An Efficient Framework to Protect Medical Images

https://doi.org/10.3991/ijoe.v18i04.27841

Mamtha Mohan(✉), Suma K V, Deepika B Banagar
Ramaiah Institute of Technology, Bengaluru, India
mamtha.m@msrit.edu

Abstract—In this work, lossless compression is considered and an efficient Encryption–then-compression (ETC) scheme is proposed for medical images. A considerably good level of security is achieved by the proposed scheme where image encryption is operated in the prediction error domain. In addition, reasonably good compression of the encrypted medical images is achieved. Comparison is done between Gradient adjusted prediction (GAP) & Median Edge Detector (MED) techniques and GAP is found to perform better with respect to PSNR, bit rate and entropy. The average values of PSNR, bit rate and entropy in decibels for MED predictor are 10.8313, 3.7695 and 3.8624 respectively. Similarly, for GAP predictor, the average values of PSNR, bit rate and entropy in decibels are 11.9025, 4.0279 and 4.1286 respectively.

Keywords—bit rate, encryption, entropy, gradient adjusted prediction, median edge detector

1 Introduction

Medical images, physiological signals and other clinical data constitute a crucial constituent of a patient care system whether during screening, the diagnostic stage or the treatment phase. Saving of this data and transmission of the same from one place to another is imminent during patient care and monitoring. During this transmission, there is increased probability of remote access and in turn, leakage, loss and modification of data. Measures to protect the data when there is infringement accidentally or purposefully has to be taken. This ensures safe guarding of integrity as well as confidentiality of information. But, these steps become effective only when the intrusion is detected.

Some of the logic protection mechanisms include access control to information using user identification systems such as biometric screening, setting up firewalls both at entry and exit phases, usage of antivirus technologies and auditing, which helps to keep track of users. These systems are complementary and hence need to be used alongside one another. Compression and encryption system meets the requirements in many secure application scenarios. Encryption aims at confidentiality, authentication, integrity and non-repudiation. For medical images, maintaining confidentiality is very critical. Compression is also vital in telemedicine, whether it be for images or other signals, daily practice or for research and teaching. In teaching, compression will allow for the

easier creation of more complete banks of images and other reference information required for medical training, and transferred via a digital medium. In clinical practice, the exchange of images between medical teams occurs every day, in order to compare or examine certain results in detail, or to draw-up images for use as reference tools. In the field of research, the sharing of digital data will revolutionize certain practices, allowing, for example, the analysis of preliminary examination results from a distance, which may prevent unnecessary journeys. The primary focus of this work is on the practical design of a pair of image encryption and compression schemes, in such a way that compressing the encrypted images is almost equally efficient as compressing their original, unencrypted counterparts. Meanwhile, reasonable high level of security needs to be ensured. The Predicted Error Clustering and Random Permutation encryption methods are performed on medical images. Lossless compression of encrypted image is to be conducted and encryption is performed in the predicted error domain to provide high level of security to the medical images.

2 Literature survey

Li-bo Zhang et.al have employed the encryption and compressive sensing to compress and encrypt the plaintext, chaotic Chebyshev map is used to generate the e measurement matrix. Then the chaos-based permutation-diffusion cipher is used to quantize the measurements. Pixel swapping is done whose position is determined by a pseudorandom number.

Med Karim Abdmouleha et.al have developed a amalgamation of symmetric and asymmetric cryptosystem algorithms. DCT is used for compression and RSA for encryption The merits of the paper are minimisation of the meting out time through the encryption and decryption operation by encrypting merely the coefficients that hold the major information about the medical image.

Mbarek Marwan, et.al.mention that the primary focus is on outsourcing data and hand over IT computation to an outside party. The second distribute essential storage space scheme by means of the Internet to complete client's burden. The authors develop a structure to make safe the storage space of medical images above cloud computing. Multi-region segmentation in addition to watermarking method are employed to uphold together privacy and reliability. All along with solitude fortification in addition to validation uprightness inspection and safety process be determined on.

Xinsheng Li1 et.al suggest a original move towards that incorporate a quantum chaotic system, sparse Bayesian learning in addition to a 3D Arnold cat map, QSBLA, intended for joint image compression as well as encryption. The fresh method of the QSBLA is introducing SBL to compress images and by means of a 3D Arnold cat map towards permute bit-level dice. Good compression presentation is achieved and is capable of resisting several types of attacks.

Hasan H Khaleel et.al have focused on mechanism in addition to functioning of a image archiving and announcement system in a example request The major PACS machinery be communicated, HL7 as well as DICOM standards were introduced, and a prototype of WebXA application was proposed. To recover, stock up, plus put on show

angiography imagery on top of a web browser. Outcome that PACS have finished in the direction of the operational of the hospital in general with on top of the living up to hope live of distinctive clinician inside several unique mission. They have put into service a trial product purpose (WebXA) pro angiography put on show moreover switch over stuck between dissimilar environmental sites.

3 Methodology

In this work, simultaneous implementation of security as well as compression of encrypted data is carried out by the designed encryption algorithm. The input medical image is selected. The preprocessing is performed on the input image in order to convert it into grayscale image. Determining the predicted error image is done by using gradient adjusted prediction (GAP) or median edge detector (MED) predictors.

The mapping of predicted error is performed. Encryption is performed on the mapped image by using K-means clustering algorithm and random permutation. The secret keys are selected and shifted cyclically in order to perform the random permutation. The cyclic shifted clusters are assembled and encrypted image is obtained. Arithmetic coding is used to perform the compression on encrypted image. Obtained compression bit stream is used at destination to get decompressed image at receiver side. Reverse row wise cyclic shifts are performed alongwith reverse column wise cyclic shifts by employing permutation keys that are employed for encryption. The clustered prediction errors are assembled to get back the original image. For lossless compression of image encryption, the gradient adjusted prediction is an efficient prediction method.

3.1 Gradient adjusted prediction (GAP)

GAP being a nonlinear and flexible predictor, has the capability to modify itself so that the intensity gradient is adjusted to be near the predicted pixel. In this algorithm, the standard range is considered i.e. from -80 to 80.

Based on the horizontal and vertical influence on the pixel, the predicted value is calculated by using Equations (1) and (2) as shown for a template. The estimation of gradient of the intensity function at the current pixel [i, j] is done using Equation (3). An example to calculate the predicted value is shown in Figure 1.

		g	h
	C	b	i
D	A	**x**	

Fig. 1. Causal template

$$d_h = |a - d| + |b - c| + |b - i| \tag{1}$$

$$d_v = |a - c| + |b - g| + |i - h| \tag{2}$$

$$\bar{X} = \frac{a+b}{2} + \frac{i-c}{4} \tag{3}$$

$$\hat{X} = \begin{cases} a\,, if(d_v - d_h > 80) // \text{ sharp horizontal} \\ \frac{(\bar{x}+a)}{2}, (d_v - d_h > 32) // \text{ horizontal edge} \\ \text{b}, if(d_v - d_h < -80) // \text{sharp vertical edge} \\ \frac{(\bar{x}+a)}{2}, if(d_v - d_h < -32) \quad // \text{ vertical edge} \end{cases} \tag{4}$$

In the example shown in Figure 2, to find the predicted value of 100, d_v and d_h are calculated by considering the surrounding pixels.

(a) Sharp horizontal				(b) Horizontal				(c)Weak			
	40	30	15		40	55	50		55	60	60
45	20	20	25	45	50	65	54	60	100	50	45
102	105	**100**		102	105	**100**		50	55	**100**	
$d_v - d_h = 105 - 8 = 97 > 80$				$d_v - d_h = 69 - 29 = 40 > 32$				$d_v - d_h = 7 - 60 = 10 > 8$			
$\hat{X} = 105$				$\bar{X} = 86$				$\hat{X} = \frac{(3*39+55)}{4} = 43$			
$e = 100 - 105 = -5$				$\hat{X} = \frac{(86+105)}{2} = 96$							
				e = 100-96= +4							
				$\frac{(3*\bar{x}+b)}{4}, if(d_v - d_h < -8)$							
				//weak vertical edge							

Fig. 2. Example of GAP

The difference between d_v and d_h is calculated using Equation (4). In case (a), if the difference is greater than 80, it is considered as the sharp horizontal edge and the predicted value will be value of "a" itself. In case (b), if the difference is greater than 32, it is considered as horizontal edge. The predicted value of the pixel is calculated. In case (c), the difference is greater than 8, it is considered as weak horizontal edge. At last the predicted error is calculated by subtracting original value and predicted value of the pixel. Thus GAP algorithm is used to calculate the predicted error image i.e. the pixel value of the image is replaced by the predicted error values. This process of prediction is done before the encryption process because it removes spatial redundancy and helps in improving the compression ratio.

3.2 Median edge detector (MED)

It is a type of predictor where selection of sub predictors is done based on whether it is in the horizontal edge or smooth edge or vertical edge. MED predictor chooses the middle esteem between three conceivable outcomes, a, b and a+b-c.

As in Figure 3 the predicted value will be found based on the vertical, horizontal, and smooth edges. To find the predicted value of x, the adjacent pixels a, b and c is considered. In first case, if value of c is greater than the maximum of a and b, then minimum of a and b is chosen as the predicted value of the pixel x. In second case, if the value of c is less than the minimum of a and b, then maximum of a and b is considered as the pixel value prediction. If neither of the two cases are met, then pixel value

prediction is taken as a+b-c. An example for a subsection of an image is shown in Figure 4.

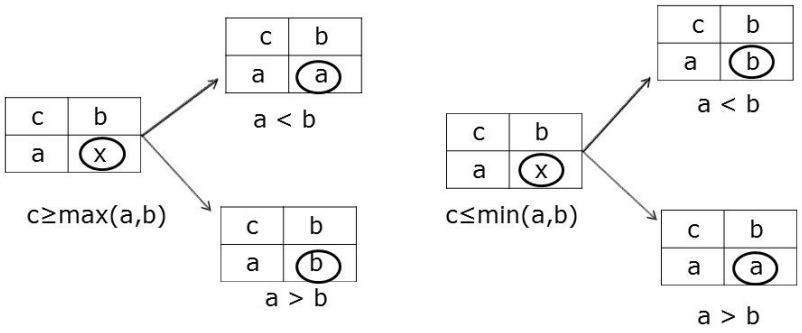

Fig. 3. Algorithm of MED

$$\hat{X} = \begin{cases} \min(a,b), if\ c \geq \max(a,b)) \\ \max(a,b), if\ c \leq \max(a,b)) \\ a + \mathrm{b} - \mathrm{c}, \quad \text{otherwise} \end{cases} \tag{5}$$

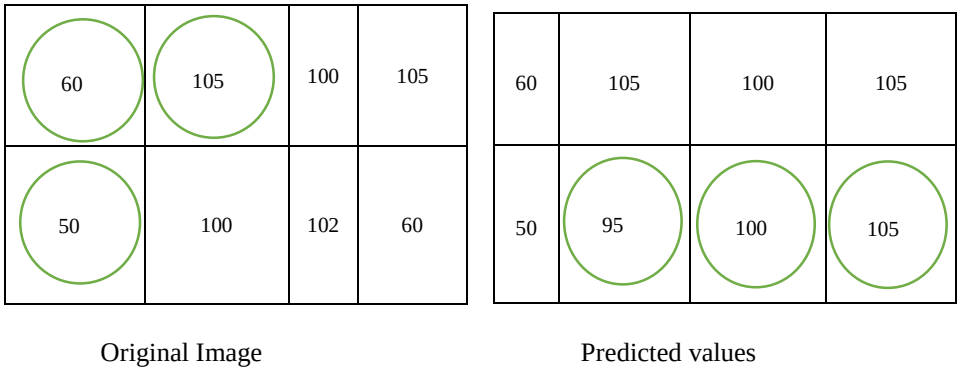

Fig. 4. Example of MED

The example in Figure 4 shows the working of the MED algorithm. Here, the predicted value of the pixel 100, 102, and 60 is to be calculated based on the neighboring pixels i.e. 50, 60, and in first case the value of c is neither greater than the maximum of a and b nor lesser than the minimum of a and b. Hence, third option is used i.e. a+b-c and the predicted value of 100 is 95. In the second case the predicted value of 102 is found by considering 100, 100, and 105 as the neighboring pixels. Here, the value of c is greater than the maximum value of a and b. As both a and bare same, the predicted value of 102 will be 100. In last case the predicted value of 60 is found. In this case the value of c is less than the minimum of a and b and also a is less than b and hence the predicted value is 105. At last the prediction error is calculated by subtracting the original pixel value of the image to predicted value. The pixel values are replaced by the predicted error value.

If the pixel value is negative, then more number of bits needed for pixel representation. In over to overcome this problem, mapping is to be performed on the pixels. The prediction can be mapped into the range [0, 255], for this consider that the predicted value is at the decoder side. The error should contain 256 distinct values. There are two ways of mapping, forward mapping and reverse mapping. The source image is scanned pixel by pixel in forward mapping and then they are copied to the appropriate position in the destination image. In reverse mapping, scan goes through the destination image pixel by pixel, and samples the correct pixel from the source image. The most important features of reverse mapping are that every pixel in the destination image gets set to something appropriate.

4 Results and discussion

There are many medical images like X-ray plane film (PF), Computed Tomography (CT) and Magnetic Resources Imaging (MRI). These images contain the information of the patient details. The CT scanned images contain information of the patients which helps in identifying the diseases. Nowadays, these digital images are being sent over the computer networks. As the computer networks are complex there is a chance of attack by attackers. The security is necessary to these images. These images contain the patient information and require more data storage. Compression is necessary to maximize the network utilization.

The Figure 5 shows the output of the work done on a medical image of size 1051×524 pixels. Here, the input medical image is selected as shown in Figure 5 (a). The preprocessed grayscale image is shown in Figure 5 (b). Before encrypting the image, predicted value of preprocessed image is found by using gradient adjusted prediction (GAP) predictor. The predicted error image is obtained by subtracting predicted pixel value from the original pixel value. Next the encrypted image is found by using k-means clustering and random permutation algorithms as shown in Figure 5 (d). The encryption is done at the source side. As only the encryption is performed at the source side, the utilization of resource will be less. The compression of the encrypted image is performed at the channel side in order to maximize the network utilization. The compressed bit stream is sent to the destination, where the original image is obtained by decompression and decryption, as shown in Figure 5 (f).

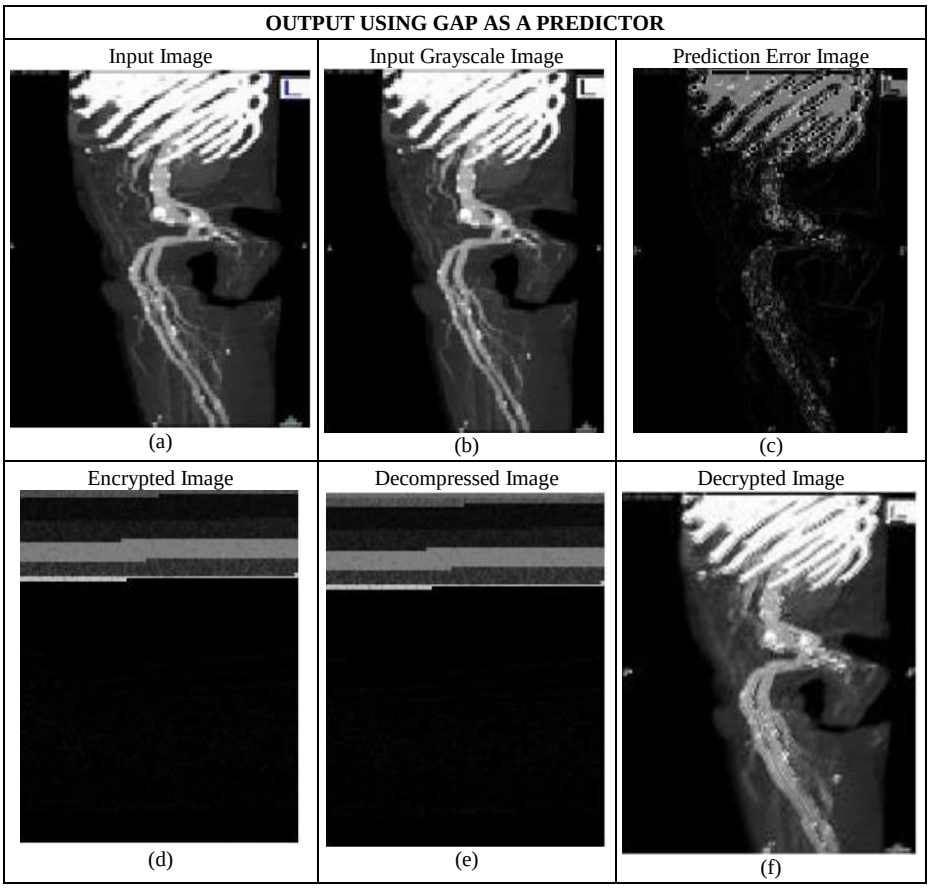

Fig. 5. Using GAP a) input image; (b) grayscale image; (c) predicted error image; (d) encrypted image; (e) decompressed image; (f) decrypted image

The Figure 6 shows the output of different stages of work done on a sample medical image of size 1051×524 pixels using MED predictor.

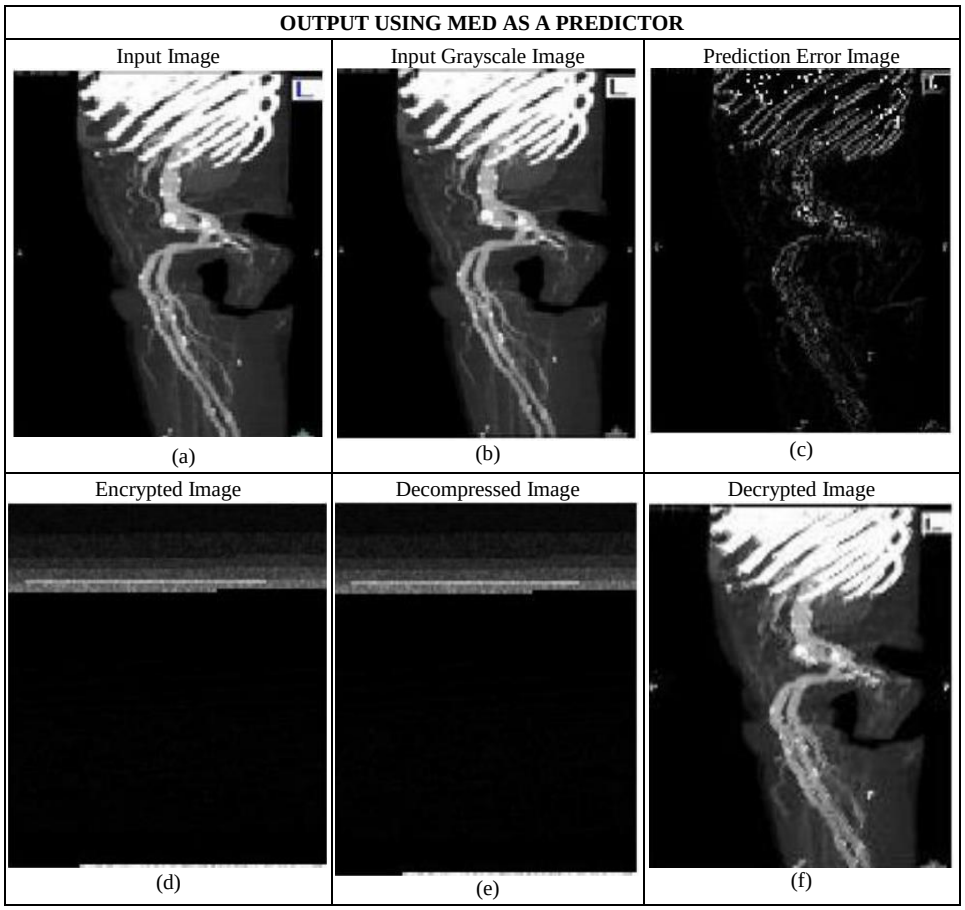

Fig. 6. Using MED a) input image; (b) grayscale image; (c) predicted error image; (d) encrypted image; (e) decompressed image; (f) decrypted image

Peak Signal to Noise Ratio (PSNR) is the performance measure of error matrix. The content of error added to the image is determined by the mean square error (MSE). MSE is computed from the value of PSNR in terms of decibels. It is the ratio of square of maximum size of image to the MSE.

Table 1 shows the values of PSNR of different CT images. As observed, the PSNR of images using GAP as a predictor is more than that of using MED as a predictor.It can be seen that the GAP gives better performance. Average PSNR obtained by using MED is 10.8313 while that using GAP is 11.9025. A graphical representation of PSNR for all the 30 images for the two methods is depicted in Figure 7.

Table 1. PSNR of images

Size in pixels	Number of images	MED as a Predictor (mean±SD in dB)	GAP as a Predictor (mean±SD in dB)
1051×524	5	8.5335±0.56	8.8543±0.601
768×276	5	12.2804±1.3	12.5219±2.1
768×552	5	10.9739±1.46	11.3406±2.03
512×512	5	5.3104±0.43	6.6219±0.38
750×1050	5	11.4362±2.1	11.6574±1.8
768×768	5	16.4537±1.96	20.4194±1.21

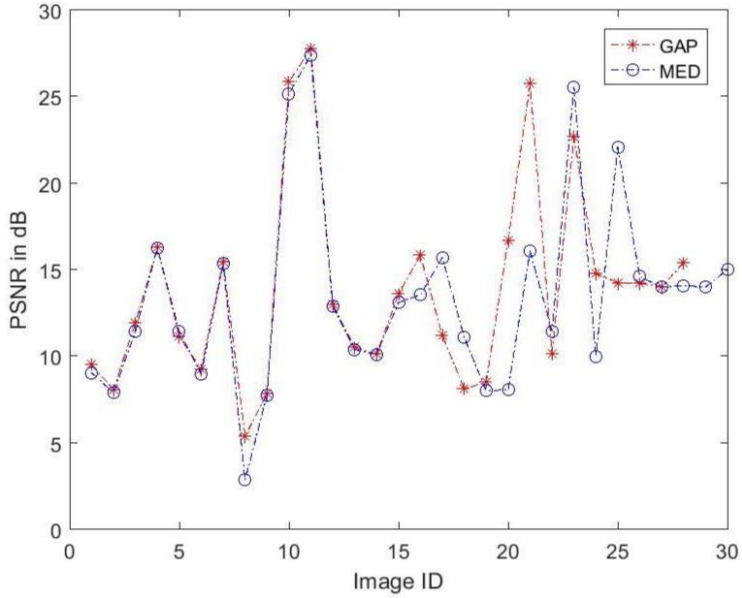

Fig. 7. Plot of PSNR vs. images

The performance of compression is measured by bit rate which is the ratio of size of original image to the size of compressed image.

Table 2 shows the bit rate of different CT images. As observed, bit rate for CT images using GAP as a predictor is more compared that of using MED as a predictor. The average bit rate computed for the images is 3.7695 when MED is employed, while it is 4.02795 when GAP is employed. Thus GAP predictor is found to give better performance than MED predictor.

Table 2. Bit rate of images

Size in pixels	Number of images	MED as a Predictor (mean±SD in dB)	GAP as a Predictor (mean±SD in dB)
1051×524	5	4.2709±0.45	4.5520±0.394
768×276	5	5.0579±0.332	5.3469±0.358
768×552	5	3.7930±0.27	3.9277±0.205
512×512	5	3.1392±0.21	3.4262±0.34
750×1050	5	3.7308±0.22	4.1160±0.287
768×768	5	2.6256±0.201	2.7989±0.235

Entropy is a performance measure that shows how effective the compression method is. The quantity of information in source is the source entropy. It is represented by bits per symbol (bps). Table 3 shows the entropy value of different CT images.

The average entropy value for the images is 3.8624 when MED is utilized as compared to 4.1286 when GAP predictor is utilized. It is observed that using GAP as a predictor the amount of information present is more compared to that of the MED as a predictor. It is observed that the GAP predictor gives better performance.

Table 3. Entropy of images

Size in pixels	Number of images	MED as a Predictor (mean±SD in dB)	GAP as a Predictor (mean±SD in dB)
1051×524	5	4.2700±0.14	4.5510±0.192
768×276	5	5.0570±0.207	5.3460±0.258
768×552	5	4.6978±0.33	4.8412±0.361
512×512	5	3.0790±0.42	3.4446±0.38
750×1050	5	3.7297±0.25	4.1150±0.392
768×768	5	2.3413±0.18	2.4740±0.21

From the discussion of results from Tables 1, 2 & 3, it can be seen that GAP gives better performance than MED. This is due to prediction technique employed by MED which selects between context of horizontal edges, vertical edges and smooth regions. However, GAP selects by employing simple estimation of vertical gradient, horizontal gradient and one threshold.

5 Conclusion and future work

The loss of information is not acceptable in medical field. The compression technique may lead to loss of information. Because of loss information there is a chance of failing to identify a life-threatening illness at the beginning stage. Efficient medical image encryption and compression is performed to secure medical images and to increase network utilization. Based on the performance metrics namely PSNR, Bit Rate and Entropy as listed in Tables 1, 2 & 3, it is shown that the performance of GAP is better than MED and hence is a suitable method for security of medical images.

The authors declare that they have no conflict of interest.

6 References

[1] Li-bo Zhang, Zhi-liang Zhu, Ben-qiang Yang, Wen-yuan Liu,2 Hong-feng Zhu, and Ming-yu Zou, "Medical Image Encryption and Compression Scheme Using Compressive Sensing and Pixel Swapping Based Permutation Approach" Hindawi Publishing Corporation Mathematical Problems in Engineering Vol. 2015. https://doi.org/10.1155/2015/940638

[2] Mbarek Marwan,, Ali Kartit, Hassan Ouahmane, "A Framework to Secure Medical Image Storage in Cloud Computing Environment", Journal of Electronic Commerce in Organizations,Vol. I6, Issue 1, 2018. https://doi.org/10.4018/JECO.2018010101

[3] Med Karim Abdmouleha, Ali Khalfallaha, Med Salim Bouhlela, "A Novel Selective Encryption Scheme for Medical Images Transmission based-on jpeg compression algorithm," Sciencedirect Procedia Computer Science, International Conference on Knowledge Based and Intelligent Information and Engineering system, pp 369-376, 2017. https://doi.org/10.1016/j.procs.2017.08.026

[4] Hasan H Khaleel, Rahmita OK Rahmat, Dimon M Zamrin, "Components and implementation of a picture archiving and communication system in a prototype application," Reports in medical imaging,

[5] Shadi M S Hilles, Mahmood Abdullah Salem, "Selective Image Encryption and Compression Technique: Review", Arrasikhun International Journal, Vol. 4, Issue 1, 2018.

[6] Xinsheng Li , Taiyong LiID, Jiang Wu , Zhilong Xie , Jiayi Shi,"Joint image compression and encryption based on sparse Bayesian learning and bit-level 3D Arnold cat maps", PLOS ONE, 2019.

[7] Deepika B Banagar, Mamtha Mohan," Positional Based Encryption and Compression on Images", International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE),Vol.4, Issue 5, 2017.

[8] Chinegeram, K., Kama, R., & Raghotham Reddy, G. (2020). Enhancement and Segmentation of Medical Images Using AGCWD and ORACM. International Journal of Online and Biomedical Engineering (iJOE), 16(13), pp. 45–57. https://doi.org/10.3991/ijoe.v16i13.18501

[9] Ch, G., & Habibulla, M. (2021). Lucas Algorithm for Medical Images Encryption and Transmission using Orthogonal Frequency Division Multiplexing for Medical Health Information Systems and its VLSI Realization. International Journal of Online and Biomedical Engineering (iJOE), 17(06), pp. 128–136. https://doi.org/10.3991/ijoe.v17i06.23107

[10] Samadi Ghoushchi, H., & Pourasad, Y. (2020). Clustering of Brain Tumors in Brain MRI Images based on Extraction of Textural and Statistical Features. International Journal of Online and Biomedical Engineering (iJOE), 16(12), pp. 116–132. https://doi.org/10.3991/ijoe.v16i12.16929

7 Authors

Mamtha Mohan is working as an Assistant Professor in the department of Electronics and Communication Engineering at Ramaiah Institute of Technology. She has completed her Ph. D in 2019 from Jain University. She is a IEEE member, Member of

ISTE and Member of IAENG. Her specialization subjects are Image processing, Optical communication networks, Computer Communication networks, Operating Systems and Data Structures.

Suma K V is working as an Associate Professor in the Department of Electronics and Communication Engineering at Ramaiah Institute of Technology, Bengaluru. She has completed her Ph. D in 2019 from Visvesvaraya Technological University. She is a senior member IEEE, Fellow of IETE, Member of IAENG AND Advisor, WIE, RITB. Her areas of interest are Biomedical Signal/Image processing, Embedded System Design and Artificial Intelligence.

Deepika Banagar is a post graduate student in the Department of Electronics and Communication Engineering at Ramaiah Institute of Technology, Bengaluru, for the specialization M Tech (Digital Electronic Circuits). She is keenly interested in research in the field of biomedical image protection.

Article submitted 2021-10-25. Resubmitted 2021-12-20. Final acceptance 2021-12-22. Final version published as submitted by the authors.