A SECURITY SCHEME FOR PATIENT INFORMATION PRIVACY IN DIGITAL MEDICAL IMAGING

Oladotun Olusola OKEDIRAN
[1]Department of Computer Science & Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[1]oookediran@lautech.edu.ng

Keywords: DICOM, encoding, encryption, patient information, privacy, ROI, RONI, security

Abstract: In recent times, many applications have emerged due to the rapid and continuous development in the field of Information and Communications Technology (ICT). One of such applications is telemedicine. Patient medical data are now in electronic formats and available within health information infrastructures which presents considerable benefits for medical providers and patients themselves, including enhanced patient autonomy, improved clinical treatment, advances in health research and public health surveillance. Accompanying these benefits is the risk of the security of patient information that are supposed to be confidential, being accessible by unauthorized users, since the transmission of these electronic medical data are always via open communication channels. Issues bordering on patient identity protection are still very contentious in health information security. In this paper, a security scheme for enhancing patient information privacy on a medical images standard format; the Digital Imaging and Communications in Medicine (DICOM) was proposed. In the proposed scheme DICOM files were partitioned to extract medical images and patient information independently. The patient information was then encoded, encrypted and embedded in the Region of Non-Interest (RONI) of the medical image component of the DICOM file. The performance of the proposed scheme was evaluated using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index Metric (SSIM). For the ten medical images used to test the scheme, the SSIM values were close to 1, while the MSE and PSNR were consistent and they returned desirable high values. The average values of the MSE and PSNR are 0.201 and 55.84 dB respectively. Hence, the proposed scheme is utterly robust and highly imperceptible; the original images can be retrieved at the receiver side without any distortion.

1. INTRODUCTION

Medical images are a central part of diagnostics in today's healthcare delivery [1]. Medical imaging includes diverse imaging techniques and procedures to pictorially represent the human body for diagnostic and treatment purposes. Some of the medical imaging modalities include: X-ray, optical and ultrasound techniques, nuclear imaging (Single Photon and Positron), X-ray Computer tomography systems (CT-Scanner), Magnetic Resonance Imaging (MRI) and so on. The significance of these images is also evident in the assessment of an ailment/syndrome previously diagnosed and/or treated. With advances in ICTs, medical images can be cross-exchanged in right time, facilitating a boost in the potentials of telemedicine applications ranging from teleconsulting, telediagnosis to mention but a few to cooperative working session and telesurgery [2]. This boost in the potentials of telemedicine applications has led to the need to apply security techniques to medical images since telemedicine essentially involves medical diagnosis and patient care with the medical provider and patient separated by distance [3].

With the transmission of medical images over open communication networks comes the risk of manipulation and replication. Medical images contain highly private contents of medical information for a person, which means they are closely related to patients' privacies and hence should be kept with upmost secrecy.

Generally, trust in digital data is characterized in terms of privacy, authenticity and integrity of the data. Privacy refers to denial of access to information by unauthorized individuals. Authenticity refers to validating the source of a message; that is, it was transmitted by a properly identified sender and is not a replay of a previously transmitted message. Integrity refers to the assurance that the data was not modified accidentally or deliberately in transit, by replacement, insertion or deletion. The focus of this paper is on the specific issue of privacy of patient information on DICOM standard format based on the following motivations. Firstly, on medical images, patient information is usually printed in the corner of the medical images for viewing hence compromising the privacy of the patient. Secondly, in the course of transmission over an open network, patient information which is visibly displayed on a medical image may be intercepted by a third party. Lastly, for scenarios such as medical imaging research, the patient information should not be accessible for any reason.

The DICOM is the standard for the communication and management of medical imaging information and related data [4]. DICOM is most commonly used for storing and transmitting medical images enabling the integration of medical imaging devices such as scanners, servers, workstations, printers, network hardware, and picture archiving and communication systems (PACS) from multiple manufacturers [5]. It has been widely adopted by medical institutions, and is making inroads into smaller applications. DICOM files can be exchanged between two entities that are capable of receiving image and patient data in DICOM format. The different devices come with DICOM Conformance Statements which clearly state which DICOM classes they support, and the standard includes a file format definition and a network communications protocol that uses TCP/IP to communicate between systems [4]. Another medical images standard format is the Health Level Seven (HL7).

In this paper, a security scheme for patient information privacy for DICOM files was proposed. In the scheme, the DICOM files were partitioned to extract medical image and patient information independently. The patient data was encoded and then encrypted. The medical image component of the DICOM files was segmented in Region of Interest (ROI) and RONI using a threshold image segmentation algorithm. The encrypted patient information was then embedded in the RONI using a Discrete Cosine Transform (DCT) based methodology. Hence, an unauthorized observer (for instance a medical imaging researcher or a hacker) can only view the medical image but cannot access the patient information. On the other hand, an observer with the valid credentials can decode, decrypt and extract the patient information from a corresponding medical image. The performance of proposed scheme was evaluated using PSNR, MSE and SSIM. The remain sections of this paper was organized as follows: Section two presents review of related works to this research; Section three details the research methodologies employed in developing the proposed security scheme; Section four presents the results and Section five summarized and concluded the paper.

2. RELATED WORKS

Lim and Feng in [6] presented a multiple block based authentication watermarking for distribution of medical images. It provides an active method of authentication for the efficient distribution of images, and this technique suggests a new method using fragmentation of the watermark information content of images. Medical imaging modalities such as Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET) and the structure of tissues contain a large amount of clinical information. Therefore, it is important to provide authentication for the safety of fragmented blocks. The proposed technique was based on the secure encryption watermark, but removes the problem of independence block wise of existing methods. This technique suggests to merge multiple signatures that were created through square blocks and blocks of fragmentation, two types of signatures shared to remove the block wise independence. The advantage of this proposed technique being able to detect the location of the modification; therefore, it neglects the tampers if the modifications are located in a Region of Non-Interest (RONI).

Tolbal *et al*. in [7] proposed a wavelet transform algorithm that maps integers to integers for perfect reconstruction of the original

image. The proposed algorithm embeds the message bit stream into the LSB's of the integer wavelet coefficients of a true-color image. The algorithm also applies a pre-processing step on the cover image to adjust saturated pixel components in order to recover the embedded message without loss.

Boucherkha and Benmohamed in [8] presented a medical image authentication based on lossless watermarking; it is used for interleaving patient information and message authentication code with images using lossless compression. At embedding process the authentication code of the image using MD5 algorithm is calculated; the authentication code and patient information are concatenated then encrypted. LSBs of all pixels are selected and compressed using Run Length Encoding (RLE) lossless compression algorithm. The compressed string and the encrypted string are concatenated and inserted into the LSB locations by adding blanks if necessary. Before embedding process the patient information is encrypted; therefore, this technique provides a high level of security for the patient information. This presented technique inherits the disadvantage of the LSB embedding process that is changing the statistical property of the cover image; therefore, the hiding process can be detected easily by computer systems.

Coatrieux *et al.* in [9] presented an adaptive reversible watermarking technique for image authentication and self-correction. In the technique, the image is divided into two regions: Region of Interest (ROI) and RONI, it embeds the ROI into the RONI, and any modification of the image will be detected and could be self-restored back to the original image by extracting the ROI from the RONI. The ROI area is depending on the availability of clinical finding and its features in the medical image, and the RONI is the background or any area, where there is not any clinical finding. The pros of this technique are providing two levels of robustness by mixing a reversible watermarking method and a robust watermarking method. This watermarking method provides the initial level of robustness of the watermark extraction process against JPEG compression; a digital signature derived from the ROI, and an authenticity code is concatenated to form a primary code to be embedded inside the RONI using the robust watermarking method. The reversible watermarking technique provides the second level of robustness by embedding another code into the ROI; this code is determined for the whole image (RONI and ROI). This proposed technique is used for a specific type of medical images that is Magnetic Resonance (MR) images; this type of medical images is very simple to identify RONI and ROI; therefore, this proposed technique is unable to authenticate other types of medical images that their RONI and ROI are hard to be separated.

Delforouzi and Pooyan in [10] developed a novel method for digital audio steganography in which encrypted covert data is embedded into the coefficients of the host audio (cover signal) in the integer wavelet domain. The hearing threshold is calculated in the integer domain and this threshold is employed as the embedding threshold. The inverse integer wavelet transform is applied to the modified coefficients to form a new audio sequence (stego signal).

Memon and Gilani in [11] proposed an adaptive data hiding scheme for medical images using integer wavelet transform. Integer wavelet transform hiding technique is used for embedding the multiple watermarks by decomposes the cover image to obtain the wavelet coefficients. Before watermark embedding process; an adaptive threshold is determined for each block; it uses iterative optimization of threshold for compression and expansion process. It avoids histogram pre and post-processing; therefore, its pros are reducing the histogram processing overhead and keeping the distortion small between the watermarked and the original images. The cons of this technique are: low imperceptibility values at normal embedding capacity (bad tradeoff between robustness and capacity) and it is not applied to color images (it is applied only for grayscale images).

Luo *et al.* in [12] presented a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on Integer wavelet transformation.

Mostafa *et al.* in [13] proposed a blind watermarking based on wavelet transform for medical image management, it hides the Electronic Patient Record (EPR) in the image: to protect patient information, to save storage space and to reduce transmission overheads. It embeds

EPR data as a watermark in the Discrete Wavelet Packet Transform (DWPT) of the image. This proposed technique enhances the robustness by encoding EPR data using BCH error correcting code. The disadvantages of this technique are that it is purely implemented for grayscale images (not for color images), and it has been low embedded capacity. The embedded process hides only one bit per a block of pixels with size 4×4 pixels, and the error correcting code reduces the actual capacity to be less than one bit per 4×4 block of pixels.

Memon in [14] developed a robust fragile watermarking technique to provide copyright protection and content authentication of medical images. It authenticates the CT scan images of the thorax area against distortions. It separates a ROI and RONI from the image. By isolating the actual lung parenchyma; this technique increases the embedding capacity of a CT scan image; it embeds a watermark only in RONI; therefore, it does not compromise the diagnostic value of the image. For embedding the watermark; it utilizes the spatial domain watermarking and LSB replacement method. The cons of this technique are it is devoted to a specific type of medical images; in addition, its robustness requires to be improved.

Rahimi and Rabbani in [15] proposed an adaptive dual blind watermarking scheme for medical images. It automatically selects the ROI and embeds the watermark with different embedding strength in ROI and RONI; it embeds watermark bits in singular values within the low-pass sub-band in the CN domain; therefore, it is more efficient and robust than embedding within the wavelet domain. This technique can be applied to DICOM image format; it has large PSNR and it satisfies high transparency for its watermarked images, but the invisibility could be enhanced. This technique is tested only using CT and MR images; therefore, it required to be tested using other types of images.

Sakkara *et al*. in [16] proposed a technique that uses secret information as a text message which is embedded in a color image. The technique is founded around the fact that most existing methods hide the information using a constant bit length in integer wavelet coefficients that increases the embedding capacity of the text message and obtained stego-image is imperceptible for human vision.

Ko *et al.* in [17] proposed a reversible watermark based on Quantization Index Modulation (QIM) to be applied to healthcare information management systems, the QIM-based watermarking is used to reconstruct the identical original image; the capacity of the watermark is increased to be one-fourth of that of the cover image. Its architecture and algorithms are simple; it can be easily implemented. However, it is tested using only grayscale images; accordingly, it is required to be tested using color images.

Pandey, Singh and Shrivastava in [18] presented a security model that combines image cryptography, data hiding and Steganography technique for denoised and safe image transmission purpose. In the model the original images is encrypted with stream cipher algorithm then embeds the encrypted image with patient information by using lossless data embedding technique with data hiding key after that for more security. Steganography is then applied to the embedded image with the private key. On receiver side when the message arrives the methods are applied in reverse order to get the original image and patient information and to remove noise we extract the image before the decryption of message.

An *et al.* in [19] proposed a watermarking framework based on wavelet-domain; it proposes a robust reversible watermark embedding and extraction procedure through histogram shifting and clustering. It provides good performance in terms of reversibility, robustness and invisibility, but the embedded capacity is less than 4×10^{-3} bpp. It is applicable in practice to many types of medical images; however, it is tested using a limited number of grayscale images; therefore, it is required to be tested using enough number of grayscale and color images.

Das and Kundu in [20] proposed a blind image watermarking technique based on Contourlet (CN) transform for the medical data-management scheme. It is robust against high JPEG and JPEG2000 compression, and it can provide information security, content authentication, safe archiving and controlled access retrieval. In this proposal, an original image is decomposed based on CN transform, then the watermark is embedded inside the image using the low pass such that the embedded

watermark can be extracted in a blind manner, finally the image is reconstructed based on the inverse of the CN transform to get the watermarked image. It can be used during a medical image acquisition process to provide authenticity, integrity and confidentiality, but the embedded capacity is very low it is less than 0.0053 bpp.

Bouslimi, Coatrieux and Roux in [21] proposed a security technique based on encryption, and watermarking to protect medical images; it enables access to the outcomes of the encrypted image integrity and of its origins. With this technique, the RC4 stream ciphers and two substitute watermarking methods are combined; these two watermarking methods are the LSB and the QIM methods. In the embedding process, the watermarking and encryption are conducted jointly; therefore, in the extraction process, the watermark extraction and decryption can be applied independently. This technique can achieve a large embedded capacity in the spatial domain (0.5 bpp) with a high Peak Signal to Noise Ration (PSNR) that is greater than 49 dB. Due to using the LSB watermarking method; the statistical property of the watermarked images is changed; accordingly, the hidden information can be detected by the attacking computer system.

Jain, Choudhary and Kumar in [22] presented a novel technique for securing the transmission of medical information of patient inside medical cover image by concealing data using decision tree concept. Decision tree shows a robust mechanism by providing decisions for secret information concealing location in medical carrier image using secret information mapping concept. RSA encryption algorithm was used for patient's unique information enciphering. The outcome of the RSA was structured into various equally distributed blocks.

Mahalakshmi, Satheeshkumar and Sivakumar in [23] developed a security model for protecting medical images with emphasis on Magnetic Resonance Imaging (MRI). In their work, three different steganographic algorithms were used; Least Significant Bit (LSB) algorithm, Division into block and Mean change modified method.

Banjan and Dalvi in [24] presented a medical data security model using a combination of cryptography and steganography with AES-LSB algorithm. In model, patient's data is firstly encrypted using Advanced Encryption Standard algorithm and then the encrypted data is hidden in a medical image using image steganography by Least Significant Bits algorithm. The hidden data in the cover image is sent to the intended receiver. The reverse of the methodology was used to obtain the original data at the receiver side.

Most of the reviewed works in literature proposed and presented schemes and systems for securing medical images but not medical meta-information, that is, the patient information. However, medical images contain highly private contents of medical information for a person, which means they are closely related to patients' privacies and hence should be kept with upmost secrecy. Third parties should not be able to associate a medical image with the corresponding medical meta-information, as this could discomfit the concerned individual may also be accompanied with unexpected losses which may be physical or financial.

3. METHODOLOGY

The outline of the steps for evolving the security scheme for patient information privacy for DICOM files proposed in this work are as follows:

i. At the sender's end, partitioning of the DICOM file into two components namely; the medical image and patient information components.

ii. Encoding of the patient information using UTF-8 Character Encoding Scheme.

iii. Encryption of the encoded patient information using a public key cipher, ElGamal.

iv. Image segmentation of the medical image component into ROI and RONI using a threshold medical image segmentation technique proposed by Coatrieux et al. in *[25].*

v. Embedding the encoded/encrypted patient information of (iii) above in the RONI using a DCT based methodology proposed by Yang and Bourbakis in [26].

vi. Transmission of the marked image over an open network.

vii. *At the recipient's end, extraction of the encoded/encrypted patient information from the medical image.*
viii. *Decryption of the encoded/encrypted patient information.*
ix. *Decoding of the encoded patient information.*
x. *Retrieval of the patient information.*

The architectural framework of the proposed security scheme is depicted in Fig. 1.

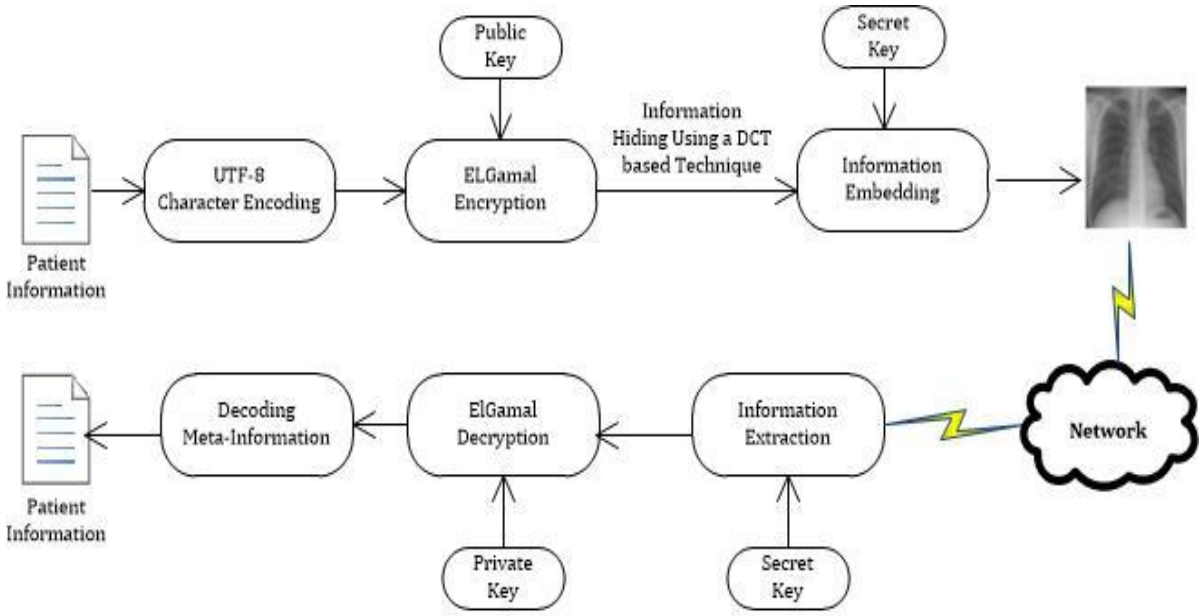

Fig. 1 Architectural Framework of the Proposed Security Scheme

In the scheme depicted in Fig. 1 above, the DICOM files were partitioned to extract medical image and patient information independently. The patient data was encoded using UTF-8 Character Encoding Scheme and then encrypted using a public key cipher, ElGamal.

The medical image component of the DICOM files was segmented into Region of Interest (ROI) and Region of Non-interest (RONI) using a threshold image segmentation algorithm proposed by [25]. The encrypted patient information was then embedded in the RONI using a DCT based technique proposed by [26]. Hence, an unauthorized observer (for instance a medical imaging researcher or a hacker) can only view the medical image but cannot access the patient information. On the other hand, an observer with the valid credentials can decode, decrypt and extract the patient information from a corresponding medical image.

The scheme was implemented using Microsoft Visual Studio (C# Programming Language) and MATLAB R2016a.

A. ElGamal Cryptosystem

The ElGamal crypto-system operates in a finite cyclic group ([27]; [28]). An ElGamal cryptosystem can be described by a 4-tuple (*p*, *g*, *x*, *y*), where *p* is a large prime and describes which group Z_p^* is used, *g* is an element of order *n* in Z_p^*, *x* is a random integer with $1 \leq x \leq n-1$, and $y = g^x$. The steps in ElGamal cryptosystem are as follows:

i. *Key generation*: Pick a large prime *p*, generator *g* of Z_p^* *p*, private key is a random *x* such that $1 \leq x \leq p-2$, and public key is 4 tuple ($p, g, y = g^x \bmod p$).
ii. *Encryption*: Pick random *k* such that, $1 \leq k \leq p-2$, and encryption function is defined as:

$$E(m) = \left(g^k \bmod p, my^k \bmod p\right) = (\gamma, \delta) \qquad [3.1]$$

$$D$$

iii. *Decryption*: Given cipher text (γ, δ), compute $\gamma^{-x} \bmod p$ and recover m such that:

$$m = \delta\gamma^{-x} \bmod p. \quad [3.2]$$

B. UTF-8 Character Encoding Scheme

UTF-8 (8-bit Unicode Transformation Format) is a variable width character encoding capable of encoding all 1,112,064 valid code points in Unicode using one to four 8-bit bytes [29]. The encoding is defined by the Universal Coded Character Set (Unicode). UTF-8 was designed for backward compatibility with American Standard Code for Information Interchange (ASCII). Code points with lower numerical values, which tend to occur more frequently, are encoded using fewer bytes. The first 128 characters of Unicode, which correspond one-to-one with ASCII, are encoded using a single byte with the same binary value as ASCII, so that valid ASCII text is valid UTF-8-encoded Unicode as well. Since ASCII bytes do not occur when encoding non-ASCII code points into UTF-8, UTF-8 is safe to use within most programming and document languages that interpret certain ASCII characters in a special way [29].

C. Image Segmentation

Coatrieux *et al.* proposed in [25] to use simple geometric shapes to separate RONI and ROI regions using an ellipse. In the case of axial and coronal of brain for instance, an ellipse is well suited. To determine the ellipse, they follow the approach summarized in Fig. 2. Firstly, the gradient of the original image is calculated (with a Sobel filter) and thresholded in order to obtain the image contours. Since the interested is only on the anatomical contours of the object, this threshold is relatively low (it is 15 for an 8-bit depth image) and its choice is not critical. The bounding rectangular box or more precisely the box which includes these contours, that is or the anatomical object is then found. The expected ellipse is the one that is included in this box. The parameters of the ellipses are quantified so as to limit the search space of the useful area for verification. This approach is however sensitive to the watermark insertion. Even if the watermark amplitude is small, it may introduce new contours. To overcome this issue, Coatrieux *et al.* introduce in the image a RONI watermark in a way so as to introduce a high gradient variation on the ellipse edge, which is at the frontier between RONI and ROI. Thus their detector just has to look for the ellipse which maximizes the image gradient on its edges. In order to reduce the complexity of such a strategy, they consider a dictionary of ellipses that is a subset of the ellipses that can be defined in an image.

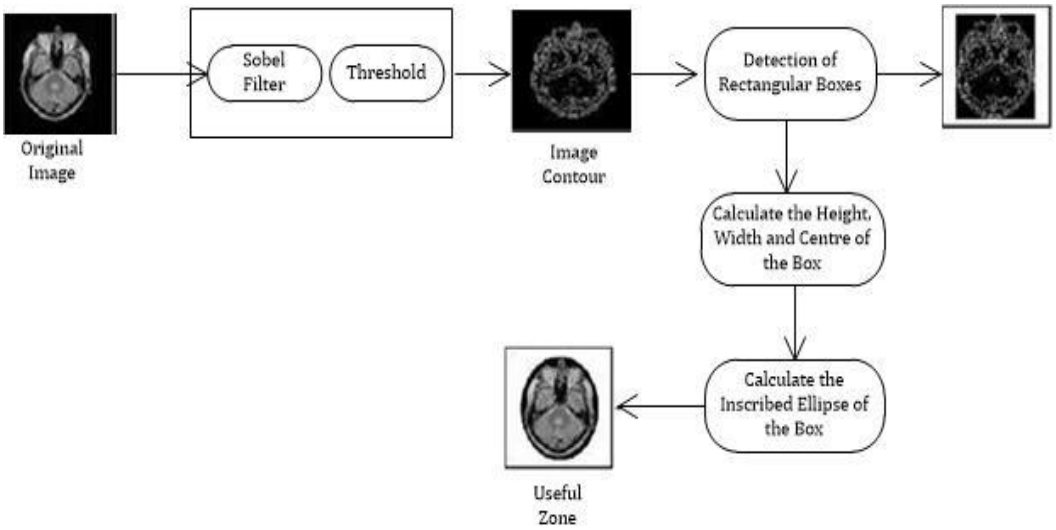

Fig. 2 ROI Definition with the Aid of Ellipse with Parameters Estimated by Image Segmentation

D. DCT

The description of the one-dimensional $(M data\ items)$ DCT for an input image *F* and an output image *T* is calculated as:

$$T_p = \propto_p \sum_{m=0}^{M-1} F_m cos \frac{\pi(2m+1)p}{2M}$$

$$for\ p = 0, 1, 2, \ldots, M-1.$$

[3.3]

The description of the two-dimensional $(M \times N)$ DCT for an input image *F* and an output image *T* is calculated as:

$$T_{pq} = \propto_p \propto_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} \cos \frac{\pi(2m+1)p}{2M} cos \frac{\pi(2n+1)q}{2N}$$

[3.4]

Where

$$0 \le p \le M-1$$

$$0 \le q \le N-1$$

$$\propto_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases} \quad and$$

$$\propto_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

where *M*, *N* are the dimensions of the input image while *m*, *n* are variables ranging from *0* to *M -1* and *0* to *N-1* respectively. Here, the input image *F* is of size $M \times N$). T_{ij} is the intensity of the pixel in row *i* and column *j*; T_{pq} is the DCT coefficient in row *p* and column *q* of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. DCT is used in steganography as the image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

Many DCT base hiding algorithms have been proposed in literature. In this paper, however, the technique proposed by Yang and Bourbakis in [26] was employed. The authors proposed using a DCT on 4×4 blocks of pixels and then modifying the eight lowest frequency coefficients, which represent the luminance of the background of the image, to embed one bit of information. In the algorithm, 1 bit is hidden within each 4×4 DCT coefficient block by means of vector quantization. Low frequency coefficients are chosen for information hiding due to their relatively large amplitudes and the corresponding small step sizes in the quantization matrix.

4. RESULTS AND DISCUSSION

The security scheme for patient information privacy proposed in this work was implemented using Microsoft Visual Studio (C# Programming Language) and MATLAB R2016a environment with a set of ten DICOM files.

In order to ascertain the efficacy of the scheme, a numbers of performance evaluation metrics were applied. These metrics include:

i. MSE is utilized to quantify the average of mean square mistake among pixels of the cover image and stego-image while whose value is calculated by utilizing:

$$MSE = \sum_{i=1}^{M \times N} \frac{(g_i - g_i')^2}{M * N}$$

[4.1]

Where g_i is a pixel value before inserting the information within the image and g_i' is a pixel value after inserting the information within the image, while, $M \times N$ denotes the size of image. The lower value of MSE means better quality of image.

ii. PSNR is utilized to calculate the quality of stego-image by relying on the standard value of the Human Visual System (HSV) with a value of (30 dB) [30]. If the PSNR value is greater than 30 dB, this implies that the inserted data inside the image is invisible to the human eye ([31]; [32]). Equation 4.2 is used to calculate the value of PSNR [33]:

$$PSNR = 10 log_{10} \frac{max^2}{MSE}$$

[4.2]

where, *max* signifies the maximum value of pixels in the image.

iii. Structural Similarity Index Metric (SSIM) is utilized to evaluate the likeness among the cover image and the

stego-image [34]. The yield of SSIM value is limited in the range between 0 and 1. If the SSIM value is close to 1 that indicates the stego-image is alike the cover image and it has high quality. Equation 4.3 is used to calculate the value of SSIM [32]:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2\mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad [4.3]$$

where, μ_x and μ_y are mean values of cover image (x) and stego-image (y) and σ_x and σ_y are standard deviation values of the cover image and stego-image while, σ_{xy} means the covariance of both two images. c_1 and c_2 are constants to stabilize the division.

One of the medical image (cover image) from the partitioned DICOM file used and its equivalent stego-image (the medical image with embedded information that is, encoded/encrypted patient information) are depicted in Fig. 3 below.

A: Cover Image Grayscale

B: Stego-image Grayscale
Fig.3 Cover and Stego-image in Grayscale

From Table 1, the PSNR has large consistent values; the minimum value is 55.54 dB while the highest value is 56.11 dB.

These large values of PSNR (that is > 30 dB) indicates that distortion due to embedding of information in the original image is very low; the embedded information did not affect the quality of the original images.

The maximum value of MSE is 0.21; an indication that the MSE has very low consistent value; therefore, the embedded information does not affect the quality of the original images.

The SSIM value is consistently close to one for all the ten images, an indication that the stego-image is alike the cover image and it has high quality.

Table 1: Results of Performance Evaluation Parameters

Medical Image	**MSE**	**PSNR (dB)**	**SSIM**
M_Image1	0.21	55.72	0.9214
M_Image2	0.19	56.03	0.9135
M_Image3	0.20	55.68	0.9211
M_Image4	0.21	55.70	0.9225
M_Image5	0.19	56.11	0.9112
M_Image6	0.20	55.54	0.9233
M_Image7	0.20	56.07	0.9215
M_Image8	0.21	55.82	0.9124
M_Image9	0.19	55.64	0.9242
M_Image10	0.21	56.09	0.9142

5. CONCLUSION

The concomitance of multimedia information and information communication technologies have boosted the usability and application potential of medical images.

Health information is increasingly available both in health databases and through online networks for telediagnosis, teleconsultation, telesurgery and cooperative work.

The availability of electronic data within the modern health information infrastructure presents significant benefits for medical providers and patients, including enhanced patient autonomy, improved clinical treatment, advances in health research and public health surveillance.

While the recent advances in information and communication technologies provide new means to access, handle and move medical images, they also expose patient information privacy to unauthorized users due to the means of transmission of these medical images.

Nowadays, questions of health information security and patient information privacy are of utmost importance.

In this paper, a security scheme for enhancing patient information privacy on a medical images standard format; DICOM, was proposed.

In the proposed scheme the DICOM files were partitioned to extract the medical image and the medical meta-information (that is the patient information) independently.

The medical meta-information were then encoded, encrypted and then embedded in the Region of Non-Interest (RONI) of the medical image component of the DICOM file.

The performance of the proposed scheme was evaluated using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index Metric (SSIM).

The direction of future work can be tune in the direction of the implementation of fragile watermark in similar security scheme as such proposed in this paper to ensure that patient data has not been compromised.

6. REFERENCES

[1]. Kester Q., Nana L., Pascu A. C., Gire S., Eghan J. M. and Quaynor N. N.," *A Cryptographic Technique for Security of Medical Images in Health Information System*" Second International Symposium on Computer Vision and Internet (VisionNet'15): Signal Processing, Image Processing and Pattern Recognition (SIPR'15), Procedia Computer Science 58., ScienceDirect, Elsevier, pp 538-543, 2015.

[2]. Coatrieux G., Maitre H., Sankur B., Rolland Y., and Collorec R.," *Relevance of Watermarking in Medical Imaging*". In: Proc. IEEE Conference on Information Technology Applications in Biomedicine, Arlington, USA, pp. 250-255, 2000.

[3]. Parthiban L. and Subramanian R., "*MRI Image Denoising for Telemedicine*" in e-Health Networking, Applications and Services, 2006. HEALTHCOM 2006. 8th International Conference on, 2006, pp. 188-191, 2006.

[4]. Pianykh O. S., "*Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide*" Second Edition, Springer, 2012.

[5]. Liu B., Zhu M., Zhang Z., Yin C., Liu Z. and Gu J., "*Medical Image Conversion with DICOM*" Canadian Conference on Electrical and Computer Engineering, 2007, IEEE, 2007.

[6]. Lim Y. and Feng D., "*Multiple Block Based Authentication Watermarking for Distribution of Medical Images*". In: International Symposium on Intelligent Multimedia, Video and Speech Processing, ISIMP 2004, Hong Kong; 2004. p. 631–634, 2004.

[7]. Tolbal M. F., Ghonemy M. A.,. Taha I. A. and Khalifa A. S.,"*Using Integer Wavelet Transforms In Colored Image-Steganography"* International Journal of Intelligent Computing and Information Sciences, 4(2):1-11, 2004.

[8]. Boucherkha S. and Benmohamed M. A., "*Lossless Watermarking Based Authentication System for Medical Images"*, International Journal of Signal Processing, 1(4):278–81, 2004.

[9]. Coatrieux G., Montagner J., Huang H. and Roux C., *" Mixed Reversible and RONI Watermarking for Medical Image Reliability Protection".* In: 29th International conference of the IEEE,

Engineering in Medicine and Biology Society, Lyon, pp 5653–5656, 2007.

[10].Delforouzi A. and Pooyan M. *"Adaptive Digital Audio Steganography Based on Integer Wavelet Transform"* Circuits System Signal Process, 27:247–259, 2008.

[11].Memon N. and Gilani S., "*Adaptive Data Hiding Scheme for Medical Images Using Integer Wavelet Transform"*. In: IEEE International Conference on Emerging Technologies, Islamabad, Pakistan; pp. 221–224, 2009.

[12]. Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong - *Reversible Image Watermarking Using Interpolation Techniques*. IEEE Transactions on Information Forensics and Security, 5(1):187–193, 2010.

[13].Mostafa S., El- sheimy N., Tolba A., Abdelkader F. and Elhindy H., *"Wavelet Packets-based Blind Watermarking for Medical Image Management*", Open Biomedical Engineering Journal, 4: 93–98, 2010.

[14].Memon N.,*" Watermarking of Medical Images for Content Authentication and Copyright Protection"*, PhD thesis, Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Pakistan, 2010.

[15].Rahimi F. and Rabbani H., *"A Dual Adaptive Watermarking Scheme in Contourlet Domain for DICOM Images"*. Biomed Eng Online, 10:1–18, available at http:// www. biomedical-engineering- online.com/content/10/1 /53, 2011.

[16].Sakkara S., Akkamahadevi D. H. , Somashekar K. and Raghu K., *"Integer Wavelet based Secret Data Hiding by Selecting Variable Bit Length"* International Journal of Computer Applications 48(19): 7-11, 2012.

[17]. Ko L., Chen J., Shieh Y., Hsin H. and Sung T., (2012*)," Nested Quantization Index Modulation for Reversible Watermarking and its Application to Healthcare Information Management Systems*" Computer Math Method Med 2012:1–8, 2012 available at http://www.hindawi.com/journals/ cmmm/2012 /839161/

[18].Pandey V., Singh A. and Shrivastava M., *"Medical Image Protection by Using Cryptography Data-Hiding and Steganography"* International Journal of Emerging Technology and Advanced Engineering, 2(1):106-109, 2012.

[19].An L., Gao X., Xuelong L., Tao D., Deng C. and Li J., *" Robust Reversible Watermarking via Clustering and Enhanced Pixel-wise Masking"*. IEEE Trans Image Process 21(8) : 3598–611, 2012.

[20].Das S. and Kundu M., "*Effective Management of Medical Information through a Novel Blind Watermarking Technique"*. Journal of Med. Syst. 36(5):3339–3351, 2012.

[21].Bouslimi D., Coatrieux G. and Roux C., "*A Joint Encryption/Watermarking Algorithm for Verifying the Reliability of Medical Images: Application to Echographic Images"*. Comput Methods Programs, Biomed, 106(1):47–54, 2012.

[22].Jain M., Choudhary R. C. and Kumar A., *"Secure Medical Image Steganography with RSA Cryptography using Decision Tree"*. In: IEEE Second International Conference on Contemporary Computing and Informatics, 2016.

[23].Mahalakshmi V., Satheeshkumar S. and Sivakumar S., "*Performance of Steganographic Methods In Medical Imaging"*, International Journal of Computational and Applied Mathematics, 12(1):549-556, 2017.

[24].Banjan N. and Dalvi P., "*Medical Data Security using Combination of Cryptography and Steganography with AES-LSB Algorithm*" International Journal of Advanced Research in Electronics and Communication Engineering, 7(7): 673-677, 2018.

[25].G. Coatrieux, *"Contribution à la sécurité d'images médicales par tatouage,"* Université Rennes 1, 2002.

[26].M. Yang, and N. Bourbakis, *"A High Bitrate Multimedia Information Hiding Algorithm in DCT Domain"*, Proceeding of World Conference of Integrated Design and Process Technology (IDPT 2005), Beijing, China, June 13th-17th, 2005.

[27].Diffie W. and Hellman M. E., *"New Directions in Cryptography"*, IEEE Transactions on Information Theory, 22(6): 644 - 654, 1976.

[28].B. Schneier, *"Applied Cryptography"*, Wiley, New-York, USA, 1996.

[29].Allen J. D, "*The Unicode Standard Version 6.0 – Core Specification"*, The Unicode Consortium, Mountain View, CA, 2011.

[30].Shen, Y., Huang, L., Yu, S., "*A Novel Adaptive Data Hiding based on Improved EMD and Interpolation"*. Multimedia Tools Appl. 77 (1), 1–17, 2017, https://doi.org/10.1007/s11042-017-4905-5.

[31].Jung, K., Yoo, K., *"Improved exploiting Modification Direction Method by Modulus Operation"*, Int. J. Signal Process. Image Process. Pattern. 2 (1), 79–87, 2009.

[32].Kuo, W., Wang, C., Huang, Y., *"Binary Power Data Hiding Scheme"*. Int. Journal of Electron. Commun. 69 (11), 1574–1582, 2015, https://doi. org/10.1016/j.aeue.2015.07.007.

[33].Alsaffawi, Z. S. Y., "*Image steganography by using Exploiting Modification Direction and Knight Tour Algorithm"*. J. Al-Qadissiya Comput. Sci. Math. 8 (1), 1–11, 2016.

[34].Wang, Z., Bovik, A., Sheikh, H., Simoncelli, E., *"Image Quality Assessment: from Error Measurement to Structural Similarity"*. IEEE Trans. Image Process. 13 (1), 1–14, 2004.