







## Secured Compression for 2D Medical Images Through the Manifold and Fuzzy Trapezoidal Correlation Function

Parvathaneni Naga SRINIVASU<sup>1,\*</sup> , Norita Md NORWAWI<sup>2</sup> , Shanmuk Srinivas AMIRIPALLI<sup>1</sup> ,  
P. DEEPALAKSHMI<sup>3</sup> 

<sup>1</sup>Department of Computer Science and Engineering, GITAM Institute of Technology, GITAM Deemed to be University, Rushikonda, Visakhapatnam 530045, India

<sup>2</sup>Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, Malaysia

<sup>3</sup>Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Tamil Nadu, India

### Highlights

- The primary emphasis of this paper is on secure compression of the data.
- The quality of the medical images on restoration post-compression.
- The space consumption of the compressed images and the entropy measure of the encrypted images.
- The assessment of the correlation of pixel post secured compression of the image.

### Article Info

Received: 25 Feb 2021  
Accepted: 01 Dec 2021

### Keywords

Lossless compression  
Image encryption  
Image decryption  
Fuzzy trapezoidal  
Correlation function

### Abstract

In biomedical imaging, the imaging of secured storage and maintaining medical images like MRI, CT, and ultrasound scans are challenging with ever-growing tremendous image data. This article has proposed a systematic approach for secured compression of the image data that would compress the image data at multiple levels at each instance that would substitute with a smaller size data block through dictionary mechanism. The resultant image is encrypted through a 256-bit symmetric key dynamically generated through the hashing-based technique for multiple rounds. In each round, a 16-bit key sequence obtained from the hashing-based technique is an integral part of the 256-bit key used in the encryption process, and the same key sequence is being used in the decryption phase. Finally, the resultant image is stored for future reference for further medical examinations. In reconstructing the original image, the same approach is performed in reverse order to get back the original image without any significant impact on the image standard through the Fuzzy Trapezoidal correlation method. The proposed mechanism is being practically implemented over the medical images, and the outcome seems to be very pleasing compared to the counterparts. It is observed on implementation. The medical images are compressed to 58% of their original size without significant impact on the quality of the image that is being reconstructed. The approximated entropy in the majority of the cases is less than zero has proven the proposed mechanism is robust for secured compression of the medical images for secured storage.

## 1. INTRODUCTION

Over the years, medical imaging has become pivotal in the procedure of ailment diagnosis and treatment. The images acquired during the diagnosis process would be stored for further investigations, and all such images need significant storage space. Resultantly they require more effort for maintenance and retrieval of such images. Moreover, the medical image is compassionate, and they are to be preserved securely from unauthorized people. One of the best practices for securing the image is encrypting it through a cryptographic mechanism, as V. Pavithra and C. Jeyamala [1] in their article on a survey of medical image encryption.

Medical image compression must be performed with extreme care as the data is crucial in the analysis. Numerous approaches are categorized as lossy and lossless mechanisms for compressing the digital image efficiently. From a practical point of view, the lossy compression mechanism would attain a high compression ratio level. When dealing with medical-related images, it is advisable to work with lossless compression techniques as the lossy mechanism might lead to data loss during image compression. Restoring the image at the same level of entropy would be a challenging task.

Lossy compression techniques are most common in image compression. There are approaches like the Joint Photographic Experts Group (JPEG). Still, the medical images cannot be compressed through lossy approaches as every minute object is crucial in the image analysis. Zuo et al. [2], in the article on improvised method for medical image compression, has normalized the region of interest from the image through an active contour approach followed by blurring the rest of the image to reduce the high intensities in the image and JPEG-LS has been implemented for compressing the non-region of interest. Thus the approach needs a significant computational effort for extracting the region of interest, and the quality of the medical image is vital in this process. Hence, the image is pre-processed to enhance the contrast and edge-related information of the image for ease of extraction of the region of interest.

Burrows-Wheeler transforms (BWT) based lossless image compression approach is being stated by Chamberlin and Balasubramanian [3] in their paper, that performs the image based on the permutations and rearrangement of the bits through Move-To-Front (MTF) transformation followed by run-length encoding and Variable-length encoding mechanisms through Huffman and Shannon based approaches. The entropy coders entirely decide the quality of the segmentation and robust spatial predictors reused as part of the compression. The MTF is crucial in an optimal level of image reduction that would need more computational efforts, and it is an almost lossless compression approach.

Discrete Cosine Transform (DCT) as stated by Messaoudi et al. [4]; Brahimi et al. [5] and Discrete Wavelet Transform (DWT) as asserted by Boucetta and Melkemi [6]; Parkale, Nalbalwar [7] The two predominantly used approaches for the lossless compression of the image are used to divide the image into multiple sub-regions. The process of image quantization is being performed to convert the image into the frequency domain. DWT uses the Lagrange interpolation approach to predict local features, and image compression occurs in the frequency domain. In converting the image, it is susceptible to noise, and the image is being smoothed, which would be challenging for segmentation of such an image. Moreover, it needs more computational time resulting in considerable computational efforts.

Lempel-Ziv-Welch approach, as mentioned by Sangeetha et al. [8]; Wang et al. [9], image compression is the most widely used compression mechanism that is practically simple to implement, that used the dictionary-based approach for the compression that makes it more suitable for text-based data compression rather than any other file type images that make the algorithm to be considered complex to implement and the memory that is needed to store the is exceptionally high. The entire string table must be searched for every pixel for a suitable match that needs more computational struggle and latency. There are many other techniques like the Fractal encoding technique stated by Joshi et al. [10] that is used in the compression of the digital image through fractal encoding the similar objects that are occurred repeatedly as the part of the image data that can be used in compressing the CT and MR images work on the principle of quad-tree based segmentation technique that needs extended computational time. Even in the later phase, the image is divided into the non-overlapping regions based on approximated threshold values.

Greyscale images are being compressed through the arithmetic coding approach, as Masmoudi et al. [11]; Lin et al. [12] work on the block's principle by block top-down approach that performs from left to right. Moreover, the probability distribution function for each block has been assessed concerning the neighboring pixel correlation. The results seem to be better with reasonable computational effort, but it suffers from a poor compression ratio. The resultant image needs not to be identical to the original image in the proposed approach because it is being compressed for storage purposes. The image needs to be decompressed for performing any investigative analysis of the image.

Medical image data is susceptible, and it is advisable to store them in an encrypted format. There are many image encryption techniques available for real-time utilization. They are categorized into symmetric (Single key), including Data Encryption Standard(DES), as Gong-bin et al.[13], Triple-DES, as mentioned by Mohammad et al.[14], Advanced Encryption Standard (AES) as stated by Shakir [15], and asymmetric approaches(Public key) that includes Rivest Shamir Adleman(RSA) based image encryption as discussed by Zhao et al. [16]; Alsaffar et al., [17] and Digital Signature Algorithm(DSA) as mention by Xiao Chen and Chun-Jie Hu[18], where the latter category of the image enhancement need two keys that are being generated through the key generator or any other alternative mechanism. There is a significant demand for the secured compression algorithm for exchanging the data over the sensor network with latest networking gateways Dener [19]. There are various security solutions like TinySec, SPINS, MiniSEC, LSec that are associated with the secure data exchanges over the wireless sensor network Dener [20].

An image can be encrypted through many other predominantly used conventional approaches without using the key that performs the pixel or the block scrambling and through substitution mechanism as mention in the survey paper by Mohammad et al. [14]; Patigar et al. [21] in substitution-diffusion based image cipher. Most of the approaches used the chaotic map-based image encryption mechanism, as Srinivasu and Rao [22]; Pan et al. [23] and Akkasaligar, Biradar [24] in their articles. In the majority of the approaches, the image is being scrambled through probabilistic methods, and then the resultant image is being encrypted through some key that is similar to the hybrid encryption algorithms as Nematzadeh et al. [25]; Viswanath, Krishna, [26]; Dener and Bostancıoğlu [27] in the article medical image encryption through a hybrid model, so that the resultant encrypted image would be considered strong decrypted by the intruders. Numerous mechanisms are being used to encrypt the image to maintain confidentiality, but the approaches mentioned above are the most predominantly used mechanism for image encryption. The Table 1 presents the various existing compression models.

**Table 1.** Resents various existing image compression techniques

| Approach  | Type of Compression | Description  | Applicability  | Limitations  |
|-----------|---------------------|--|--|--|
| JPEG      | Lossy               | The widely used technology in the current day digital cameras and the standard used on the internet to exchange image data.  | They are used in digital cameras and various other image rendering equipment.    | JPEG is a lossy compression technique that might miss out on some crucial information in the image. Moreover, it supports only an 8-bit format that might not be sufficient to display high-definition images. |
| JPEG 2000 | Lossy/<br>Lossless  | The enhanced version of JPEG technology enables better compression and lossless image compression, primarily used in High Definition imaging technology. JPEG 2000 relay on the discrete wavelet transforms. | They are used in multimedia devices and widely used internet distributed images. | JPEG2000 is comparatively slower and complicated to implement. The technology is less content-adaptive. Resultantly the applicability in medical technology is sparse.   |
| PNG       | Lossless            | PNG technology is the improvised version of GIF format that supports a wide magnitude range.   | They are used for images on web pages and icons.                                 | It does not support the widely used color formats like RGB and does not allow store metadata about the image   |

|       |          |  |   |   |
|-------|----------|--|---|---|
|       |          |  |   | used at the time of processing.   |
| DICOM | Lossless | DICOM is a widely used technology for the compression of medical images, commonly used in the storage and communication of medical images. | They are used in storing medical images.        | The compression process involves too many fields to be entered, and inappropriate filling of those values may lead to a misleading outcome.                               |
| BMP   | Lossless | BMP is the compression standard put forward by Microsoft and widely used technology in the windows platform.                               | BMP technology is used in the windows platform. | The outcome of the compression still leads to a larger file size despite compression.   |
| TIFF  | Lossless | TIFF is the technology used by the scanners and fax machines for compressing the acquired documents.                                       | TIFF technology is used in scanner devices.     | TIFF technology consumes more disk space than the other models. Moreover, many replication files are created in the process that makes it complicated to handle the data. |

## 2. INTENT OF THE ARTICLE

Medical images do have sensitive data that has to be maintained confidential from the outside world. The images are needed to be stored for future examinations and investigations of the cases. Through this article, the authors focus on addressing the challenge of the occupancy of the storage space and the confidentiality of the image. The proposed approach is novel in address the challenges mentioned above for the medical images. The proposed algorithm would compress the image to almost half of its size. That resultant image upon compression would be chaotic that nearly seems to be like a cipher image. Then the resulting image is encrypted through reversible binary operations through an identical key for multiple rounds. As the proposed mechanism involves various algorithms to be executed simultaneously, the algorithm is designed to be computationally efficient and consume minimal computing-intensive efforts. Moreover, the proposed algorithm would significantly reduce the image's size and result in efficient storage space management and a distinguished level of information confidentiality.

## 3. SECURED COMPRESSION OF MEDICAL IMAGE

The medical images are initially compressed, and then the compressed image data is encrypted through cryptographic techniques for multiple rounds. Then the resultant image is being stored securely in the storage device for future reference. In the initial phase, the image is compressed through substitution by replacing, and then the resultant image is further encrypted through the key for multiple rounds.

### 3.1. Image Compression

In image compression, the original image is compressed through the process of substitutional downsizing, as experimented by Rehman et al. [28], the data used in representing the image. In the process of image compression, as the medical data is described in a greyscale image, the pixel intensities for the greyscale image lie in a range of 0 (representing the full dark black color) and 255 (that means the full bright pixels that denote complete white). Moreover, 8-bits are needed to represent the image pixel, and the proposed approach focuses on downsizing the pixels through replacement of more extensive size pixel data with a smaller size data, i.e., 8-bit size data to 6-bit size data and 6-bit size data to smaller size data over iterations

and probabilistic mechanisms. The image compression model of the proposed model is being presented in Figure 1.

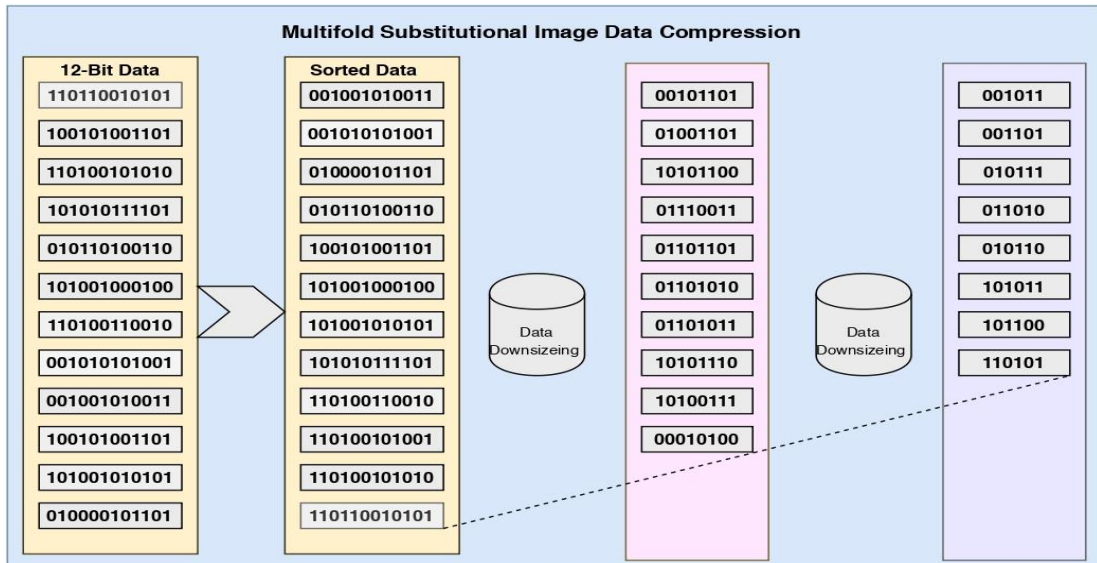


Figure 1. Sample image representing the data compression through substitution

### 3.2. Image Decompression

Image decompression is vital in attaining a high-quality image as image decompression is performed through a probabilistic approach while replacing the image's pixels. In the decompression process, once the pixel is mapped from 6-bit to 8-bit, the number of 8-bit data samples arises compared to 6-bit data samples. For the replacement with the larger size data elements moving towards the decompression, the probability of appropriate 8-bit data is assessed among the correlated data. The higher likelihood sample is suitable for replacing the existing pixel data based on the assessed probability. The same process is continued to replace the data from 8-bit to 12-bit using the probabilistic measure. Finally, the actual pixel values are placed in the appropriate positions through the indexing approach. The image is restored to its original state without significantly losing its quality through fuzzy Trapezoidal Correlation Function through Brier Score. The image decompression model of the proposed approach is being presented in Figure 2.

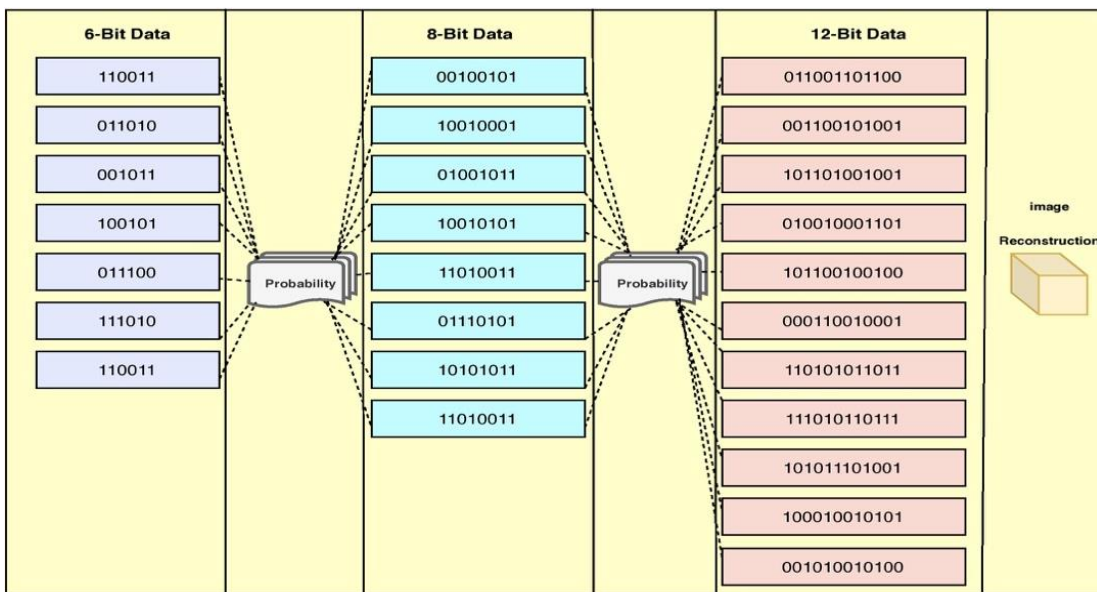


Figure 2. The image representing the data decompression through the probabilistic mechanism

### 3.3. Image Encryption

The image data compressed earlier is encrypted through a symmetric key generated from a hash key generator implemented by Gopalakrishnan & Srinivasan [29], size 256-bit long for multiple rounds. Then the resultant image is being stored. The image pixels are modified at the compression phase due to a higher compression level through substitution of smaller size code that would result in the pixel's modified intensity level that seems like an encrypted image using a substitution cipher. Then the resultant compressed image is encrypted over multiple rounds. In the encryption phase, the image is encrypted by performing logical XOR as implemented by Singh et al. [30]; Belazi et al. [31] with the same key for multiple rounds, as shown in Figure 2. In every consecutive round, the binary string is reversed, and then the XOR operation is performed on the resultant string that is fed as input for the next successive round. The 256-bit key is further sub-divided in a 16-bit size sequence, and each 16-bit key sequence is used in each round of encryption for 16 rounds, as shown in Figure 3.

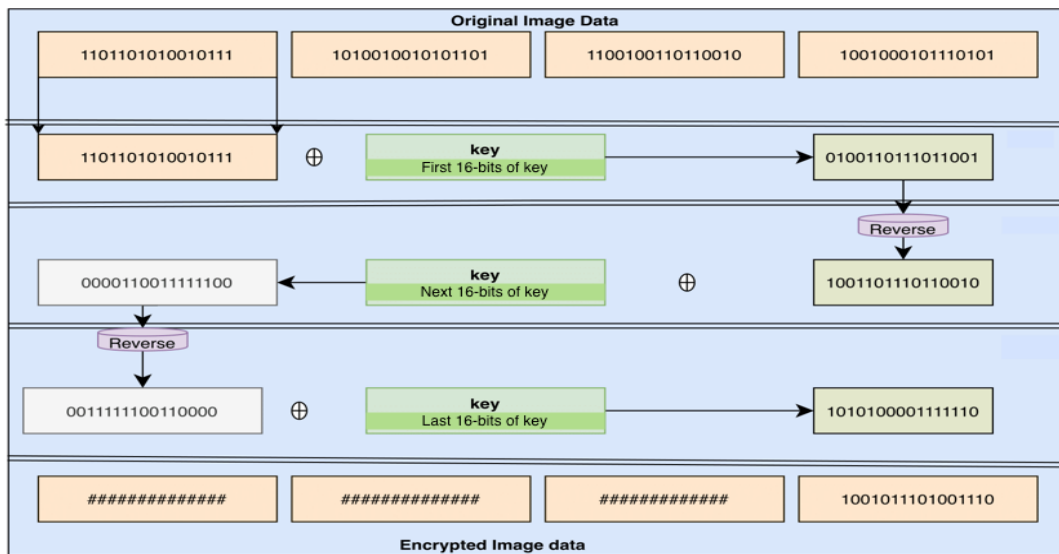


Figure 3. Image Encryption through symmetric key

Finally, the encrypted image is saved in the storage device for future reference. On the practical implementation, the image seems reasonable, with good resistance against the differential attacks on the data. The performance is that the proposed approach is assessed through entropy analysis presented in the paper results section.

### 3.4. Image Decryption and Decompression

The image is initially decrypted with the same key that was used at the encryption stage. The same XOR operation is performed for multiple rounds entirely reverse to the process performed at the encryption stage. The obtained resultant string is reversed in each consecutive round, and upon completion of the final round, the resultant decrypted image is fed as input for the decompression phase. The resulting image data is decompressed through the reverse-sequence of operations performed as part of the image compression. Upon completion of the process, the final original image is identical to the original image. As the proposed approach is lossless, the image quality is retained upon decompressing the data.

### 3.5. Working Procedure of the Proposed Approach

In the entire process of secured compression of the medical images, many intermediate tasks are performed. Initially, the acquired image is compressed to reduce the size, resultantly the image is de-Figured, and further, the image is encrypted by repeated XOR operations for multiple rounds. The entire process is as stated below

### Compression and Encryption

- Original medical image is acquired from the dataset for processing.
- The entire image is organized in a 1-D string of pixel intensities.
- All the pixels are re-arranged in descending order of their occurrence.
- The pixel intensities are represented in binary values, and they are downsized from 12-bit to 8-Bit and further from 8-bits to 6-bits through the dictionary approach.
- The resultant compressed image is then fed as an input for the encryption algorithm.
- All the pixel intensities are arranged as a stream of data (Like continuous, binary data)
- The 256-bit key that is generated by the key generator would be used for performing the XOR operation.
- The first 16-bits of the 256-bit key were used for round one, and the next consecutive 16-bit was used for the next round. Likewise, it is practiced for all 16 rounds.
- The string is resultant reversed, and again XOR operation is performed on the resulting string. This is repeated twice finally before we get the secured encrypted image for storing.

### De-Compression and Decryption

- The stored image that underwent secured compression is considered for reconstructing the original image.
- The XOR operation is performed on the acquired string through the 16-bit key used in the encryption process.
- The resultant string is reversed, an XOR operation is performed twice by reversing each operation's string.
- Now the resultant string is divided into blocks of 6-bit each.
- Using the probabilistic measures, the 6-bit data block is replaced with an 8-bit data block, and in turn, an 8-bit data block is replaced with the 12-bit block using the probabilistic mechanism.
- All the pixels are re-arranged through the dictionary approach, and all the pixels are placed in an appropriate position.

### 3.6. Technical Tradeoffs

The proposed approach involves two algorithms to be executed simultaneously for performing the secured compression of the image. The image is compressed through substitution from multiple rounds, from 12-bit of block size to 8-bit and further from 8-bit to 6-bit using the multi-fold mechanism. And further compression of the image from 6-bit to 4-bit needs a tremendous effort at both the compression and decompression end. On the compression side, the pixel data must undergo at least one extra single level of substitution. When it comes to the decompression side, the image data need to assess the probability with 2-4 pixel values for each pixel at each substitution level that needs exponential efforts. Adding one extra substitution layer on the compression side requires a tremendous effort during the decompression process. Moreover, too much image compression might compromise the quality of the reconstruction of the image Srinivasu et al. [32].

On the other hand, for the encryption process, the proposed algorithm needs feasible computational efforts. XOR-based data encryption does not require immense effort. The encryption is performed three times on

the encryption side. The string is reversed at each time. The same set of operations are performed on the decryption side as well. As the data related to image pixels are modified during the compression process, the pixel data of the resultant image is more robust to security attacks. An increase in several operations would demand more computational efforts with almost the same level of security.

#### 4. METHODS AND SPECIFICATIONS

The entire procedure of the secured compression of the medical images involves many tasks that involve trivial tasks like substitution, probabilistic reconstruction, dynamic symmetric key generation, performing XOR operation as stated by Srinivasu and Lalitha [33]. This section discusses the proposed approach's various methods, including the brier score approach for the probabilistic estimation and the hashing-based dynamic symmetric key generation for the encryption process.

##### 4.1. Brier Score Based Probabilistic Forecast

In the process of image compression, the higher-order bits, that is, 12-bit data, are replaced with 8-bit data, then resultantly distinct combinations would be missing that would compromise the quality of the image if the image is not restored with appropriate pixel values. Likewise, when the pixel information is further down-sampled from 8-bit to 6-bit. The image pixel data is being substituted for multi-folds rather than straight away downsizing from 12-bit to 6-bit data. The reason behind choosing the multi-fold architecture is to attain higher accuracy in image reconstruction when the prediction is needed to be performed, and the search space is divergent, the outcome would be compromising. To avoid all such complications, the architecture is multi-folded for better accurate predictions at each level.

In the re-construction of the image back to the natural condition, in the process of reverting, the appropriate pixel intensity value has to be predicted for which brier score mechanism, as stated by Wallace and Dahabreh [34], is incorporated for assessing the probabilistic scores in the decompressing phase of the proposed approach. The quality of the image is dependent on the probabilistic measure for choosing the appropriate pixel value. The Brier score is the aggregate of class-wise squared error of pixel-wise probabilistic assessment. It would help determine the accuracy of the approach and the level of confidently accurate the proposed approach works. The multi-pixel evaluation is performed through the following Equation (1)

$$P_s = \frac{1}{p_i} \sum_{x=1}^{P_i} (P_p - r_x)^2 . \quad (1)$$

In the above Equation (1), the variable designates the probabilistic score, represents the total predicted instances, and is the probability of prediction—the resultant variable aftermath of prediction. The value of  $x$  would not be 0; it would always be a non-zero value, i.e., represents the probabilistic instances. The smaller the value of the brier score represents the best prediction accuracy.

##### 4.2. Accuracy Assessment for Predictions

The accuracy of the predictions made for identifying the appropriate pixel value is assessed from Equation (2) stated below

$$P_a = \frac{1}{|P_1|} \sum_{\text{range=start}}^{\text{end}} (\hat{l}_r = l_r). \quad (2)$$

From the above Equation (2), the variable  $P_a$  designates the prediction accuracy and the variable  $P_1$  represents the prediction list and the variables  $\hat{l}_r, l_r$  represents the chosen values and the actual value of the pixel. The value of the  $P_1$  is following the ratio of compression in the considered problem. When the image is straight away compressed from 12-bit to 6-bit, the elements in the  $P_1$  would be considerably more than that might compromise the quality of the image.



### 4.3. Hash-Based Symmetric Key Generator

The key generated through the hashing techniques is size 256-bit, the sum of 4 \*64-bit sub-keys. The critical generator relay on the Permutation Order Generator (POG) and Diffusion Data Generator (DDG). The permutation order generator relay on logistic sine-map that is stated by Hua et al. [35] through the equation stated below

$$\alpha_{x+1} = \{(v\alpha_x(1 - \alpha_x) + (5 - v)\sin(\pi\alpha_x)/4\} \text{mod} 1. \quad (3)$$

In the above Equation (3), the variable  $\alpha_x$  represents the initial parameter, the value of the variable  $v$  would be in the range (0-4). The value of the initial parameters are determined from the Equations (4-6) as stated below through the logistic sine-map

$$\text{key}_1 = \text{key\_gen}_1 \times \text{key\_gen}_2 \quad (4)$$

$$\text{key}_2 = \text{key\_gen}_3 \div \text{key\_gen}_4 \quad (5)$$

$$\text{key}_3 = (\text{key}_1 + \text{key}_2) \text{mod} 1 \quad (6)$$

$\text{key}_1, \text{key}_2$  shown in the Equations (4) and (5) would determine the value of the  $\text{key}_3$  that are randomly generated indexes. The indexes are redo values that are randomly generated through the logistic sine-map. The increase in the permutation would also assure the increased security of the data that is encrypted. For Diffusion Data Generation, it is a combination of Logistic Tent Map(L.T.) by Sayed et al. [36] and Tent Sine Map(T.S.) by Hua et al.[37], The logistic Tent map can be approximated through s (7) stated below

$$\beta_{x+1} = \left( v\beta_x(1 - \beta_x) + \frac{(5-v)\beta_x}{2} \right) \text{mod} 1 \quad (7)$$

$$\beta_{x+1} = \left( v\beta_x(1 - \beta_x) + \frac{(5-v)(1-\beta_x)}{2} \right) \text{mod} 1. \quad (8)$$

Equation (7) is considered when the value of the variable  $\beta_x < 0.5$ , and the Equation (8) is considered when the value of the variable  $\beta_x \geq 0.5$ . The value of  $v$  lies between 0 and 5. The equation of the Tent-Sine map is defined through the Equations (9) and (10) stated below

$$\gamma_{x+1} = v\gamma_x/2 + (5 - v) \sin(\pi\gamma_x) / 5 \text{mod} 1 \quad (9)$$

$$\gamma_{x+1} = \frac{v(1-\gamma_x)}{2} + (5 - v) \sin(\pi\gamma_x) / 5 \text{mod} 1. \quad (10)$$

Equation (9) is considered when the value of the variable  $\gamma_x < 0.5$ , and the Equation (10), when the value of the variable is  $\gamma_x \geq 0.5$ , and the value of  $v$  always lies between 0 and 5 assumed from the pre-existing studies.

### 4.4. Fuzzy Trapezoidal Correlation Function

In the process of image decompression, the pixels are again restored to their original position. The actual challenge lies in identifying the best optimal pixel for the restoration of the image. To identify the most suitable pixel to replace at the corresponding position using the fuzzy trapezoidal correlation function. The function that evaluates the membership can be practically implemented as follows

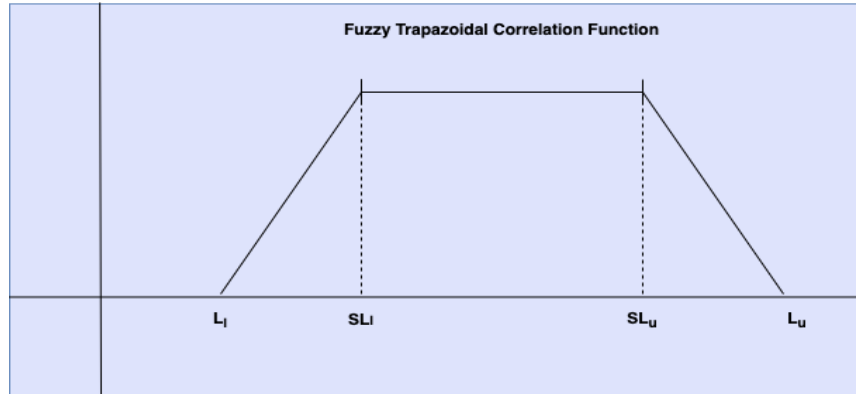
$$\text{pix}_{mem} = \alpha + \beta + \gamma \quad (11)$$

$$\alpha = \left( \frac{x_{med} - L_l}{S_{L_l} - L_l} \right) \times (\text{Correlation}_{component}) \quad (12)$$

$$\beta = \sum_{g_x=1}^n \omega_x(t) \sigma_x^2(t) \quad (13)$$

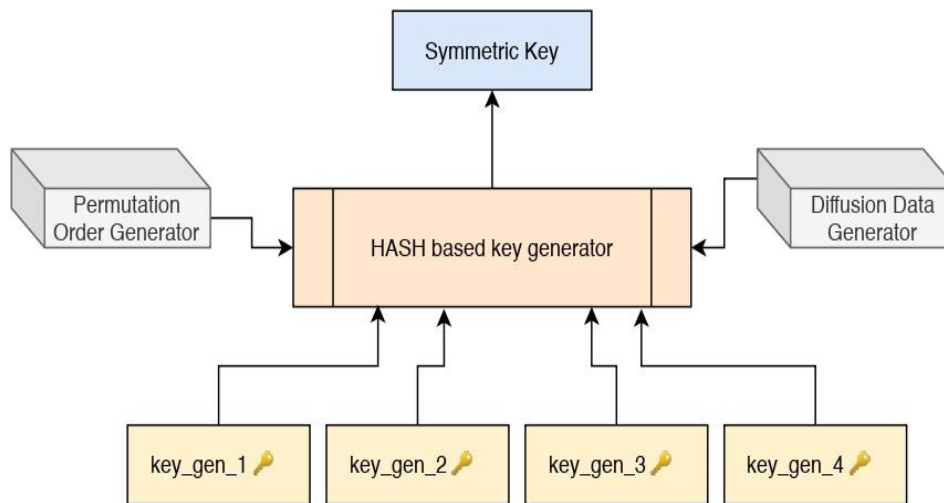
$$\gamma = \frac{L_u - x_{med}}{L_u - S_{L_u}} \times (\text{Correlation}_{component}) \quad (14)$$

$$\text{Correlation}_{component} = \frac{\sigma_x^2}{(\sigma_x^2 + \frac{\sigma_e^2}{2})}. \quad (15)$$



**Figure 4.** Represents the hash-based symmetric key generation

The correlation component is assessed from the above Equation (15) to determine the likelihood of the pixel being the appropriate pixel to be replaced.  $pix_{mem}$  Variable in Equation (11) is the fuzzy trapezoidal correlation value. The variables  $\alpha$  and  $\gamma$  from the Equations (11), (12) and (14) represent the lower limit and upper limit support variables for determining the optimal value, respectively. The variable  $\beta$  is the variance that is being considered for evaluating the membership assessment. The variables  $L_l$  and  $L_u$  These variables determine the lower and upper limits of the pixel values be replaced, and the variables  $SL_l$  and  $SL_u$  are the support lower and upper limit variables, respectively. The variable  $x_{med}$  determines the median variable of the ranges of pixels that are being considered for the replacement. Figure 4 represents the lower and upper bounds of the range of the pixels from where the maximum likelihood pixel is being considered.



**Figure 5.** Represents the Hash-based symmetric key generation

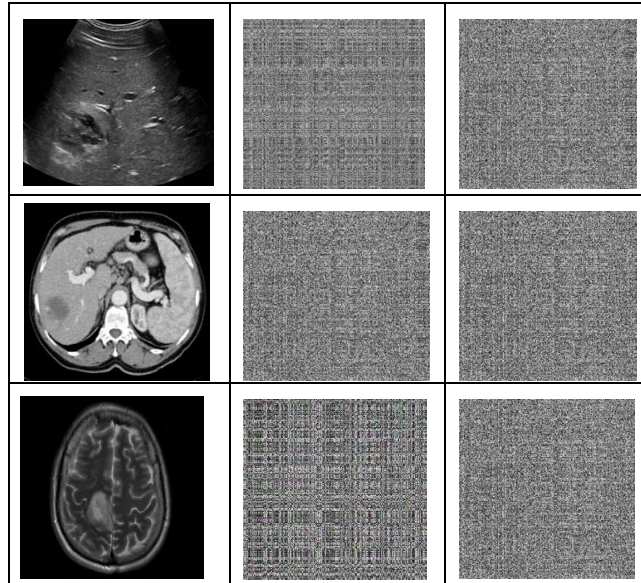
Hash-based key generator is responsible for generating the symmetric key based on four other additional keys. Figure 5 represents the symmetric key generation procedure through the Hash-based key generator by incorporating the Permutation Order Generator and the Diffusion Data Generator.

#### 4.5. Data Source

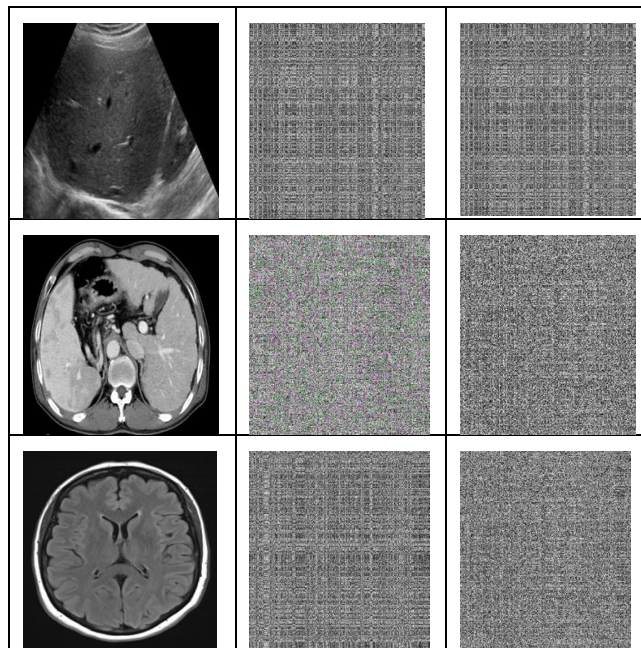
The data for execution has been acquired from various sources for the experimental study. The experimentation is performed on the standard sizes like 128 x 128, 256 x 256, 512 x 512. The medical MRI images associated with the human brain are acquired from the online repository Oasis, the CT scan images of the liver are acquired from the open-source repository Cancer Imaging Archive, and the Ultrasound images of the liver are obtained from the subset of ultrasound images that are part of MICCAI open-source imaging repository. The images are re-structured where so ever required to fit the input assumption as part of the predefined experimental assumptions.

## 5. RESULTS AND DISCUSSION

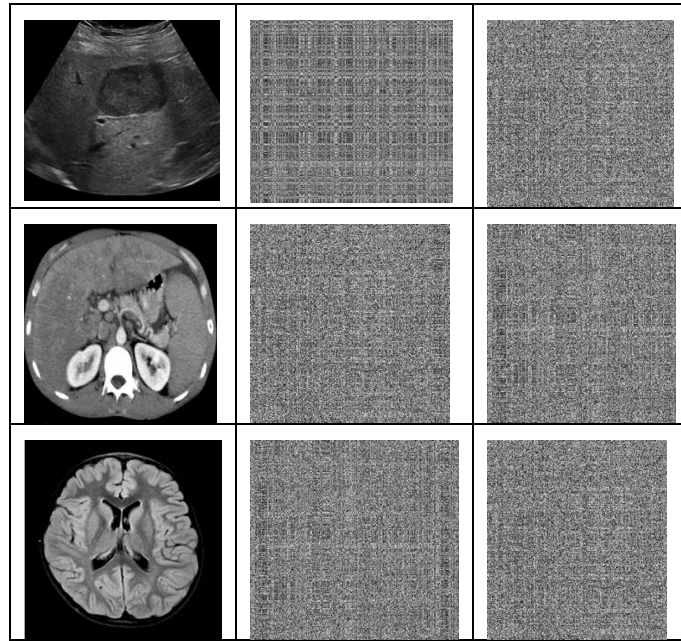
The proposed approach seems to be computationally efficient in the process of image compression, followed by encryption. The proposed approach's performance is being assessed through various performance evaluation techniques like PSNR, MSE, RMSE, and size of the resultant image in case the compression algorithms and the entropy is being considered for the measuring of performances in encryption algorithms as evaluated in Srinivasu et al. [38]; Srinivasu et al. [39]. The experiment carries various medical images, including MRI, CT, and Ultrasound, acquired from open-source repositories like fMRI and BrainWeb. The experiments are performed over various sizes like 128 x 128, 256 x 256, 512 x 512. The results of the proposed approach are being tabulated below in Tables 2 and 3.



*Figure 6. Resultant outcomes on execution for medical image oversize 128 x 128*



*Figure 7. Resultant outcome on executing over the medical image of size 256 x 256*



**Figure 8.** Resultant outcomes on execution over the medical image of size 512 x 512

Figure 6, stated above, represents the proposed approach to experimenting with the medical image of size 128 x 128. The leftmost image represents the original image that is considered and the second image from the left represents the resultant of the compression. The third image is the final image after performing the image's encrypting through the dynamically generated symmetric key. Likewise, Figure 7 represents the experimental results on performing over the medical images of size 256 x 256, and Figure 8 represents the outcome of experimenting over the image of size 512 x 512. The resultant image on experimentation can be observed that the image compression makes more Chios, and the resulting image will be encrypted for multiple rounds, making the image data more robust over the security attacks. The size analysis of various medical images of distinct dimensions before and after compression is presented in Table 2.

**Table 2.** Resents the size of the medical image before and after compression

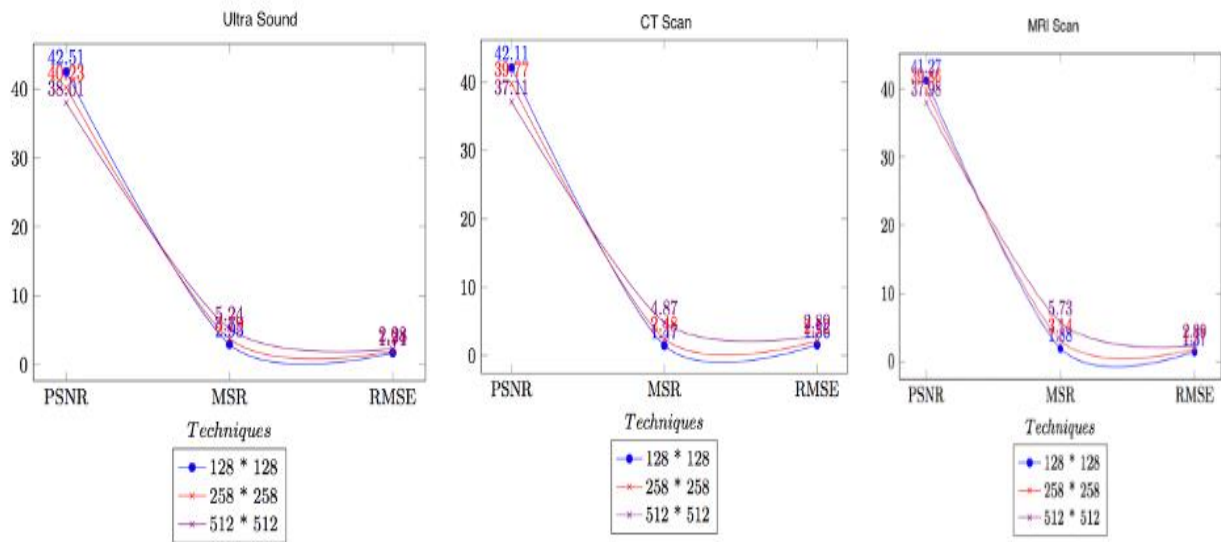
| Type of Image | Image Size | Size before compression (bytes) | Size after compression (bytes) | Size reduced (bytes) | Compression Time (In sec) |
|---------------|------------|---------------------------------|--------------------------------|----------------------|---------------------------|
| UltraSound    | 128 x 128  | 81920                           | 47514                          | 34406                | .48291                    |
|               | 256 x 256  | 327680                          | 190054                         | 137626               | .89211                    |
|               | 512 x 512  | 1310720                         | 760218                         | 550502               | 1.21834                   |
| MRI           | 128 x 128  | 131072                          | 76022                          | 55050                | .62382                    |
|               | 256 x 256  | 524288                          | 304087                         | 220201               | 1.04304                   |
|               | 512 x 512  | 2097152                         | 1216348                        | 880804               | 1.32288                   |
| CT            | 128 x 128  | 98304                           | 57016                          | 41288                | .51341                    |
|               | 256 x 256  | 393216                          | 228065                         | 165151               | .93201                    |
|               | 512 x 512  | 1572864                         | 912261                         | 660603               | 1.29243                   |

The image's quality is being evaluated upon performing the image decompression to assess the performance of the proposed approach. Table 3, stated below, holds the values of the various metrics like Peak Signal to Noise ratio (PSNR), Mean Square Error (MSE), and Root Mean Square Error (RMSE) among the original image and restored image upon decompression. It can be observed from the measured values that the proposed approach is reasonably fair in preserving the quality of the original image. The model outperforms for smaller size images over the larger size images for all types of the medical images.

**Table 3.** Represents the performance analysis of the proposed approach

| Type of Image | Image Size | PSNR  | MSE  | RMSE |
|---------------|------------|-------|------|------|
| UltraSound    | 128 x 128  | 42.51 | 2.95 | 1.71 |
|               | 256 x 256  | 40.23 | 3.79 | 1.94 |
|               | 512 x 512  | 38.01 | 5.24 | 2.28 |
| MRI           | 128 x 128  | 41.27 | 1.88 | 1.37 |
|               | 256 x 256  | 39.86 | 3.14 | 1.77 |
|               | 512 x 512  | 37.98 | 5.73 | 2.39 |
| CT            | 128 x 128  | 42.11 | 1.47 | 1.56 |
|               | 256 x 256  | 39.77 | 2.48 | 2.12 |
|               | 512 x 512  | 37.11 | 4.87 | 2.89 |

From the above tables, Tables 2 and 3, it is observed that the performance of the proposed compression algorithm is reasonably fair when the size of the image is reduced to almost half of the size of the original image. And the approach is computationally efficient that needs minimal computational time. Figure 9 represents the graphical representation of the tabulated values of Tables 2 and 3.



**Figure 9.** Represents the values of PSNR, MSE, RMSE of the proposed technique

The performance of the proposed secured compression model is assessed against the other existing models like Optimal Discrete Wavelet Transform and Run Length Encoding Technique (ODWT-RLE) [40], Bit plane Run Length Coding (BRLC) [41], Multilevel Block Truncation Coding (MBTC) [41], Differential Predictive Coding (DPC) [41] that have experimented over the similar data and the mean of those obtained values are presented in Table 4 and the corresponding graphs are shown in Figure 10. The assessed values like PSNR, MSE, and RMSE make the proposed model outperforms various compression techniques.

**Table 4.** Represents performance analysis of various existing compression techniques

| Approach          | PSNR  | MSE   | RMSE |
|-------------------|-------|-------|------|
| ODWT-RLE          | 40.74 | 5.46  | 2.33 |
| BRLC              | 34.64 | 22.56 | 4.75 |
| MBTC              | 32.44 | 47.33 | 6.88 |
| DPC               | 34.65 | 22.46 | 4.74 |
| HUFFMAN           | 34.65 | 22.37 | 4.73 |
| Proposed approach | 41.96 | 2.08  | 1.54 |

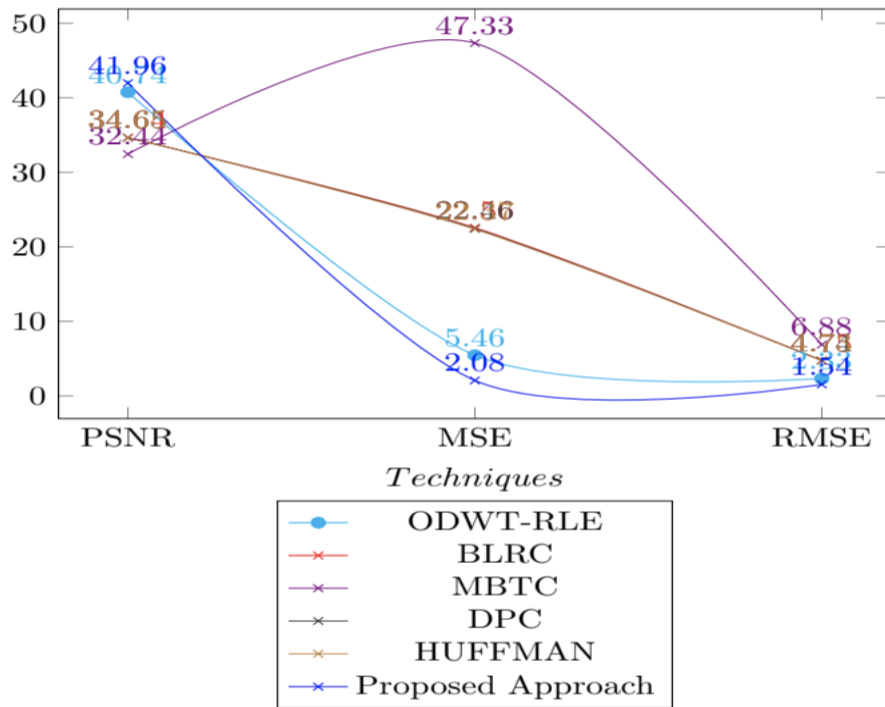


Figure 10. Comparative analysis of the proposed technique

The encryption algorithm's performance is assessed through the entropy on the practical implementation of the proposed approach presented in Table 5. It is desired to have the entropy value close to 8 for a better encryption algorithm, and zero would be the least. The following equation assesses the value of the entropy that determines the strength of the encryption algorithm

$$E_S = \sum_{x=0}^{2^n-1} \text{prob}(s_x) \log_2 \frac{1}{\text{prob}(s_x)} \tag{16}$$

The above Equation (16) shows that the variables are the information source and approximated information through the proposed approach. The tabulated value from Table 5 stated below proves that the proposed algorithm is robust upon entropy attacks.

Table 5. Represents the entropy analysis of the proposed compression approach

| Type of Image | Image Size | Entropy |
|---------------|------------|---------|
| UltraSound    | 128 x 128  | 7.898   |
|               | 256 x 256  | 7.472   |
|               | 512 x 512  | 7.014   |
| MRI           | 128 x 128  | 7.727   |
|               | 256 x 256  | 7.129   |
|               | 512 x 512  | 6.929   |
| CT            | 128 x 128  | 7.740   |
|               | 256 x 256  | 7.009   |
|               | 512 x 512  | 6.875   |

The correlation coefficient is the other statistical analysis approach that assists in assessing the encryption algorithm's efficiency. The correlation coefficient evaluates the pixel's relations with the adjacent horizontally, vertically, and diagonally connected pixels. The robust encryption algorithm would shrink the value of the correlation coefficient. For assessing the correlation among the original image and the resultant image of the encryption algorithm, 1500 pairs of pixels are considered in assessing the correlation

coefficient value that is assessed through the Equations (17), (18), (19) and (20), that is stated in the article by Hasanzadeh, Yaghoobi [42].

$$P_{i,j} = \frac{\text{cov}(i,j)}{\sqrt{V(i)}\sqrt{V(j)}} \quad (17)$$

$$E(i) = \frac{1}{x} \sum_{i=1}^x i_x \quad (18)$$

$$V(i) = \frac{1}{x} \sum_{i=1}^x (i_x - E(i))^2 \quad (19)$$

$$\text{cov}(i, j) = \frac{1}{x} \sum_{i=1}^x (i_x - E(i))(j_x - E(j)). \quad (20)$$

From the above Equations, the variables  $i, j$  hold the values of the two adjacent pixels, and the variable  $E(i)$  is associated with expectation, and the variable,  $V(i)$  is related to the variance. The proposed approach initially compressed the image almost to half of the original image through substitution, resulting in a distorted image. Table 6 below represents the value of the correlation coefficient value post-compression of the image. The values are close to zero. Less than zero illustrated the poor correlation among the adjacent pixels, and Table 7 below are the approximated correlation coefficient values on encrypting the compressed image.

**Table 6.** The correlation table of the compressed image concerning the original image

| Type of Image | Image Size | Horizontal | Vertical  | Diagonal  |
|---------------|------------|------------|-----------|-----------|
| UltraSound    | 128 x 128  | -0.000057  | -0.005437 | 0.000383  |
|               | 256 x 256  | -0.000138  | -0.007834 | 0.000378  |
|               | 512 x 512  | -0.000234  | -0.008292 | 0.000288  |
| MRI           | 128 x 128  | -0.000326  | -0.000987 | 0.000262  |
|               | 256 x 256  | -0.000782  | -0.002091 | 0.000117  |
|               | 512 x 512  | -0.000981  | -0.005710 | -0.095221 |
| CT            | 128 x 128  | -0.000121  | -0.002498 | 0.000316  |
|               | 256 x 256  | -0.000597  | -0.004593 | 0.000062  |
|               | 512 x 512  | -0.000718  | -0.009002 | -0.089212 |

**Table 7.** The correlation table of encrypted data concerning the original image

| Type of Image | Image Size | Horizontal | Vertical  | Diagonal  |
|---------------|------------|------------|-----------|-----------|
| Ultra Sound   | 128 x 128  | -0.000898  | -0.006214 | -0.000071 |
|               | 256 x 256  | -0.000962  | -0.009156 | -0.000435 |
|               | 512 x 512  | -0.001271  | -0.010091 | -0.000974 |
| MRI           | 128 x 128  | -0.001026  | -0.002087 | -0.000262 |
|               | 256 x 256  | -0.003627  | -0.005022 | -0.000610 |
|               | 512 x 512  | -0.007215  | -0.009326 | -0.001041 |
| CT            | 128 x 128  | -0.000921  | -0.006542 | -0.000039 |
|               | 256 x 256  | -0.003207  | -0.009043 | -0.000298 |
|               | 512 x 512  | -0.006419  | -0.020129 | -0.000569 |

The values from Tables 6 and 7 depict the efficiency of both the compression algorithm and the encryption algorithm. The minimum the value is, the better the image's security; lesser values portray that the adjacent pixels are poorly correlated in the resultant compressed and encrypted images.

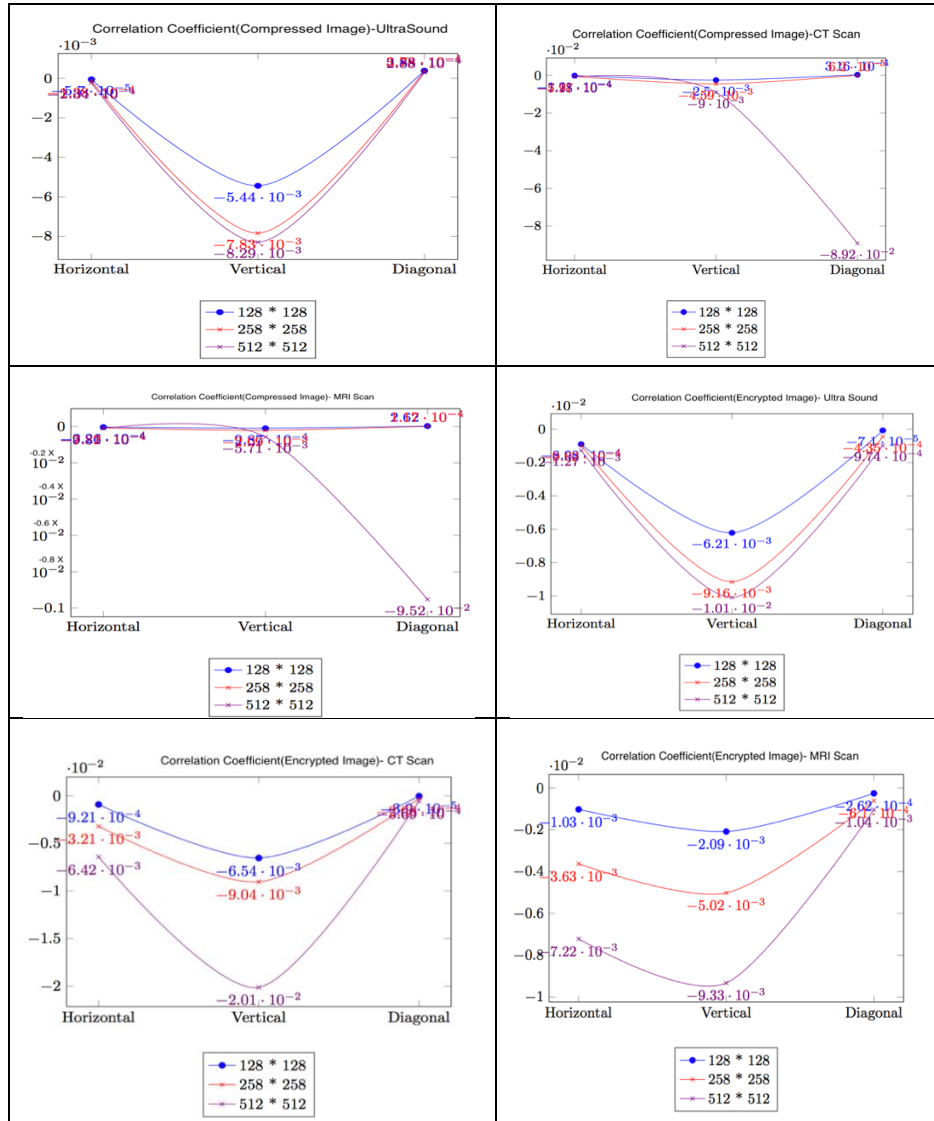


Figure 11. Graph representing the correlation coefficient on implementation of the proposed approach

Figure 11 presents the graphical representation of the coefficient correlation on implementing the proposed approach, the first three images from the top represents the correlation values estimated over the compressed images that are obtained from Table 6 and, the next three images represent the correlation values obtained on executing the encryption algorithm over the compressed image the values that are obtained from Table 7. The minimal horizontal, vertical, and diagonal values indicate that the proposed approach outperforms ensuring the data's privacy.

## 6. CONCLUSION

In the context of secured storing sensitive medical-related data like patient reports, clinical records, and diagnosis reports. The proposed approach focus on secured compression of the medical imaging data that involves Ultra Sound, MRI scans, CT scans for storing purpose. It is observed on practical implementation. The proposed algorithm has reduced the storage space to almost half of the original size with the image that conserves the storage space. The algorithms used in either of the processes are lightweight that need minimal computation for substitution, XOR operation, probabilistic estimation, and string reversals that are pivotal in the proposed algorithm. The approach is mechanized so that the compression process needs multiple levels of pixel data substitution at the compression side. The pixel value prediction outcome's brier score at the decompression side would be a better choice for appropriate pixel value prediction during the image reconstruction. The performance metrics like PSNR, MSE, RMSE, and entropy have  $p$ . The reconstructed image is almost close to the original image without any significant data logistical analysis.



The results presented in the previous section confirm that the outcome of the proposed approach is promising for all three types of imaging technologies that include Ultrasound, CT, and MRI scans. The image data is further encrypted post-compression of the image that ensures a better level of image security. The correlation coefficient assessed against the compressed and encrypted medical images and the assessed values have proven robust the proposed encryption algorithm.

## 7. FUTURE SCOPE

The proposed approach can be further improvised though incorporating the multi-class classifier that could address the issue of densities and motivation that is caused due to limited data in the decompression process, and incorporation of the probabilistic multi-class classifier would be efficient in replacing with the appropriate pixel in the process of restoration of the image. Furthermore, blockchain technology can be assimilated to encrypt the resultant compressed image, resulting in a better security level with good computational efforts. The work can be further carried forward to implement it over the RAID and distributed architecture to handle the data.

## CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

## ACKNOWLEDGMENT

We thank the anonymous reviewers for their helpful ideas for the improvisation of the paper.

## REFERENCES

- [1] Pavithra, V., Jeyamala, C., "A Survey on the Techniques of Medical Image Encryption", IEEE International Conference on Computational Intelligence and Computing Research, Madurai, India, 1-8, (2018).
- [2] Zuo, Z., Lan, X., Deng, L., Yao, S., Wang, X., "An improved medical image compression technique with the lossless region of interest", *Optik*, 126(21): 2825-2831, (2015).
- [3] Chamberlin, P., Balasubramanian, S., "Near lossless medical image compression using block BWT-MTF and hybrid fractal compression techniques", *Cluster Computing*, 22: 12929–12937, (2019).
- [4] Messaoudi, A., Benchabane, F., Srairi, K., "DCT-based color image compression algorithm using adaptive block scanning", *Signal Image and Video Processing*, 13: 1441–1449, (2019).
- [5] Brahim, N., Bouden, T., Brahim, T., Boubchir, L., "A novel and efficient 8-point DCT approximation for image compression", *Multimed Tools and Applications*, 79: 7615–763, (2020).
- [6] Boucetta, A., Melkemi, K.E., "DWT Based-Approach for Color Image Compression Using Genetic Algorithm", In: Elmoataz A., Mamass D., Lezoray O., Nouboud F., Aboutajdine D. (eds) *Image and Signal Processing. Lecture Notes in Computer Science 7340*, Springer, (2012).
- [7] Parkale, Y.V., Nalbalwar, S.L., "Application of 1-D discrete wavelet transform based compressed sensing matrices for speech compression", *SpringerPlus*, 5: 2048, (2016).
- [8] Sangeetha, M., Betty P., Kumar., G. S. N., "A biometric iris image compression using LZW and hybrid LZW coding algorithm", 2017 International Conference on Innovations in Information, Embedded and Communication Systems, Coimbatore, India, 1-6, (2017).
- [9] Wang, H., Xia, Y., Wang, Z., "Dictionary learning-based image compression", 2017 IEEE International Conference on Image Processing, Beijing, China, 3235-3239, (2017).

- [10] Joshi, M., Agarwal, A.K., Gupta, B., "Fractal Image Compression and Its Techniques: A Review", In: Ray K., Sharma T., Rawat S., Saini R., Bandyopadhyay A. (eds) *Soft Computing: Theories and Applications, Advances in Intelligent Systems and Computing*, 742, Springer, Singapore, (2019).
- [11] Masmoudi, A., Bouhlel, M., Puech, W., "Efficient Adaptive Arithmetic Coding Based on Updated Probability Distribution for Lossless Image Compression", *Journal Electronic Imaging*, 19(2), (2010).
- [12] Lin, S., Gao, Z., Han, Y. S., "Arithmetic Coding Based on Reflected Binary Codes", 2019 Ninth International Workshop on Signal Design and its Applications in Communications, Dongguan, China, 1-5, (2019).
- [13] Gong-bin, Q., Qing-feng, J., Shui-sheng, Q., "A new image encryption scheme based on DES algorithm and Chua's circuit", 2009 IEEE International Workshop on Imaging Systems and Techniques Shenzhen, China, 168-172, (2009).
- [14] Mohammad, O. F., Rahim, M. S., Zeebaree, S. R. M., Ahmed, F., "A Survey and Analysis of the Image Encryption Methods", *International Journal of Applied Engineering Research*, 12: 13265-13280, (2017).
- [15] Shakir, H.R., "An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling", *Multimedia Tools Applications*, 78: 26073–26087, (2019).
- [16] Zhao, G., Yang, X., Zhou, B., Wei, W., "RSA-based digital image encryption algorithm in wireless sensor networks", 2010 2nd International Conference on Signal Processing Systems, Dalian, V2-640-V2-643, (2010).
- [17] Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Alqahtani, H. F., Alqahtani, N. N., Alshammari, G. N., Ali, A. A., "Image Encryption Based on AES and RSA Algorithms", 3rd International Conference on Computer Applications & Information Security (ICCAIS) Riyadh, Saudi Arabia, 1-5, (2020).
- [18] Xiao, C., Chun-Jie, H., "Adaptive medical image encryption algorithm based on multiple chaotic mapping", *Saudi Journal of Biological Sciences*, 24(8): 1821-1827, (2017).
- [19] Dener, M., "A new gateway node for wireless sensor network applications", *Scientific Research and Essays* 11, 20: 213-220, (2016).
- [20] Dener, M., "Security Analysis in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, 1-9, (2014).
- [21] Patidar, V., Pareek, N., Sud, K., "A new substitution–diffusion based image cipher using chaotic standard and logistic maps", *International Journal of Network Security & Its Applications*, 4(7): 3056-3075, (2009).
- [22] Srinivasu, N. P., Seshadri, Ch., "A Multilevel Image Encryption based on Duffing map and Modified DNA Hybridization for Transfer over an Unsecured Channel", *International Journal of Computer Applications*, 20(4): 1-4, (2015).
- [23] Pan, H., Lei, Y., Jian, C., "Research on digital image encryption algorithm based on double logistic chaotic map", *Journal Image Video Processing*, 142, (2018).

- [24] Akkasaligar, P., Biradar, S., "Medical Image Encryption with Integrity Using DNA and Chaotic Map", Recent Trends in Image Processing and Pattern Recognition (RTIP2R) Solapur, India, Communications in Computer and Information Science, 1036, Springer, Singapore, (2018).
- [25] Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F.G., Coelho, V. N., "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices", Optics and Lasers in Engineering, 110: 24-32, (2018).
- [26] Viswanath, G., Krishna, P., V., "Hybrid encryption framework for securing big data storage in multi-cloud environment", Evolutionary Intelligence, (2020).
- [27] Dener, M., Bostancıoğlu, C., "Smart Technologies with Wireless Sensor Networks", Procedia - Social and Behavioral Sciences, 195: 1915-1921, (2015).
- [28] Rehman, A. U., Wang, H., Shadid, M. M. A., Iqbal S., Abbas, Z., Firdous, A., "A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512", IEEE Access, 7: 162786-162802, (2019).
- [29] Gopalakrishnan, T., Srinivasan, R., "Chaotic Image Encryption with Hash Keying as Key Generator", Institute of Electronics and Telecommunications Engineers Journal of Research, 63(2): 172-187, (2017).
- [30] Singh, P. K., Singh, R. S., Rai, K. N., "An image encryption algorithm based on XOR operation with approximation component in wavelet transform", 2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), Patna, India, 1-4, (2015).
- [31] Belazi, A., Abd El-Latif, A. A., Belghith, S., "A novel image encryption scheme based on substitution-permutation network and chaos", Signal Processing, 128: 155–170, (2016).
- [32] Srinivasu, N. P., Bhoi, K., Nayak, S., Bhutta, M., Woźniak, M., "Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network", Electronics, 10(12): 1437, (2021).
- [33] Srinivasu, N. P., Lalitha, R., "An Efficient Data Encryption Through Image via Prime Order Symmetric Key and Bit Shuffle Technique", Lecture Notes in Networks and Systems 5. Springer, Singapore, (2017).
- [34] Wallace, B. C., Dahabreh, I. J., "Improving class probability estimates for imbalanced data", Knowledge Information System, 41: 33–52, (2014).
- [35] Hua, Z., Zhou, B., Pun, C., Chen, P., "Image encryption using 2D Logistic-Sine chaotic map", IEEE International Conference on Systems, Man, and Cybernetics (SMC) San Diego, CA, USA, 3229-3234, (2014).
- [36] Sayed, W. S., Fahmy, H. A. H., Rezk A. A., Radwan, A. G., "Generalized Smooth Transition Map Between Tent and Logistic Maps", International Journal of Bifurcation and Chaos, 27(1), (2017).
- [37] Hua, Z., Zhou, B., Zhou, Y., "Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation", IEEE Transactions on Industrial Electronics, 66(2): 1273-1284, (2019).
- [38] Srinivasu, P., Balas, V. E., "Self-Learning Network-based segmentation for real-time brain M.R. images through HARIS", PeerJ Computer Science, 7: e654, (2021).

- [39] Srinivasu, P., Rao, T. S., Balas, V. E., "Volumetric Estimation of the Damaged Area in the Human Brain from 2D M.R. Image", *International Journal of Information System Modeling and Design (IJISMD)*, 11(1): 74-92, (2020).
- [40] Sundara, R., Priya, V., Fred, A.L., "An Efficient Compound Image Compression Using Optimal Discrete Wavelet Transform and Run Length Encoding Techniques", *Journal of Intelligent Systems*, 28(1): 87-101, (2019).
- [41] Devaraj, S. J., Ezra, K., Kasaraneni, K., "Survey on Image Compression Techniques: Using CVIP Tools", In: Meghanathan N., Chaki N., Nagamalai D. (eds) *Advances in Computer Science and Information Technology, CCSIT 2012, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 86*, Springer, Berlin, Heidelberg, (2012).
- [42] Hasanzadeh, E., Yaghoobi, M., "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys", *Multimedia Tools and Applications*, 79: 7279–7297, (2020).