Medical images standard form called DICOM (Digital imaging and communications in Medicine). When we are outsourcing these medical images which contains sensitive information about patient such as medical status about the patient there is a need to give privacy for this information. Where security is considered a valuable issue, in this study proposes a novel framework to enhance the protection of DICOM images and privacy of patient info. In the proposed system the DICOM file that contain medical images and the patient information will face partition process in order to extract medical image and patient information and encrypt the image and upload it with patient info to the cloud, the cloud will store patient info inside oracle data base and encrypted image inside file, the keys of this encrypted image will saved in database, if client (doctor) that registered in cloud request to download any medical image, the cloud will perform steganography method using least significant bit (LSB) in order to embed the patient medical data inside the encrypted medical image and the key for decrypt the image, and send encrypted image with steganography information to the doctor. The proposed system assures 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 spicily a high PSNR values by comparison with other study on the medical images uses another encryption algorithm.*

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

Date of Submission: 29-01-2018 Date of acceptance: 15-02-2018

I. 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 provider and client 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 [1]. This leads to improvement 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 [2], 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 [3]. 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 [4] this data has to have the guarantee to avoid attacks it may face. The security of medical information, obtained from strict ethics and legislation laws, gives rights to the patient and responsibilities to the health ethics [5]. 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.

DOI: 10.9790/0661-2001026575

In the review of literature a great deal of studies have improved medical images security, 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. [6]. Mor Peleg Et Al. (2008) had the aim to state cases of request for patient's data access for preserving the privacy of patients [7]. Stallings (2010) emphasized on security problems in his book [8]. 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. [9]. 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 effectiveness of data sharing between patients and their doctors [10]. T. Neubauer et al. (2011) presented safeguarding medical files from illegal access where patient data is stored, and determine the certified people [11]. 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 [12]. 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 [13]. M. Ahmad et.al. (2012) suggested a paradigm for protecting the patients' medical images for secure tele diagnosis. The permutation and diffusion procedures of the model offer high security for encrypted information [14]. 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 [15]. M. Milutinovic et al (2013) presented privacy preserving protocols based on an innovative e-health system model, to ensure protecting user data [16]. C. Huangc et al. (2013) proposed a histogram shifting approach for reaching high bit depth medical images [17]. 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 [18]. Maria .S et al. (2015) introduced an interpolation method with lower degree of complexity, less blurring and higher resolution [19]. J. Anbarasi et al. (2015) introduced a multi secret image sharing approach for sharing multiple images based on the interpolation polynomial [20]. Akila et al. (2015) proposed an approach performance of which is measured with the use of enhancement and PSNR [21]. 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 [22]. 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 [23]. 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 [24]. 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 [25]. 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 [26].

This 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 logistic map, 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 (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.

II. Methodology

IN this study 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 patent 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 [27] 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 [28] (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. In the database a table was created, containing seven columns: (PATIENTID, PATIENTNAME, STUDYID, SERIESNUMBER, INSTANCENUMBER, MODALITY, and SOPCLASS) for saving patient information.

2.1 DICOM file partitioning: 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).the proposed system splits the image from the medical meta information as shown in 1st step and handle each one in a separate way in the forwarded steps of the system.

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

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

Table 1: DICOM file partition steps

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.

1.2 Encryption processes

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 study, 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, a good encryption algorithm must be able to maintain the main security goals to these digital medical images, Chaos theory and its behavior have been used in medical image encryption in this study, 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 a chaos-based medical image encryption algorithm based on the traditional chaos-based image cryptography architecture produced by Fridrich [17] 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, Fig: 1 illustrates an example of the input image into the encryption operation.

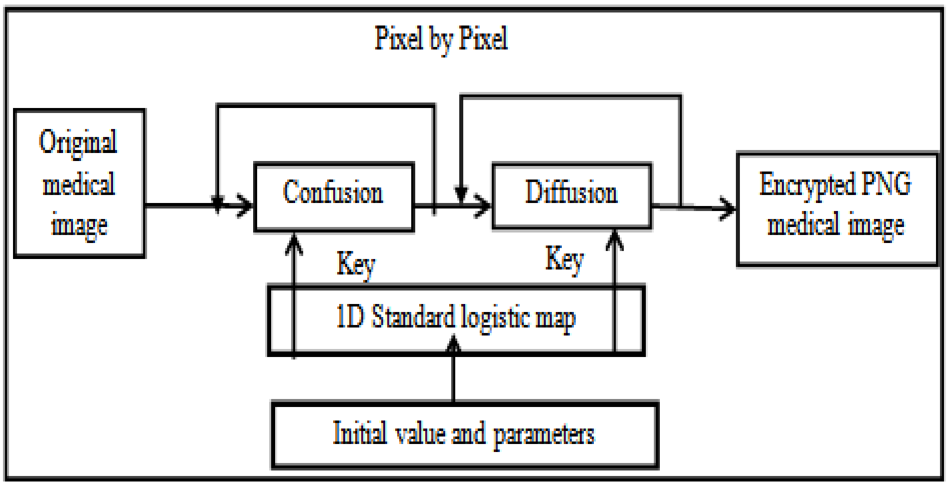


Fig (1): Block diagram of medical image encryption process

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, 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, 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_n and one control parameter μ which give varying results and properties when altering its value as inputs, generally this map can be described as follow:

$$Xn + 1 = \mu Xn(1 - Xn)\ for\ n = 0,1,2,3$$

The experimental results of this map shows that it is chaos when $x_n \in [0,1]$ and its control parameter $\mu \in [0, 4]$ and for more accuracy the logistic map is always chaotic and have appositive Lyapunov exponent when $3.58 \leq \mu \leq 4$ [29]. 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 of the medical image in this study

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

Table 2: medical image encryption steps

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, 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 Stenography 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, 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 Fig:2.

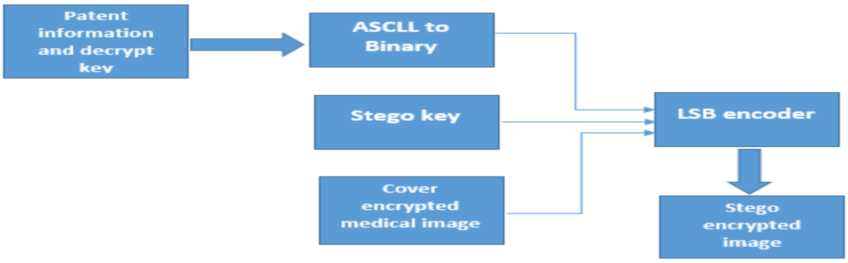

Patent information and decrypt key
ASCLL to Binary
Stego key
Cover encrypted medical image
LSB encoder
Stego encrypted image

Fig (2): the block diagram of LSB embedding in encrypted medical image

3rd step illustrate the propose system steps of embedding steganography data in the encrypted medical image.

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

Table 3: patinet info hiding steps

2.3 Retrieval processes

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 study; 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:

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.
4th step illustrate the steganography extraction steps from the encrypted medical image.

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

Table 4: patient info extraction steps

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, The process of decryption of medical images in this study 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.

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

Table 5: medical image decryption steps

III. Experimental Results

The results of the proposed system have been carried out inside NetBeans IDE by using java programming language to build main system (graphic user interfaces, encryption process. steganography and decryption process) and Oracle 10g to store data and secure it by creating a backup for medical information data. We use Oracle 10g to store patent information that produced from DICOM file partitioned, performance analyzing applied by python programming language using Anaconda3-5.0.1 environment with a set of 26 DICOM files (CR,CT,MR, and OT),Moreover, medical images were used for further investigation of the proposed system efficiency. Then, in order to check the quality of the system, numbers of quality metrics were applied. These metrics include Mean Square Error (MSE) and peak signal to noise ratio that were calculated using (1) and (2) respectively. Structural Similarity (SSIM) index address was also applied to measure the local images similarities and it was measured through (3). The number of changing pixel rate (NPCP) and the unified averaged changed intensity (UACI) metrics to check the number of changed pixels and the number of averaged changed intensity respectively between encrypted and decrypted images were also calculated using (4), (5) and (6) respectively[32]. Also histogram analysis shows the distribution of pixel value based on intensity. For encrypted image based on the scatter of pixel value the cryptanalysis judge the strength of image encryption algorithm.

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

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

Where R is the maximum fluctuation in the input image data type, M, P are the sizes of the original medical image (OMI) and the retrieved medical images (RMI) respectively [30], The attributes of PSNR that is under 30dB mean that the quality is low, (example of that, the distortion that is caused by embedding is high) a PSNR of dB that is over 40, means there will be high quality image encryption. [31].

$$SSMI(OMI,RMI) = LC(OMI,RMI)^{\alpha} \; xCC(OMI,RMI)^{\beta} \; xSC(OMI,RMI)^{\lambda} \qquad (3)$$

Where: OMI, RMI are the original and the reconstructed medical images respectively? LC is the luminance, CC is the contrast and SC is the structure of OMI and RMI α, β AND λ are ≥ 1 and are used to weight the importance of each of the three components [31].

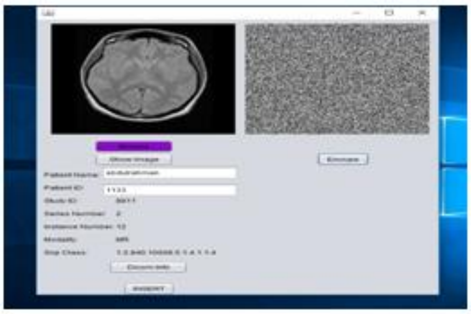
$$D(i,j) = \begin{cases} 0, if\ OMI(i,j) = RMI(i,j) \\ 1, if\ OMI(i,j) = RMI(i,j) \end{cases} \qquad (4)$$

$$NPCR: N(OMI,RMI) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \qquad (5)$$

$$UACI: U(OMI,RMI) = \sum_{ij} \frac{|OMI(i,j) - RMI(i,j)|}{F.T} \times 100\% \qquad (6)$$

Where F denotes the largest supported pixel value of the image format and T represents the size of the OMI and RMI [32].

Before going through these measurements, the process of the overall system were illustrated in fig: 3, 4 and 5. These results were computed on a personal computer worked with Intel (R) Core (TM) i7-2640M, CPU 2.80 GHz and installed memory (RAM) of 4.00GB (3.89 GB usable) "windows 10 64 bit".



Patient Name: abdulrahman
Patient ID: 1133
Study ID: 3311
Series Number: 2
Instance Number: 12
Modality: MR
Sop Class: 1.2.840.10008.5.1.4.1.1.4

Fig (3): DICOM file partition and image encryption (1st application)

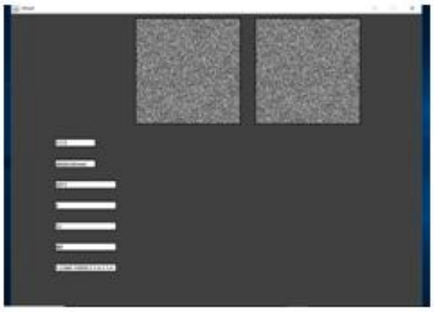
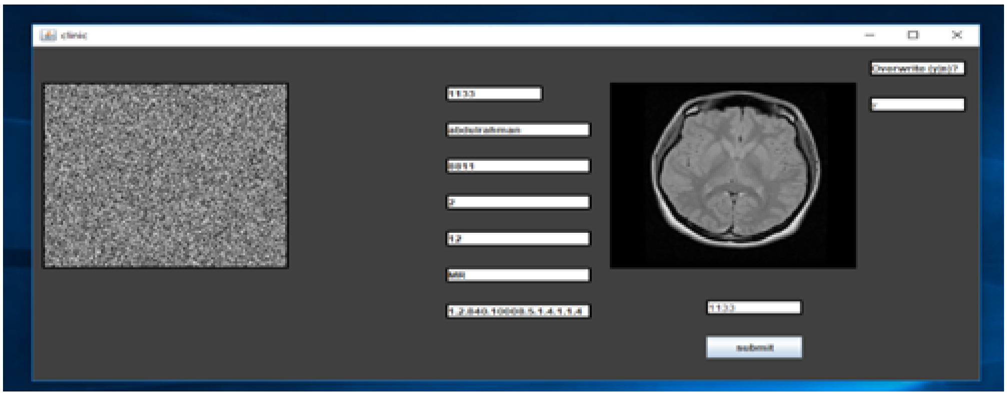


Fig (4): steganography method inside cloud (2nd application)



1133

abdulrahman

8811

2

12

MRI

1.2.840.10008.5.1.4.1.1.4

1133

y

Fig (5): Retrieve patient info and decrypted medical image (3rd application)

The result in figure (3) is DICOM file has been Divided and medical image Were separated from Meta data after that medical image encrypted by using chaos logistic map, the encrypted medical image with extracted patent information was uploaded to the cloud by using INSERT button. in figure (4) show how steganography method performed inside the cloud by using lest significant bit insertion algorithm in order to hide patent information inside encrypted medical image before sending it to the doctor (Clint) and figure (3) show how Clint application (doctor app) used patent ID to request patent image and how it received the encrypted-stego image and retrieved patient information and then decrypted medical image and display the result to the doctor.

Quality analysis

Now, to evaluate the images quality we picked sample from set of used images, Table (6) were constructed, to show that the proposed system guarantees lossless reconstruction of the transferred medical images, Table (6) shows some degree of distortion due to the encryption and steganography operations performed during the system stages. But it still provides very acceptable quality results as shown especially for the SSIM that considered as an ideal metric for testing similarities in medical images due to focusing on the local rather than global image similarity and placing more emphasis on the Human Visual System than PSNR [30]. In general, the high results of the system performance have been achieved due to the usage of the chaos logistic map and lest significant bit insertion algorithm.

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

Table 6: Quality evaluation of system

Histogram analysis

The pixel distribution of an image is represented as a graph called histogram. Since the proposed system licenses and diffuses the pixels of the image completely, the distribution of encrypted pixels has become more symmetrical which will not supply any meaningful information to an attacker, Fig: 6: (A, B, and C) three sample images and histogram for original images and encrypted CR CT MR images shows if an attacker tries to analyze the statistical characteristic of the cipher image from the histogram and tries to infer pixel information. This style of attack is known as cipher only attack. This system resists the cipher only attack

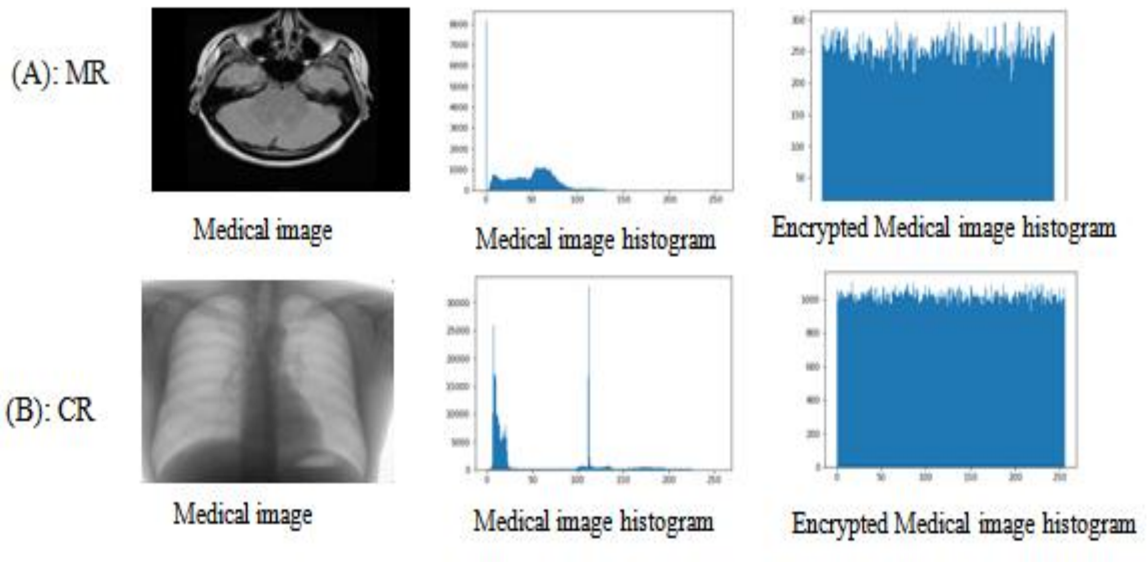


Figure 6: Histogram analysis

IV. Comparison

The scheme presented in [33], [34] and [35] also provides a lossless retrieval of the shared image while preserving the resulting images from pixels amplification. But The presented system here preserve the images from pixels expansion; guarantee high level of quality of the retrieved images and at the same time offers high levels of security for the shared data, Tables 7 and 8 and fig: 7 shows that our proposed system provide higher degree of robustness by comparison with [33] [34] and [35] this means that our system help to deliver the shared data to the other side of the communication with very acceptable level of quality.

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 7: Quality evaluation of [33]

Image	**MSE**	**PSNR(db)**	**SSIM**	**NPCR**	**UACI**
Image 1	0.001220703125	77.37	0.999988018665477	0.119018554688	0.000466739430147057
Image 2	0.00149536132813	76.30	0.999984424536379	0.152587890625	0.00059838388480392
Image 3	0.00143432617188	76.66	0.999985968801158	0.140380859375	0.000550513174019606
Image 4	0.000175619834711	75.69	0.999997790332674	0.0175619834711	0.0000688705234159779
Image 5	0.000091552734375	88.51	0.99999899415064	0.0091552734375	0.0000359030330882352
Image 6	0.000114440917969	87.54	0.999998344114482	0.0114440917969	0.0000448787913602941
Image 7	0.00048828125	81.24	0.999996150248731	0.048828125	0.000191482843137254

Table 8: Quality evaluation of our system

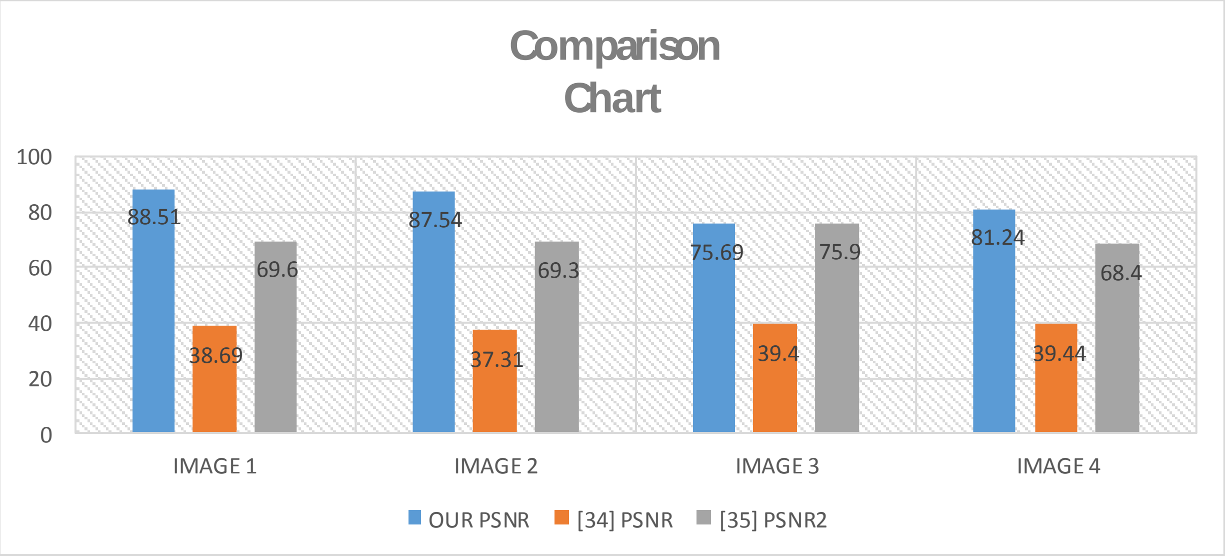


Figure (7): PSNR Comparison between our system and [34] and [35]

V. 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 application for medical image clinic and the second is cloud and last one is doctor or clinic application with aim of providing the mean of the trust management between the parties of the cloud computing environment that considered as unsecure environment to deal with. The system uses well established and common methods to create a system which can authorize, authenticate and secure communications between Clint and cloud and clinic, two main algorithm used in this system, chaos logistic map algorithm to encrypt medical images that extracted from DICOM file and least significant bit (LSB) for steganography patient information inside encrypted image, The proposed model assures 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 spicily a high PSNR values by comparison with other study uses another algorithm in [4] (used spatial watermarking technique and also a hybrid spatial and transform techniques) and in [5] (used two step watermarking first step used DCT and other step used DWT coefficients for embedding) and in [6] (used AHF and ACC algorithms), also distribution of encrypted pixels has become more symmetrical in our system which will not provide any meaningful information to an attacker and that means the system resists the cipher only attack.

The future work has an aim of implementing the hybrid model using other encryption technics such as AES algorithm with least significant bit algorithm or using chose logistic map with watermarking method such reversible watermark, and evaluates the results in order to maximize the robustness against the attacking attempts. Also it has an aim of applying the proposed approaches in other sorts of medical data and test the consequent performance.

References

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

[2]. E. Borko Furht, HandBook of Cloud computing, Springer Science + business Media, LLC, 2010.

[3]. D. C. a. Yanjun, "A Study on Secure Data Storage Strategy in Cloud Computing," *ournal of Convergence Information Technology*, vol. Volume 5, September 2010.

[4]. G. U. V. V. N. Mustafa Ulutas, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *The Journal of Systems and Software*, 2011.

[5]. W. B. a. C. B. H. Nyeem, "review of medical image watermarking requirements for teleradiology," *Journal of Digital Imaging*, vol. 26, p. 326 – 343, 2013.

[6]. T. B. a. T. Giorgino, "Health dialog systems for patients and consumers," *Journal of Biomedical Informatics*, vol. 39, pp. 556--57, 2006.

[7]. D. B. D. D. a. Y. D. Mor Peleg, "ituationBased Access Control: Privacy management via modeling of patient data access scenarios," *Journal of Biomedical Informatics*, vol. 41, pp. I 028-1040, 2008.

[8]. W. Stallings, Cryptography and network Security, 2010.

[9]. K. Faraoun, "Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption," *Int Journal ofInformation Technology,* vol. 7.

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

[11]. T. N. a. h. Heurixb, "A methodology for the pseudonymization of medical data," *International Journal of medical informatics,* vol. 80, pp. 190-204, 2011.

[12]. G. U. a. V. V. N. Mustafa Ulutas, "Medical image security and EPR hiding using Shamir' s secret sharing scheme," *The Journals of systems and software,* vol. 84, pp. 341-353, 2011.

[13]. G. C. C. a. C. a. R. Dalel Bouslimi, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images," *IEEE Transaction on Information Tech in Biomedicine,* vol. 5, 2012.

[14]. M. A. a. T. Ahmad, "A Framework to Protect Patient Digital Medical Imagery for Secure Telediognosis," *Procedia Engineering,* vol. 28, pp. 1055 - 1066, 2012.

[15]. S. V. B. Jardim, "The Electronic Health Record and its Contribution to Healthcare Information Systems Interoperability," *Procedia Technology,* vol. 9, pp. 940 - 948, 2013.

[16]. M. M. a. B. D. Decker, "Privacy-preserving data management in eHealth systems," *Int. Conf. on Health and Social Care Information Systems and Technologies,* vol. 9, pp. 1085-1092, 2013.

[17]. L.-Y. T. a. M.-S. H. Li-Chin Huangc, "A reversible data hiding method by histogram shifting in high quality medical images," *The Journals of systems and software,* vol. 86, pp. 716-727, 2013.

[18]. J. C. a. S. Smith, "Privacy-preserving screen capture Towards closing the loop for health IT usability," *Journal ofBiomedical Informatics,* vol. 46, pp. 721- 733, 2013.

[19]. M. C. V. a. Muneeswaran.K, "Hiding of Confidential Data in Spatial Domain Images using Image Interpolation," *Int.I Journal of Network Security,* vol. 17, pp. 722-727, 2015.

[20]. M. a. M. N. Jani Anbarasi.L, "DNA based Multi-Secret Image Sharing," *Int. Conf. on Information and Communication Technologies,* vol. 46, pp. 1794-1801, 2015.

[21]. J. a. V. Akilaa.K, "Mammographic image enhancement using indirect contrast enhancement techniques," *Procedia Computer Science,* vol. 47, pp. 255 - 261, 2015.

Al-Haj, "Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images," *J Digit Imaging,* 2015.

[22]. S. B. Prema T. Akkasaligar, "Secure Medical Image Encryption based on Intensity level using Chao's theory and DNA Cryptography," *IEEE International Conference on Computational Intelligence and Computing Research,* 2016.

N. M. B. H. J. M. Z. Syifak Izhar Hisham, "Numbering with spiral pattern to prove authenticity and integrity in medical images," *Pattern Anal Applic,* 2017.

A.-H. &. A. M. &. A. Amer, "Crypto-Watermarking of Transmitted Medical Images," *J Digit Imaging,* 2017.

U. &. G. Ulutas, "A New Medical Image Watermarking Technique with Finer Tamper Localization," *J Digit Imaging,* 2017.

[23]. J. FRIDRICH, "SYMMETRIC CIPHERS BASED ON TWO-DIMENSIONAL CHAOTIC MAPS," *International Journal of Bifurcation and Chaos,* vol. 6, no. 8, 1998.

[24]. R. a. F. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications,* vol. 16, 1998.

[25]. S. W. a. X. M. Hua Xue, "Study on One Modified Chaotic System Based on Logistic Map," *Research Journal of Applied Sciences, Engineering and Technology,* 2013.

[26]. F. R. a. H. Rabbani, "A dual adaptive watermarking scheme in contourlet domain for DICOM images," *BioMedical Engineering,* 2011.

[27]. M. G. a. R. D. Jessica Fridrich, "Detecting LSB Steganography in Color and Gray-Scale Images," Binghamton.

[28]. J. P. N. S. A. Yue Wu, "NPCR and UACI Randomness Tests for Image Encryption," *Journal of Selected Areas in Telecommunications (JSAT),* 2011.

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

A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment," in *2017 40th International Conference on Telecommunications and Signal Processing (TSP),* 2017.

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

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Sefer kurnaz, Abdulrahman Ahmed Jasim "Cloud System for Encryption and Authentication Medical Images." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 20, no. 1, 2018, pp. 65-75.