MEDICAL IMAGE PROTECTION IN CLOUD SYSTEM

Philomina Jees[1], Diya Thomas[2]
[1]Department of computer science, Rajagiri School of Engineering and Technology
[2]Assitent Professor, Department of computer science
Rajagiri School of Engineering and Technology
Email: jeesmoljoseph@gmail.com[1], diyat@rajagiritech.ac.in[2]

Abstract

In digitizing era, we can digitize the medical images and store it on cloud and retrieve from cloud. Medical images are digitized in the standard form called DICOM (Digital imaging and communications in medical standard) format.

When we are outsourcing these medical images which contains sensitive information about patient like medical status about the patient we need to give privacy for this information. If a hacker wants to identify sex of a fetal, he can easily identify the particular fetal image from the set of images because the patients information in embedded inside the image.

This paper proposes a novel framework to enhance the protection of DICOM images and privacy of personal data. In the proposed system metadata and image is extracted from DICOM image and encrypted separately using user defined key. The metadata is encrypted using modified AES algorithm and this encrypted data is again encrypted to enhance the security. When a doctor from remote location wants to access a medical image for diagnosis purpose, he can access the encrypted metadata and corresponding encrypted medical image from the database in cloud and decrypt it. A user specific key is needed for decrypting them.Owner will pass the user-specific key to the requested user if he is a authorised user.

I. INTRODUCTION

Digital technology has entered into every aspects even in the medicine. Medical images are usually stored as hard copy and need large storage space. In digitizing era, the development in the imaging devices help us to form digitized medical images in a standard format and store it on cloud and retrieve from cloud. Medical images are digitized in the form of DICOM (Digital imaging and communications in medical standard) format. When we are outsourcing these medical images which contains sensitive information like medical status about the patient, there is a chance of attack from both inside and outside . If a hacker wants to identify sex of a fetal, he can easily identify the particular fetal image from the set of images because the patients information in embedded inside the image as metadata.

DICOM (Digital imaging and communications in medicine) is a standard designed by NEMA (National electrical manufacture association) for handling, storing, printing and transmitting information. Data obtained from different devices like CT, MRI, SPECT are of DICOM standard. DICOM image consist of header which consist information about patient, image study, image dimensions, matrix size, colour space and host information needed to correctly display the image.[1]

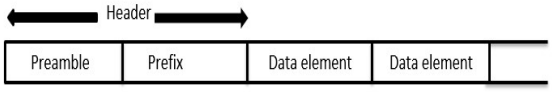

Fig. 1. DICOM Format

Header includes 128 bit preamble which is followed by 4 byte D, C, O, M which indicates that its a DICOM format image. Information in header are organized in different groups. Data set consist of number of data elements, each of which contains image. Data element consists of Tag, value Representation (VR), Value Length (VL), Value Field (VF)

Advanced Encryption Algorithm (AES) is a symmetric block cipher encryption algorithm which uses 128 bit data block. The key length can be 128-bit, 192-bit and 256- bit. The algorithm consist of 4 phases.

- Byte substitution
- Shift rows
- Mix columns
- Add round key

The algorithm consist of iteration of these phases for N rounds. The number of rounds depends on the key length. All the operations in this algorithm is byte oriented. The 128- bit data block is copied into matrix initially. The output of each stage is copied to a matrix called state matrix[2],[3].

This paper proposes a framework to enhance the protection of DICOM images. In the proposed system metadata and image is extracted from DICOM image and encrypted separately using user defined key. The metadata is encrypted using modified AES algorithm and this encrypted data is again encrypted.When a doctor from remote location wants to access a medical image for diagnosis purpose, he can access the encrypted metadata and corresponding encrypted medical image from the database and decrypt it, using the common key known to all users in the cloud. To decrypt the metadata, and image which should know the user-specific key. He will request for key to the user, he will pass the key to the doctor and he can access the data and image[4].

This section gives a brief introduction about the DICOM standard and Advanced Encryption Standard (AES).Section II includes the literature survey on medical image security. Section III describe about the proposed security model.Section IV includes experiment and results and section V include the conclusion.

II. LITERATURE SURVEY

So many methods are proposed for the privacy of data related to medical imaging field.

In [5], noise in the image is detected using scanning matrix and a key matrix is generated to encode the text into noise of image. In [6],Patient informations are embedded into segmented liver region of the CT image. It utilizes the characteristics of difference images and modifies pixel values slightly to embed data while keeping high visual quality.

Watermarking medical images using Discrete Cosine Transform is considered in [7] which combines the visual feature vector of images and encryption technology with third party authentication.A method of encrypting and embedding DICOM metadata into DICOM image is discussed in [8].

A new method that combines image cryptography, data hiding and steganography is mentioned in [9].Original image is encrypted and embed the encrypted image with patient information using lossless data embedding technique.In [10] a high efficient reversible data hiding technique is used. Image is divided into tiles and shifting histograms of each image tile between its minimum and maximum frequency. Data is then inserted at pixel level with largest frequency.

A data hiding method using integer wavelet transform coefficient is proposed in [11] where original medical image histogram is modified in this method. A method using wavelet transform is considered in [12] where a dual-tree wavelet transform with bivariate shrinkage is used.

III. PROPOSED SYSTEM

DICOM image contains both data and image. Figure 2 show a example of a DICOM image.In the proposed system, the owner extracts metadata and image set from the DICOM image.

Metadata and image are encrypted separately using modified AES algorithm. Encrypted metadata is again encrypted and stored on a database. The encypted image is also stored on a database and pushed to cloud Figure 3 shows the owner level framework.

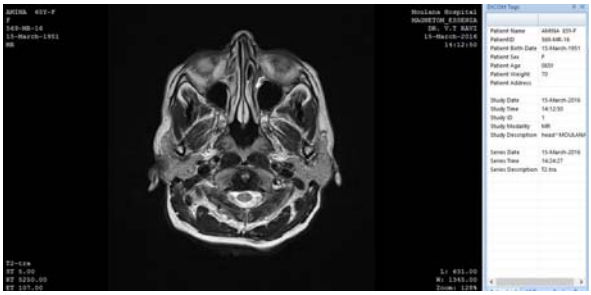

Fig. 2. An example for DICOM image

In order to provide more security for data encryption the AES algorithm is modified. In the proposed model the s-box is modified. Some permutations are done on the user specific key. And using the modified key,a pivot element is selected from the modified key. Using this pivot element, the existing s-box is modified. Using the modified s-box, the encryption algorithm is performed.

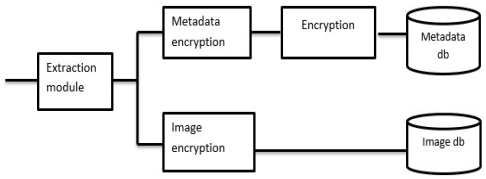

Fig. 3. Owner level framework

The 128-bit key is organized as 4X4 matrix. First element of first row is selected. The hexadecimal digits of th e first element is added together. To obtain the index value that sum is divided by 4 and obtain the remainder. This index value decides how many times should the particular row left rotated. And the next element to be selected from the next row is decided using this index value. The next element is selected and the operations are repeated for all the four rows. The sub keys are generated using this modified key.

The index values calculated are added up. After 4 rows permutation, total index sum is obtained. To select the pivot element, this sum is used. Two position values are needed for that. First position value is obtained by dividing sum by 4 and second value is obtained by taking the remainder on dividing sum by 4. Using that pivot element, the existing s-box is modified. And this modified s-box is used for the encryption.

Same operations are done on inverse s-box for decryption

Algorithm for obtaining pivot element

- Key[4][4] is the key matrix.
- Select key[0][0]. Add 2 hexadecimal digits.

$$rindex = sum\%4 \quad (1)$$

- Left rotate the row rindex times.
- Select next element. Key[1][rindex] and repeat steps 2 and 3.
- Obtain sum of all rindex values.

$$ni = rindexsum/4 \quad (2)$$

$$nj = rindexsum\%4 \quad (3)$$

- select the pivot element using ni,nj.

pivot = Key[ni][nj]

When a user request for image the user should decrypt the encrypted metadata and image. To decrypt metadata and image, the user should know the user defined key. User will request for the key to owner. Owner will pass the key by confirming whether the requested user is a authorized user. Figure 4 shows user level framework.

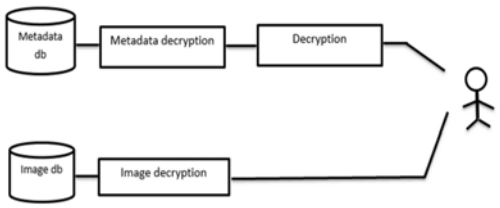

Fig. 4. User level framework

A. Extraction module

The information about the patient which is embedded in th DICOM image is extracted into a text file and image is converted into JPEG image using Dcm4che3 toolkit.

B. Metadata encryption module

The metadata which was extracted from DICOM image is encrypted using modified AES.Rijindl

s-box is modified with respect to user defined key.Some permutations are performed on the key before modifiying the sbox.After permutation pivot element is selected.Each element of s-box is modified usin this pivot element. *newsbox*[*i*] = *sbox xor pivotelement.*

c. Image encryption module

The image extracted from the DICOM image is converted into pixel array.Some kind of permutations are done on the image key before passing it to encryption algoithm.The pixel array is encrypted using the new key using modified AES.

IV. EXPERIMENTS AND RESULTS

The experiment was conducted on set of DICOM images.

An example of dataset is shown in figure 5.

Fig. 5. Image under experiment

Metadata was extracted from this DICOM image and stored on a text file and image was saved as jpeg file. Metadata and image was encrypted separately using modified AES. Encrypted metadata is double encrypted using modified AES and stored to database on cloud. Encrypted image is forwarded to database on cloud. Figure 6 shows extracted metadata and
figure 7 shows encrypted metadata.Figure 8 shows extracted image. Encrypted image will not be a viewable format.

AMINA 65Y-F569-MR-16DR. V.T RAVI

Fig. 6. Extracted metadata

þxV&^‡aVWè-1↑À940ðŕ3|n¦←[“¡þÙ┴Á℗’ð³øüõ‘=ü←‘{\Î,¶ý

Fig. 7. encrypted metadata

When a user request for image the user should decrypt the encrypted metadata and image. To decrypt metadata and image, the user should know the user defined key. User will request for the key to owner. Owner will pass the key by confirming whether the requested user is a authorized user

Fig. 8. Extracted image

V. CONCLUSION

In the proposed model, the medical images are securely outsourced to cloud with high degree of protection.The metadata information which includes the patient information is extracted from DICOM image and stored seperatly as text file and image as JPEG format. The image and text information is encrypted seperatly using modified AES encryption algorithm.

In the modified encryption algorithm, the sbox is modified based on the user specific key.Some permutations are performed on the user specific key and a pivot element is selected.Using that pivot element the sbox is modified.Using the modified sbox the text data is encrypted.

The image is converted into pixel array and the pixel array is the encrypted using the modified AES encryption algorithm.

When a user request for image the user should decrypt the encrypted metadata and image. To decrypt metadata and image, the user should know the user defined key. User will request for the key to owner. Owner will pass the key by confirming whether the requested user is a authorized user.

The proposed model assures that encryption using modified AES can be done effective than other methods with very small delay. In modified AES, modification is based on user-specific key which makes the cryptanalysis difficult.

REFERENCES

[1] Mario Mustra, Kresimir Delac, Mislav Grgic, "Overview of the DICOM Standard" ,*50th International Symposium ELMAR-2008,10-12 September 2008 ,Zadar,Croatia.*

[2] Joan Daemen, Vincent Rijmen " The Design of Rijndael AES: The Advanced Encryption Standard" ,*2001*

[3] Xiaona Lv,Liping Xu,"AES encryption algorithm keyless entry system" ,*International Journal of Computer Applications(0975-8873)Volume 62N.11,January 2013.*

[4] Bernardo Ferreira, Jo'ao Rodrigues, Jo'ao Leit'ao, Henrique Domingos "Privacy-Preserving Content-Based Image Retrieval in the Cloud" ,*IEEE 34th Symposium on Reliable Distributed Systems,2015.*

[5] Bharti, Gaurav Mittal "A Novel Approach for Lossless Data Hiding for Medical Images" ,*International Journal of Computer Technology and Applications,2014.*

[6] Bharti, Gaurav Mittal "Lossless Data Hiding for Medical Images with Patient Information" , *IEEE International Conference on Image Processing ,Volume:3 ,2007.*

[7] C. Dong, J. Li, Y. Chen," A DWT-DCT Based Robust Multiple Watermarks for Medical Image", *Photonics and Optoelectronics (SOPO), 2012 Symposium on , vol., no., pp.1,4, 21-23 May 2012.*

[8] J Blackledge,A.Al-Rawi and P.Tobin "Stegacryption of DICOM Metadata", *ISSC 2014/CIICT 2014,Limerick,June 26-27.*

[9] Vinay Pandey, Manish Shrivastava "Medical Image Protection using steganography by crypto-image as cover Image", *International Journal of Advanced Computer Research.*

[10] M. Fallahpour, D. Megias, M. Ghanbari, "High Capacity, Reversible Data Hiding in Medical Images, Image Processing (ICIP)", *2009 16 th IEEE International Conference on , vol., no., pp.4241,4244, 7-10 Nov. 2009*

[11] N. A. Memon,S. A M Gilani, "Adaptive Data Hiding Scheme for Medical Images Using Integer Wavelet Transform", *Emerging Technologies, 2009. ICET 2009. International Conference on , vol., no., pp.221,224, 19-20 Oct. 2009*

[12] R. M. Kongo, L. Masmoudi, N. Idrissi, N. Hassanain, M. Cherkaoui, A. Roukhe, "A Medical Image Watermarking Scheme Based on Dual-Tree Wavelet Transform", *Innovative Computing Technology (INTECH), 2012 Second International Conference on , vol., no., pp.144,152, 18-20 Sept.*