Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020) Pp-194-202

BBRC
Bioscience Biotechnology Research Communications

Selective Image Encryption of Medical Images Based on Threshold Entropy and Arnold Cat Map

Kiran[1] and Parameshachari B. D[2]
[1]*Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India*
[2]*Department of Telecommunication Engineering, GSSS institute of Engineering for Women, Mysuru, Karnataka, India*

ABSTRACT

In medical image applications, selective image encryption plays an important role as it reduces computational cost and time. Lot of existing full image encryption algorithms may be more complex and uses traditional techniques. Effective method has been developed for protection of medical images. Combination of threshold entropy and Arnold Cat Map (ACM) are used in the algorithm to encrypt only selected part of medical image. Threshold entropy value used for separating the significant and insignificant blocks in the original image. In order to reduce the blocking artifacts after the partition of medical image, neglect the insignificant pixels present in the image sub blocks based on the thresholding of Lower four binary planes. At last Least significant Bit (LSB) embedding algorithm employed to achieve lossless encryption. The proposed technique is achieves the low computational complexity and also fast execution time.

KEY WORDS: SELECTIVE ENCRYPTION, ACM (ARNOLD CAT MAP), ENTROPY, LEAST SIGNIFICANT BIT (LSB), BASIC INTENSITY IMAGE (BII).

INTRODUCTION

Recent development in the internet applications, a high level security needed for all types of multimedia transmission. Encryption provides the security for the multimedia information especially for images. They are different types of encryption namely full image encryption, selective image encryption and partial image encryption. Based on the type of application anyone of the encryption type can use. Most importantly for medical image transmission, bandwidth plays an important role. To reduce the computational complexity and time selective image encryption should be implemented. Because small amount of encryption in medical images leads to higher security and very difficult for third party person diagnosis correctly.

MATERIAL AND METHODS

This paper described selective image encryption based of contribution of image bit planes. with the help of one way coupled lattice encrypt the portion of significant bits of pixels and also extended this method for RGB images (Xiang, T et al 2007). selective encryption method in frequency domain with the help of wavelet transform has been proposed and this work gives lossy encryption result (Kulkarni et al 2008). Security for medical images using LSB and chaotic map patient ID text information embedded into LSB of medical image followed by encryption algorithm (Bremnavas et al 2011). Partition based encryption technique for medical images. Where AES technique applied to region of interest and gold code is applied to background region of medical image(Mahmood, A.B. and Dony, R.D 2011).

Fractional wavelet based selective image encryption method has been proposed. Initally image divided into number of different sub bands. Chaotic stream cipher

ARTICLE INFORMATION

*Corresponding Author: kiran.mtech12@gmail.com
Received 14th Oct 2020 Accepted after revision 30th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31)
A Society of Science and Nature Publication,

Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.13/27

method applied to significant sub bands. method can reduce the computational time with high security (Taneja et al 2011). Pixel of interest based selective image encryption with the help of singular value decomposition. To confuse the position of pixels, saw tooth space filling curve applied and later selecting the significant pixels using pixel of interest method (Bhatnagar et al 2012). In this work reduction in the amount of data to be protected with the help of chaotic map. 2D chaotic standard map used to de-correlate the pixel relationship (Yousif et al 2013). Chaos based partial encryption scheme to reduce speed and time compared to traditional full image encryption based binary bit planes of image, important bit planes are encrypted using pseudo random binary number generator(Som, S. and Sen, S 2013).

Automatic and manual based region selecting encryption method has been proposed. In manual selection, image is segmented into number of non-overlapped blocks and randomly selected the sub blocks for the encryption. but for automatic, morphological techniques are applied to select region of interest(Panduranga, H.T. and Naveenkumar, S.K 2013). Full and selective medical image encryption using chaos has been proposed. Pseudorandom matrix employs for improve the speed of the algorithm (Kanso, A. and Ghebleh, M 2015). Edge map based medical image encryption algorithm consists of three parts. they are bit plane decomposition, random sequence generation and permutation. Different edge maps generated using various edge algorithm with threshold values (Cao et al 2017).

Copyright protection scheme arranging the separates the edge blocks in descending order (Murali, P. and Sankaradass V 2018). Partial encryption for medical images has been proposed which uses the DNA encoding and addition techniques. (Parameshachari B.D et al 2017). In this image encryption method where the amount of encryption easily controlled by the help of LSIC and chaotic map (Parameshachari B.D et al 2019). In the present information technology, hiding the image information to cover file technology is become more important (Zhou et al 2016). The least significant bit (LSB) embedding algorithm is most efficient and simple technique to hide large amount of data into its cover file and that will not affect to clarity of cover image (Al-Sanjary et al 2020). Region of interest based encryption used for reduce computational complexity and fast execution. To select region of interest active contour method has been employed (Parameshachari B.D et al 2020).

In the proposed method, the following techniques are utilized to encrypt only the region of interest part in the medical images. Figure 1 depicts the overall architecture of the proposed method.

3.1. Arnold Cat Map (ACM): Arnold cat map is one of the important random shuing methods (Madhusudhan K.N. and Sakthivel P 2020). Which is defined by following equation 1. It consists of p and q positive integer and can be considered as key.

$$\begin{bmatrix} s' \\ r' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} s \\ r \end{bmatrix} \quad (1)$$

Where (s, r) and (s', r') are the picture coordinates of the input and permuted image respectively. Arnold cat map having a periodicity problem that after some number of iteration original image will be reconstructed and periodicity depends the size of the image and also the positive integer p and q. Table 1 shows the periodicity of ACM. Where N is number of row in the input image.

Table 1. Periodicity of ACM

Period	Number of cat maps	Values of p and q
T=1	1	p=0,q=0
T=N	2N-2	p=0,q≠0 p≠0,q=0
T=2N	N-1	Pq=2N-4 mod N

3.2 Least Significant Bit (LSB) Embedding Algorithm: Proposed algorithm uses LSB algorithm to replace information in the least bit of cipher image with significant blocks information. Because at the decryption side, need to reconstruct original image without loss of any information original image. In the proposed method after encryption entropy of significant blocks are altered so in order to keep the significant blocks information, LSB embedding algorithm employed in the proposed algorithm. As we know that every grey scale image information is distributed into eight binary bit planes where least significant bit plane contains very least information. Therefore all the significant block index numbers are converted into bit stream then this bit stream are inserted into LSB of cipher image. The LSB modification does not result in cipher image distortion and thus the resulting cipher image will look identical to the original cipher image.

3.3 Proposed selective encryption method: Proposed selective image encryption of medical image consistes of following steps.

- **Selection of Significant area:** The orignal image is paritioned into 16*16 non overlapping sub block and induvisual block entropy can be calculated and refered as {E1,E2,E3,..........En}. Threshold entropy can be calculated from the input medical image using following equation (1). Therefore threshold entropy vary for different images.

$$\text{Threshold\_entropy} = \frac{\text{sum of entropy of all induvisual sub blocks}}{\text{Total number of induvisual sub blocks}} \quad (2)$$

Based on the calculated threshold entropy significant sub blocks can be separated and their index will be saved for the lossless encryption. Further reduction of blocking artifacts can be done by separating insignificant pixels in each significant sub blocks using threshold which can be calculated form lower 4 binary bit planes of input medical image.

$$\text{Threshold\_value}= \sum_{i=0}^{3} 2^{i} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

• **Encryption process:** Once the calculation of significant sub blocks with significant pixel done. Encryption process applied to that blocks. For the encryption process simple and reversible effective XOR operation is used. Pseudo random matrix generated by applying ACM to basic intensity image. Basic intensity image is the one where it consists of all the pixels from 0 to 255 in the form of 16*16 matrices. Different basic intensity images as shown in the figure 4. At last selective medical encrypted image obtained.

• **LSB Embedding Algorithm:** While performing medical image encryption needs to concentrate on lossless decryption method. For the purpose of reconstruction of lossless medical image, saved index of significant sub blocks embedded into the LSB bit plane of selective encrypted image by using LSB Embedding algorithm.

Algorithm for Selective image encryption:

Step 1: Input the medical image of size M*N.

Step 2: Divide the original plain image into 16*16 sub-blocks represented as

Blocks= [b1,b2,b3,b4......................$b_{M*N/(16*16)}$].

Step 3: Calculate the entropy of every 16*16 sub-blocks represented as

E=[E1,E2,E3,..................................En] where n=M*N/(16*I16).

Step 4: Using equation 2 calculate threshold entropy.

Step 5: Based on the threshold entropy in step 4 segregate the significant blocks and in significant blocks from the total blocks labeled Block.

Step 6: Using another threshold value from equation 3 to differentiate significant pixels in the significant blocks.

Step 7: Apply ACM to Basic intensity image to generate pseudo random matrix.

Step 8: Perform XOR operation between random matrix and significant blocks.

Step 9: for encrypting next selected block, goto step 7 and treat random matrix as basic intensity image for next iteration.

Step 10: Resulted selective encrypted image is obtained.

Step 11: Using LSB embedding algorithm to embed the index of significant blocks into selective encrypted image.

Decryption Process: Decryption is reverse process of encryption. Decryption should be performed at the receiver side to extract original image from encrypted image transmitted through unsecured channel. Proposed method employed lossless encryption technique because reconstructed image obtained after decryption process exactly equal to the original image. Figure 3 shows the block diagram of proposed decryption process. Algorithm form decryption process as explained below.

Algorithm for Selective image Decryption:

Step 1: Input the encrypted medical image of size M*N.

Step 2: Divide the encrypted medical image into 16*16 sub-blocks represented as

Blocks= [b1,b2,b3,b4...$b_{M*N/(16*16)}$].

Step 3: Apply the LSB extraction method to encrypted medical image for extract the index of significant blocks.

Step 4: According to the extracted index values, pic the significant block in the set of 16*16 sub blocks.

Step 5: Using threshold value from equation 3 to differentiate significant pixels in the significant blocks.

Step 6: Apply ACM to Basic intensity image to generate pseudo random matrix.

Step 7: Perform XOR operation between random matrix and significant blocks.

Step 8: for decrypting next selected block, goto step 7 and treat random matrix as basic intensity image for next iteration.

Step 9: Resulted decrypted image is obtained.

Experimental Setup and Performance Evaluation: Performance analysis of proposed work is to be validated and implemented using MATLAB 2017b.The medical images used are taken from Open-i image database. The size of medical images is 256 × 256, 512x512 and 1024x1024. Table gives the medical images used for simulation. In the following section explained about parameters used for evaluating performance of proposed work.

4.1 Histogram analysis: Image histogram graphically characterizes the spreading of pixels based on their occurrence. For highly secured encryption technique, histogram of cipher image should be uniformly distributed. Table 3 displays the histograms of the different plain medical image and the cipher medical images. Histogram of cipher medical images clearly indicates that their pixel distribution is random and uniform.

4.2 Entropy Analysis: Entropy gives the measure of information randomness in the image (Ahmad J and Ahmed F 2018). The equation for entropy is given by

$$H(S) = \sum_{i=0}^{2^M-1} P(si)\log_2 \frac{1}{P(si)} \ldots\ldots\ldots\ldots\ldots \quad (4)$$

Table 2 shows entropy of some sample images and their corresponding cipher images. In addition, the local entropy can better represent the randomness of the image, it may be defined as:

$$H_k T_B(m) = \sum_{i=1}^{k} \frac{H_{bi}}{k} \quad (5)$$

Where non-overlapping image blocks b1; b2; ....bn, with TB pixels for a test image S are randomly chosen, H(bi) represents information entropy for image block bi, and k is the block number.

4.3 Mean Square Error: Mean squared error (MSE) is defined as an average of the square of the difference between plain image and encrypted image (Ahmad J and Ahmed F 2018). The MSE is given by the equation

$$MSE = \frac{1}{MXN} \sum_{i=1}^{M} \sum_{j=1}^{N} [X(i,j) - Y(i,j)]^2 \quad (6)$$

4.4 Number of Pixel Change Rate (NPCR): Plain image and encrypted image represented by C1 and C2 respectively. C_1 (i, j) and C_2(i, j) are original image pixel and encrypted image pixel respectively(Wu et al 2011). The NPCR is then defined as,

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} X100\% \quad (7)$$

Where, D is bipolar array.

$$D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, \quad otherwise \end{cases}$$

4.5 Peak Signal to Noise Ratio (PSNR): The peak signal to noise ratio is evaluated in decibels and is inversely proportional to MSE(Ahmad J and Ahmed F 2018). It is given by the equation

$$PSNR = 10\log_{10} \frac{255}{MSE} \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

4.6 Unified average changed intensity (UACI): It is used measure the intensity rate difference between the plain image and cipher image((Wu et al 2011).

4.8 Time efficiency: The volume of the data will decide the computational complexity of the proposed scheme. Only the ROI data is encrypted in the

$$UACI = \frac{1}{N}\left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255}\right] \quad (9)$$

4.7 SSIM (structural similarity index matrix): To find the similarity between the input and encrypted image SSIM used. Equation for SSIM is

$$SSIM(x,y) = \left[\frac{(2\mu x\mu y + C1)}{(\mu x^2 + \mu y^2 + C1)} \frac{(2\sigma xy + C2)}{(\sigma x^2 + \sigma y^2 + C2)}\right] \quad (10)$$

Where C1,C2 are two constants and are used to stabilize the division with weak denominator.

4.8 BER (bit error rate): It is the parameter that is used to measure the similarity between the two images. BER can be mathematically represented as:

$$BER = \sum_{i,j} \frac{S(i,j)}{T_{pixels}} \quad (11)$$

T_{pixels} denote the total number of pixels present in an image. Thus, higher the value (close to 1) of BER better is the encryption technique.

proposed scheme. Table 8 gives the comparison of encryption time and data ratio. Encrypted data ratio represents the ratio of encrypted data to the whole data stream. The encryption time represents the time required for encrypt the ROI part.In our proposed scheme, only the ROI of the plain image is encrypted, and thus we examine only the histogram of the ROI. Table 3 illustrates the ROI histograms of the plain images, cipher images, and decrypted encrypted image are evenly distributed, similar to white noise.

From Table 5, all the 8-bit cipher images' local entropies are more than 7:901, and close to the ideal value. This better proves our algorithm has good local randomness and can effectively resist entropy attacks. The ideal value for UACI is approximately 33.3333%, while the ideal value for NPCR is approximately 99:9985%. We tested different images to obtain NPCR and UACI using the proposed encryption scheme. The test results are listed in Table 7, which shows that our encryption scheme meets the robustness requirements against differential attacks.

Table 6 gives the MSE and PSNR values for different medical images. As from observation our proposed method gets higher values of MSE and lower values of PSNR. From the SSIM calculation table 9 gives lower values of SSIM. The SSIM value between original image and encrypted image should be as small as possible, that shows the effectiveness of encryption algorithm. From Table 9 it is clear that using our method higher values of BER are obtained. Thus, higher the value (close to 1) of BER better is the encryption technique.

Smaller encryption time is a desirable feature in real time applications. Table 8 gives the encryption time and encryption ration of proposed method. From Table 8 it is clear that we have obtained lesser encryption time and around 50% region in original images is encrypted. This is achieved because instead of full encryption of medical image we are doing selective encryption of ROI-image and time taken to perform the XOR based encryption is small as it is light weight encryption technique. Figure 5-9 shows the graphical analysis of all the performance parameters which are calculated between original medical image and encrypted image.

Figure 1: Block diagram of the proposed encryption method

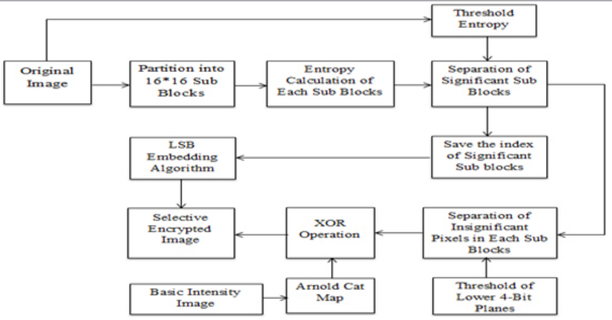


Figure 4: (a-b) matrix form of different basic intensity images

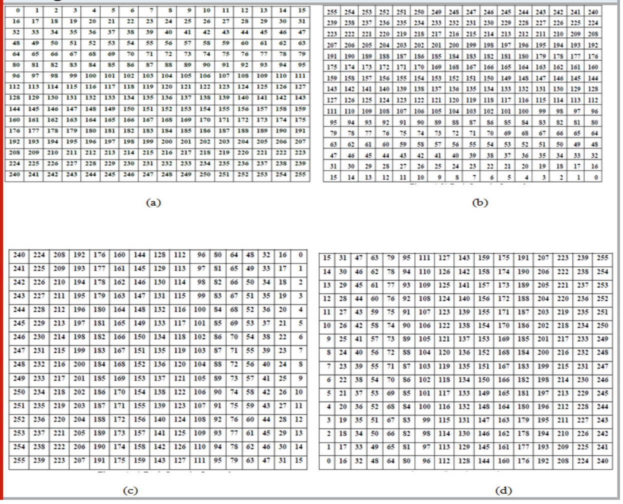


Table 3: Histogram Analysis of proposed system

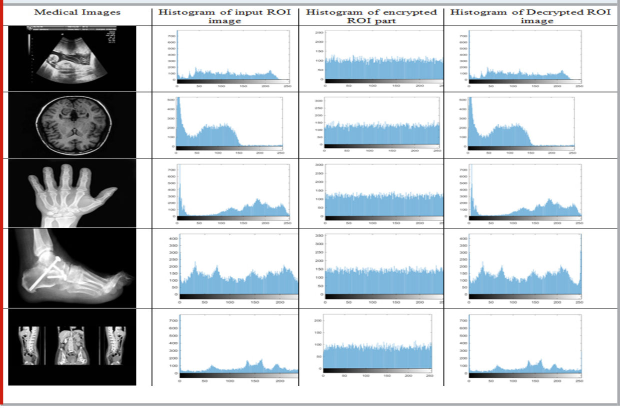


Figure 2: Block diagram of the proposed Decryption method

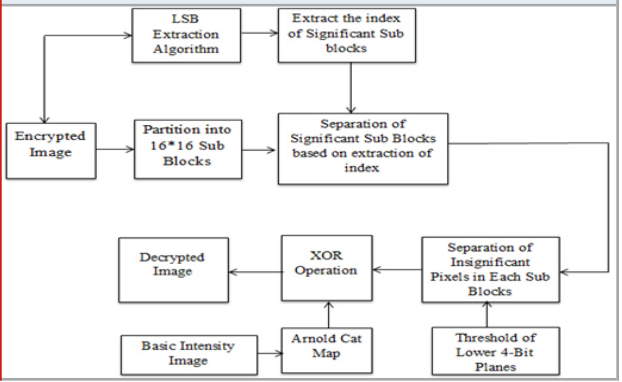


Table 2. medical images used in the proposed system

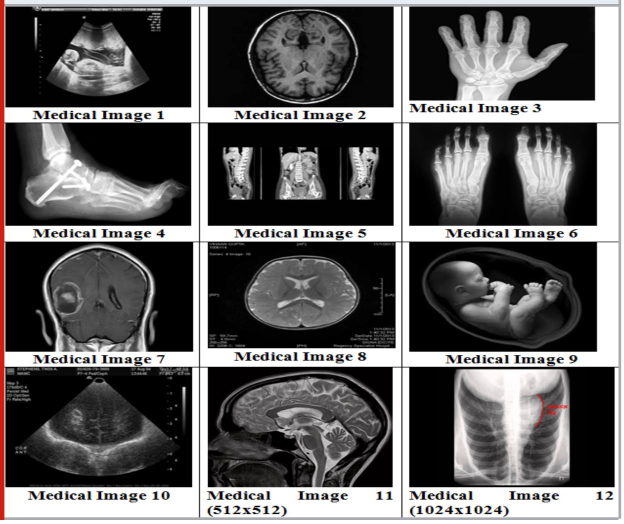


Table 4. Histogram Analysis of proposed system

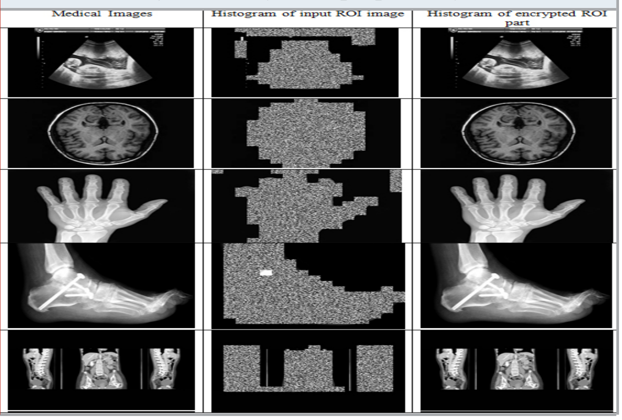


Table 10 shows the performance analysis for different basic intensity images used in the encryption process. Less effect of performance can observe by changing the order of pixels in the basic intensity image compared to first basic intensity image. Because of XOR based diffusion operation will not get more effect by changing position of

Continue Table 3

pixels values. Therefore different basic intensity images will not effect to encryption algorithm.

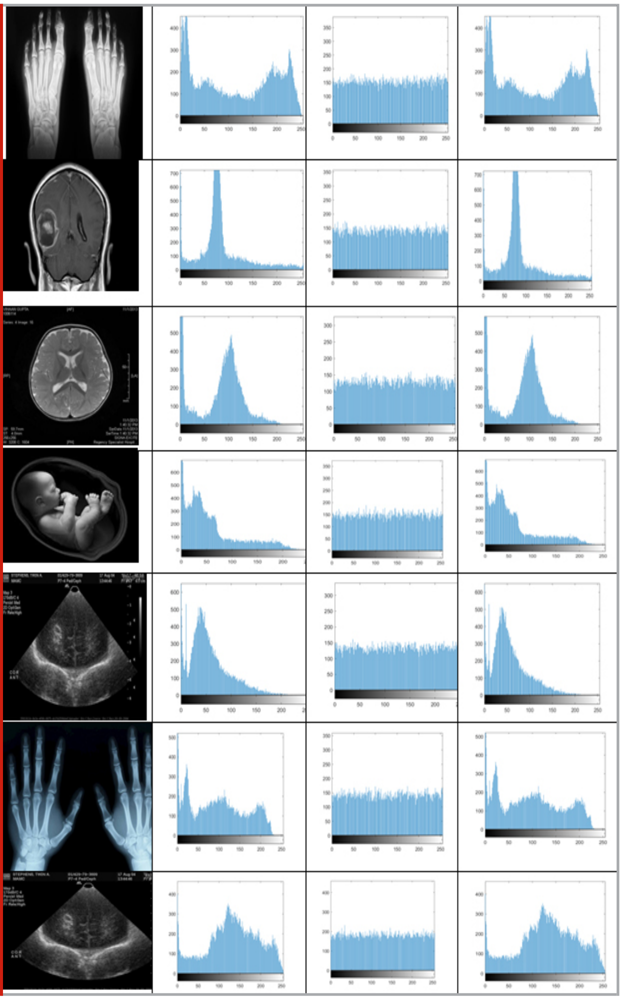


Table 5. Local Entropy analysis of proposed method

Medical Images	Input ROI Entropy	Cipher ROI Entropy
Medical Image1	6.9843	7.9936
Medical Image2	7.1965	7.9940
Medical Image3	7.0466	7.9948
Medical Image4	7.8532	7.9954
Medical Image5	6.7640	7.9935
Medical Image6	7.7746	7.9955
Medical Image7	6.8826	7.9944
Medical Image8	6.9101	7.9945
Medical Image9	7.0543	7.9949
Medical Image10	6.9067	7.9956
Medical Image11	6.758	7.9992
Medical Image12	7.312	7.9991

Continue Table 4

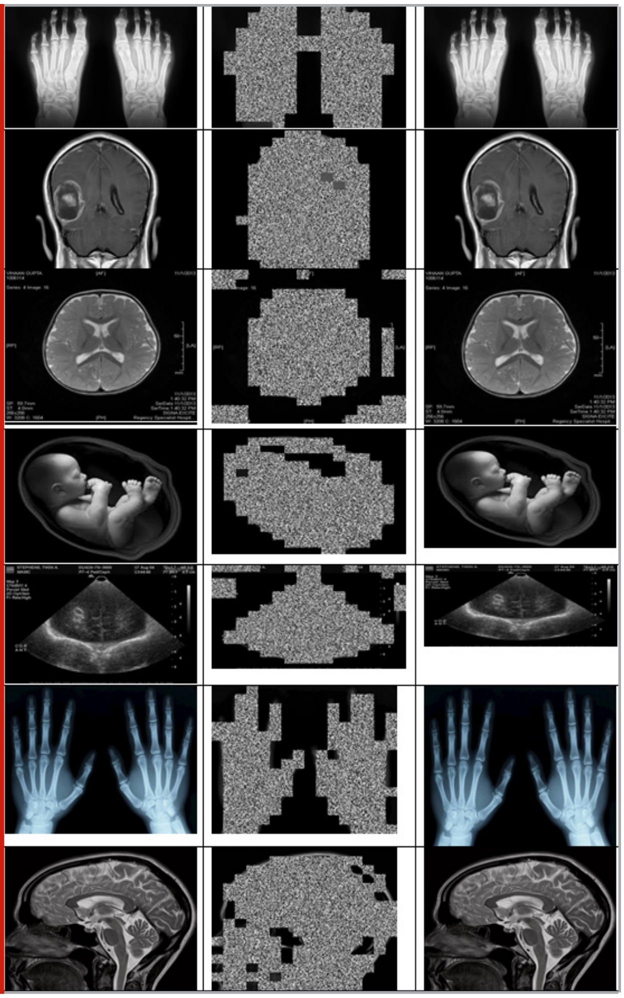


Figure 5: Graphical analysis of Entropy between original image and encrypted image

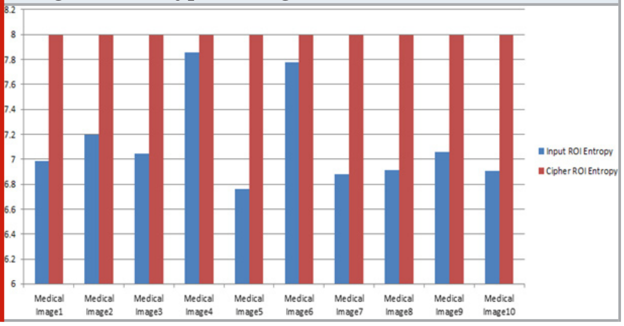


Figure 6: Graphical analysis of MSE and PSNR between original image and encrypted image

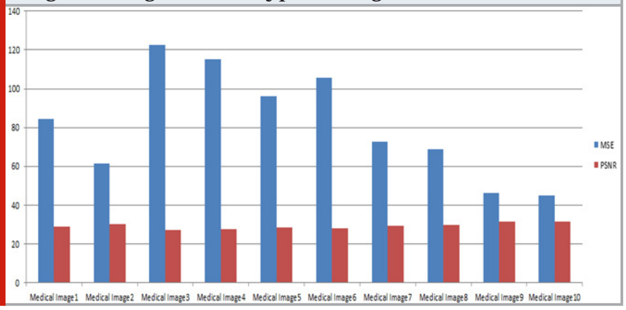


Table 6. MSE and PSNR analysis of proposed method

Medical Images	MSE	PSNR
Medical Image1	84.2939	28.8728
Medical Image2	61.3464	30.2529
Medical Image3	122.5335	27.2483
Medical Image4	115.1305	27.5189
Medical Image5	96.3051	28.2943
Medical Image6	105.6275	27.8930
Medical Image7	72.4975	29.5276
Medical Image8	68.5918	29.7681
Medical Image9	46.3214	31.4730
Medical Image10	44.8085	31.6172
Medical Image11	65.698	28.954
Medical Image12	89.283	32.589

Table 7. NPCR and UACI analysis of proposed method

Medical Images	NPCR (%)	UACI (%)
Medical Image1	100.0000	35.2105
Medical Image2	100.0000	34.5423
Medical Image3	100.0000	35.8772
Medical Image4	100.0000	34.3851
Medical Image5	100.0000	36.5464
Medical Image6	100.0000	35.8520
Medical Image7	100.0000	32.5425
Medical Image8	100.0000	33.0140
Medical Image9	100.0000	37.8668
Medical Image10	100.0000	36.3599
Medical Image11	100.0000	33.566
Medical Image12	100.0000	35.678

Figure 7: Graphical analysis of NPCR and UACI between original image and encrypted image

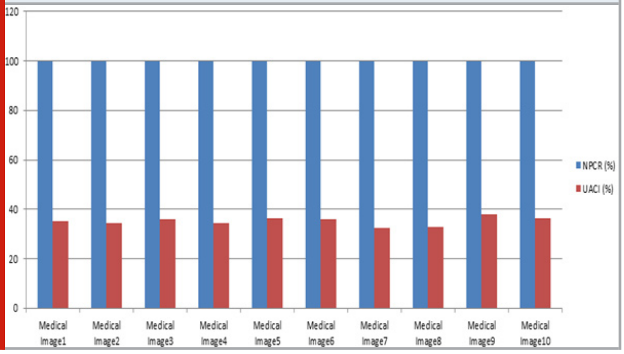


Figure 8: Graphical analysis of encryption time and encryption ratio between original image and encrypted image

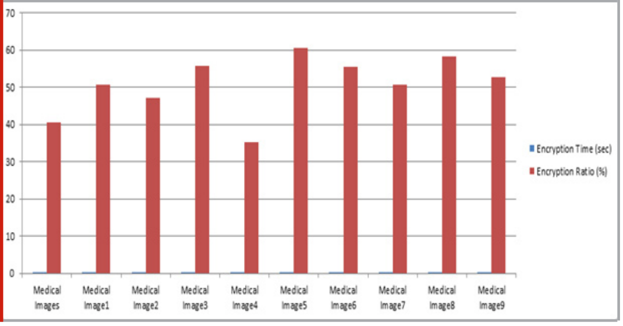


Table 8. Efficiency of proposed ROI encrypted system

Image Name	Encryption Time (sec)	Encryption Ratio (%)
Medical Images	0.2287	40.6250
Medical Image1	0.1310	50.7813
Medical Image2	0.1225	47.2656
Medical Image3	0.1098	55.8594
Medical Image4	0.1167	35.1563
Medical Image5	0.1126	60.5469
Medical Image6	0.1073	55.4688
Medical Image7	0.1083	50.7813
Medical Image8	0.1102	58.2031
Medical Image9	0.1112	52.7344
Medical Image10	0.2287	40.6250
Medical Image11	0.3357	55.8923
Medical Image12	0.3678	60.546

Table 9. SSIM analysis of proposed system

Image Name	SSIM	BER
Medical Images	0.5129	0.4081
Medical Image1	0.4193	0.5149
Medical Image2	0.4607	0.4773
Medical Image3	0.3577	0.5644
Medical Image4	0.5486	0.3568
Medical Image5	0.2919	0.6119
Medical Image6	0.3766	0.5621
Medical Image7	0.4121	0.5125
Medical Image8	0.3039	0.5917
Medical Image9	0.3914	0.5296
Medical Image10	0.5129	0.4081
Medical Image11	0.4779	0.5123
Medical Image12	0.3952	0.4954

Figure 9: Graphical analysis of SSIM and BER between original image and encrypted image

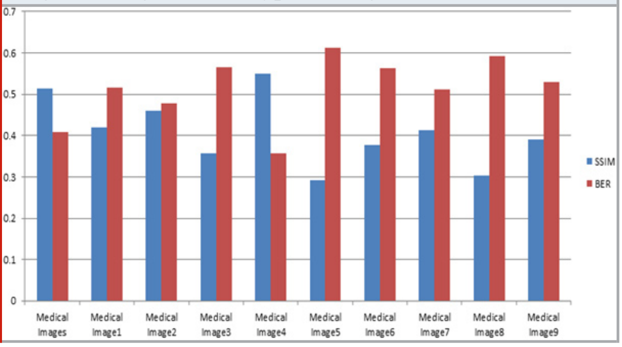


Table 10. Performance analysis for different basic intensity images

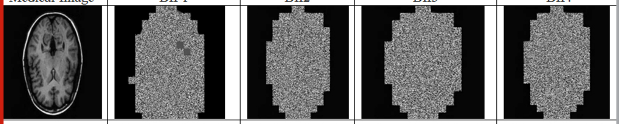
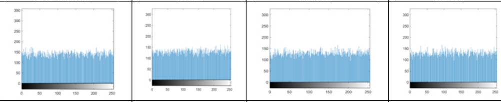
Medical Image	BII 1	BII2	BII3	BII4
				
Histogram Analysis				
Entropy	7.9940	7.9970	7.9960	7.9953
MSE	61.3464	82.3464	60.3464	71.3464
PSNR	30.2529	25.2529	34.2529	40.2529
NPCR	100.0000	100.0000	100.0000	100.0000
UACI	34.5423	33.5423	35.5423	32.5423
SSIM	0.4607	0.3607	0.5607	0.3707
BER	0.4773	0.3773	0.5773	0.4273

Table 11. Comparison of proposed method with existing methods

Image	Proposed method		Ref.[20]		Ref.[21]		Ref.[22]	
	Time (sec)	Entropy	Time (sec)	Entropy	Time (sec)	Entropy	Time (sec)	Entropy
Medical image 2	0.065	7.982	21.86	7.8	59.11	7.44	0.068	7.65

Comparative analysis: From the comparison table 9 we can conclude that speed of the proposed encryption method is very small compared to other existing algorithms and also entropy is more as compared to existing methods. For any selective image encryption method should have very less time and less complexity.

CONCLUSION

In this proposed method, an efficient selective medical image encryption has been proposed. This approach combines the concept of the Entropy calculation and ACM. To select the significant blocks of plain image threshold entropy has been employed. The proposed algorithm decreases the execution time of the encryption process. Blocking artifacts also reduced due to threshold of lower 4 bit planes. LSB embedding algorithm used to provide lossless encryption. The experimental results show that the proposed technique provides lower computation complexity, higher entropy and faster execution. In the future, FPGA implementation of proposed algorithm can be done for real time medical image transmission applications.

REFERENCES

Al-Sanjary, O.I., Ibrahim, O.A. and Sathasivem, K., 2020, June. A New Approach to Optimum Steganographic Algorithm for Secure Image. In 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS) (pp. 97-102). IEEE.

Ahmad, J. and Ahmed, F., 2010. Efficiency analysis and security evaluation of image encryption schemes. computing, 23, p.25.

Ayoup, A.M., Hussein, A.H. and Attia, M.A., 2016. Efficient selective image encryption. Multimedia tools and applications, 75(24), pp.17171-17186.

Bhatnagar, G. and Wu, Q.J., 2012. Selective image encryption based on pixels of interest and singular value decomposition. Digital signal processing, 22(4), pp.648-663.

Bremnavas, I., Poorna, B. and Kanagachidambaresan, G.R., 2011. Medical image security using LSB and Chaotic Logistic Map.

Cao, W., Zhou, Y., Chen, C.P. and Xia, L., 2017. Medical image encryption using edge maps. Signal Processing, 132, pp.96-109.

Kanso, A. and Ghebleh, M., 2015. An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation, 24(1-3), pp.98-116.

Khashan, O.A. and AlShaikh, M., 2020. Edge-based lightweight selective encryption scheme for digital medical images. Multimedia Tools and Applications, 79(35), pp.26369-26388.

Kulkarni, N.S., Raman, B. and Gupta, I., 2008. Selective Encryption of Multimedia Images.

Madhusudhan, K.N. and Sakthivel, P., 2020. A secure medical image transmission algorithm based on binary bits and Arnold map. JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING.

Mahmood, A.B. and Dony, R.D., 2011, December. Segmentation based encryption method for medical images. In 2011 International Conference for Internet Technology and Secured Transactions (pp. 596-601). IEEE.

Murali, P. and Sankaradass, V., 2018. An efficient ROI based copyright protection scheme for digital images with SVD and orthogonal polynomials transformation.

Optik, 170, pp.242-264.
Panduranga, H.T. and Naveenkumar, S.K., 2013. Selective image encryption for medical and satellite images. International Journal of Engineering and Technology (IJET), 5(1), pp.115-121.
Parameshachari, B.D., Panduranga, H.T. and Naveenkumar, S.K., 2017, October. Partial encryption of medical images by dual DNA addition using DNA encoding. In 2017 international conference on recent innovations in signal processing and embedded systems (RISE) (pp. 310-314). IEEE.
Parameshachari, B.D., Kiran, R.P., Rashmi, P., Supriya, M.C., Rajashekarappa and Panduranga, H.T., 2019, January. Controlled partial image encryption based on LSIC and chaotic map. In ICCSP (pp. 60-63).
Parameshachari, B.D., Panduranga, H.T. and liberata Ullo, S., 2020, September. Analysis and Computation of Encryption Technique to Enhance Security of Medical Images. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012028). IOP Publishing.
Rijmen, V. and Daemen, J., 2001. Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, pp.19-22.
Som, S. and Sen, S., 2013. A non-adaptive partial encryption of grayscale images based on chaos. Procedia Technology, 10, pp.663-671.
Taneja, N., Raman, B. and Gupta, I., 2011. Selective image encryption in fractional wavelet domain. AEU-International Journal of Electronics and Communications, 65(4), pp.338-344.
Wu, Y., Noonan, J.P. and Agaian, S., 2011. NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2), pp.31-38.
Xiang, T., Wong, K. W., & Liao, X. (2007). Selective image encryption using a spatiotemporal chaotic system. Chaos (Woodbury, N.Y.), 17(2), 023115.
Yousif, A.M. and Ali, M.M., 2013. A Selective image encryption based on chaos algorithm. journal of kerbala university, 11(1), pp.136-149.
Zhou, X., Gong, W., Fu, W. and Jin, L., 2016, June. An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS) (pp. 1-4). IEEE.