A NOVEL APPROACH FOR MEDICAL IMAGE SECURITY IN PACS

[1]Nineesha P, [2]Panchami V
[1]Postgraduate Student,Toc H Institute of Science & Technology, Kochi
[2]Assistant Professor, Toc H Institute of Science & Technology, Kochi

ABSTRACT

Picture archiving and communication systems (PACS) outplace the former film based medical images and the workflows in hospitals and medical practices. In a PACS, images are obtained from medical imaging modalities like Computer Tomography (CT), X-ray and are stored digitally. It thenpre-processes these images and makes them easily accessible from different reading room within a medical environment. But PACS has restrictedits availability in many parts of the world and imposed major costs for those who handle them. Public cloud serviceis a solution that could give much more flexibility and reduce the cost of ownership for PACS implementations.But a security policy is required while moving the PACS system to cloud. So here we propose JPEG 2000 image compression and image scrambling technique based on transposition of image-blocks method for secure storage and transmission of medial image within the PACS in cloud.

Keywords: Image compression, Image encryption, Entropy, PACS, Public cloud

INTRODUCTION

Security of data in network is provided with the help of encryption techniques. Classical and modern crypto systems were used to protect the data. But in case of image security this data encryption methods were insufficient due to its complex pixel features. So a sufficient algorithm is required to protect the image as well as it still maintains the quality of the image.

Digital images are used in tremendous area. And the popularity of digital sensors in medical sciences has flourished extensively. The amount of digital images produced in hospitals and medical practices has increased drastically. Besides digital technologies, such as Computer Tomography (CT), nuclear medicine imaging or Medical Resonance Imaging (MRI), former analog technologies such as X-ray became able to produce digital images instead of analog films. PACS [4] provided an efficient method for handling medical imaging. Current PACS are storing, proceeding and converting the medical data in a hospital or a medical practice. As a result they are making it easy accessible from different locations, long-term available and editable. The images can be viewed and compared at special workstations, providing lots of advantages such as simultaneous viewing on different locations and powerful graphics software.

Medical imaging systems have been normally constrained to the limits of the healthcare provider. These facilities incur major costs to provide the infrastructure for the medical imaging systems. Cost of ownership has been a major constraint to small scale healthcare providers and in less developed areas. Cloud computing provides an environment where services can be rapidly scaled up or down while costs incur only on a 'pay per use' basis without upfront capital costs [5]. Real monetary saving can come from utilizing cloud computing for both small and large organizations. Other benefits include more robust cost-effective business continuity planning such as disaster recovery, and allowing more focus to be put on providing healthcare services than managing infrastructure. These benefits do not come without risks. Maintaining the security and integrity of the data with a cloud environment becomes a major concern. So moving these systems to the public cloud requires an encryption policy for communications to be established within the PACS environment.

In a PACS environment communication over the internal hospital network is protected by a firewall from outside intruders. As the communication extends over public networks i.e. storage in cloud, security becomes an issue. Here an intruder or malicious attacker gets tremendous of opportunity to tamper the image data sent over open networks or to espionage right into the heart of the hospital network through the networktunnel piggybacking on a trusted user. Conventional Internet security methods are not sufficient to guarantee that medical image had not been compromised during data transmission. Techniques including virtual private network (VPN), data encryption, and data embedding are being used for additional data protection in other fields of applications like financing, banking, and reservation systems. However, these techniques have not beensystematically applied to medical imaging partly because of the lack of urgency.So a strong algorithm is needed to secure the image data while storing in cloud and that it still maintain the quality of the image even after encryption. The security of medical image is provided by combined compression - encryption algorithm.

In this paper section 2 discuss about the related works. Section 3 describes about how to secure the medical images by compressing and encryption by performing the scrambling of image. Section 4 presents the algorithm of this proposed system. Section 5 illustrates the experimental result of the algorithm. Finally section 6 concludes the paper with the highlights.

RELATED WORKS

Imagesare used in varied fields. And the usage of digital images has increased in medical domain[1] too. Most of the medical instruments exploit images to diagnose the patient for various diseases and sometimes a deep analysis leads doctors to choose correct treatment for patient. If looking towards the criticality of information stored in these images and importance of open network to share these images,[2] security is big concern. People have no other options apart from using public open network to send images over long distance in quick time and in this process images are usually accessed by unauthorized users.

It has become the need of time to keep images secure and a distance apart from the access of unauthorized users and for the same, various methods are proposed under the head

of image encryption. The field of image encryption [3] has gain so much popularity nowadays because of use of image in various domains and amount of information which can be save under images.Image encryption techniques can be divided as spatial domain methods or frequency domain methods. Basically the encryptionschemes are categorizedinto three methods namelypermutation, substitution and combination of both.Some of the works are like the chaotic confusion and pixel diffusion [6] methods proposed by Friedrich perform the permutations using a chaotic 2-D [7] combined with alterations of Grey-Level values of each pixel in a sequential manner. Repeated steps of permutations and alterations where used to achieve higher security and resistance to attacks. It was experimentally verified that the amount of time overhead in performing complex calculations and the complex diffusion process had led to large time complexity of the system.

Many highly effective and secure algorithms like RSA[8], DES [9] where used efficiently to encrypt the textual data. But in the case of the Image Encryption, these algorithms have proved to be less effective or rather impractical dueto the characteristic features of images like the high byte sizeof the data to be encrypted and the complex structure of theimage data.

The initial methods of encryption the image using the pixel shifting and altering of the grey levels provided a large key space. The pixel shifting was performed by the nonlinear chaotic algorithm [10][11]. Though this method didn't change the shading or colour profile of the pixel considerably so as to fully withstand the clever attacking algorithms. And in Image Encryption Based on Explosive Inter Pixel Displacement of the RGB Attribute of a Pixel [12] focus was more on the inter pixel displacement rather than just manipulation of pixel bits value and shifting of pixel completely from its position to new position. RGB value of pixel was untouched in this method, but R value of pixel jumps to another location horizontally and vertically same as in chaotic method. In the similar manner, G and B values of pixel also shift from its position in both direction and jumping factor depends on confidential key. But this method is continuous working of algorithm on whole image in one go.

In image encryption using block-based transformation algorithm [13] encryption is done by first at block level and then using Blowfish method to encrypt image. And in image encryption approach using a combination of permutation technique followed by encryption [14] Image is divided into 4 x 4 pixel block and then these blocks were rearranged into a permuted image using a combination of permutation technique. This permuted image later on encrypted using the Rijndael Algorithm. In each casealgorithm tries to reduce correlation between pixel values by rearrangement of blocks within image.

Cloud computing is still a developing industry where benefits and concerns are still being explored. Rosenthal et al [15] evaluates how cloud computing could be used for the healthcare industry. Some benefits discussed are reduced management decisions concerning infrastructure, scalability, increased resiliency and cost reductions. Even within a cloud environment, security management is still principally the responsibility of organization and is not outsourced to the cloud provider. Some additional considerations for organizations when moving to the cloud include the jurisdiction the cloud application will be under, additional risk of hackers and protecting data from the cloud provider and other tenants using cloud.Buyya et al [16] analyses the trends of cloud computing and how they might be used by

industry. Also included is an analysis of cloud computing infrastructure and some of theleading commercial cloud providers.

The above all works has its own limitation. So one of the motivation for this work is to secure the medical images by encryption policy without affecting the quality of the image while storing in cloud. And thereby the flexibility and robustness of the PACS system can be improved.

PROPOSED SCHEME

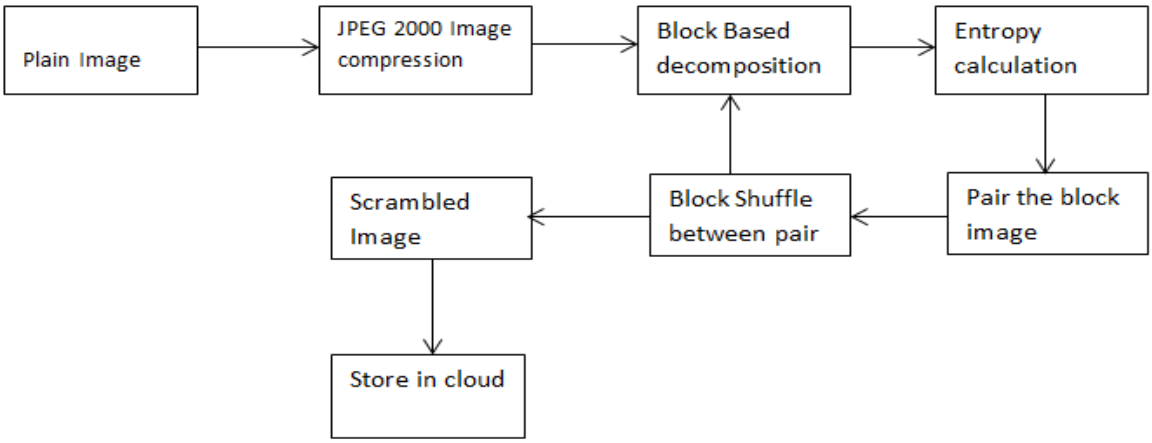

Fig 1. Proposed Method For Encryption

The proposed method involves two steps i.e. compression using jpeg 2000 and second step is encryption using block image scrambling technique. In the PACS system after the image obtained from different modalities the image is converting it to a standard, which is supportedby the PACS (i.e. the DICOM standard). This image is then secured and stored in cloud. So here in the proposed system the image is first converted to JPEG 2000 image standard [17] and then the image encryption process is done.

In the encryption policy, the information theory concept 'Entropy' is the key of the algorithm. Entropyis a measure of the uncertainty in a randomvariable and which also quantifies the expected value ofthe information contained in a message. Keeping entropy as thefundamental theme the proposed encryption approach convert ahomogeneous image into a heterogeneous image by shuffling ofsmaller image blocks contained by the image/imageblock. The objective is to make the image more and moreheterogeneous by successive block decomposition followed byshuffling of image blocks.

Here the compressed image is converted to heterogeneous image. After compression, at each level animage/image block is divided into four equal sizedblocks. The blocks are supposedly more homogeneousthan the image itself. As depicted in fig 1 after the image isdecomposed into four smaller sized blocks theentropy of each block image is calculatedand then the image blocks are sorted according to the entropy value. Then the images blocks are

paired and the blockshuffling is carried out between the pair. Shuffling of a subset of blocks between the pair at each level will result in a moreheterogeneous image block at the previous level. This process is continued until the minimumsize of the blocks is reached. The scrambled image cango through further encryption using some conventionalalgorithm if one more level of security is preferred.And this scrambled image is stored in cloud.

Decryptionis the reverse process of encryption.Afteraccessing the image from cloud,the scrambled image undergoes the reverse process of encryption and then this is converted to DICOM standard which is supported in PACS system.

ALGORITHM

Input: Plain image, minimum block size
Output: Scrambled Image

Step 1: compress the plain image

Step 2: Split the image into four image blocksof equal size (first level image blocks).

Step 3: Calculate the entropy of each image block using equation 1.Let S be the sorted array of image blocks based onentropy of individual image blocks.

$$S_n = \sum_{i=0}^{255}(p(i) * \log_2(1/p(i))) \qquad (1)$$

Step 4: Pair image blocks S_n and $S_{n+1-i}$for i=1, 2 ,…., *n*for all *n* image blocks.

Step 5: Divide the image blocks (first level image blocks)further into four equal-sized blocks (second level image blocks).

Step 6: Between each pair of image blocks (first level imageblocks) perform shuffling of image blocks (second level imageblocks) by swapping a subset of blocks from first levelblock with a subset to other first level block inthe pair.

Step 7: Now with second level image blocks as first level image blocks repeat step 3 to step 6 until theimage block isdecomposed into blocks of minimum block size.

EXPERIMENTAL RESULT

Experiments were carried out on various images using this proposed algorithm. The proposed scheme was developed on the NetBeans platform using java. The result tested on a image of size 512x512 is shown in the fig 2 to fig 4. First the image is compressed by jpeg 2000 compression. Lossless image compression is carried out so as to maintain the quality of the image. The result is as shown in fig 2.

Fig 2.Compressed Image

Fig 3. Encrypted Image

Fig 4. Decrypted Image

Then the encryption is carried out until the image is decomposed to a minimum size of 2x2. The output is shown in fig 3. And it is seen that even after encryption and decryption process the image quality is maintained. This is shown in fig 4. This is then converted to DICOM standard which is supported in PACS system.

CONCLUSIONS

The implementation of this proposed system demonstrates that a medical imaging server placed on public cloud services can secure the communications with its clients.In this paper, combined compression and encryption process is carried out to secure the medical image stored in cloud. Decomposition of image into smaller size blocks and able permutation of image in a simple yet efficient scheme for image has been developed. The proposed scheme scramble the image by making the image more heterogeneous at each step and thereby maintain the quality of image as it is. And storage of image in public cloud service has improved the flexibility of PACS system.

REFERENCES

[1] AmneshGoel and Nidhi Chandra*"A Prototype Model for Secure Storage of Medical Images and Method for Detail Analysis of Patient Records with PACS*" 2012 International Conference on Communication Systems and Network Technologies

[2] Jinyang Li, Frank Dabe, "*F2F: reliable storage in open networks*", (http://project-iris.net/).

[3] William Stallings - Network security and cryptography

[4] Maximilian Hecht,"*PACS - Picture Archiving and Communication System*", Vienna University of Technology, University of Paderborn

[5] Tim Rostrom, Chia-Chi Teng, "*Secure Communications for PACS in a Cloud Environment*", 33rd Annual International Conference of the IEEE EMBS, Boston, Massachusetts USA, August 30 - September 3, 2011.

[6] M. Salleh, S Ibrahim and I.F. Isnin, "*Image encryption algorithm based on chaotic Mapping"*.JurnalTeknologi, 39(D) Dis. 2003: 1–12 UniversitiTeknologi Malaysia.

[7] R.Kadir, R.Shahri and M.A.Maarof, "A modified image encryption scheme based on 2D chaotic map" 978-1-4244-6235-3/10/2010 IEEE.

[8] RSASecurity.http://www.rsasecurity.com/rsalabs/faq/3-2-6.html

[9] DES. ttp://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[10] Sobhy, M. I. and A. R Shehata. 2001. "*Chaotic Algorithms for Data Encryption*". IEEE, 0-7803-7041-4.

[11] Z.Minguming and T.Xiaojn,*" A multiple chaotic encryption scheme for image"*. 978-1-4244-3709-2/10/2010 IEEE

[12] Reji Mathews , AmneshGoel , PrachurSaxena, VedPrakash Mishra, "*Image Encryption Based on Explosive Inter pixel Displacement of the RGB Attributes of a pixel*", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol IWCECS 2011, October 19-21, 2011, San Francisco, USA.

[13] Mohammad Ali BaniYounes and AmanJantan, "*Image Encryption Using Block – Based Transformation Algorithm*" IAENG, 35:1, IJCS_35_1_03, February 2008.

[14] Mohammad Ali BaniYounes and AmanJantan, "*An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption*" IJCSNS, vol 3 no 4, April 2008.

[15] J. Harauz, L. M. Kaufman, B. Potter, "*Data security in the world of cloud computing*," IEEE Security & Privacy, July 2009.

[16] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "*Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility*," Future Generation Computer Systems, vol. 25, pp. 599-616.

[17] MajidRabbani*, Rajan Joshi, "An overview of the JPEG2000 still image compression standard", Signal Processing: Image Communication 17 (2002) 3–48