Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Securing Medical Records with Multi Level Encryption

L. Iruthaya Isabella Anbarasi[1] & Ms. C. Fancy[2]
[1]Information Security and Cyber Forensics, Department of Information Technology, Faculty of Engineering and Technology, SRM University, Chennai, India
[2]Assistant Professor, Department of Information Technology, Faculty of Engineering and Technology, SRM University, Chennai, India

Abstract **-** *This paper proposes a novel encryption and segmentation based technique provides high level security for the medical records. There is a need for secure transmission of medical records since telemedicine is increasingly being used. Moreover, retaining the details of the medical image is particularly important for accurate diagnosis. The efficient delivery and storage of medical image data is becoming more and more difficult due mainly to the increasing size of volumetric datasets. Compression can potentially be used to alleviate this problem. However, in the case of medical image data it would be unacceptable to use a compression technique that would reduce the quality of the data.*
In this paper we present lossless compression scheme to reduce the size without compromising the quality of the medical image .AES CBC mode of encryption is used to encrypt the image to secure the medical image. More enhancement of security, segmentation concept is introduced in this project to slice the image which provides more security on medical images. Additional patient details are secured by using onetime pad encryption.

1. Introduction

A medical image data set consists typically of one or more images representing the projection of an anatomical volume onto an image plane (projection or planar imaging), a series of images representing thin slices through a volume (tomographic or multi slice two-dimensional imaging), a set of data from a volume (volume or three-dimensional imaging), or multiple acquisition of the same tomographic or volume image over time to produce a dynamic series of acquisitions (four- dimensional imaging). The file format describes how the image data are organized inside the image file and how the pixel data should be interpreted by a software for the correct loading and visualization.

Encryption and Segmentation are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable cipher text. During segmentation Slicing the medical image into equal size of slices with certain number.0 Onetime pad encrypting technique provides more powerful security to additional medical data.

In this paper we provide high level security for medical records .In this scheme we used lossless compression technique for medical image compression. During Segmentation, compressed image is sliced into equal size with certain number. Sliced Medical Image is encrypted by using AES CBC (Cipher Block Chain) mode encryption. AES CBC is a mode of operation for a block cipher. It provides an information service such as confidentiality and authenticity. It requires Initialization Vector (IV) .IV has to be non-repeating and random as well. The initialization vector is used to ensure distinct cipher texts are produced even when the same plaintext is encrypted multiple times independently with the same key.

Onetimepad encryption technique provides high level security for additional medical data. Encryption key is generated randomly. Key can be created randomly in 3 ways such as binary stream, vigenere square, number pads. Symmetric key is created and shared among senders and receivers. Both sender's and recipient's keys are automatically destroyed after use, so that erroneous re-application of the same key is impossible. Also if the key is not used after a particular time, key will be destroyed automatically.

2. Literature Survey

In this section, we talk on various research carried out pertaining to Image compression and security.

In this paper [1], the image provider encrypts a plaintext image using the public key of probabilistic cryptosystem pk. Public-key cryptosystems based on Paillier cryptosystem with composite degree of residues classes and

Carmichael theorem. For each pixel value m(i, j) where (i, j) indicates the pixel position, the image provider calculates its cipher text value.

$$C(i, j) = E(pk, m(i, j), r(i, j))$$

Where E is the encryption operation and r (i, j) is a random value. Then, the image provider collects the cypher text values of all pixels to form an encrypted image .with paillier system two large primes p ,q ,calculate n=p. q , lambda=lcm(p-1,q-1) and public key is composed of n, random value ,private key is composed with lambda .

In this scheme data hider embeds some additional data into the encrypted image by multi-layer wet paper coding [1], under a condition that the decrypted values of new and original cipher-text pixel values must be same. The receiver knowing the data hiding key may extract the embedded data.

Some part of Cipher text pixel values replaced with additional data. Additional data embedded into several LSB plane of cypher text pixels. Embedded data can be directly extracted from the plane. The data embedding does not affect the decryption of the original plain text image. In receiver side the additional data cannot be retrieved after decryption of the original image. Adding additional data into a cypher text plane leads to little pixel over saturation.

In the reversible scheme [7], a pre-processing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values.

The original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image. Note that the data-extraction and content-recovery of the reversible scheme are performed in plaintext domain, while the data extraction of the previous lossless scheme is performed in encrypted domain and the content recovery is needless. There is a slight distortion.

Image compression [2] is broadly classified in two types of compression techniques viz. Lossy and Lossless compression. Lossless compression is usually used in medical images, military signatures and applications where quality dilapidation cannot be tolerated. Lossy compression schemes realize high compression ratios due to Human Visual Perception (HV S) property.

The scheme [3] begins with segmentation. This stage extracts the entire body region from the original image. Segmentation [3] is achieved using seeded region growing with a threshold of -700Hu. Once the entire body has been extracted, it is preferable to store the outline information rather than the whole body region, in order to save space. The body outline is obtained using the Roberts edge detector. At this point, the location of the RoI is defined by the chain code.

3. Proposed Work

In previous methods, quality of the image is reduced. Data loss will be there. Medical records need to be maintained with high quality, the computation time should be less and data loss must not be there. To avoid this we introduce lossless segmentation based encryption for medical records. Also introducing one time pad encryption for the additional medical data to increase the security.

This system is developed in Python. The main steps of the proposed scheme are outlined below.

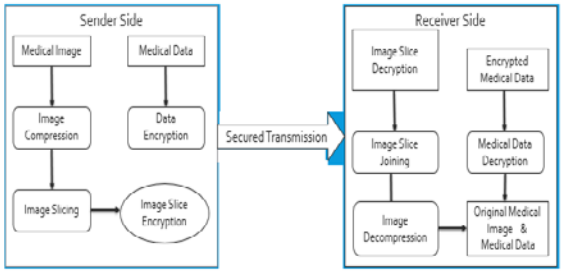

Figure 1. Flow diagram for proposed scheme

3.1 Lossless Image Compression
3.2 Slicing the compressed Image
3.3 Encryption on Image Slices
3.4 Additional Data Encryption

3.1. Lossless Image Compression

This scheme begins with lossless compression. The test medical image is taken as an input of the scheme. Lossless compression technique is applied on test medical image. The image is compressed .The maximum compression range is obtained and there is no data loss. Image quality is maintained.

3.2. Slicing the Compressed image

In this section compressed medical image is taken as an input and split in to no of slices. The size of the image and its coordinates are used to divide the image into specified no of slices. Each slice is named according to its file name, columns and rows. An image illustrating the output of the slicing stage is presented in Figure3.

3.3 Encryption on image slices

In this section image slices are taken as an input. Each slice is encrypted by using AES CBC encryption technique. Each slice stored with .enc extension, output is presented in Figure3. These files cannot be viewed by anyone before decryption. In AES CBC encryption IV (Initialization Vector) is created randomly. Key is created and shared between senders and receivers securely.

3.4 Additional Data Encryption

In this section additional data file is taken as an input .The content of the file is encrypted using onetime pad encryption. It is the only existing mathematically unbreakable encryption. The encryption key is created randomly and securely shared between sender and receiver. The key size should be same as the message size. Both sender's and recipient's keys are automatically destroyed after use, so that erroneous re-application of the same key is impossible. Key can be created in 3 ways such as binary stream (modulo2), vigenere square (modulo26), number pads (modulo10).

In this scheme the processed medical image with medical data will be made more secure to avoid hacking. Even though we applied the encryption mechanism, there are hackers always look for opportunity to hack the data during data transfer. The processed medical image slices are grouped and send in multiple pockets. This will avoid the hackers to easily hack the medical image. Also it is very difficult to gather all the slices and arrange it in proper order to get the original medical image and data.

4. Experimental Result

Set of medical images are taken as inputs and executed successfully. Test result are analyzed. Lossless compression is achieved. Output is presented in Figure2. Medical Image is sliced successfully and encrypted. Additional medical data is encrypted successfully. Output is presented in Figure2. Keys are created randomly. Image is transmitted securely .On receiver's side reprocess the image and got the original image back. The quality of the image is maintained. There is no data loss. Data integrity and confidentiality is maintained (see Figure4. This system is providing multilevel security, faster computation, reduced size and faster transmission on medical images.

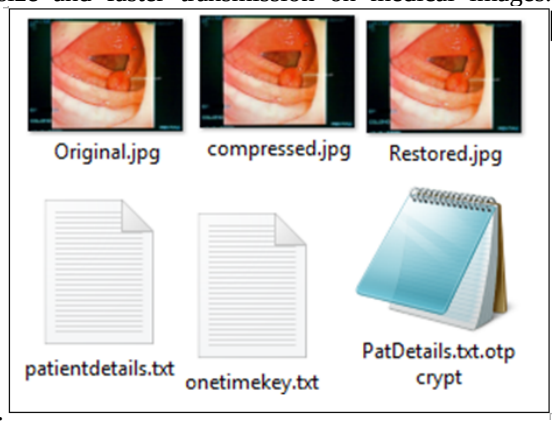

Figure 2. Result of Compression & Onetimepad

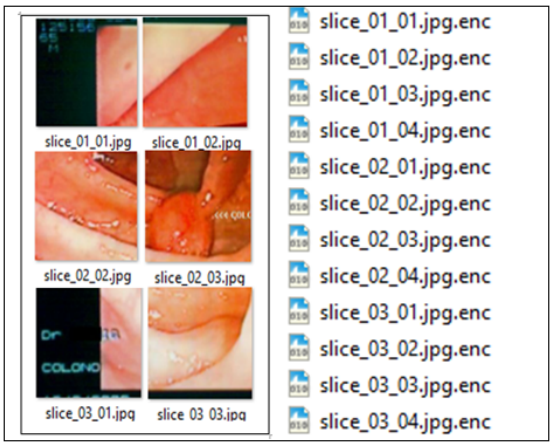

Figure 3. Result of Image Slicing & Encryption

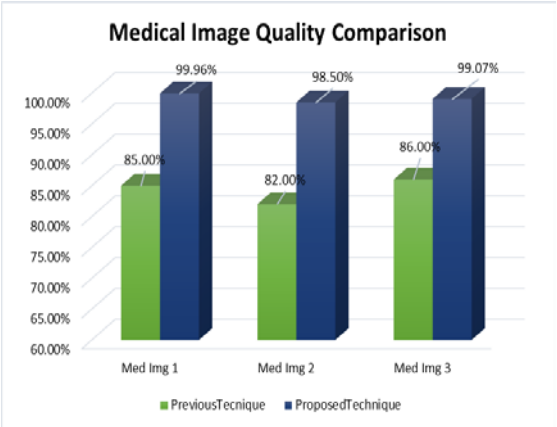

Figure 4. Image Quality Comparison

Table 1.Result & Analysis

	Quality (%)	Data Loss (%)	Security
Previous Method	84.33	15.67	Minimum Level
Proposed Method	99.17	0.83	Very High Level

5. Conclusion

A secured Medical records with multilevel encryption provides secure system for medical records. Also reduced size of the images provide faster transmission of records .we can maintain the quality of the images. Provides security and good accessibility. Data integrity and confidentiality is achieved.

Acknowledgement

We wish to acknowledge contributions from our medical friends. Particularly Dr.Rita Thilipan, Dr.Roshini Cath , Dr.Thomas Jishanth .

References

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng "*Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography*", IEEE .1109/TCSVT.2015.2433194

[2] M. Mohamed Sathik, K. Senthamarai Kannan and Y. Jacob Vetha Raj ", *Hybrid jpeg Compression using Edge Based Segmentation*," Signal & Image Processing: An International Journal (SIPIJ) Vol.2, No.1, March 2011

[3] Qiusha Min, Robert J.T. SadleirA "*A segmentation based lossless compression scheme for volumetric medical image data*", 978-0-7695-4629-2/11 $26.00 © 2011 IEEE DOI 10.1109/IMVIP.2011.26

[4] Z. Qian, X. Zhang, and S. Wang, "*Reversible Data Hiding in Encrypted JPEG Bitstream*," IEEE Trans. on Multimedia, 16(5), pp. 1486−1491, 2014

[5] M. S. A. Karim, and K. Wong, "*Universal Data Embedding in Encrypted Domain*," Signal Processing, 94, pp. 174-182, 2014.

[6] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "*Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption*," IEEE Trans. Information Forensics & Security, 8(3), pp. 553-562, 2013.

[7] W. Zhang, K. Ma, and N. Yu, "*Reversibility Improved Data Hiding in Encrypted Images*," Signal Processing, 94, pp. 118-127, 2014.

[8] Y.-C. Chen, C.-W. Shiu, and G. Horng, "*Encrypted Signal-Based Reversible Data Hiding with Public Key Cryptosystem*," Journal of Visual Communication and Image Representation, 25, pp. 1164-1170, 2014.

[9] Amol Baviskar, Shweta Ashtekart, Amruta Chintawar "*Performance Evaluation of High Quality Image Compression Techniques* " Department of Electronics Engineering, Ramrao Adik Institute of Technology, Navi Mumbai - 400706, India