ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(16), DOI: 10.17485/ijst/2016/v9i16/92213, April 2016* ISSN (Online) : 0974-5645

A Comprehensive Compression and Encryption Scheme for Secured Medical Images Communication

G. Saravana Kumar[1*], V. Parthasarathy[2] ,E. Praveen Kumar[1], S. Thiyagarajan[1], S. Siva Saravana Babu[1] and S. Sudhakar[1]

[1]Department of ECE, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai 600062, Tamil Nadu, India; g.saravanakumar@velhightech.com, praveenkumare@velhightech.com,thiyagaraj@velhightech.com, sivasaravanababu@gmail.com, sudhakars106@gmail.com

[2]Department of CSE, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai 600062, Tamil Nadu, India; sarathy.vp@gmail.com

Abstract

Background/Objectives: Among a gamut of evolving domains in medicine exchange of medicinal data and images amid multiple entities constitutes a pivotal aspect for telemedicine. An effective bandwidth allocation and management scheme is essential to accomplish the telemedicine communication requirements. This necessitates the requisite to develop and implement a compression and encryption scheme for medical images. **Methods:** This paper recapitulates the diverse transformation techniques employed in compression and identifies the constraints associated with the techniques. This paper summarizes the comparison of encryption methods such as Rivest Cipher 4(RC4), Rivest Cipher 2(RC2) and Data Encryption Standard (DES) in terms of time consumed to complete encryption and decryption operations. **Findings:** This paper considers Peak Signal-to-Noise Ratio (PSNR) and Compression Ratio (CR) as performance measures and establishes the proposed algorithms's effectiveness over Set Partitioning Hierarchical Trees (SPIHT). **Application:** This algorithm can be utilized for medical image compression, transfer and archiving operations.

Keywords: Compression Ratio (CR), Data Encryption Standard (DES), Peak Signal-to-Noise Ratio (PSNR), Rivest Cipher 4(RC4), Rivest Cipher (RC2), Set Partitioning Hierarchical Trees (SPIHT)

1. Introduction

Developments in communication between computers influence the efficacy of diagnostic techniques and surgical measures. These communication modules can extend their link to far away distances[1]. One of the major challenges associated with computer security is administering fortification of medical image contents. This necessitates formulation of security mechanisms to extend concealed privacy, reliability and traceability[2]. To use the bandwidth effectively, image compression is used which reduces the size of an image during communication. Compared to JPEG standard, numbers of advantages are available in JPEG 2000. Also both lossy and lossless compressions are present in JPEG 2000. A higher quality final image and a higher compression ratio are offered in lossy compression environments of JPEG 2000 process. A rate distortion advantage is present in the JPEG 2000 image compression system over the original JPEG. To protect information confidentially, this paper uses Data encryption techniques and Digital Signature. The RC4 scheme had established an authenticity as general-purpose approach to public-key encryption. Electronic Patient Record (EPR) which consists of patient's data like name, Identification Number, ailment narrative, measures and doctor's data is preserved in medical image

* *Author for correspondence*

knowledge digest. The medical images are shared along with miniscule addend caption information and the caption files are subjected to corruption during multiple operations which leads to forfeiture of information during file format conversion. This phenomenon can be observed during Digital Imaging and Communication (DICOM) image conversion and the resultant multimedia file does not possess, caption information. For a better quality image Compression Ratio and PSNR ought to possess highest values[3]. Compression ratio is a measure to point out the effectiveness of the process in reducing the size of physical space used to store the data.

Different research fields highlight the amount of information incurred by the compression techniques and it leads to classification of compression techniques as lossy and lossless compression techniques The Discrete Cosine Transform based procedures reveals the supremacy over methods based on Wavelet Transforms. A sizeable amount of upright outcomes in storage of digital images can be accomplished by Set Partitioning In Hierarchical Trees (SPIHT), for JPEG 2000[4,5]. The Maxshift technique countenances the Region of Interest compression. In a method, engagement of low scaling standards by modifying the quantization step size of the coefficients at the encoder side produces a compression approach. These approaches are employed for Echo Cardio Graphic images encompassing macromedia flash formats, while Doppler images can be handled integer wavelet transform based techniques[6,7]. The effectiveness at the receiver can be ensured by maintaining a genuine and reliable bench mark image. The preferred sturdiness alongside genuine discrepancies are delivered by distributed source coding although distinguishing proscribed alterations is restrained. The decoder integrating expectation maximization algorithms can validate images which have experienced details, edges and affine warping modifications[8].

The Encryption and Decryption algorithm entails of twofold mechanisms: medical image clambering and medical image coded description. Medical image clambering is grounded on a muddled technique, while medical image coded description is completed by means of DES and 3DES. Image clambering is a significant portion of the procedure and is used to realize a higher range of misperception[9]. To scheme a capricious and protected application of the projected algorithm, a differential equation is constructed based on muddle map has been operated. To attain sophisticated values of Volatility and arbitrariness in the clamouring process, the factors of this differential equation have been selected with precise judging. The application of the process is malleable and individual component is unstable. A muddle map that delivers decent excellence in clambering results can be substituted with the projected muddle map and localization of a prime threshold is a wearisome process. A small threshold value will hold the noisy constants whereas a hefty threshold value leads to the loss of coefficients that transport image signal particulars[10]. The steps involved in denoising an image are presented in Figure 1.

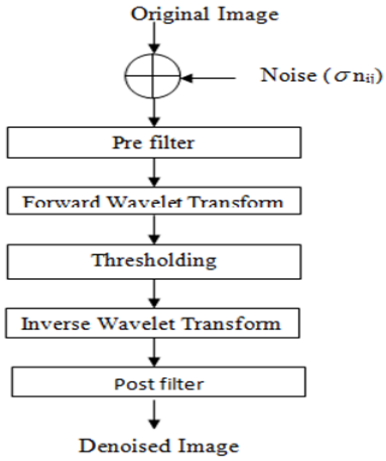

Figure 1. Steps for wavelet transform based image denoising.

In the 3DES algorithm, a medical image is administered by means of a muddled map to clamber the yield images and accomplish a sophisticated level of misperception, after which the DES algorithm is employed to perform encoding or decoding operations on the medical image. The amalgamation of muddle and block ciphers will provide supplementary safety and multifarious qualities paralleled to other algorithms and delivers more features[11].

2. Methodology

There are two phases in the procedure and specifically referred as initialization and Manoeuvre. In the primary stage of initialization, the complete gray level scale table, A is populous, by means of the key, B as a seed. As statistics is encoded the state table endures to be improved in a consistent outline. Pseudo code recapitulates the

initialization procedure. The output of the producer, entitled as a key stream, is acquired by merging one byte at a period with the plaintext stream by means of the bitwise XOR(exclusive OR) operation[12].

The footsteps for RC4 encoding procedure as follows,
Step 1: Foremost select the information to be encoded and key stream.
Step 2: Create a pair of similar characteristic element groups.
Step 3: One array is initiated whose range falls within gray levels.
Step 4: The additional group is filled with the nominated key.
Step 5: The primary group is subjected to sampling centred on the group's key.
Step 6: Apply sampling on the first group in the interior to cause the ultimate key.
Step 7: The ultimate key is subjected to Exclusive OR process with the information to be encoded to generate aspired output.

2.1 Slepian-Wolf Coding

Juxtaposing with an encoding mechanism it can be pointed that shouldering the information streaks leads to autonomy; the distinct encoding mechanisms can attain improved efficiency by manipulating the datum and the data streaks are possessing high degree of similarity. This perception is elucidated in the Slepian-Wolf theorem. The astounding consequence is that Slepian-Wolf scheme can in fact realize the same efficiency as the finest single encoding scheme that has all similar looking data streaks as inputs. The Slepian-Wolf scheme is depicted in Figure 2 has real-world significances for schemes where the similar information streaks are tangibly detached or where the scheme has imperfect computing capacity. It can be extended to sensor networks such as those for observing fluctuations in heat or beneath-the-earth rock movements where wireless masts, dispersed over around unspecific milieu, assemble information and communicate it to a principal locality[13]. Similar looking outputs are manufactured by two masts that are adjacent to each other which sagacious analogous standards. When the strength of power is restricted the system's presentation is upgraded by communicating at larger storage space requirements. The Slepian-Wolf theorem has real-world solicitation even when the coding scheme has null inhibition to the multiple similar looking data streams. The condensed intricacy for image and video signals for wireless telephones shall be accomplished by encoding the streams separately without reducing the compression rate.

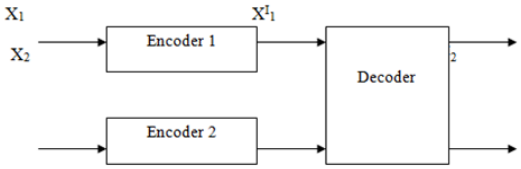

Figure 2. Selpian Wolf Coding block.

3. Results and Discussion

This section deliberates on the performance of encryption and compression algorithm with three different channel conditions for communication of medical images.

3.1 Threshold Selection

An image is habitually besmirched by artifacts throughout its acquirement or communication. The artefact removal procedure is to eliminate the artifacts while retentive and not misrepresenting the eminence of the administered image. The conventional method of image artefact removal is filtering. These approaches are mainly founded on segregation based on the detail and approximation coefficients of chosen transform, which have been exaggerated by non-multiplicative Gaussian signal encompassing all frequency components. Figure 4 shows the input medical image considered for transmission, Figure 5 shows the input image with noise and Figure 6 shows the results obtained by soft thresholding process with $\sigma = 0.\Theta$.

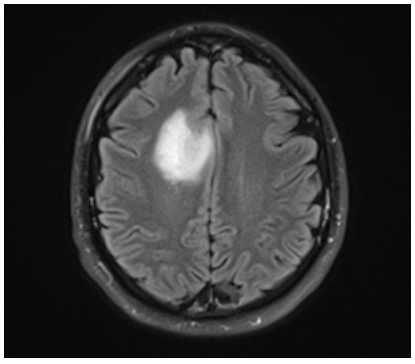

Figure 4. Input image.

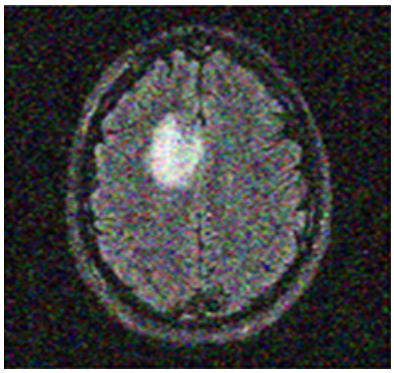

Figure 5. Noisy image.

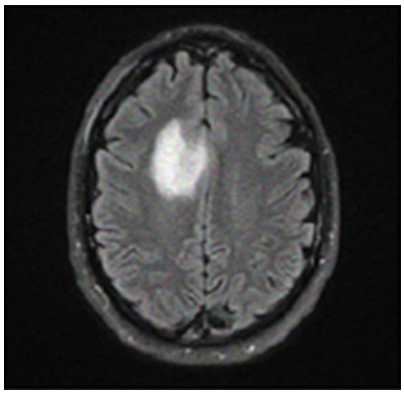

Figure 6. Soft thresholded image.

Figure 7 shows the input medical image considered for transmission, Figure 8 shows the input image with noise and Figure 9 shows the results obtained by hard thresholding process with$\sigma = 0.\Theta$.

Figure 8 shows the input medical image considered for transmission, Figure 9 shows the input image with noise and Figure 10 shows the results obtained by soft thresholding process with $\sigma = 0.\Theta$.

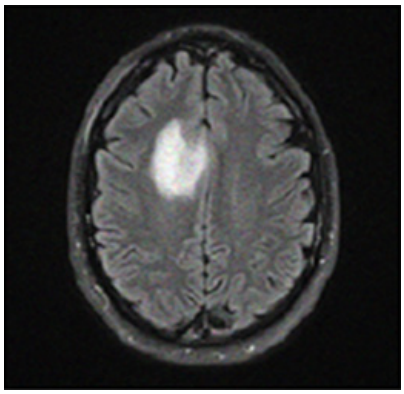

Figure 5. Input image.

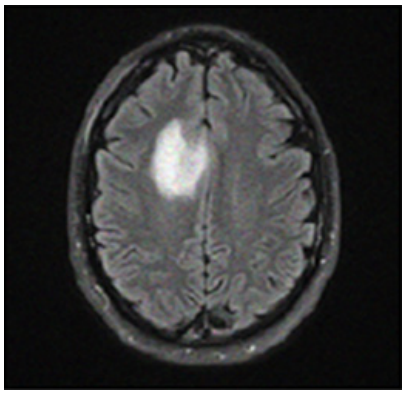

Figure 6. Noisy image.

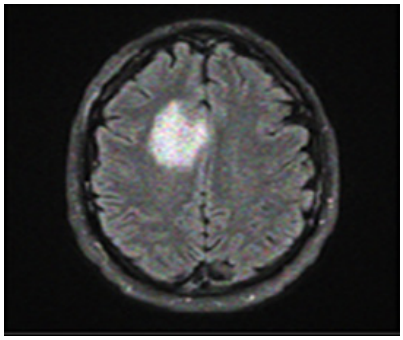

Figure 7. Hard thresholded image.

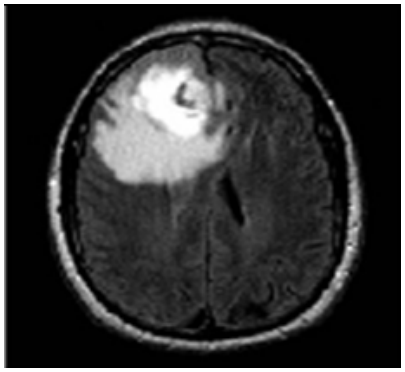

Figure 8. Input image.

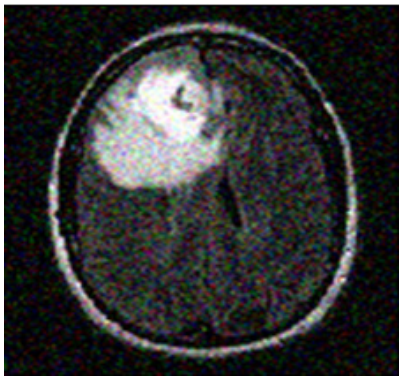

Figure 9. Noisy image.

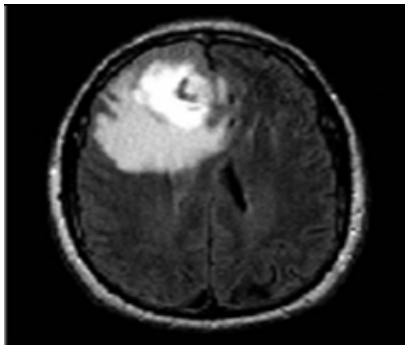

Figure 10. Soft thresholded image.image.

Figures 11, 12 and 13 shows the results obtained by soft thresholding process for glioma images with σ = 0. Θ.

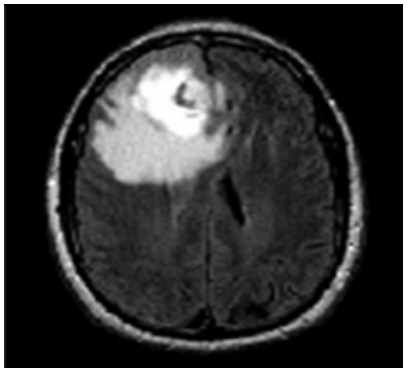

Figure 11. Input image.

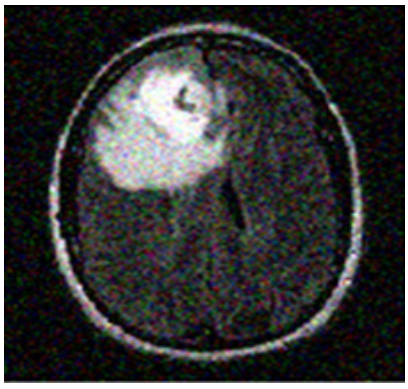

Figure 12. Noisy image.

The above experimental results reveal the pre-processing step for both medical and conventional images. This selection helps to analyse the various DWT Thresholding of De-nosing the Images with noise level σ = 0. Θ.

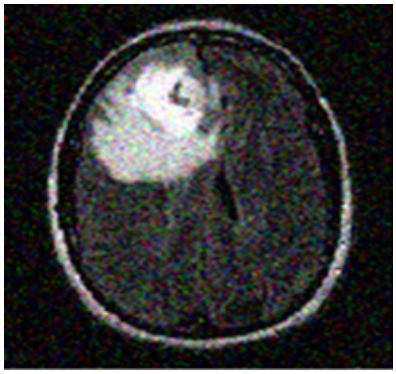

Figure 13. Hard thresholded image.

The investigations were piloted to observe and analyse the appropriateness of diverse wavelet sources and also the dissimilar approaches of onset or reduction. The result shows that the Soft thresholding gives the better result than the hard thresholding in term of SNR value and it exhibits quick processing time. It also shows that among all wavelet bases, the coiflet wavelet gives the better result for image de-noising because it has maximum SNR.

3.2 Encryption and Compression

The Encryption and Compression of Low sub band level is presented in the Figure 13 and Figure 14. One of the symmetric key algorithms is RC4 a stream cipher. As the data stream is subjected to XOR operation with the spawned key structure, this paper uses the similar process for both encoding and decoding. The plaintext used does not affect the key stream. It consumes a flexible dimension key spanning complete gray level scale to adjust another comprehensive state table. Pseudo-random bits are generated by the state table is and a virtual existing stream are generated which are subjected to exclusive OR operation with the text to be coded and producing the aspired cipher text.

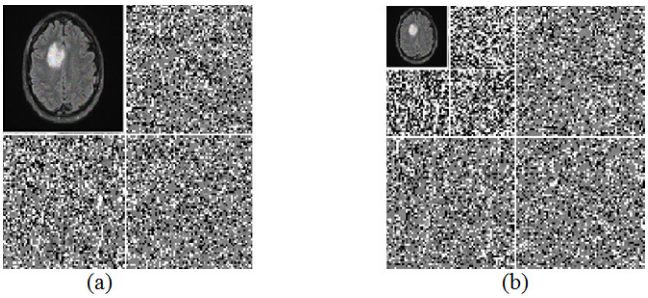

Figure 13. Low Resolution Sub band level of Encryption for Tumour Images (a) First Level of Decomposition (b) Second Level of Decomposition.

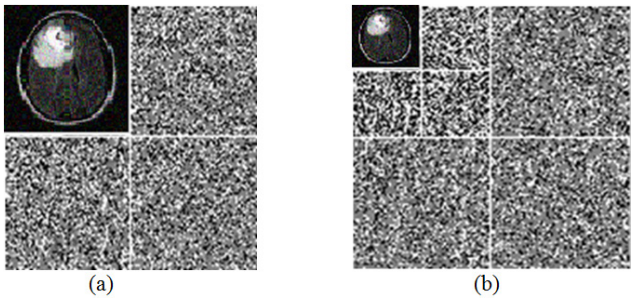

Figure 14. Low Resolution Sub band level of Encryption for Giloma Image (a) First Level of Decomposition (b) Second Level of Decomposition

The experimental result of Medical image Encryption using RC4 Algorithm and Compression is done by using Selpian- Wolf Coding Technique reveals that SWF is achieves the better result in terms of chosen performance metrics, when paralleled against SPHIT Algorithm. DWT is used to separate the various sub band level of original Input images. Using two level of sub band decomposition the output is better than the other level of decomposition method. When the sub band level proliferations occur, the output superiority of the image is reduced and the PSNR gets reduced.

The algorithm of RC4 can be fragmented into two junctures: initialization, and manoeuvre. In the primary stage the complete gray level scale, K is inhabited, by employing the, L as a seed. Upon the completion of state table, the values are scrupulously subjected to adjustments in a systematic arrangement as data is encoded. Table 1 shows the various comparison of encoding schemes. RC4 Algorithm is principally utilized for safeguarded communication as in the encoding of circulation to and from protected websites by means of the SSC Protocol.

Table 1. Performance of encryption algorithm

Medical Images	Algorithm	Encryption Time (Sec)	Decryption Time (Sec)
Tumor	RC4	2.8	1.7
	RC2	4.5	3.0
	DES	6.5	3.5
Glioma	RC4	2.3	1.3
	RC2	3.8	2.9
	DES	5.2	3.2

Table 1 indicated that the performance of Encryption Algorithm for medical image and conventional image. It may be observed from Table 1 that the Encoding and Decoding Time of RC4, RC2 and DES, RC4 gives the better Encoding and Decoding Speed compare to other two algorithms.

3.3 Decompression and Decryption

After encoding the image, the image can be transmitted from the sender to the receiver. The receiver decodes the encoded image for the decoding process selpian wolf coding is adopted. Through this technique the exact transmitted image is recovered back. This technique provides the efficient way for decoding method. Even though the compression ratio is better the image suffers from the loss of edge pixels hence we go for interpolation.

Figures 15 and 16 (a) show the process of encrypting the image gain the secrete key from the image pixels of the input image, hence they do not need any external key. From the Figures 15 and 16(b), it may be inferred that the De-compression of decrypted image can be retrieved by some amount of damaged pixel.

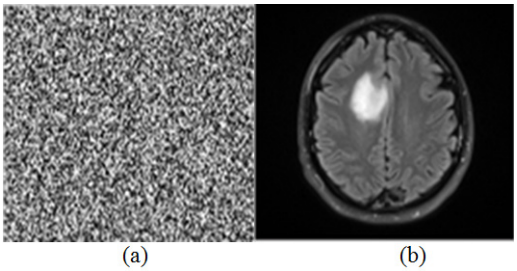

Figure 15. Decode tumour image **(a)** Decryption image **(b)** De-Compression image.

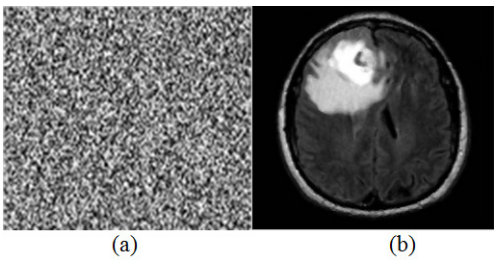

Figure 16. Decode Giloma image **(a)** Decryption image **(b)** De-Compression image.

Figure 17 and Figure 18 shows the result of interpolation process, where by the technique incorporate the edge pixels are using prior knowledge of neighbouring pixels.

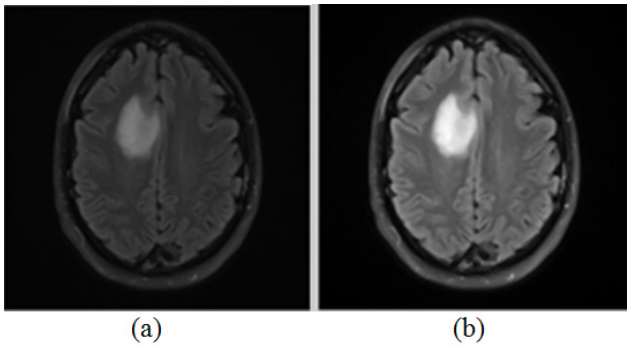

Figure 17. Interpolation process **(a)** First level interpolation **(b)** Second level of interpolation.

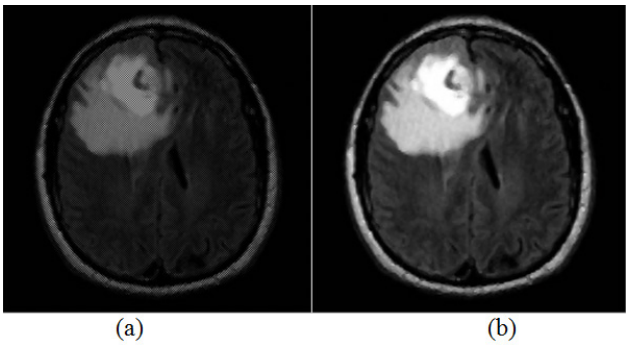

Figure 18. Interpolation process **(a)** First level interpolation **(b)** Second level of interpolation.

3.4 Recovered Image

Finally, the image is recovered by using the Decompression technique, the input image is in the dimension of 512X512. In the recovered image is abridged to the dimension of 256X256 for the transmission purpose and reduced storage capacity through this technique.

From the Figure 19 and Figure 20, it was inferred that the quality relationship between the two ends of the process is same but the size of the image is condensed. Table 2 shows the performance comparison of various compression algorithms.

Table 2. Performance of compression algorithm

Medical Images	Performance parameter	SPHIT	Proposed Method
Tumor	PSNR	31.32	38.66
	CR	3.789	4.564
	CORR	1.8522	1.0546
Glioma	PSNR	29.45	35.75
	CR	2.985	3.658
	CORR	1.9765	1.0413

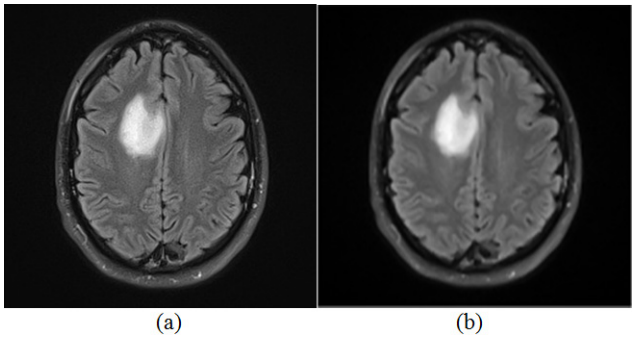

Figure 19. Recovered image for tumour **(a)** Input image **(b)** Output image.

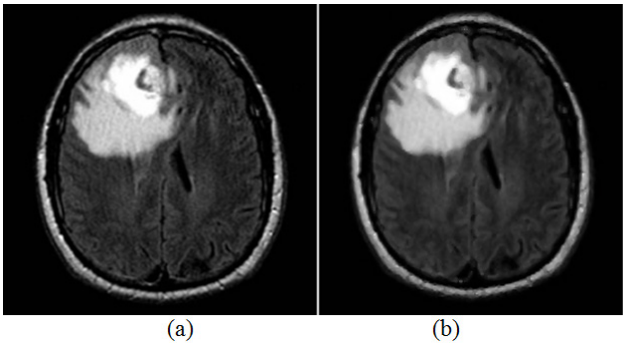

Figure 20. Recovered image for tumour **(a)** Input image **(b)** Output image.

4. Conclusion

Medical Images have prodigious reputation owing to the importance of patient data and medical management tenacity. The unsanctioned and illegitimate use of these images escalates the reputation of the safekeeping of system. This paper implements secured and effectual medical image encryption algorithm based on RC4 and utilize the medical image storage and transmission. This projected algorithm is appropriate and can be applied for conventional scenarios in order to retain the memory requirement requirements and memory sharing process for precarious and trustworthy medical images safe and dependable. To analyse numerous broadcast schemes for long range communication networks that permits the Medical image communiqué methods, subjugate a trifling bandwidth by a novel amalgamation method, and also deliver low-dormancy for methods whose efficiency is dependents on deferrals. This improvement in computation time is due to reduced input data size (or

image size) for encryption and decryption. The results show the AWGN channel produces a low BER when compared to that of the Rayleigh and Rician Channel. The achievement of PSNR is better when compared to the SPHIT. The proposed work shall be extended to compression of encrypted videos and various Medical Images.

5. References

1. Quantin C, Fassa M, Coatrieux G, Breton V, Boire J-Y. Giving patients secure "google-like" access to their medical record. ICMCC Event 2008; London: United Kingdom; Ios Press; 2008 Jun. p. 1–8.
2. Pan W, Coatrieux, NG, Cuppens-Boulahia F, Ch Roux C. Medical image integrity control combining digital signature and lossless watermarking. Data Privacy Management and Autonomous Spontaneous Security: 4th International Workshop, DPM 2009 and Second International Workshop, SETOP 2009; 2009. p. 153–62.
3. Grgic S, Grgic M, Zovko-Cihlar B. Performance analysis of image compression using wavelets. IEEE Transactions on Industrial Electronics. 2001: 682–95.
4. Said A, Pearlman WA. A new fast and efficient image codec based on set partitioning in hierarchical trees. IEEE Transactions on Circuits & Systems for Video Technology. 1996 Jun; 6:243–50.
5. Tahoces PG, Varela JR, Lado MJ, Souto M. Image compression: Maxshift ROI encoding options in JPEG2000. Computer Vision and Image Understanding. 2008 Feb; 109(2):139–45.
6. Hang X, Greenberg NL, Thomas JD. Compression of pre-scan-converted echocardiographic video using wavelet packet and integer wavelet transforms. Image and Vision Computing. 2006 Sep; 24(9):915–25.
7. Somasundaram K, Palaniappan N. Adaptive low bit rate facial feature enhanced residual image coding method using SPIHT for compressing personal ID images, AEU - International Journal of Electronics and Communications. 2011 Jun; 65(6):589–94.
8. Lin Y-C, Varodayan D. Image authentication using distributed source coding. IEEE Transactions on Image Processing. 2012 Jan; 21(1):273–83.
9. Johnson M, Ishwar P, Prabhakaran VM, Schonberg D, Ramchandran K. On compressing encrypted data. IEEE Transactions on Signal Processing. 2004 Oct; 52(10):2992–3006.
10. Mohideen SK, Perumal A, Sathik, SM. Image de-noising using discrete wavelet transforms. International Journal of Computer Science and Network Security. 2008 Jan; 8(1):213–16.
11. Caglar M. Long-range dependent workload model for packet data traffic. Mathematics of Operations Research. 2004; 29:92–105.
12. Mantin I, Shamir A. A practical attack on broadcast RC4. Proceedings of Fast Software Encryption; 2001. p. 152–64.
13. Chong C-Y, Kumar SP. Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE. 2003 Aug; 91(8):1247–56.