ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

Positional Based Encryption and Compression of Medical Images

[1]Deepika B Banagar, [2]Mamtha Mohan.

[1] M Tech, RIT,[2] Assistant Prof., RIT, Bengaluru

Abstract - **The expanding selection of data frameworks in social insurance has prompted a situation where understanding data security is increasingly being viewed as a basic issue. Permitting quiet data to be in danger may prompt hopeless harm, physically, ethically, and socially to the patient, conceivably shaking the validity of the medicinal services foundation. Therapeutic images play a the urgent part in such setting, given their significance in analysis, treatment, and research. In this paper the the compresssion of encrypted medical images is performed in order to provide the security and reduce the storage capacity. The positional based encryption is performed and arithmetic compression is used to compress the encrypted image.**

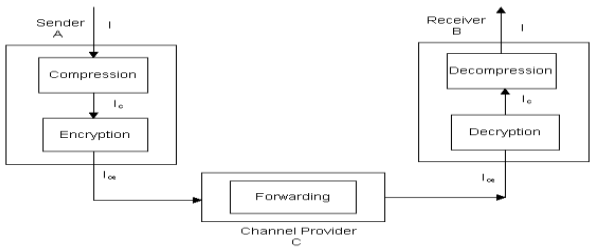
Keywords: **Encryption and Compression, Prediction error domain approach, Arithmetic Coding.**

I. INTRODUCTION

Medical information, Composed of clinical data, Images and other physiological signals, has become an essential part of a patient's care, whether during screening, the diagnostic stage or the treatment phase. Data in the form of images and signals form part of each patient's medical file, and such have to be stored and often transmitted from one place to another. The development of this digital imaging creates the obvious problem of the transmission of the images within healthcare centers, and from one establishment to another, as well as the problem of storage and archival. Image Encryption and Compression techniques can, therefore, be extremely useful when we consider the large quantities of data in question.

Consider an application scenario, A and B are two parties want to communicate with other. Let's say sender A wants to send some confidential information to receiver B. In multimedia communication, there is a chance of attack by the third party say attacker C. The attacker C may change or hack the information before receiver B gets the information. To avoid this kind of attack by the third party we need to provide security to the information. The information may be in terms of data, image or video.

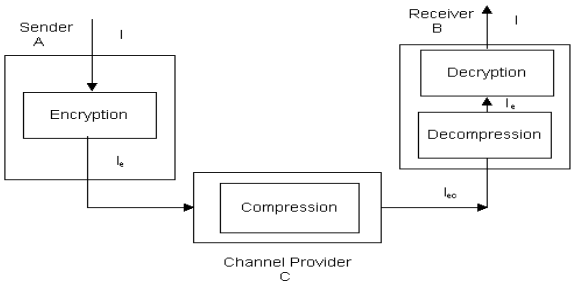
Compression and Encryption system meets the requirements in many secure application scenarios. The applying of Compression-then-Encryption needs to be reserved in some other situations. As the sender A is always interested in protecting the information of the image I through encryption. Sender A has no reason to compress his data, and hence, will not use his limited computational resources to run a compression algorithm before encrypting the data. This is especially true when sender A uses a resource-deprived mobile device. In contrast, the channel provider C has an overriding interest in compressing all the network traffic so as to minimize the network utilization. It is in this manner greatly wanted if the compression errand can be appointed by channel supplier C, who regularly has in exhaustible computational assets. A major undertaking inside such Encryption and compression structure is that compression must be directed in the encoded space, as channel supplier does not access to the mystery key K. As shown in Fig.1.



(a)

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017



(b)

Figure.1. (a) Traditional Compression and Encryption System ;(b) Encryption and Compression.

In [1] they focused on both lossless compression of encrypted bi-level images and lossy compression of encrypted real-valued data's separately. Distributed source coding theory is used in this work. [2] This work follows the graphical model for compression of encrypted images. This graphical model consists of three components connected together. They are source model, encryption model, and compression model. Source model is a 2-D spatially correlated model. Which includes an image pixel and its corresponding four neighboring pixels such as up and down, left and right. The second model is the encryption model. Stream cipher technique is used for encryption. Encrypted data is obtained by performing exclusive-or operation with key and data. For compression, it uses the code model, which includes linear transformation matrix. This matrix is used for the conversion of the encrypted data into compressed form. In [3] they used the spatial and cross-plane correlation between pixels and correlation between color bands are used to compress the encrypted gray level and color images. Subdivided the grey-level image into bit-planes and consider each of them as a separate black and white image. Before performing encryption the image is stored, in such a way that spatial correlation between bit-planes is removed. They used two methods to remove spatial correlation between bit-planes. [4] In this paper pseudo-random permutation based encryption method is used to obtain the cipher text. Cipher text is compressed by removing the excessive rough and fine information available in the transform domain. Then combined decoding and decryption are performed by the spatial correlation exist in the natural image. This is refined by the iterative reconstruction process. [5] Encryption is done in two ways. It may be stream cipher or block cipher. In stream cipher sequence of bits are considered for encryption using XOR operation. But in the case of block ciphers block of codes are used. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are examples for block cipher encryption. In block ciphers, there is a practical limitation of mapping two separate plain text block to a single cipher block. Compression is done by exploiting the correlation between the plain text and cipher text without having any knowledge about the key. [6] Multilayer decomposition is used for lossy compression of encryption gray scale images. Encryption operation is started from dividing images into sub-images. Prediction errors are calculated for different layers of the image. Then the sub image and prediction error are encrypted by exclusive-or operation and a pseudo-random permutation. Channel provider compresses the encrypted images by performing quantization and optimization with rate-distortion criteria on a various layer of the permuted prediction errors At the receiver, compressed the encrypted image is de-quantized and decrypted with the help of the key known by the receiver.

II. PROCEDURE FOR PAPER SUBMISSION

The existing Encryption and compression system uses the cipher text method to encrypt the image. This method fails in achieving the good compression efficiency. In order to overcome the drawback of existing system the system is proposed which uses the positional based encryption method for encrypting the image and Arithmetic coding lossless the compression technique for compressing the encrypted image.

2.1. The algorithm for Encryption and compression system can be summarized as follow:

Step 1.Input image - In this step the medical image is taken as input image.

Step 2.Gradient adjusts prediction (GAP) and Median Edge Detector (MED) - Here, the GAP and MED is performed on the medical image.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

Step 3 Determine prediction errors and mapping – In this step the predicted error image obtained by the GAP and MED are mapped.

Step 4.Prediction error clustering – In this the clustering is performed on the mapped image.

Step 5.Create 2D tables from the clusters

Step 6.Generate Random Permutation based keys for cyclic shifts – Here; the key is selected in order to perform the random permutation.

Step 7.Perform column wise cyclic shifts and Row wise cyclic shifts – the cluster index values are shifted cyclically

.

Step 8.Assemble the cyclic shifted clusters

Step 9.Encrypted image as shown in Fig. 2.

Step 8.De-Assemble to clusters

Step 9.Arithmetic coding as shown in Fig. 3.

Step 10.Compressed bit stream

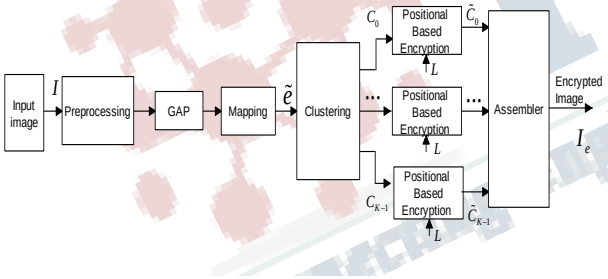


Figure. 2. Schematic diagram of image encryption.

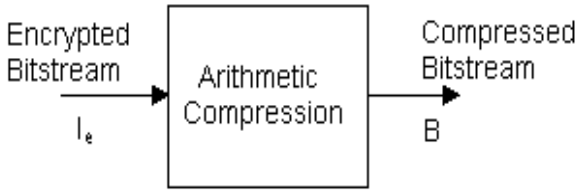


Figure. 3. Schematic diagram of compressing the encrypted data.

2.2. The algorithm for Decompression and Decryption system can be summarized as follow:

Step1.Compression Bit stream

Step 2.De-Assemble to clusters

Step 3.Arithmetic De-coding

Step 4.Perform Reverse Row wise cyclic shifts and reverse column wise cyclic shifts using permutation keys used during encryption

Step 5.Assemble the clustered prediction errors

Step 6.Add prediction pixels with prediction

Step 7.Reconstruction medical image as shown in Fig. 4.

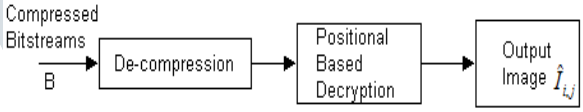
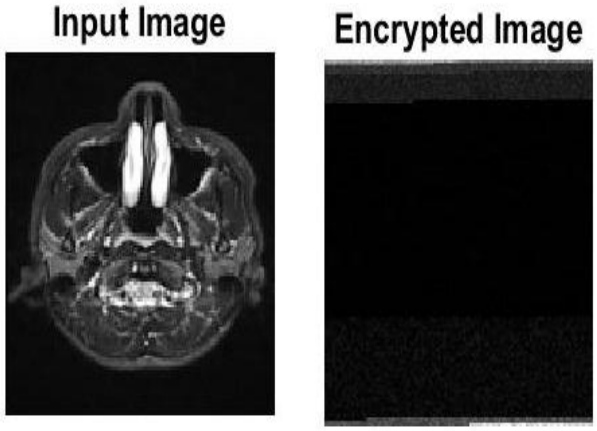


Figure. 4. Schematic diagram of consecutive decryption and decompression.

III. RESULTS

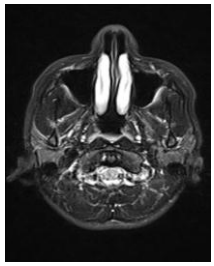


(a) (b)

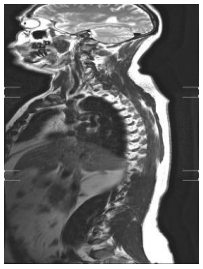
Figure. 5. (a) Input scanned image;(b) Encrypted image.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017



(1)



(2)

(3)

(4)

(5)

(6)

TABLE. 1. Compression Ratio

Scanned Images	Proposed Work	
	MED as a Predictor	GAP as a predictor
CT_1	1.8576	1.8189
CT_2	1.5817	1.4962
CT_3	2.1464	1.9476
CT_4	2.4257	2.3717
CT_5	2.1443	1.9437
CT_6	1.7491	1.6705

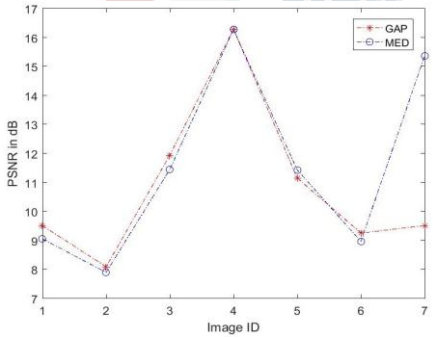


Figure. 6. PSNR of encrypted scanned images

This paper analyzes the two aspects of scanned image compression in encrypted domain, the compression ratio and PSNR using two predictors GAP and MED. As we can see in the Table. 1, the compression ratio of the images is more using MED as a predictor and less using GAP as a predictor and also in the graph, we can see that the PSNR of images is more using GAP as a predictor and less using MED as a predictor as shown in Fig. 6. By this we can visualize that GAP predictor is more efficient than the MED predictor.

IV. CONCLUSION

In this paper, the proficient medical image encryption and compression framework are composed. The proposed work incorporates the positional based encryption and exceedingly effective compression of the encrypted data has then been acknowledged by an arithmetic coding approach. In future, we can use this proposed work and compare the compression efficiency with the state-of-art output.

REFERENCES

[1] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption-then-compression system," in Proc. ICASSP, 2013, pp. 2872–2876.

[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[3] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.

[4] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[5] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural

networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, 452–468, Jun. 2011.

[6] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating pri-vate recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp.1053–1066, Jun. 2012.

[7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[8] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compres-sion of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.

[9] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.