JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190, Special Issue, No.-7, February (2020) pp 49-57 ISSN (Print) 0973-8975

SECURED ENCRYPTION THEN COMPRESSION TECHNIQUESFOR MEDICAL IMAGING APPLICATIONS

C. Priya[1] , C. Ramya[2]

[1]Associate Professor Department of ECE, Karpagam College of Engineering, Coimbatore.

[2]Associate Professor Department of ECE, PSG College of Technology, Coimbatore.

E-mail: [1]priyakarthikayeni@gmail.com, [2]ramyamaharajan@yahoo.in

https://doi.org/10.26782/jmcms.spl.7/2020.02.00003

Abstract

In the real time scenario, image encryption has been carried out early to the compression for maintaining the safety of the image. In this paper, a highly efficient image Encryption-Then-Compression (ETC) system has been designed, where the lossless compression is taken into account. The proposed image encryption method is operated with image encryption AES and RSA algorithm with Set Partition in Hierarchical tree(SPIHT) which shows logically high security compression technique. The ETC method is proved to be more simpler and efficient method while analyzing the parameters like Compression Ratio (CR), Peak Signal to Noise Ratio (PSNR).

Keywords: Compression, Encrypted Image, Decrypted Image, Decompression

I. Introduction

Nowadays, e-health service is achieving much attraction to preserve and transmit the medical transcriptions through online. This provides the physician for clear clinical interpretation without carrying the documents for analysis the disease of a patient. For compressing of the medical image interpolation technique is used, it gives better compression ratio. A combinational hybrid compression algorithm also used for compression of medical image which is implemented for lossless compression. A method using EZW encoder with Huffman Encoder which provides good Compression Ratio (CR) and Peak-Signal to- Noise (PSNR) for different threshold values ranging from 6 to 60 for decomposition level 8[IV].Progressive transmission through subsampling which enables the spectral correlation it results in improved decoding performance. This method provides better performance comparing with the-state of- the-art 3D methods, including existing distributed source coding (DSC) technique[V].In recent times, using the Haar wavelet transform used on the encrypted image which yields high compression ratio, mean square error. A novel method which was hybridization of two lossless image compression techniques

The Paper Presented at 14th International Conference on Intelligent System and Control (ISCO'20) Organized by The Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, India

in order to give better results. Initially, the data folding was applied to the image which was followed by arithmetic coding techniques to provide better compression ratio and lesser Bits per Pixel[VIII].Under encrypted domain, prediction error was used for encryption and context-adaptive coding the prediction error was tear into N number of clusters .Encryption is done by permutation method which strengthens the encryption. And then adaptive arithmetic coding was followed for compression. This methods provides high security and better compression ratio [IX].

This paper contains the following sections as: describes the proposed method, discussed about the results and discussion and conclusion of the work.

II. Proposed Method

In this work, an efficient algorithm is designed based on image Encryption – Then - Compression system. The main advantage of ETC system is it provides a secure compression for the medical image. A novel technique is proposed here for image encryption of medical image. The proposed method compares and analysis two techniques using AES with SPIHT compression and RSA with SPIHT coding for compression. Here, the ETC method will increase the compression ratio, peak signal to noise ratio and Structural similarity. Both the proposed method achieves better security, high PSNR, high compression ratio .Figure 1 indicate the proposed ETC method functional structure.

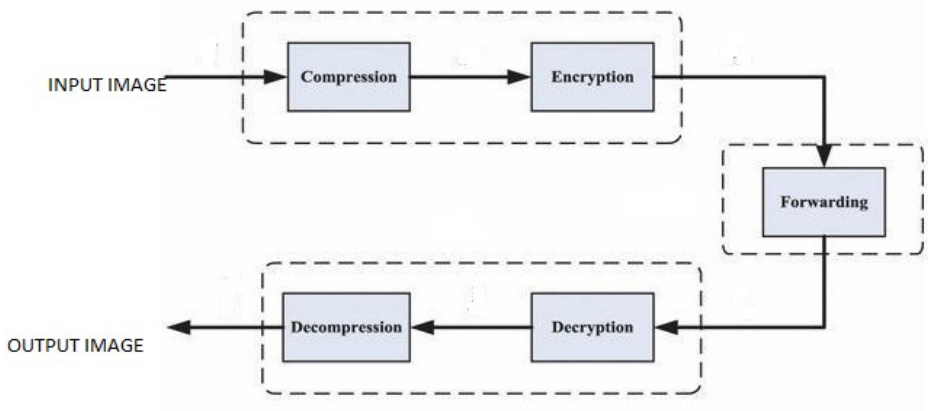


Fig. 1: Proposed method functional structure

Image Encryption

AES Algorithm

AES algorithm is used to converts the plain text into cipher text by taking plain text's block at once and operate on constant-length group of bits called Blocks. Three different key sizes is employed in AES algorithm like 128, 192 and 256 bits . It uses same size of input and output blocks respectively. Second key is required for the AES algorithm, which is that the secret key. In AES algorithm uses 4 different byte oriented layer for both its Cipher and Inverse Cipher they are 1) Using a

substitution table (S-box) 2) State array is replaced by various offsets 3) Combining the information within coloumn of the State array 4) Adding a Round Key to the State5)Adding the cipher text bits.

RSA Algorithm

RSA algorithm is an acknowledged and established absolute public key system with respect to speculation and application. Applying the RSA algorithm within pre-processing stage of data hiding to confirm the safety of the information.RSA algorithm is performs modular and exponent function.

Pseudocode:

(a) Calculate the largeprimes p, q.

(b) Determine: w = p x q, j = (p- 1) x (q-1).

(c) Chooserandom number athat must be lower than w and prime to z, there shouldnot exist a common factor between a and z.

(d) Choose a value as k, where (a*k-1) is dividable by j.

(e) The public key (w, a) and private key (w, k).

(f) Encryption: Decryption:

s = x ^ a mod w. d = s ^ k mod w.

Where x - message and cipher text – d

SPIHT Algorithm

SPIHT is arrangement of the tree is based on wavelet transform coefficient and transmits the coefficient progressively based on the increasing refined version of the original image.

SPIHT introduces three list of wavelet coefficient:

a)List of insignificant pixels(LIP)

b) List of significant pixels(LSP)

c) List of insignificant sets(LIS)

Pseducode:

1a. Initialization

Output $[\log_2 (\max|Coeff|)]$;

Set LSP as empty;

Add all the elements $(i, j) \in H$ to LIP;

Add the element $(i, j) \in H$ with descendants to list LIS

1b. Sorting pass

Process LIP:

for each element (i,j) in LIP output $U_n(i,j)$

if $U_n(i,j)=1$

Move (i,j)to the LSP

Process LIS:

for each (i,j) in LIS

if type Qnext

Output U_n (M (i,j))

if U_n (M(i,j))=1

forevery (u, l) $\in$ R (i,j) do

Output U_n (u, l)

if U_n (u, l) =1 next

add (u, l) to the LSP

if U_n (u, l) =0 then

add (u, l) final of LIP

if the entry is of type A

output U_n (L(i,j))

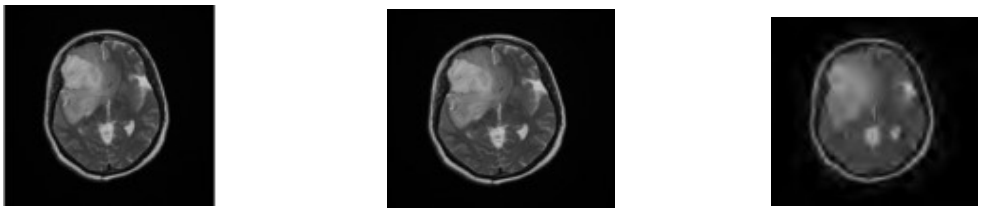
1c. Refinement Pass

For each entry (i, j) in the LSP, excluded the last sorting pass

Result of the n^{th} MSB of $|C_{i,j}|$.

III. Results and Discussion

To evaluate the performance of the proposed method various medical images are taken to compare and analyze the efficiency of the proposed encryption then compression method. The proposed methodology is applied over 50 MRI image each of size 512x512 pixels. Initially, encryption method followed by compression technique is applied to the original image. This work shows comparative analysis of two ETC methods. Figures2(a), 3(a) shows the samples of original testimage. Figure 2(b),3.(b) shows the resultant image after applying AES with SPHIT compression technique and finally, figure 2(c),3(c) shows the resultant image of RSA with SPIHT technique.



(1) **(2)** **(3)**

Fig.2:(1)Original test image 1 (2) Result of AES with SPIHT (3) Result of RSA with SPIHT

(1) **(2)** **(3)**

Fig.3:(1)Original test image 2 (2) Result of AES with SPIHT (3) Result of RSA with SPIHT

Performance Analysis

Visual observations of the test images are not enough to approximate the resultant compression compatibility of the proposed method. The proposed two ETC methods is also evaluated objectively with Peak Signal to Noise Ratio (PSNR), Structural Similarity (SSIM) and Compression ratio (CR)

Peak Signal to Noise Ratio:

The proposed method PSNR value is compared in figure 4 and in table 1.Its reported that in table 1,foran example in the image 7 the PSNR value for the proposed ETC methods asAES –SPIHT has 27.095 and for RSA-SPIHT is 34.423. It is also evaluated for multiple set of test images and found the results. But the proposed RSA-SPIHT method which shows the improved PSNR value than AES-SPIHT method .Hence it preserves the quality of the image.

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{1}$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i.j) - \tilde{I}(i,j)]^2 \text{ ------} \tag{2}$$

Where MAX-maximum pixel value of the image

MSE - Mean square error ;MxN -Size of the image,

I(i,j) -Original image ; $\tilde{I}(i,j)$ -Compressed image

Table 1.Comparision of PSNR(%) for theproposed Method

Test Image	AES with SPIHT	RSA with SPIHT
Image 1	37.687	42.433
Image 2	35.473	40.351
Image 3	24.685	33.423
Image 4	33.942	45.634
Image 5	35.321	36.241
Image 6	37.671	37.931
Image 7	27.095	34.423
Image 8	36.873	37.231
Image 9	37.562	40.312
Image 10	34.231	47.231
Image 11	34.312	45.532
Image 12	39.341	40.345
Image 13	33.563	40.934
Image 14	30.324	39.766
Image 15	33.532	35.569

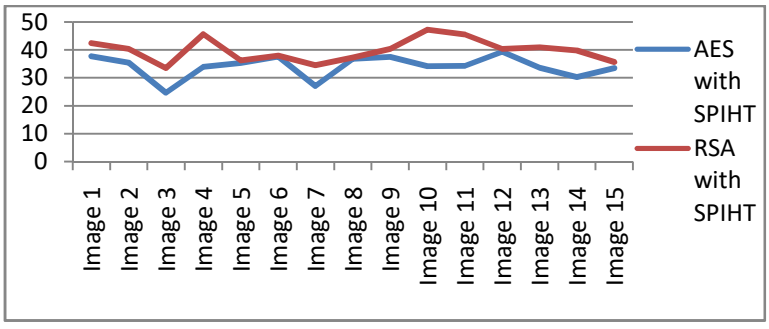


Fig. 4: Comparison of PSNR value for the proposed methods

Structural SIMilarity Index Method :

SSIM is the current technique which shows the similarity between the two images. It values must lies between [0 1].Table 2 shows the SSIM values between the proposed methods. For example in image 3, the SSIM value for the AES with SPIHT is 0.899 and for RSA with SPIHT is 0.901 respectively.

SSIM is given as

$$SSIM(X,Y)=\frac{(2\mu_x+\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^{\,2}+\mu_y^{\,2}+C_1)(\sigma_x^{\,2}+\sigma_y^{\,2}+C_2)} \quad (3)$$

Where μ_x, μ_y is the mean intensity; σ_x, σ_y is the standard deviation

σ_{xy} is the correlation coefficient ; C_1, C2 are the constant.

Table 2.Comparision of Structural Similarity(SSIM) for the proposed Method

Test Images	AES with SPIHT	RSA with SPIHT
Image 1	0.901	0.972
Image 2	0.900	0.918
Image 3	0.899	0.901
Image 4	0.901	0.921
Image 5	0.888	0.899
Image 6	0.900	0.951
Image 7	0.876	0.892
Image 8	0.891	0.901
Image 9	0.900	0.934
Image 10	0.895	0.913
Image 11	0.866	0.898
Image 12	0.879	0.902
Image 13	0.857	0.894
Image 14	0.860	0.893
Image 15	0.862	0.897

Compression Ratio(CR%):Compression Ratio defines the amount of redundancy removed from the original image. From the table 3, it is clearly observed that the method RSA with SPIHT achieves better compression ratio than the AES with SPIHT method. Compression ratio is represented as

CR(%)=Uncompressed file size/Compressed file size -- (4)

Table.3. Comparison of Compression Ratio (CR %) for theproposed Methods

Test Images	AES with SPIHT	RSA with SPIHT
Image 1	25.26	35.28
Image 2	15.00	19.78
Image 3	18.01	28.11
Image 4	26.23	38.18
Image 5	28.48	30.94
Image 6	27.23	34.45
Image 7	35.21	40.28
Image 8	30.25	34.23
Image 9	30.12	36.32
Image 10	31.00	35.23
Image 11	27.36	34.21
Image 12	23.36	29.23
Image 13	30.63	38.23
Image 14	23.39	28.12
Image 15	28.26	33.69

IV. Conclusion and Future Work

Here,a most efficient ETC method has been designed and discussed in this paper. The proposed work is image encryption has been achieved via AES and RSAencryption algorithm. The image is encrypted using image encryption AES and RSA algorithm and then encrypted image is compressed and decompressed under SPIHT. The ETC method which improves the Compression Ratio (CR), Peak Signal to Noise Ratio (PSNR), structural similarity.The outline of the work is to achieves high efficiency with improved performance which is clearly shown in theresults . Also high level of performance and the security has been retained by applying the

ETC method.In future,the proposed technique isused for the color image and volumetric images.

References

I. C.Priya , T.Kesavamurthy & M.UmaPriya , An Efficient Lossless Medical Image compression using Hybrid Algorithm, Advanced Materials Research,No.984,pp. 1276-1281,2014.

II. Hussain, N., Boles, W and Boyd, C.,A review of medical image water-marking requirements for teleradiology, J. Digital Imag., Vol.26,No .2,pp 326–343, 2013.

III. Jablon, D. ,Strong password only authenticated key exchange, computer communication review, ACM SIGCOMM Comput. Commun. Rev.,Vol. 26,No.5,pp.5-26,1997.

IV. Janaki.R and Dr.Tamilarasi.A, "Still Image Compression by Combining EZW Encoding with Huffman Encoder" IJCA, VOL.1, NO.7, 2011.

V. .Jinlei Zhang, Houqiang Li and Chang Wen Chen, "Distributed Lossless Coding Techniques for Hyperspectral Images" IEEE Journal of Selected Topics in Signal Processing, Vol.1,No2,pp.2-5, 2015.

VI. Prior, F., Ingeholm, M.L., Levine B.A.andTrabox, L., Potential Impact of HITECH Security Regulations on Medical Imaging, in Proc. Eur. Molecular Biol. Conf., , pp. 2157-2160 , 2009.

VII. Ramya,C. and Subha Rani ,S.,Contrast Enhancement for Bio-Medical Image Sequences ,International J. of Computer and Electronics Engineering, pp.121-124,2012.

VIII. RichaGoyal and SouravGarg, "Lossless Image Compression using Data Folding followed by Arithmetic Coding" IOSR Journal of Computer Engineering, e-ISSN: 2278-0661, p-ISSN:2278-8727, VOL.17, No. 2,2015.

IX. Zhou "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation" IEEE Transactions on IFS, VOL.9, NO.1, 2014.