ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 9, September 2016

Quaternion Rotational Approach for Encryption of Images

C. Lakshmi Sai, M. N. Giri Prasad

***Abstract*—Image encryption is a vital process used in many applications like defence, military, medicine etc. which require secure transmission of data. Advancements in information and technology made it necessary to cope up with the new encryption techniques that are evolving day-to-day. This paper proposes one such advanced technique for image encryption which maintains a trade-off between the speed and security. This paper mainly focuses on quaternion based loss-less encryption of medical (DICOM) images, but this technique can also be applied to other images also. The special property of quaternions i.e., quaternion rotation is the fundamental principle of the entire encryption process. In this paper we analyze the already existing quaternion based image encryption method and we make some significant changes in the algorithm that ensures the increase in the security level of the encrypted image. Detailed analysis with regard to security analysis and implementation are given.**

***Index Terms*—Encryption, Quaternion rotation, Security, medical images.**

I. INTRODUCTION

Digital image is a two dimensional arrangement of pixels such that they give information about the positions, sizes and inter-relationship between the objects. Acquiring information by looking at an image is more convenient than going through the text. Hence digital image processing has acquired irreplaceable position in our day to day activities.

As the world is entering into a fully digitalized era, the same is happening even with the medical industry. Instead of sending the reports of patients in a paper format, now they are digitalized and are transmitted over computerized networks with full security as some of them might be confidential and while transmitting them over computerized networks, they are prone to vulnerable attacks. So it is quite necessary to encrypt the medical data before transmitting it over a network.

A. *Background*

Digital imaging and Communication in Medicine (DICOM) [1] is a standard for handling, storing and transmitting information in medical imaging. The DICOM standard was developed for reliable and secure transmission of medical data. It also offers low degree of security and it is the choice of implementer to decide the degree of security features needed. Due to the increasing importance of information, secured transfer and storage of data has become a serious issue. Currently, the techniques used in the transmission and communication of medical data i.e., DICOM images are Advanced Data Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES) algorithms [1]. These are the traditional methods used in encryption and cryptography that take substantial time and are vulnerable to advanced security attacks. Hence there is a need to meet the requirements of the modern day technology. Here, Quaternions come into the picture which will offer more security than the existing traditional methods along with the increased speed of operation when implemented effectively.

B. *Contribution*

In this paper, we analyze an algorithm for encryption of images based on quaternion rotation. While developing our encryption algorithm, we observed that it is possible to modify the cipher to achieve security as well as fast computation speed. The main purpose of this paper is to show that it is possible to secure large volumes of medical data by introducing a lossless and fast encryption process. Though some changes are needed to be made in the DICOM network structure, it will add on with another benefit of increased security than the existing methods. While analyzing the algorithm and comparing the existing methods, it is necessary to obtain a trade-off between the security and computation speed. Securing medical data through adaptive encryption is very promising for reducing the processing time and improving the security level. Encryption based on quaternions can be computed quickly than matrix multiplication. The secondary focus is to propose ideas for future research and analysis. The content of this paper could be considered a potential impetus to proceed for further research. There is a lot of scope for future work in this area and can be worked upon to achieve tremendous result towards cryptography.

C. *Structure*

Information regarding quaternion calculus is given in section 2. The main principle involved in this proposed encryption algorithm is explained in section 3. The key matrix required for the encryption and its generation is defined in section 4. Section 5 gives detailed explanation of the proposed algorithm, its structure and flow charts. Section 6 and section 7 explains the simulation results and comparison of the proposed algorithm with that of existing algorithm [9]. Various security attacks are presented in section 8. Conclusions are discussed in section 9.

Manuscript received Sep, 2016.
***C Lakshmi Sai**, ECE Department, JNTUA College of Engineering, JNTU Anantapuram, Anantapur, India, 8500219759*
***M.N.Giri Prasad**, ECE Department, JNTUA College of Engineering, JNTU Anantapuram, Anantapur, India.*

II. QUATERNION CALCULUS

Quaternions [2] are hyper complex numbers of rank 4 and have two parts – a scalar part and a vector part which is an ordinary vector in 3D space. A quaternion q is defined by a formula [2],[3]:

$$q = a + bi + cj + dk \quad (1)$$

where a, b, c, d are real coefficients of quaternion and i, j, k are the imaginary units with the following properties:

$$i^2 = j^2 = k^2 = ijk = -1;$$
$$ij = k = -ji;$$
$$jk = i = -kj; \quad (2)$$
$$ki = j = -ik;$$

A quaternion could also be considered a column vector represented as

$$q = [\text{a b c d}]^T$$

$$\text{or } q = (\text{a}, \vec{v}) = (\text{a}, [\text{b c d}]^T) \quad (3)$$

The sum of two quaternions q1, q2 is obtained by adding the corresponding coefficients similar to that of adding two complex numbers [2], [3]:

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k \quad (4)$$

The product of two quaternions is more complicated due to the anti-commutative property i.e., as in the real numbers, the product of two quaternions is not commutative. The product of two quaternions q1, q2 consists of a scalar product and a vector product.(◦ denotes the scalar product and × denotes the vector product) [4]:

$$q_1.q_2 = (a_1 a_2 - \vec{v_1} \circ \vec{v_2}, a_1 \vec{v_2} + a_2 \vec{v_1} + \vec{v_1} \times \vec{v_2}) \quad (5)$$

In this paper,'.'denotes the quaternion multiplication. It is important to define other properties of quaternions like conjugate, norm and inverse of a quaternion.

Conjugate $q^* = a - bi - cj - dk$

Norm $\|q\| = \sqrt{a^2 + b^2 + c^2 + d^2}$

Inverse $q^{-1} = \frac{q^*}{\|q\|^2} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$

III. QUATERNION ROTATION

There are many ways of representing rotations of objects in three-dimensional space. One of them is by using quaternions. The possibility of using the Euler representation also exists; however, quaternions, due to their unique properties, have become much more popular. In order to obtain 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 three-dimensional space, then we will be able to implement the idea of quaternion encryption. Let us consider two quaternions $P=[b\ c\ d]^T$ and $q=[w\ x\ y\ z]^T$, where a vector $[b\ c\ d]^T$ represents vector part of the quaternion P with a zero scalar part will store information about a piece of data which we want to rotate around quaternion q. The obtained quaternion P_{rot} will be a spatial mapping of the rotated data vector $[b\ c\ d]^T$. The quaternion rotation is represented as:

$$P_{rot} = q.P.q^{-1} \quad (6)$$

The above equation forms the pillar for the entire encryption process proposed in this paper.

IV. GENERATION OF KEY MATRIX

In order to perform encryption of the image or data, we need a Key or Cipher matrix which is generated using the Rotation matrix of the quaternions. The rotation matrix for a given quaternion $q=[w\ x\ y\ z]^T$ is represented as follows[4]-[6]:

$$\Gamma(q) = \begin{bmatrix} w^2 + x^2 - y^2 - z^2 & 2xy - 2wz & 2xz + 2wy \\ 2wz + 2xy & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wx & w^2 - x^2 - y^2 + z^2 \end{bmatrix} \quad (7)$$

The rotation matrix defined above will allow us to calculate the quaternion key matrix without the additional need of quaternion calculation tools. The rotation matrix shown in equation (7) is directly linked to the given quaternion. It is also possible to calculate higher rotation matrices which will increase the security of the encrypted data. The process of creating first order quaternionsfrom initial rotation matrix can be as shown in the following figure:

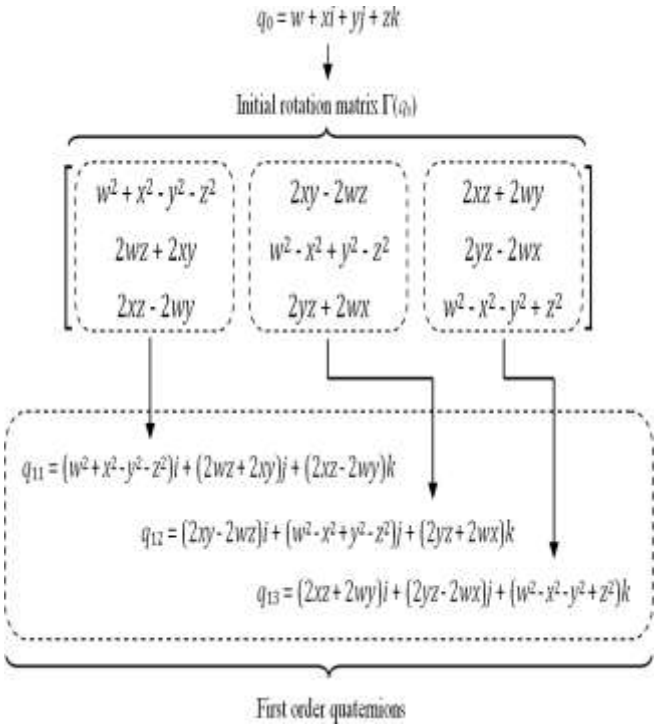

Fig. 1. Creating first order quaternions from initial rotation matrix

From the above figure, it is easy to notice that as the rotation order increases, more number of quaternions of that

order will be obtained, from which other rotation matrices can be calculated. If we assume m as a rotation order, then the number of rotation matrices obtained for that order n will be equal to 3^n. So, in order to obtain higher order matrices, we need to define lower order matrices first i.e. the process is iterative.

V. Proposed Scheme

A. Encryption Concept

The quaternion encryption method implemented in our algorithm is entirely based on quaternion rotation (6). The medical image i.e. DICOM image is a 16-bit image. As the quaternions can be currently applied to only 8-bit images, it is needed to split the DICOM image into two 8-bit images by separating higher and lower order pixels as shown in the following figure:

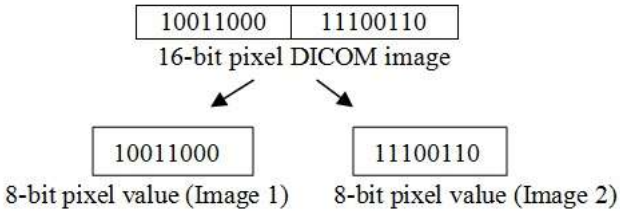

Fig. 2. Decomposition of a DICOM image

After decomposing the DICOM image into two binary images, encryption has to be performed on each 8-bit image independently. If there is a 32-bit image, then it is to be divided into 4 eight bit images and encryption has to be done to each image individually.

Let the given image be B and initial quaternion be q, then the encryption and decryption processes are based on the following equations:

$$B_{rot} = q.B.q^{-1} \quad (8)$$

$$B = q^{-1}.B_{rot}.q \quad (9)$$

where Brot is the rotated quaternion B. Each data quaternion B can be encrypted with a different higher order quaternion key q computed according to the rotation matrix algorithm (Fig. 1).

B. Quaternion rotation based algorithm

The proposed algorithm can be used to images as well as textual data. The proposed scheme is based on a modified Fiestel cipher network which is similar to the one proposed by Sastry and Kumar [8].

In order to encrypt a 16-bit DICOM image of size p xq, we need to first decompose it into two 8-bit gray tone images each of size p x q as shown in (Fig. 2). The two images are taken as input to our algorithm. Each image will be encrypted separately.

Let us now consider a plain text T, which is taken from one of the two obtained gray tone images. The plain text is written as matrix **T**of equal size (p x q). Each element of the matrix is in range 0-255. Now, for the purpose of algorithm, the matrix has to be rearranged into m rows and 2m columns. If the numbers of elements in the matrix are not sufficient, then the remaining elements are to be filled with random numbers in the range 0-255. The new obtained matrix is divided into two square matrices each of size (m x m) **L** and **R.** These matrices are then written as quaternions L and R. In our work, the matrix multiplication is replaced with quaternion multiplication.

The algorithms for encryption and decryption are shown in the following figures.

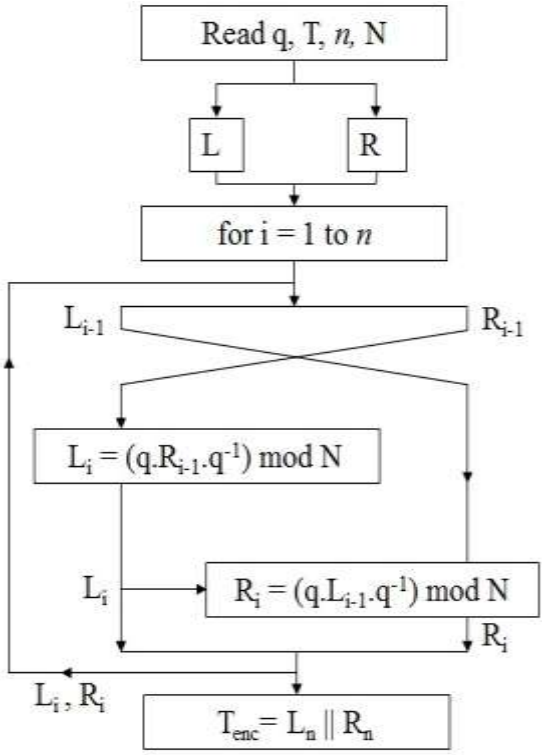

Fig. 3. Process of Encryption for the proposed quaternion scheme

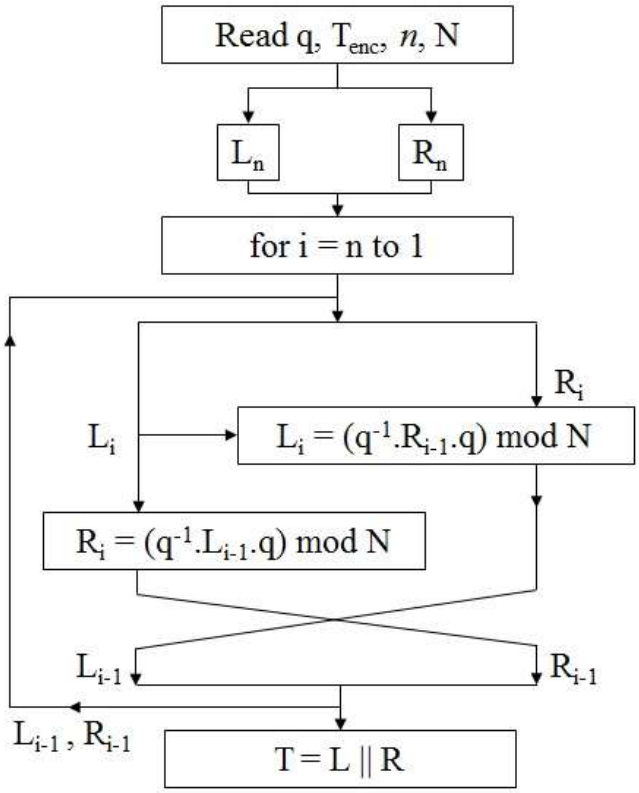

Fig. 4. Process of Decryption for the proposed quaternion scheme

VI. Simulation Results

The proposed scheme is scrutinized on computer based simulation. The entire algorithm is implemented in MATLAB2014a. For our tests we performed 4 rounds in the proposed scheme (each round with two different quaternion keys) and compared it with the existing quaternion encryption method [9] over a machine whose configuration is Intel(R) Core(TM) i3-5020U CPU @ 2.20GHz, 4 GB RAM, 64 bit Win 10; The results of encryption and decryption are shown in the following figures:

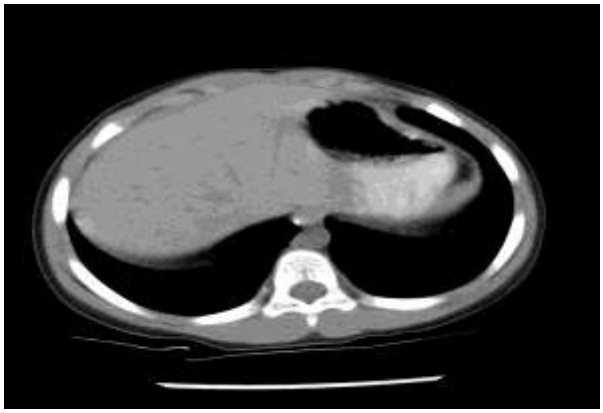

Fig. 5. Original Image

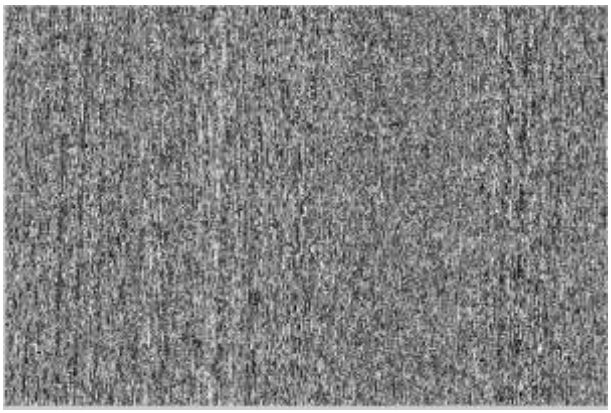

Fig. 6. Encrypted Image

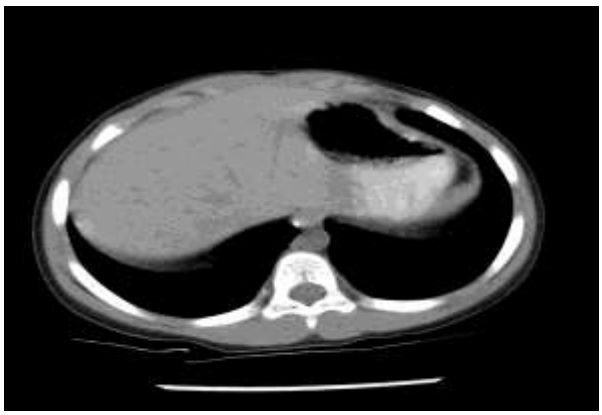

Fig. 7. Decrypted Image

The histograms of both encrypted and original images are shown in the following figures:

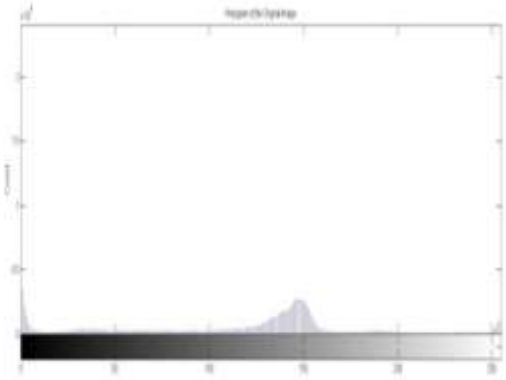

Fig. 8. Histogram of the original image

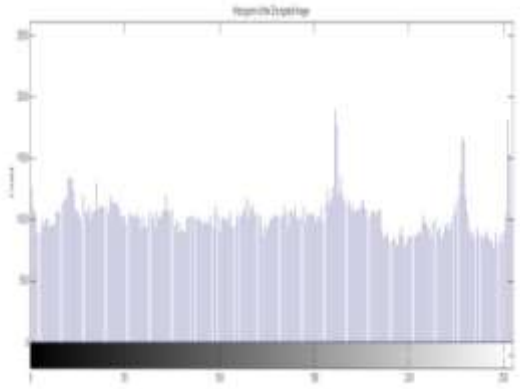

Fig. 9. Histogram of the encrypted image

From (Fig.8), we can see that the pixels of the encrypted image are governed by the uniform distribution.

VII. Comparison

The following table shows the performance of both existing method and the proposed method in terms of various parameters.

Table 1

Comparison of Various Parameters of Existing and Proposed Algorithms

Parameter	Existing Algorithm	Proposed Algorithm
Execution time [s]	5.36	4.23
Correlation	1	1
MSE	7.727e-07	4.846e-18
PSNR(dB)	30.79	32.68

VIII. Security Attacks

The proposed algorithm is implemented and checked against various attacks like plain text attack, brute search attack and differential attacks. It is impossible for the intruder to predict the correct image even if he knows 99% information regarding the cipher. The proposed algorithm is verified for the avalanche effect i.e. if one bit change occurs in the key, then there will be 50% difference between the original encrypted image and the obtained image.

IX. CONCLUSION

According to the simulated results given in this paper, we can conclude that the good randomness of bit sequences can be obtained using the proposed method and the vulnerability to attacks is also verified considering various security attacks. The proposed method is also efficient in terms of speed and security even for the large volumes of medical data. Hence, this quaternion based method will assist as an important application for encryption of image as well as data. This quaternion based encryption method can be further improved to apply directly for 16-bit image and changes can be made to the algorithm to make it more robust in future.

REFERENCES

[1] *Digital Imaging and Communication in Medicine (DICOM) Part 15: Security and System Management Profiles*, NEMA, Rosslyn, VA,USA, 2008
[2] R. Goldman, "Understanding quaternions," *Graph Models*, vol. 73, no. 2, pp. 21-49, 2011.
[3] F. Zhang, "Quaternions and matrices of quaternions," *Linear Algebra,Appl.*, vol. 251, pp. 21–57, Jan. 1997.
[4] D. Eberly. (2010). Quaternion algebra and calculus. Geometric Tools, LLC.[Online]. Available: http://www.geometrictools.com/ Documentation/Documentation.html
[5] T. Nagase, R. Koide, T. Araki, and Y. Hasegawa, "Dispersion of sequences for generating a robust enciphering system,"*ECTI Trans. Comput. Inf. Theory*,vol. 1, no. 1, pp. 9–14, May 2005.
[6] C. Corrales-Rodrigáñez, "Rotations and units in quaternion algebras," *J. Number Theory*, vol. 132, no. 5, pp. 888–895, 2012.
[7] 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.
[8] V. U. K. Sastry and K. A. Kumar, "A modified Feistel cipher involving modular arithmetic addition and modular arithmetic inverse of a key matrix," *Int. J. Adv. Comput. Sci. Appl.*, vol. 3, no. 7, pp. 40–43, 2012
[9] 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.

C Lakshmi Saiis currently pursuing post-graduation in Digital Electronics and Communication Systems specialization from ECE Department, JNTUA College of Engineering, Anantapur, Andhra Pradesh, India.

M.N.GiriPrasad,is currently a professor in JNTUA College of Engineering, Anantapur, Andhra Pradesh, India. His current research mainly focuses on Digital Image Processing, VLSI Design and Embedded Systems.