A ROBUST ENCRYPTION AND DIGITAL WATERMARKING SCHEME FOR DICOM IMAGES USING QUATERNIONS AND DWT-SVD

FATHIMA NASREEN.K[1], P.CHITRA[2]
[1](Department of ECE, Coimbatore Institute of Technology, Coimbatore, India)
[2] (Associate Professor, Department of ECE, Coimbatore Institute of Technology, Coimbatore, India)

Abstract*—The Digital Image and Communication On Medicine (DICOM) images are now subjected for transmission over the internet which bring about concerns regarding data security. The security of the medical images over the DICOM network currently relies on encryption techniques such as Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). These techniques however consume substantial processing time for the medical images. A new lossless encryption technique using quaternions can be adopted which reduces the processing time enormously. The quaternion technique is implemented using counter mode of encryption and modular arithmetic operations. The security of the medical image transmission can even be enhanced by incorporating digital watermarking which serves as an authentication of the sender and also reduces the difficulty in maintenance of multiple documents. The signature of the patient and the patient data are used as the watermark images and they are embedded in the DICOM image using DWT-SVD (Digital Wavelet Transform- Singular Value Decomposition).

***Keywords*— Cryptography, image processing, quaternions, lossless scheme, DICOM, digital watermarking, DWT, SVD.**

I.INTRODUCTION

A. Background

The medical industry has proceeded into the digital age. In every modern hospital the medical images are used in their digital form in the field of diagnosis and treatment of patients. These digital images are also transmitted and shared over the internet where the problem arises concerning the security. To facilitate safe and reliable transmission the Digital Image and Communication On Medicine (DICOM) standard was introduced. DICOM, which has become the most widely implemented and supported communications standard for medical imaging, provides a standard interface and interactive agreement for all sorts of medical imaging equipment produced by different manufacturers. Apart from the above specified standards DICOM also offers security features which are of low degree and the user has to decide and implement the better security features. Encryption is one of the most selected feature for securing the images in the DICOM system. The Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (3DES) are the algorithms which are currently used for encrypting the medical images in the DICOM system and consume more processing time. Hence there is a need for a new algorithm which fulfills the security aspects as well as lessens the processing time.

B. Contribution

In this paper, we propose a new encryption algorithm based on quaternion rotation [2,4,6]. This encryption algorithm not only brings high security but also fast computation speed. In addition to robust and fast encryption, the security of the transmission can also be improved by fusing digital watermarking [12]. The watermark is used as an authentication mechanism for the medical image which avoids a patient's record being altered with another one. The important note is that the proposed algorithm is an ongoing work and hence further studies and understanding are necessary.

C. Structure

The rest of the paper is organized as follows. Section II describes about the related work. The DICOM network is explained in section III. Quaternion calculus and basic concepts are described in section IV and V. Section VI deals with the proposed scheme. Section VII presents the simulation results. Conclusion is drawn in section VIII.

II.RELATED WORK

The DICOM standard did not associate security mechanisms in the earlier versions. As a result, sensitive data were transferred in plain text. The pervasive use of internet in the medical sector necessitates the security measures.

In order to achieve the security, the content is encrypted with AES or 3DES and the keys are exchanged via RSA encryption. It is then possible to store the encrypted content securely with the Picture Archiving and Communication System (PACS).

The objective of this paper is to suggest an alternative way of encrypting DICOM files. It is possible to find some solutions that already address the problem of low efficient encryption with the AES algorithm. However, many of the proposed algorithms achieve higher encryption efficiency than AES, but at the same time they must maintain a trade-off between efficiency and security. This paper is the successor of the one proposed by Dzwonkowski [1]. In his work, he proposed the quaternion encryption for DICOM images and the algorithm was implemented using modified fiestel structure. In this paper the algorithm is implemented using counter mode of encryption which satisfies the security requirements by involving more randomness in the cipher with the use of additional input matrices such as counter matrix and initialization matrix. Hence the intruder has to know the key ,the counter matrix and the initialization matrix in order to break the cipher. This method also reduces the processing time compared to earlier encryption standards (AES). Further improvement of robustness is achieved by using watermarking which acts as an authentication mechanism.

III. DICOM NETWORK

Medical data security is an issue that is evolving simultaneously along with technical development. Due to the rising importance of information, secured data transfer and storage have become a serious problem. Although the DICOM standard defines security in several fields, security in commonly used solutions is focused on outside data transferring. The exemplary DICOM solution uses the TLS, HTTPS, and VPN protocols (defined in the Secure Transport Connection Profiles) for data transfer and access, which obviously correspond to sharing data through the Internet (Fig. 1).

The model presented here assumes that both the internal network, i.e. the network that provides communication between the DICOM storage server and medical equipment, and the storage itself are safe. Because the above can be true in the context of the internal network, the storage server is usually open for external connection, which makes it vulnerable to various attacks. In order to improve security of the data we propose using an encryption server (a front-end server) (Fig. 2) whose primary task is to catch, encrypt (with the proposed quaternion method) and relay the medical data to the storage server without writing data on any media storage. The use of a front-end server eliminates the basic weakness of the standard DICOM network model, i.e. the possibility of accessing unsecured data on the storage server.

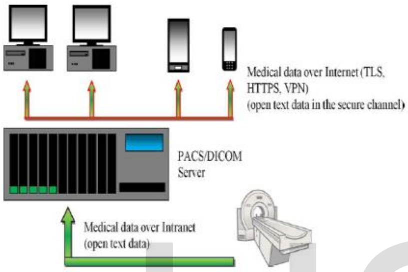

Medical data over Internet (TLS, HTTPS, VPN) (open text data in the secure channel)
PACS/DICOM Server
Medical data over Intranet (open text data)

Fig. 1. The DICOM network

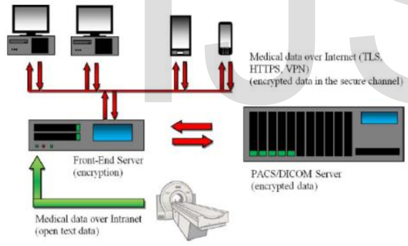

Medical data over Internet (TLS, HTTPS, VPN) (encrypted data in the secure channel)
Front-End Server (encryption)
PACS/DICOM Server (encrypted data)
Medical data over Intranet (open text data)

Fig. 2. The proposed DICOM network with Front end server

IV. Quaternion Calculus

Quaternions are hyper-complex numbers of rank 4 and have two parts – a scalar part and a vector part, which is an ordinary vector in a 3D space R3. A quaternion q is defined by formula [3,5]:

$$q = w + xi + yj + zk \quad (1)$$

where w, x, y, z are real coefficients of quaternion q, and i, j, k are imaginary units with the following properties [3,5]:

$$i^2 = j^2 = k^2 = ijk = -1,\ ij = -ji = k,\ jk = -kj = i,$$
$$ki = -ik = j\ .$$

A quaternion could also be considered as a vector represented by a column matrix (all vectors in this paper are represented by column matrices) or as a composition of scalar part w and vector part v.

$$q = [w\ x\ y\ z]^T \text{ or } q = (w,\ v) = (w,\ [x\ y\ z]^T) \quad (2)$$

The sum of two quaternions $q1$, $q2$ is defined by adding the corresponding coefficients of those quaternions, i.e. in the same manner as for complex numbers [3,5]:

$$q_1 + q_2 = (w_1 + w_2) + (x_1 + x_2)i + (y_1 + y_2)\, j + (z_1 + z_2)k \quad (3)$$

The product $q1 \cdot q2$ of two quaternions $q1$, $q2$ is more complex due to the anti-commutativity of the imaginary units of those quaternions during the multiplication process. The product of the two quaternions $q1$, $q2$ consists of scalar and vector products (∘ denotes the scalar product and × denotes the vector product) [3,5]:

$$q_1 \cdot q_2 = (w_1w_2 - v_1 \circ v_2, w_1v_2 + w_2v_1 + v_1 \times v_2) \quad (4)$$

In this paper · denotes the quaternion multiplication. Furthermore, it is important to define the other properties of quaternions: a conjugate $q*$, a norm $||q||$ and an inverse $q-1$ of a quaternion q:

$$q^* = w - xi - yj - zk, ||q|| = \sqrt{w^2 + x^2 + y^2 + z^2} \quad (5)$$

$$q-1 = \frac{q*}{||q||} \quad (6)$$

It is important to notice that in the case of a unit quaternion, for which the norm is equal to 1, there is the following relation: $q-1 = q*$.

V. Basic Concepts

In order to perform a quaternion rotation, we need to possess a quaternion around which we will be rotating another quaternion. If we consider the rotated quaternion as a data vector in a 3D space, then we will be able to implement the idea of quaternion encryption.

Let us consider two quaternions $q = [w\ x\ y\ z]^T$ and $P = [0\ a\ b\ c]^T$, where a vector $[a\ b\ c]^T$ which represents the vector part of quaternion P with a zero scalar part will store information about a piece of data which we want to rotate around quaternion q. In our case, quaternion P can store the pixel values of a DICOM image. The obtained quaternion $Prot$ will be a spatial mapping of the rotated data vector $[a\ b\ c]^T$. The quaternion rotation is written as:

$$Prot = q \cdot P \cdot q-1 \quad (7)$$

A. Key Generation

The robustness of the algorithm is enhanced by using unique quaternion keys for each round. By using the rotation matrix defined in quaternions infinite number of keys can be generated. By using formula (7) and applying formulas (4), (5), and (6), it is possible to introduce a rotation matrixand write:

$$\text{Prot} = \Gamma(q)\text{P}$$
$$\text{P} = [\text{a b c}]^T,\ \Gamma(q)$$
$$= \begin{bmatrix} \begin{matrix} w^2 + x^2 - \\ -y^2 - z^2 \end{matrix} & 2xy - 2wz & 2xz + 2wy \\ 2wz + 2xy & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wx & \begin{matrix} w^2 - x^2 - \\ -y^2 + z^2 \end{matrix} \end{bmatrix} \quad (8)$$

The key generation procedure is explained in Fig. 3. The key idea is that, treat every column of the rotation matrix as the new quaternion key with the scalar part as zero except for the initial quaternion key. As the number of keys are increased the security is also high. The key note is that higher the rotation order is more quaternion keys of that order is generated. In general, if the number of rounds is n then 3^n number of rotation matrices can be produced. The generation process is iterative in the sense that to get the higher order keys, the lower order keys has to be generated at first.

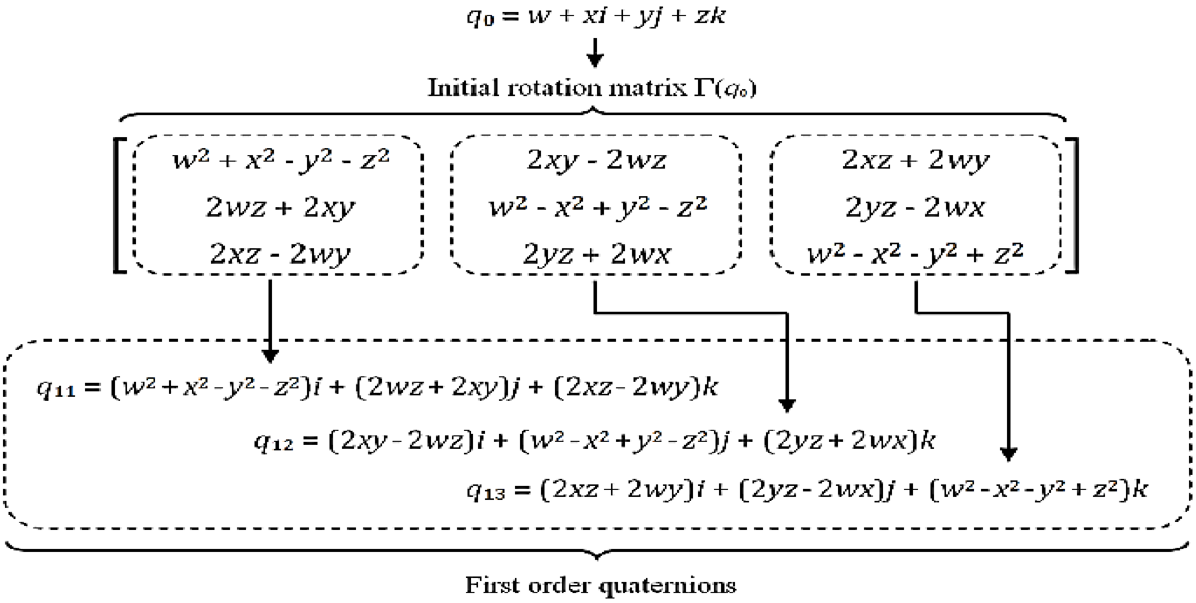

$q_0 = w + xi + yj + zk$
Initial rotation matrix $\Gamma(q_0)$
$w^2 + x^2 - y^2 - z^2$
$2wz + 2xy$
$2xz - 2wy$
$2xy - 2wz$
$w^2 - x^2 + y^2 - z^2$
$2yz + 2wx$
$2xz + 2wy$
$2yz - 2wx$
$w^2 - x^2 - y^2 + z^2$
$q_{11} = (w^2+x^2-y^2-z^2)i + (2wz+2xy)j + (2xz-2wy)k$
$q_{12} = (2xy-2wz)i + (w^2-x^2+y^2-z^2)j + (2yz+2wx)k$
$q_{13} = (2xz+2wy)i + (2yz-2wx)j + (w^2-x^2-y^2+z^2)k$
First order quaternions

Fig. 3.Method of producing first order quaternions from an initial rotation matrix

B. Encryption Concept

The rotation process using quaternions can be optimized by extending the vector part of quaternion P which leads to the new quaternion B ,as shown in the equation (9).

$$P=[0,(a\ b\ c)^T]\ ,\quad B=(0,\begin{bmatrix} a1 & a2 & a3 \\ b1 & b2 & b3 \\ c1 & c2 & c3 \end{bmatrix})\quad (9)$$

The encryption and decryption process for the quaternion method with the new extended quaternion *B* (meant to store data information) is shown in (10) and (11) respectively.

$$Brot= q \cdot B \cdot q{-}1 \quad (10)$$

$$B = q{-}1 \cdot Brot\cdot q \quad (11)$$

Where *Brot* is the rotated quaternion *B.*

C. Discrete Wavelet Transform (DWT)

Wavelet domain is a promising domain for watermark embedding. Wavelet refers to small waves. Discrete Wavelet Transform is based on small waves of limited duration and varying frequency [7]. DWT decomposes image hierarchically, providing both spatial and frequency description of the image [8]. It decompose an image in basically three spatial directions i.e, horizontal, vertical and diagonal in result separating the image into four different components namely LL, LH, HL and HH. LL level is the lowest resolution level which consists of the approximation part of the image.Rest three levels i.e., LH, HL, HH give the detailed information of the image. HVS (Human Visual System) is more sensitive to the low frequency parts (the LL sub-band), so watermark is preferably placed in other three sub-bands to retain the quality of original image.

D. Singular Value Decomposition (SVD)

Singular Value Decomposition transform is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing [9]. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions m x m is given by:

$$M = USV^T \quad (12)$$

where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M.

There are two main properties of SVD to employ in digital watermarking schemes [9, 10]:

1. Small variations in singular values does not affect the quality of image and,
2. Singular values of an image have high stability so; they do not change after various attacks.

E. DWT-SVD

DWT and SVD are used together to improve the quality of the watermarking [10]. Advantages of both these techniques are employed in this watermarking scheme. DWT and SVD are novel techniques used for watermarking so their fusion makes a very attractive watermarking technique.

The algorithm used for watermarking using DWT-SVD is as follows:

1. Use one-level Haar DWT to decompose the cover image into four subbands (i.e., LL, LH, HL, and HH).
2. Apply SVD to HH subband and the watermark, i.e.,$Ak= USV^T$
3. Modify the singular values in HH subband with the singular values of the watermark.
4. ***Signature generation:*** The inputs to the signature generation step are the two orthogonal matrices U and V obtained from the above step and the key.
   i. Sum the column of orthogonal matrices(Usum and Vsum respectively) and choose threshold values for both U and V matrices based on the median value(Uthresh and Vthresh respectively).
   ii. Convert the matrices Usum and Vsum to binary values as follows:
   Usum (or Vsum) >Uthresh (or Vthresh) = 1
   Usum (or Vsum) <Uthresh (or Vthresh) = 0

iii. XOR the two matrices obtained from the above step (UVxor) .

iv. Generate a PSRNG sequence, which is equal to the size of the key and XOR it with UVxor. The resultant matrix is the signature.

5. ***Signature embedding:*** The inputs to this step are the LL subband of the cover image and the signature generated from the above step.

i. Decompose the LL band further to the fourth level using the Haar wavelet.

ii. Concatenate LL4 and HH4 bands which are the resultant from the fourth level decomposition.

iii. Replace the n-thbit position of the above coefficient with the signature bit.

iv. Apply the inverse DWT (4 level) with modified LL4 and HH4 band coefficients.The resultant matrix is named as LLmod.

6. Apply SVD to obtain the modified HH band (HHmod) and apply inverse DWT with LLmod & HHmod band to obtain the watermarked image.

The watermark extraction is the reverse process of the watermark embedding algorithm.

VI. Proposed Scheme

A. Watermark Embedding And Encryption

Initially the DICOM image (cover image) is watermarked with the patient data (watermark) which is in the .txt format using the above specified algorithm. This watermark serves as the verification data to avoid the confusion in maintaining multiple documents belonging to various patients.

The proposed algorithm is designed in such a way that it can encrypt only 8-bit DICOM images. If the image is of 16-bit then it has to be divided into two 8-bit images or of the image is of 32-bit then it has to be divided into four 8-bit images. The encryption is carried out after decomposition for each 8-bit images individually.

A 16-bit DICOM image of size r x c is decomposed into two 8-bit gray color images each of size r x c. One of the two gray tone images is considered as the plaintext B. The plaintext can be written as matrix **B** of equal size (*r* ×*c)*. Each element of matrix **B** is a value in the range of 0-255. The matrix **B** should be rewritten as a matrix with *m* rows and 2*m* columns. If the number of elements in such a matrix exceeds the original amount of the images' pixels then the additional elements are filled with random numbers in the range of 0-255.

The initialization matrix **IM** and the counter matrix **CTR** each of size equal to the data matrix **B** are necessary to be defined in the counter mode of encryption (Fig. 4). Those two matrices consists of random integer values in the range 0-255. In the block diagram n represents number of rounds and N represents modulus value (i.e., 257).However, in every subsequent step, values of elements of the counter matrix **CTR** are incremented modulo 256. The matrices **IM** and **CTR** are XORed together using modulo 256 addtion to yield a new matrix called **CMOD**. Elements of matrix **CMOD** are in the range 0-255 (8-bit data), thus quaternion *C*MOD is considered to be a Lipschitz integer [2,4,6] (a quaternion of integer components). A modular arithmetic of the whole quaternion encryption process was implemented to maintain the Lipschitz integer representation. The matrix **CMOD** is converted to quaternion CMOD and then apply rule (7). Here P is replaced by CMOD.

i.e., $\text{CMOD}' = q \,.\, \text{CMOD}.\ q^{-1}$ (13)

After the quaternion encryption the obtained Lipschitz integer *C*MOD' is converted to matrix **CMOD'** for a bitwise binary addition with a data matrix **B**. As a result the encrypted data matrix **B'** is obtained.

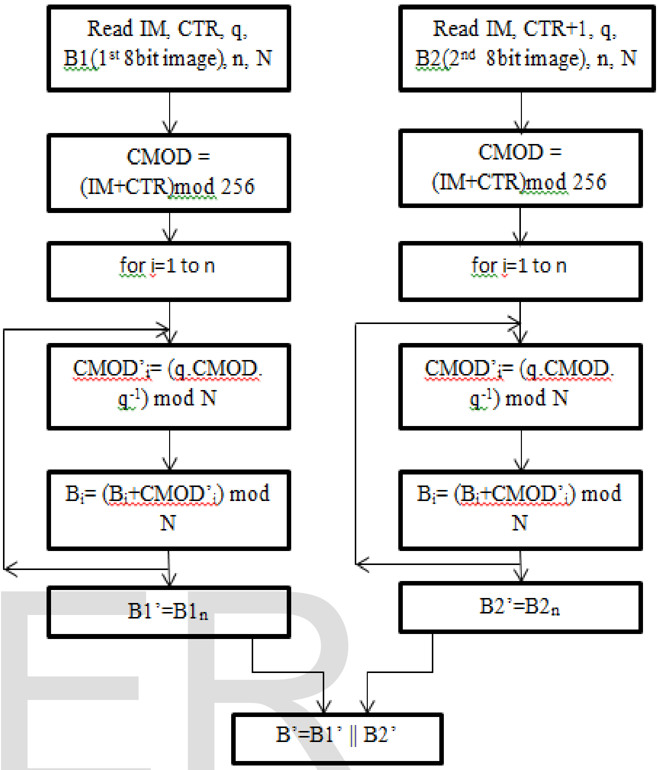

Read IM, CTR, q, B1(1st 8bit image), n, N
CMOD = (IM+CTR)mod 256
for i=1 to n
CMOD'i= (q.CMOD. q-1) mod N
Bi= (Bi+CMOD'i) mod N
B1'=B1n
Read IM, CTR+1, q, B2(2nd 8bit image), n, N
CMOD = (IM+CTR)mod 256
for i=1 to n
CMOD'i= (q.CMOD. q-1) mod N
Bi= (Bi+CMOD'i) mod N
B2'=B2n
B'=B1' || B2'

Fig. 4. Block Diagram of Counter mode of Encryption

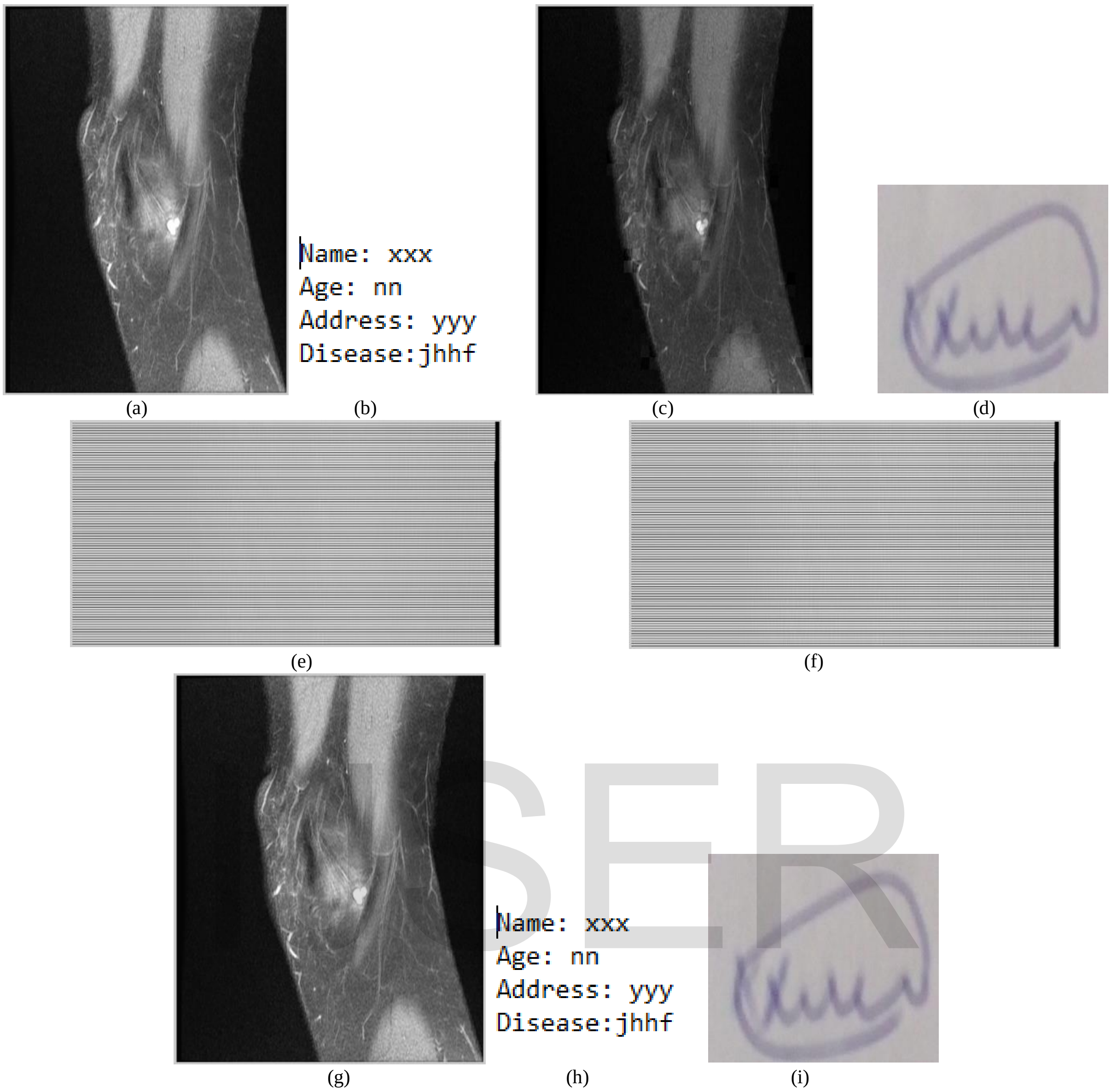
Finally apply the watermarking algorithm to the encrypted data **B'** (cover image) and the signature of the patient (watermark) which is in the .jpg format. This watermark serves as the authentication data which mainly preserves the concept of proof of ownership.

B. Watermark Extraction And Decryption

1. The watermarked image consisting the signature of the patient and the encrypted data is extracted to authenticate the file.
2. The decryption is carried out in the reverse process as that of encryption using counter mode.
3. The watermarked image consisting the decrypted image and the patient data is extracted to verify the file.

C. Modular Arithmetic In Quaternion Encryption

In order to calculate a modular inversion of any integer from the range 0-255, thus also a modular inversion of a Lipschitz integer (which is needed according to rotation rule (7)), it was necessary to choose a special modulus value (a prime number) that together with all the integers in 0-255 would yield their GCD (Greatest Common Divisor) equal to 1. That is why for the grey-tone image we cannot go for the most obvious choice and select a modulus of value 256, because such a number is not prime (256=28)



Name: xxx
Age: nn
Address: yyy
Disease:jhhf

Name: xxx
Age: nn
Address: yyy
Disease:jhhf

Fig. 5. (a) original image (b) patient data(.txt format) (c) watermarked image (with patient data) (d) patient signature (.jpg format) (e) encrypted image (f) watermarked image (with patient signature) (g) decrypted image (h) extracted watermark(patient data) (i) extracted watermark (patient signature).

and will not make it possible to calculate a modular inversion for most cases. Instead, we use a modulus equal to prime integer 257 – therefore obtaining values of the range 0-256 for all matrices **CMOD’**. Such values do not affect the decryption process because of two facts. Firstly, in order to decrypt data matrix **B’** a matrix **CMOD’** is needed (due to XOR operation) and is obtained in the same manner as in the en-cryption process. Secondly, all additional values equal to 256 in matrix **CMOD’** are interpreted as 0 when XOR’ed with values of data matrix **B**. Thus values obtained in encrypted data matrix **B’** are of range 0-255.

VII. SIMULATION RESULTS

The simulation is carried out for different size of images for 9 rounds. For simplicity , we present the result for a 512 x 512 image (Fig. 5). The images are acquired from the dicom library [13]. The encrypted image is of size 364 x 728 (m x 2m).

A.Computation Speed

The computation speed of the counter mode of encryption is compared with the AES. The machine used for the test was: Intel Pentium(R) CPU A1018 2.10 GHz, 1.89 GB RAM. From Table I, it is shown that counter mode of encryption reduces the processing time.

VIII. CONCLUSION

In this paper a robust encryption and digital watermarking scheme for DICOM images has been presented. The encryption is carried out using counter mode of encryption and the watermarking is applied using DWT-SVD technique. The fast computation speed of the

TABLE I Comparison of computation speed

AES	256 x256 px	512 x512 px
Encryption time (s)	4081.677	8120.635
Decryprion time (s)	4667.859	9113.308
Counter mode	256 x256 px	512x512 px
Encryption time (s)	162.976	304.732
Decryption time (s)	188.564	347.065

encryption makes it useful for encrypting large size medical data. The robustness is still enhanced by the watermarking technique. The patient data can be used as the verification data in times when the documents are confused with one another. The watermark serves as the proof of ownership of the medical data.

REFERENCES

[1]Mariusz Dzwonkowski, Michal Papaj, and Roman Rykaczewski, “A New Quaternion Based Encryption Method for DICOM Images”, IEEE Transactions on Image Processing, vol. 24, no. 11, November 2015.

[2]T. Nagase, M. Komata, and T. Araki, “Secure signals transmission based on quaternion encryption scheme,” in *Proc. 18th Int. Conf. Adv. Inf.Netw. Appl. (AINA)*, vol. 2. 2004, pp. 35–38.

[3]F. Zhang, “Quaternions and matrices of quaternions,” *Linear Algebra Appl.*, vol. 251, pp. 21–57, Jan. 1997.

[4]M. Dzwonkowski and R. Rykaczewski, “Quaternion encryption method for image and video transmission,” *Telecommun. Rev. + Telecommun.News*, vol. 8, no. 9, pp. 1216–1220, 2013.

[5]R. Goldman, “Understanding quaternions,” *Graph. Models*, vol. 73, no. 2, pp. 21–49, 2011.

[6]B.Czaplewski, M.Dzwonkowski, and R.Rykaczewski, “Digital fingerprinting based on quaternion encryption scheme for gray-tone images,” *J. Telecommun. Inf. Technol.*, vol. 2, pp. 3–11, Jul. 2014.

[7]Chunlin Song, SudSudirman, MadjidMerabti, “Recent Advances and Classification of Watermarking Techniques in Digital Images*”, ISBN: 978-1-902560-22-9* © 2009 PGNet.

[8]Vaishali S. Jabade,Dr. Sachin R. Gengaje, “ Literature Review of Wavelet Based Digital Image Watermarking Techniques”, *International Journal of Computer Applications (0975 – 8887*) , Volume 31– No.1, pp. 28-35, October 2011.

[9]Manjunath. M, Prof. Siddappaji, “A New Robust Semi blind Watermarking Using Block DCT and SVD”, *IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),* pp. 193-197, 2012.

[10]Chih-Chin Lai, Cheng-Chih Tsai, “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition”, IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, November 2010.

[11]Xing-Yuan Wang, Sheng-Xian Gu,” New chaotic encryption algorithm based on chaotic sequence and plain text”, Published in IET Information Security, doi: 10.1049/iet-ifs.2012.0279.

[12]P. Viswanathan, Member, IEEE, and P. Venkata Krishna, Senior Member, IEEE , “A Joint FED Watermarking System Using Spatial Fusion for Verifying the Security Issues of Teleradiology”, IEEE journal ofbiomedical and health informatics, vol. 18, no. 3, May 2014.

[13]Dicomimages :[online] Available: www.dicomlibrary.com.