ATLANTIS PRESS

Advances in Engineering Research (AER), volume 142

International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)

Homomorphic Protocol for Medical Images using Data Packing

[1]M. Jayanthi, [2]Dr. Kannan Balasubramanian, [3]A. Muthumari
[1]Research Scholar, [2]Professor, Department of Computer Science and Engineering,
Mepco Schlenk Engineering College, Sivakasi, Virudhunagar, India
[3]Assistant Professor, Department of Computer Science and Engineering,
University College of Engineering,
jayanthimathanan@mepcoeng.ac.in, kannanbala@mepcoeng.ac.in, muthu_ru@yahoo.com,

***Abstract*— This research analyses the medical image encryption based on homomorphic encryption and the resultant image compression. First the Medical records are encrypted using somewhat homomorphic encryption. Next the encrypted results are compressed to reduce the storage size of the resultant image. The problem deals with the secure computation homomorphic technique to maintain the privacy. The similarities between the encrypted images are compared before the compression to show the performance, security strength and computational efficiency. The efficiency of the cryptanalysis is also analyzed using homomorphic technique.**

Keywords—public key encryption, somewhat homomorphic, compression, privacy preserving encryption, asymmetric encryption

INTRODUCTION

Since the wired and wireless IP networks are open networks, they are vulnerable. Confidentiality is more important to secure multimedia information over the networks. Conventional cryptographic schemes have been applied for protecting alphanumeric data. When compared to the images they are at low density. So the enciphering schemes with a significantly low computation cost are feasible. The encryption and decryption computation is often more complex images and video contents than alphanumeric data. The leakage of the privacy, data can make serious threats to the privacy of the user. Privacy protected encryption is an important one which can be applied to many fields (2). To maintain security the privacy, data should be protected before sending to the receiver or server.

CONVENTIONAL SOLUTIONS TO MULTIMEDIA PRIVACY

In 1992, Bourbakis and Alexopoulos have proposed an image encryption scheme which utilizes the SCAN language to encrypt and compress an image simultaneously(3). Fridrich demonstrated the construction of a symmetric block encryption technique based on 2D standard baker Map. Recently, Chen. et al proposed a symmetric image encryption.

Multimedia encryption Types

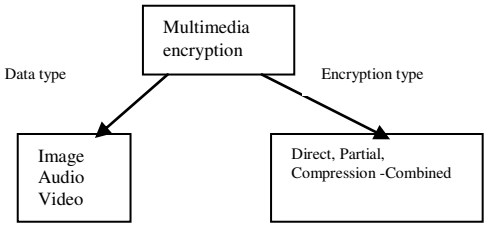

Figure 1. Encryption types based on the Types

Based on the type of data and encryption, there are various kinds of encryption schemes in cryptography. The traditional encryption technique converts the data from the original form into an unknown form. AES, RSA and DES are used in text or binary data encryption. These Symmetric and Asymmetric encryption methods are involved in Data encryption. The size of the data is huge. So it is not easy to use them in Image or Video encryption. Encrypting images directly is time consuming and not suitable for real-time applications. Some new encryption algorithms are needed for Image and Video encryption. Image encryption technology development can be partitioned into three categories as raw data encryption, compressed data encryption and partial encryption (2). Image encryption is done by pixel scrambling or permutation to make the resultant image as unintelligible.

The exchange pixel operation changes the place and value of the pixels, which will make the compression operations not work (2). These types of encryption algorithms are applied to the files which needs no compression. In image encryption the original image is converted into another ciphered image. So it is not easy to identify the difference by a normal person. The encryption algorithms are coming under direct encryption, partial encryption and compression-combined encryption. In direct encryption the data is encrypted using the traditional methods directly. In partial encryption only some parts of the data are encrypted. The encryption operation is combined with compression in the combined approach (2).

Data Packing

There are some reasons for compression. It needs large storage. The network bandwidth is also a reason for Data Packing.

Cryptographic Security

It is the resisting ability of cryptanalysis methods with attacks such as differential analysis, related-key attack and statistical attack (13).

Histogram Analysis

Histogram Analysis is one of the ways of pixel representation in an image. This pixel positions tells the accuracy and quality of the image. For analysis, the original image is compared with the histogram of a cipher text. Histogram is a method of specifying the continous data. The comparison of the original image and the ciphered image histogram denotes the quality of the encryption technique in our system(1).

Statistical Analysis

Homomorphic encryption scrambles the pixels of the image in the cipher text. So that it decrease the correlation among the pixels to get lower correlation among the pixels.

Correlation coefficient Analysis

Correlation coefficient gives the measurement of the association between the image pixel values. The measure met of the correlation is high means it is well encrypted. If the difference between, the correlation value of an original image and an encrypted image is low means, it can also be improved. If the correlation, association is completely varying means the ciphered image is highly encrypted.

Encryption Quality

Encryption Quality is calculated by the evaluation of image encryption techniques. The Quality and accuracy of the encryption are measured using the correlation value. The encryption algorithm is evaluated using the time it takes to run the algorithm and the size of the key used in the algorithm.

Pixel Change Rate

The number of pixel change rate and Unified average change in intensity are the methods to observe the result of a small change in the input image. From these methods the consequential correlation among the pixels of the original image and encrypted image can be found (14).

Key Sensitivity

It is defined as the ciphertext's changes are caused by the key changes(12). The slight difference in the keys should cause great changes in the ciphertexts.

$$KS = \frac{Dif(Co, C1)}{n} * 100$$

HOMOMORPHIC ENCRYPTION PROTOCOL

Homomorphic encryption is a public key encryption scheme, like most of the encryption schemes used to protect financial transactions on the Web. Using public key encryption anybody can encrypt a message using a key that given, but only the holder of the secret key can decrypt it.

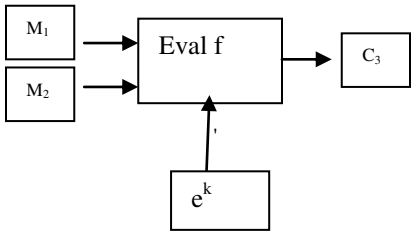

Fig.2. Homomorphic Protocol

This public key encryption schemes are more secure than their private key encryption schemes. In this encryption both the sender and the receiver will not have any prior agreement.

The public key encryption schemes are related to most critical mathematical calculations. This can not be done easily. So it is more secure. Homomorphic encryption gives a way of calculations on the encrypted data. When compared to typical method of encryption this gives more tedious computations as well as more security. There are different types of homomorphic cryptosystems in the public key encryption. Additively Homomorphic encryption is one of the important application, Hence it allows the linear operation on the encrypted text.

PROPOSED METHOD

In the proposed method, encryption keys are produced. Initially the image block is applied with the symmetric cryptosystems. The cipher text is then encrypted with the public key cryptosystems. The code word substitution method is applied to the original image.

In the receiver end, the hidden data extraction is accomplished, in the encrypted version. The main use of the proposed method is that the file is strictly preserved (7). Digital Asset Management Systems handle with the media data in the compressed and encrypted form. Assume that the size of the image is 512 X 512. It is divided into small MXM blocks. If M=32, the size of the block is 32X32.(15)

A number of pairs of coefficients (A, B) in the block are chosen as A=a1, a2… an, B=b1, b2,…. bn. Based on pseudo random numbers. For encryption, two coefficient value (ai,bi) is encrypted using the cryptosystem. This is continued for the M size, number of times (15). Each block is encrypted accordingly.

Y	Y
Y	Y

Fig. 3. Encryption on a Matrix

The conventional ciphers like IDEA, AES, DES, RSA can be applied only to the traditional image encryption. These ciphers require a large computational time and high computing power. The Proposed encryption scheme which uses an advanced encryption technique takes time for calculation. But the quality of the security is very high for the real time processes.

The proposed encryption method uses an secret key for encryption. The secret key size depends the size of the image. The key is divided by the number of blocks of the given image. The Figure 2 shows the encryption protocol of an Image sharing with privacy preserving.

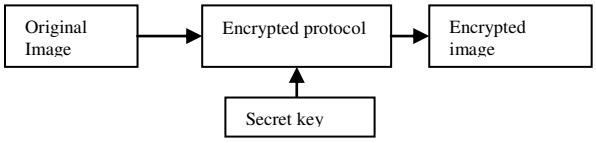

Fig.4. Homomorphic Protocol

Homomorphic protocol gets the original image. That image is undergone with the procedure of homomorphic property. The output is more secure than the other encryption technique. Various key sizes are given and compared with the property. Since the medical image is homomorphicallly secured the privacy of the patient is hidden.

$$C_j = \frac{N\sum_{j=1}^{N}(Xj * Yj) - \sum_{j=1}^{N} Xj * \sum_{j=1}^{N} Yj}{H}$$

$$H = \sqrt{\left(N\sum_{j=1}^{N} Xj2 - \sum_{j=1}^{N} Xj2\right) * N\left(\sum_{j=1}^{N} Yj2 - \sum_{j=1}^{N} Yj2\right)}$$

X,Y adjacent pixels in the image.

N – Total number of pixels selected from the image for the calculation.(9)

Image X = $\{x_1, x_2, \ldots x_n\}$

Encrypted Image C=$\{c_1, c_2, \ldots c_n\}$

TABLE I

KEY SIZES VS KEY SENSITIVITY

Key Size	Key Sensitivity C0-C1digits Correlation coefficient	
16	>8	Low
32	>18	High
64	>38	Higher
128	>67	Highest
256	>134	Highest
512	>270	Highest

The parameters used are showing the encryption quality of the data. If the key sizes increases, it increases the Key sensitivity. The correlation coefficient gives the pixel relation in the original image and encrypted image.

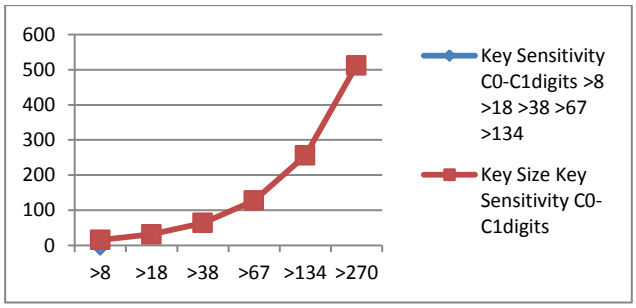

Fig. 5. Key Size Vs Encryption time

Figure 5. Shows the Various Key sizes and its Encryption time. Each and every pixel in the image is encrypted by different key sizes. The number of bits in the encrypted value of each pixel is counted here by the number of bits in the encrypted value of the pixel. The size of the resultant value is of large number. So the sizes are considered.

CONCLUSION

In this paper, We have presented Secured Homomorphic protocol. Using the asymmetric cryptographic technique, the personal image data is sent to the server. The receiver gets the data from the server and uses the data for treatment. This protocol gives more security over the personal data of the user when compared to the existing encryption techniques.

REFERENCES

[1]. Alireza Jolfaei and Abdolrasoul Mirghadri, " A new approach to measure Quality of Image encryption", International Journal of Computer and Network Security, vol.2, No.8, 2010.
[2]. Shiguo Lian, "Multimedia content encryption techniques and applications", 2008
[3]. N.K.Pareek, Vinod patidar, K.K. Sud, " Image encryption using chaotic logistic map", Image and Vision Computing, 2006
[4]. Zhan, Bi Sheng, and Duan Liu, " An image Transmission System Utilizing Chaos –Based Watermarking Technique", Applied Mechanics and Materials, 2013
[5]. S. Ye, Y. Luo, J. Zhao, and S.S.Cheung, "Anonymous Biometric Access Control", EURASIP Journal of Information Security, vol. 2009, Article ID865259, 17 pages, 2009.
[6]. Y.Huang, D.Evans, J.Katz and L.Malka, "Faster Secure two party computation using garbled circuit", in USENIX Security Symposium, 2011.
[7]. I.Cox, M.Miller, J.Bloom, J.Fridrich, T.Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008
[8]. John R.Smith and Shih-Fu Chang ," Tools and Techniques for Color Image Retrieval", Storage and Retrieval for Image and Video Databases, vol 2670.
[9]. XiaoJun Tong, "Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation", Science in China Series F information Sciences.

[10]. D.Rappe, Homomorphic cryptosystems and their applications, Cryptology ePrint archive, Report 2006/0011,2006
[11]. J.Giesl, K.VLcek, ICGST international Journal of Graphics, Vision and image processing, GVIP 09, 2009.
[12]. Hermassi, Houcemeddine, Mimoun Hamdi, Rhouma and Safya Mdimegh Belghith," A joint encryption-compression codec for speech signals using the ITU-T G.711 standard and chaotic map", Multimedia Tools and Applications, 2015
[13]. A. Nehal, Mostafa A., and Alaa Zaghloul, "Improving Image encryption using 3D Cat Map and Turing Machine", International Journal of Advanced Computer Science and applications, 2016
[14]. Hermassi, Houcemeddine, Mimoun Hamdi, Rhouma Rhouma, and Safya Mdimegh Belghith, " A Joint encryption-compression codec for speech signals using the ITU-T G.711 standard and chaotic map", Multimedia Tools and Applications, 2015
[15]. Zhan, Bi Sheng, and Duan Liu, "An image Transmission System utilizing chaos Based watermarking technique", Applied Mechanics and Materials, 2013