

# A Secured Patient Health Record Using Encryption Algorithm

<sup>1</sup>Sheela Sobana Rani.K, <sup>2</sup>Ms.R.Lavanya, <sup>3</sup>Ms.Gayathri.R

<sup>1</sup>Associate Professor, <sup>2,3</sup>Assistant Professor

<sup>1</sup>Sri Ramakrishna Institute of Technology, Coimbatore-641010, India

**Abstract -** Medical data includes diagnosis results, patient medical data details and recommendation by the doctors. In hospitals these data are considered as a valuable asset and it is stored securely. The Encryption Technique is proposed to secure and store the medical images; this method is done by MATLAB operator. The medical images as CT scan and MRI scan is given as input image, it gets confused and diffused image to obtain an encrypted image. In the encryption process, a single private key is generated which is same for decryption process. This single private key is known only by authorized users where unauthorized parties are prevented from accessing these medical data. The Inverse process of confusion and diffusion is performed to obtain the decrypted image. Then Hash Algorithm is performed at the output of the confused image, Hash cannot apply in the diffused image that is an encrypted image. When applying MD5, 32 digit hexadecimal number is got as output for given image. Hence with the single private key for both encrypted and decrypted image is stored securely by using MATLAB operator.

**Index Terms -** CT scan, MRI scan, MD5, PSNR, Histogram.

## I INTRODUCTION

The health care industry is the most predominant and it is the fastest developing industries in the world. [4, 7, 9] It comprises of preventive, diagnostic, remedial and prescriptive details by physician, nurses and hospitals. It also contains medical equipment for treatment, pharmaceutical and health insurance firms. All the documents of health care industry consider as medical image should retain for future use and analysis of health information.

In order to maintain standards of those medical images, Digital Imaging and Communication in Medicine (DICOM) format is used by health care organizations. [1] Short and long term history about the health information of the country and other related information can be easily collected using these medical data.

There are many ways to compromise the user data. Deletion or alteration of files without backup of the original contents is an obvious example. Loss of an encoding key may result in active destruction of data. [3, 5] Unauthorized parties must prevent from accessing the sensitive data. Data security involves encrypting the data and also ensuring that appropriate policies adopted for data sharing.

For patient's medical data, CIADS (Confidentiality-Integrity-Authentication based Data Store) is provided.

## II Related Work

### *Secure threshold multi authority attribute based encryption without a central authority:*

This paper considers a stronger adversary model that the corrupted authorities are allowed to allot in appropriate secret keys to the users. The security proof is based on the secrecy of the underlying joint zero secret sharing protocol and joint random secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. [2, 7]

### *Efficient Multi-level Threshold Attribute Based Encryption:*

In this paper a new methodology is presented for a multi-level threshold attribute established encryption method whose cipher text size is independent of the amount of features and it is based on the size of the policy. [8]

### *Attribute-Based Encryption with Fast Decryption:*

This work focuses on designing ABE schemes with fast decryption algorithms. [9] This restrict our attention to expressive systems lacking of system-wide bounds or restrictions, such as placing a limit on the number of features used in a cipher text or a private key. In this setting, present the first key-policy ABE system where cipher texts can be decrypted with a constant number of pairings.

### *Cipher text-Policy Attribute-Based Encryption with Short Keys:*

Cipher text-policy attribute-based encryption (CP-ABE) allows a user with some attributes to decrypt the cipher texts associated with these attributes. [6]

### *Multi-Authority Attribute Based Encryption:*

This scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. [8, 10]

### *Distributed Attribute-Based Encryption:*

In DABE, a number of parties is present to continue attributes and their matching secret keys. This is in stark contrast to the classic CP-ABE schemes, [7] where all secret keys are distributed by one central trusted party. During encryption and decryption process construction of DABE scheme is very efficient because of its constant number of pairing operations.

### III PROPOSED METHOD

For handling, storing, transmitting and printing information in medical imaging DICOM images are used. It includes a network communication protocol and file format definition.



Figure 1. DICOM images

#### 3.1 Encryption:

Encryption is a technique when the input is given, it is converted into cipher text or confused image. Encryption consists of confusion and diffusion process. Pseudo code 1 and 2 explains the functions done for encrypting the patient's medical data. Let image of size  $M \times N$  is the input of the algorithm.

Encrypted image of the same size will be the output. Let  $I$  denotes the image pixel matrix. Confusion column creates a scrambled image from the input image. In the algorithm row sum is calculated by adding all the elements of the a row. Then modulo2 is calculated for row sum . If the result of the modulo is zero then right circular shift with  $KR$  applied, else left circular shift applied. This activity carried out for all the rows of the matrix. Once the row confusion completed, then the column confusion is done with the key  $KC$ .

Confusion columns are obtained by adding all the elements of a column, and use those information for up or downshift and it is done based on the  $colmod$  value. Apply for all the columns, resulting scrambled image taken as input for diffusion and carried for rows and columns. XORing the row pixel values with the corresponding  $KC$  value gives the row diffusion. Column diffusion by ing the column pixel values with the corresponding  $KR$  value and applied to all the rows and columns respectively, producing encrypted image.

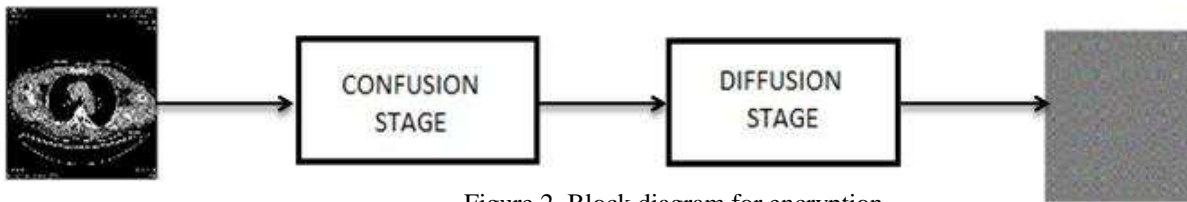


Figure 2. Block diagram for encryption

*Flow chart for encryption:*

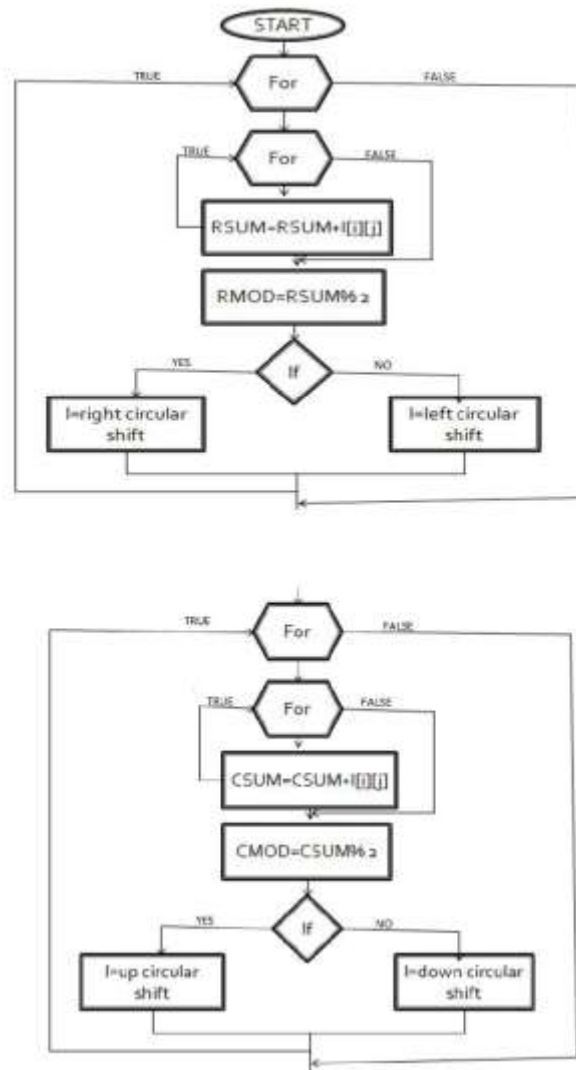


Figure 3. Flow chart for encryption

**3.2 Decryption:**

Decryption is a reverse process of encryption, its convert the cipher text into original image or text. Decryption adopts inverse diffusion and confusion. Algorithm 3 and 4 details the pseudo-code for above said operations. Inverse diffusion applied for encrypted image.

First the column elements are XORed with the corresponding KR value. Then the row elements are XORed with the corresponding KC value. Because of this process, a scrambled image is formed from encrypted image and also inverse confusion obtains scrambled image. The column elements are added together to get colsum and it uses modulo2 operation. Depending on the modulo value, up or down shift is done and performed for all the columns. Modulo2 operation is applied for rowsum to get rowmod., Right or left shift is used which is based on rowmod value and the same operation is done for all the columns which inturn produces original image.

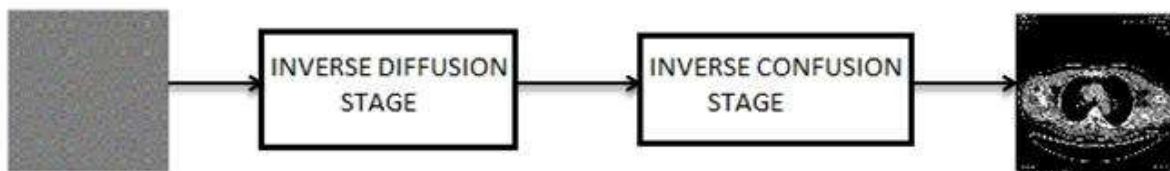


Figure 4. Block diagram for decryption

**3.3 Hash Method:**

Hash method is calculated from the output of confusion process. Since the diffusion leads to the collision process, hash cannot apply for the output of diffusion that is an encrypted images. 128 byte message digest of the confused image is calculated by using SHA-512 algorithm. Dividing the output eight 16 byte and performing XOR operation with neighboring value. Logistic map operation performance for the XOR-ed output. Uses MD5 for concatenating the result of the previous operation. When applying MD5, a 32 digit hexadecimal number is got as output for given image. The resultant hash value verifies the integrity of user's data.

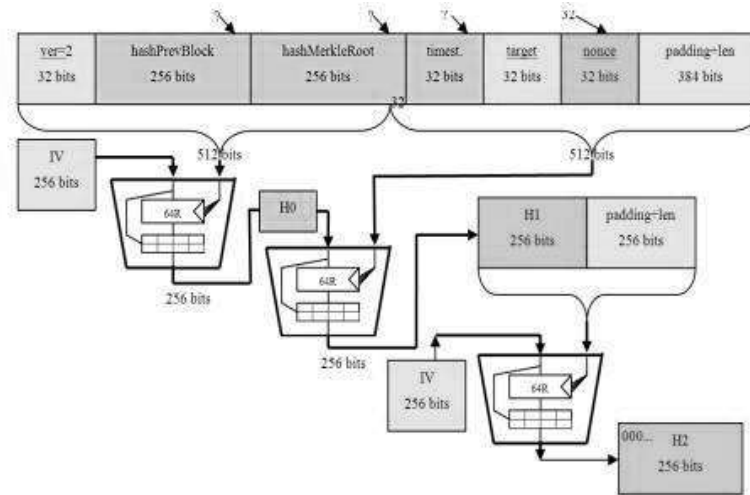


Figure 5. Block diagram for hash method

**3.4 MD5:**

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is a nonlinear function. One function is used in each round denotes a 32-bit block of the message input, and key, denotes a 32-bit constant, different for each operation denotes a left bit rotation by s places. MD5 process a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words). The message is padded so that its length is divisible 512.

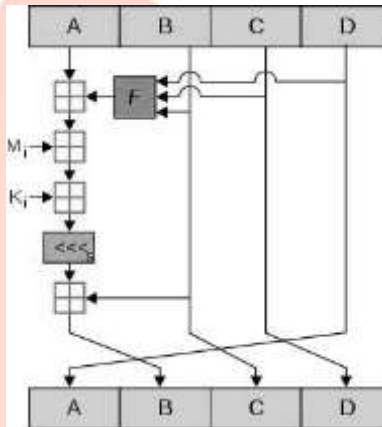


Figure 6. Block diagram for MD5

**Algorithm 5 –Combined Hash +MD5algorithm:**

**Input:** Frames  
**Output:** Hash Value for each frame  
**for** each frames **do**  
 128 byte message digest = SHA-512 of the image  
 divide 128 bytes into eight 16 bytes  
 calculate XOR for the nearest pair, that produces four output  
**for** each XOR output **do**  
 $X_{n+1} = Y_{n+1} (1 - X_n)$   
**end for**  
 concatenate  $X_{n+1}$  values  
 MD5 to obtain 32 digit hexadecimal number  
**end for**

**IV RESULTS AND DISCUSSION**

Medical image database contains diagnostic, preventive, re-medical and prescriptive details by physicians, nurses and hospitals maintained in DICOM format. The preprocessed data is given as input to proposed method for encryption. Sample test images CT scan images are given as input. Then these test images are encrypted using the pseudo code algorithm.

**4.1 CT scan output:**

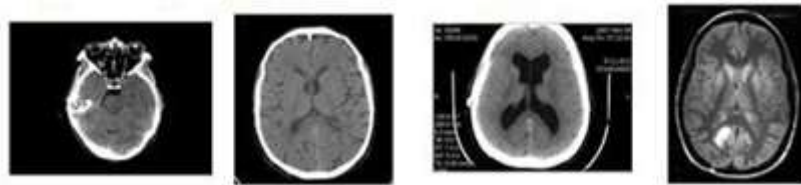


Figure 7. Input image-CT



Figure 8. Confused image-CT

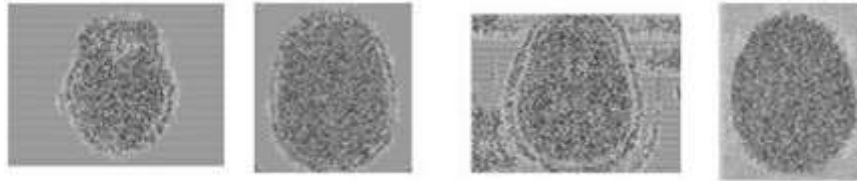


Figure 9. Encrypted image-CT

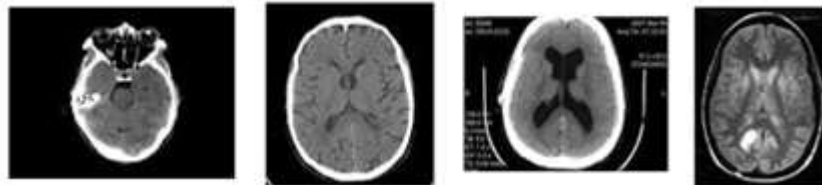


Figure 10. Decrypted image-CT

**4.2 MRI scan output:**



Figure 11. Input images -MRI



Figure 12. Confused image-MRI

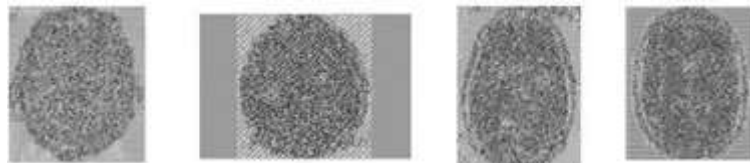


Figure 13. Encrypted images-MRI



Figure 14. Decrypted image

**V EXPERIMENTAL ANALYSIS**

**5.1 PSNR analysis:**

The proposed new encryption algorithm is applied to various DICOM format images, and taking the outputs. Verify the results with PSNR values for QoS analysis. Quality parameters of the reconstructed compression images or videos are measured by Peak Signal to Noise Ratio (PSNR) value. In this analysis, original DICOM data is considered as a signal and the compressed data is considered as noise. PSNR value is calculated by using the Equations 1, 2 and 3 used to analyze the quality of reconstructed health care data.

The equations to calculate PSNR values as follows,

Mean Square Error [MSE]:

$$d(f(x, y), f^*(x, y)) = \|(f(x, y) - f^*(x, y))\|^2 \tag{1}$$

$$= 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ((f(i, j) - f^*(i, j))^2)$$

Where  $f(x, y)$  is the original image and  $f^*(x, y)$  is the reconstructed image,  $m$  and  $n$  are the size of the image.

Table 1 represents PSNR values of CT scan- ABE algorithm vs. proposed algorithm

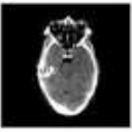
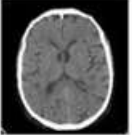






S.No.	Image	ABE Method	Proposed Method
1		26	30
2		40	43
3		29	31
4		50	51

Table 2 represents PSNR calculations of MRI scan- ABE algorithm vs. Proposed algorithm

S.No.	Image	ABE Method	Proposed Method
1		42	43
2		26	28
3		50	51

4		42	43
---	---	----	----

**CT scan:**

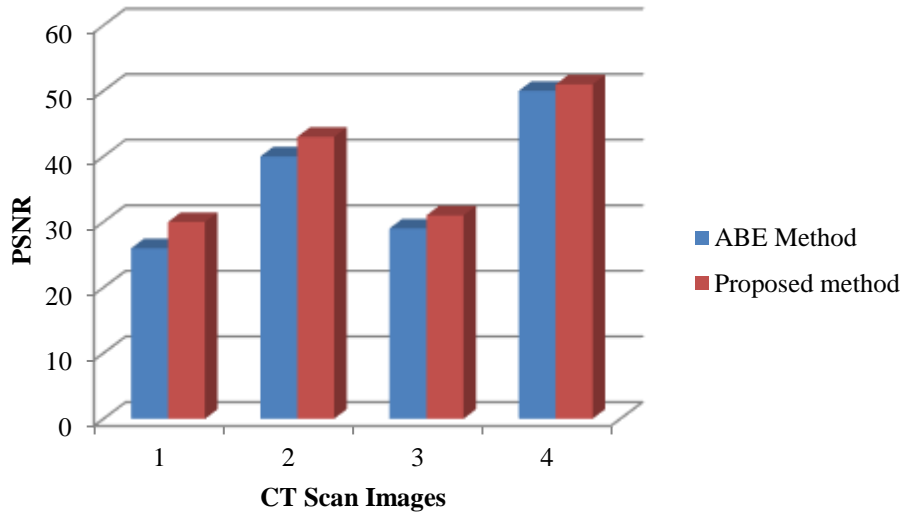


Figure 15. PSNR values-proposed algorithm vs ABE algorithm

**MRI scan:**

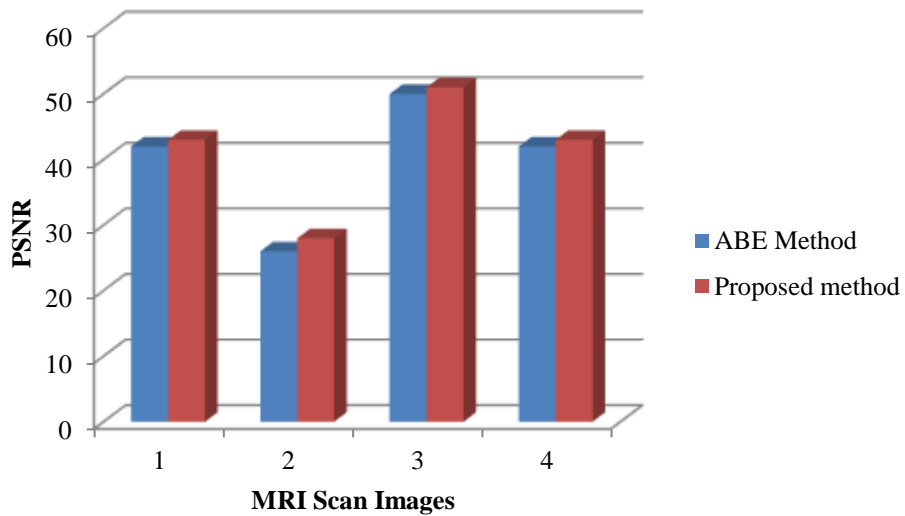


Figure 16. PSNR values- Proposed algorithm vs ABE algorithm

The above table (5.1) shows the comparison of PSNR value between proposed method and existing method (ABE algorithm). The proposed method has high PSNR value than the existing method.

**5.2 Histogram analysis:**

Figure (5.3) illustrates the histogram result of the input image, encrypted image and decrypted image. This result shows that the encrypted image entirely differs from the original images due to this, middle way attacks are not possible, implies statistical attacks; differential attacks are avoided due to variation between original and encrypted image. This analysis reveals that the quality of the retrieved data is much similar to the original data.

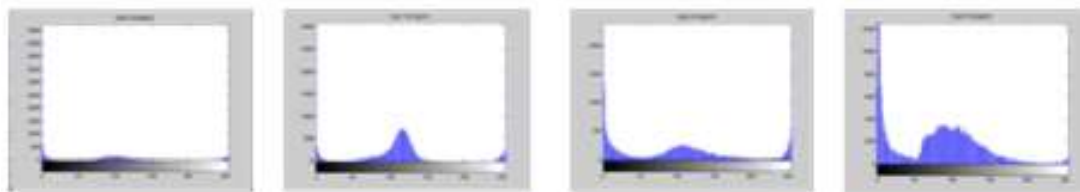


Figure 17. Histogram image for CT input

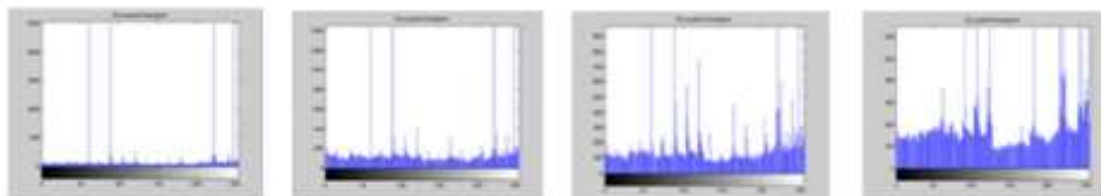


Figure 18. Histogram of encrypted image for CT scan

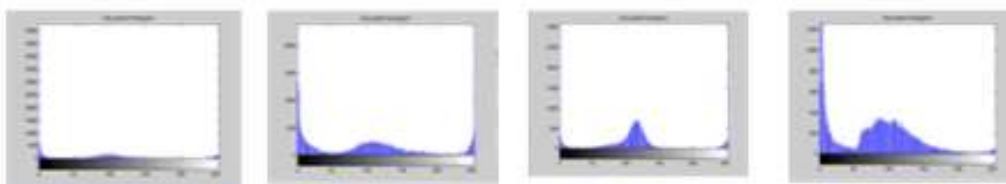


Figure 19. Histogram of decrypted image for CT scan

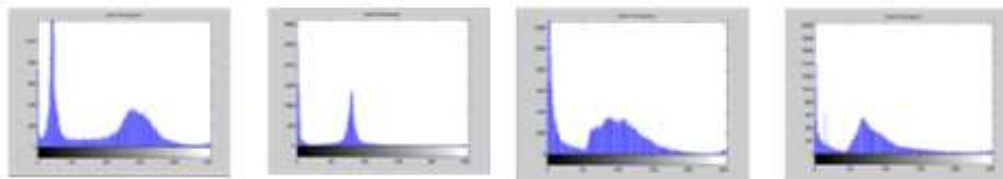


Figure 20. Histogram image for MRI input

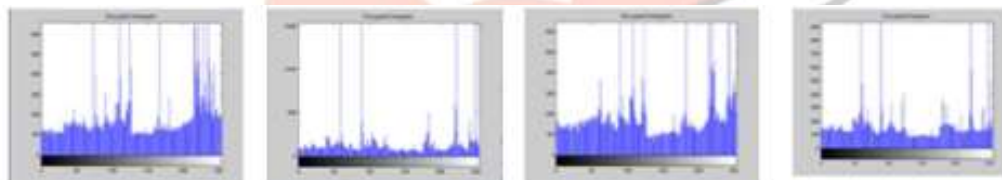


Figure 21. Histograms of encrypted image for MRI scan

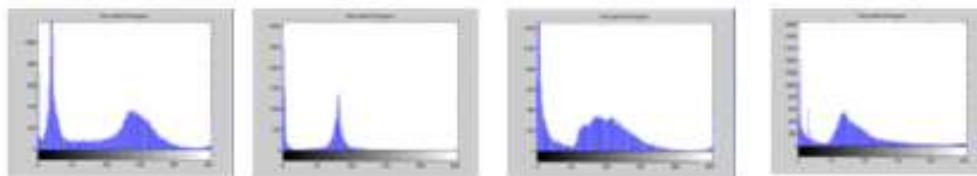


Figure 22. Histograms of decrypted image for MRI scan

**5.3 Hash algorithm analysis:**

Table (5.2) shows the number of bits changed in the SHA-512, MD5 and proposed hash value when replacing one pixel in the confused image.

The graph (figure) shows the comparison of changes in confused image hash value of SHA-512, MD5 and proposed algorithm when changing the pixel. Yellow block denotes SHA-512 values, green block denotes MD5 values and red block denotes the hash value changes of proposed algorithm. It denotes that the proposed algorithm has higher efficiency than the existing hash algorithms.

Table 3 represents hash algorithm analysis for CT scan

S.No.	Image	SHA 512 Algorithm	MD 5 Algorithm	Proposed Algorithm
-------	-------	-------------------	----------------	--------------------




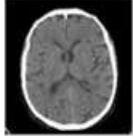
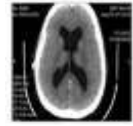
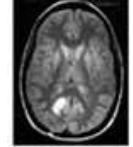
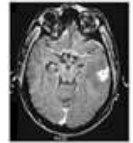
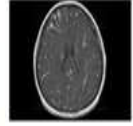
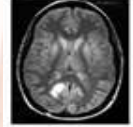

1		52	53	55
2		31	32	33
3		32	33	34
4		34	35	36

Table 4 represents hash algorithm analysis for MRI scan

S.No.	Image	SHA 512 Algorithm	MD 5 Algorithm	Proposed Algorithm
1		29	30	31
2		44	47	48
3		35	36	37
4		34	35	36

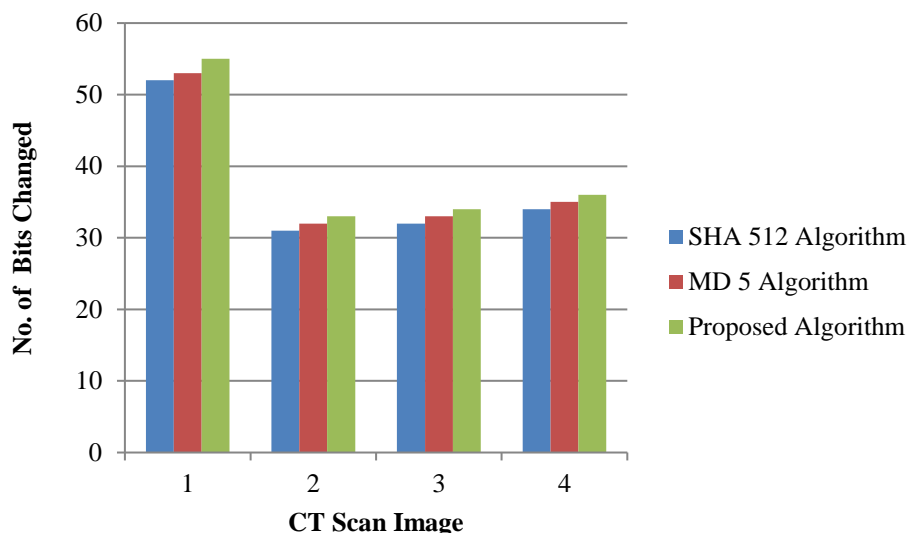


Figure 23. Hash function analysis for CT scan

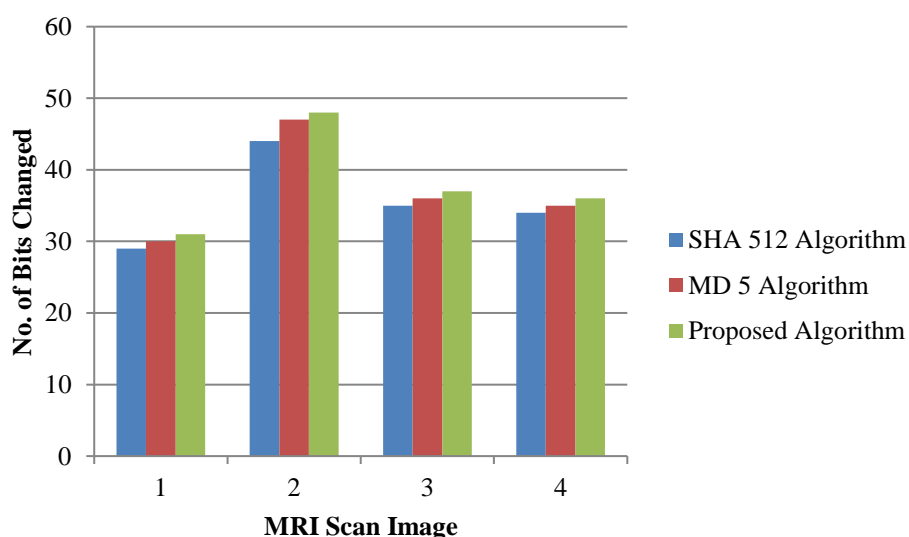


Figure 24. Hash function analysis for MRI scan

## VI CONCLUSION

The proposed encryption and decryption method provides three-fold securities for maintaining the confidentiality, integrity and authorization of patient's medical data. Confidentiality is achieved by our proposed method. It improves the QoS of the retrieved data than the existing methods and also ensures the integrity by means of combining traditional hash algorithm. Authorization is achieved by implementing encryption certificate authority. As all systems have limitations, our system is developed securely to store DICOM medical images. In the future, this will be extended to store all medical data. Also, it can be implemented for all data not only images, but also for documents and other files.

Data growth of the medical industry is in an explosive state. In future, these challenges can be countered by implementing "Big Data" repositories.

## REFERENCES

- [1] Jui-hung kao, chien-yeh hsu, yu-ping sung, wei-pan Liao, "DICOM-based multi-centre electronics medical records Management System", International journal of Bio-Science and Bio-technology, No vol 2, No.2.2010.
- [2] V, Kher and Y. Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems," proc. ACM workshop storage Security and survivability (stroageSS), V. Atluri, P. samarati, W. Yurcik, L. Brumbaugh, and Y. Zhou, eds., pp.9-25, 2005.
- [3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," IACR Cryptology Print Archie, vol 2008, P.114, 2008.
- [4] L. C. Huang, H. C. Chu, C. Y. Lien, C. H. Hsiao, and T. Kao, "Privacy preservation and information security protection for patient's portable electronic health records," Comput. Biol. Med., vol. 39, no. 9, pp. 743-750, 2009.
- [5] Boldyreva A, Goyal V, Kumar . Identity based encryption with efficient revocation proceeding of the 15<sup>th</sup> ACM conference on Computer and communications security. ACM, 2004:417-426.

- [6] Ibraimi L, Petkovic M, Nikova S, et al. “Cipher text-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes” .University of Twente,Tech.Re,2009.
- [7] Ibraimi L,Asim M, Petkovic M. “Secure management of personal health records by applying attributed-based encryption wearable Micro and Nano Technologies for Personalized Health (pHealth),6<sup>th</sup> International Workshop on IEEE,2009:71-74.
- [8] M. Chase and S.S Chow, “Improving Privacy and Security in Multi Authority Attribute Based Encryption” Proc.16<sup>th</sup> ACM Conf. Computer and Comm. Security (CCS’09),pp.121-130,2009.
- [9] Li M,YU S, Zheng Y, et al. “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J].Parallel and Distributed Systems, IEEE Transactions on,2013,24(1):131-143.
- [10] Chase M. “Multi-authority attribute based encryption” Theory of Cryptography .Springer Berlin Heidelberg, 2007:515-534

