Modified Arnold's Cat Map-RC4 Encryption Technique for Medical Images

[1]Marwa T. Saleh, Mohamed A. Wahby Shalaby[1, 2], Hesham N. Elmahdy[1]

[1]Department of information technology, Faculty of Computers and Artificial Intelligence, Cairo University, Egypt

[2]Smart Engineering Systems Research Center, Nile University, Egypt

m.tarek@fci-cu.edu.eg,m.wahby@fci-cu.edu.eg,ehesham@fci-cu.edu.eg

Abstract

Information security has become a requirement these days, there is this highly sensitive data needs to be transmitted securely over networks to prevent data modification. Therefore, the medical images and the specific medical condition of the patient must be kept secure. In this paper, a medical image encryption technique is proposed. This technique uses first a Butterworth High Pass Filter (BHPF) to improve the medical image details to avoid any possible damage during the encryption-decryption method. The proposed technique is then developed by modified Arnold's cat map technique combined with the RC4 (Rivest Cipher 4) algorithm. A comparative study discusses the efficiency of the proposed technique concerning Arnold's Cat Map with AES (Cat-AES). One of the factors used in this paper is the absolute correlation coefficient near zero value to appear uncorrelated between the original image and the encrypted image. the result is shown the correlation coefficient equal zero on 13 from 20 of the brain CT for the proposed technique but CAT-AES is 2 from 20 of CT Brain Image and decreasing both the time of the encryption/decryption process is 35.24 second in the proposed technique and 75.37 second on CAT-AES and energy-efficient without changing the quality of medical images.

Keywords: *RC4 Encryption-Arnold's cat map- BHPF- Medical Image Encryption-The Correlation Coefficient –UACI-NPCR.*

1. Introduction

One of the most important needs at present is the encryption of images for transmission via the Internet. Therefore, such medical images must be exchanged or transmitted securely. Security has different parts one of these is encryption Image encryption has applications in medical imaging, multimedia systems, Internet communication, etc. [1]. Since images are different, in nature, compared to regular text data, there is a need to have image-based encryption algorithms to encrypt images. This is mainly due to two reasons; first, the image size is usually much larger than that of text data. Thus, the traditional algorithms took a long time for encrypting the image pixels directly. The second reason is that the decrypted text must be equal to the original text. However, this requirement is not necessary for images, since images have data capacity and high redundancy which are troublesome for traditional encryption. [1]. The traditional encryption techniques such as advanced encryption standard (AES), data encryption standard (DES) and Rivest–Shamir–Adleman (RSA) are no longer suitable for image practical applications [2]. Security has now become an important issue for photos to transfer over networks. Since it is so easy to access important information and use it illegally. [1]

The medical information system is used to control healthcare processing. For some applications, the medical images are important in diagnostic like CT & MRI [3]. Any image encryption technique aims to convert the original image into a cipher image which is difficult to be viewed. And hence, the encryption key is used by the receiver to gain legal access to the original image [4].

The traditional algorithms have low encryption and decryption operation speeds, these algorithms have significant latency. But the RC4(Rivest Cipher 4) was chosen as a result of it has advantages over different algorithms, RC4 is a simple, quick block cipher and is appropriate for Hardware or software implementation. RC4 is adaptable to process various word lengths. RC4 is iterative in structure, with a different number of rounds. RC4 algorithm has a variable-length symmetric cryptographic key. RC4 has a low memory requirement and gives high security. [5]

In this research work, the proposed approach is called modified Arnold's Cat map-RC4 (MARC4-264) encryption technique. In this technique, the proposed technique consists of three phases. First, a preprocessing phase is developed using Butterworth high pass filter in the frequency domain for sharping and enhancing original image details. This sharpening preprocessing phase is crucial since medical images usually contain many edges that correspond to the important medical information. Then, the second phase of the proposed encryption technique is the modification of image pixels' location by employing the Arnold Cat map. Finally, the third phase is to apply the RC4 encryption to the image. The proposed technique show encryption efficiency by 3 factors, one of these is the absolute correlation coefficient which appears uncorrelated between the original and encrypted image and fewer run time compared with CAT-AES.

The following sections of this paper are: First, Section 2 is presented the related work. Section 3 is then explained by the proposed technique. Section 4 is presented the discussions of the experimental results and analysis. Finally, Section 5 are discussed the conclusion and future scope.

2. Related Work

Kumari1, et al [6] introduced a novel image encryption algorithm based on Fractional Fourier transform (FFT) and chaotic system, the encryption process includes two stages. First, the image is encrypted twice the random phase using the Fractional Fourier domain. Then, the image is encrypted using a matrix generated by a chaotic system and the encrypted fingerprint image is obtained. The decryption technique is the reverse of the encryption technique [6].

Image Encryption requirements are outlined. The various properties of a good encryption algorithm (key) are clarified. Image encryption by strong key(s) gives high security. The process of the algorithm can be finished if the key(s) or Initialization Vector (IV) is detected. The solution for this key distribution issue might be the utilization of Visual Cryptography schemes. To summarize, both the Key(s) and Keyless Approaches are useful in real-time encryption algorithms of image. Both techniques have advantages and liabilities. There are several properties to be considered for planning an ideal image encryption algorithm, thus it is a challenge for any researcher to structure and maintain a good encryption scheme. [7].

AlZain, et al [8] developed an efficient chaotic image encryption cipher for improving security and encryption efficiency. The digital chaotic image cryptosystem has a new one is A chaotic tent map (CTM). The characteristics of CTM are very appropriate for the design of

encryption schemes. The CTM-based image cryptosystem planned against brute-force, differential, and statistical attacks is an adjective from hard cryptographic. Experimental tests are performed with detailed analysis confirming the high security of the designed CTM-based image cryptosystem. [8]

Ranvir Singh Bhogal, et al [9] developed an encryption technique using a chaotic map combined with the standard AES algorithm to achieve better encryption quality. In this technique, the presented algorithm, CAT-AES, iterates first through Arnold's cat map to change the location of pixels. Then, the image encryption is completed by applying the standard AES encryption algorithm on the resultant image.

In this research work, have 3 mission, first, the encrypted image doesn't show any information of the original image, secondly, decrease the run time for encryption/ decryption process, finally, the decrypted image near equal the original image for diagnosis.

3. The Proposed Technique MARC4

Medical images are produced and stored in digital pixels. Diagnosis is the most important information in Medical images. Therefore, encrypting medical images from unauthorized usage is a vital requirement. Since most of the medical images are generated either from CT scan or MRI, a benchmark dataset of CT and MRI images is used in developing the proposed technique.

The proposed technique consists of three steps, the first phase applies a Fast Fourier Transform (FFT) for the image then applies Butterworth high pass filter (BHPF) for sharping edges. This sharping phase is important to maintain the important image details for medical diagnoses. After that, the inverse Fast Fourier Transform is applied to recover the image in the spatial domain again. Then, the second phase changes image pixel via several iterations by applying Arnold's cat-map. Finally, the third phase is to design the RC4 (256 bit), to generate encrypted images for transmission. For decryption Steps to receive the original image again by two steps. The first step is to apply an RC4 (256 bit) decryption. Finally, the second step is to apply the rest of the iteration of modified Arnold's cat-map to generate the original image. The following Figure.1 contains the flow chart of the proposed MARC4-264 encryption and decryption technique.

Encryption /Decryption technique

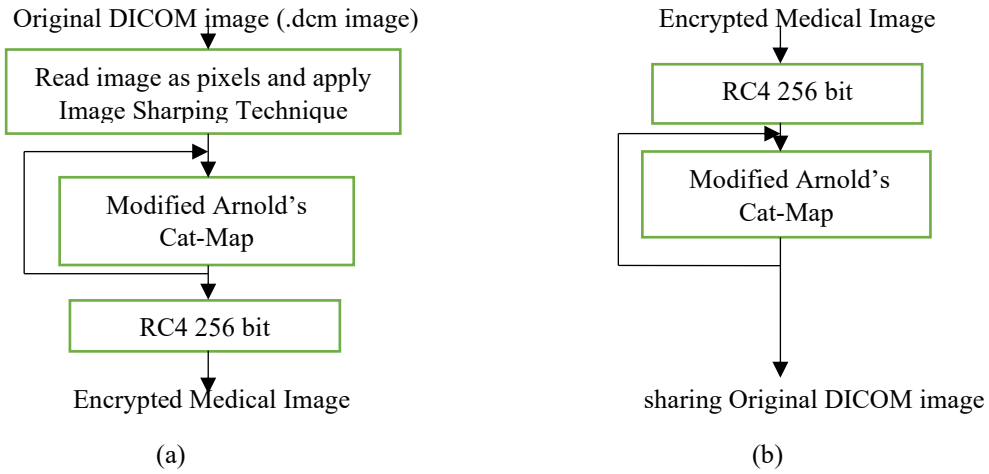


Figure.1: Flowchart of proposed MARC4 (a) Encryption technique, (b) Decryption technique

3.1 Image sharping technique

The medical image includes mainly edges, in the frequency domain, these edges are represented by high-frequency components. In the frequency domain, At first, the preprocessing step is read DICOM medical image (.dcm) to pixels by dicomread function in Matlab after that the fast Fourier transform is applied to convert the image into frequency components as shown in Figure.2 [10]. Then, the image frequency components are filtered using the well-known Butterworth high pass filter (BHPF). It is the type of sharpening filter keep frequencies outside radius D0 and removes values inside. A BHPF has cutoff frequency D0 equal 100 is better in Sharping edges like [10] and order m equal 4 is characterized as Equation 1. [10] After the sharping filter is applied, the inverse FFT is then used to generate the image pixels in the spatial domain. Finally, the post-processing step is to show image pixels in real-time in DICOM format by dicomwrite function in Matlab. Figure 3 contains two samples of medical images and their recovered images after applying the proposed MARC4 scheme with and without BHPF. It is seen that the decrypted images in Figure 3 (c) contain a more sharpened image than the decrypted image in Figure 3 (b). An advantage of the Butterworth filter is that we can control the sharpness of the filter with the order m.[10]

$$H(u,v) = \frac{1}{1 + \left[\frac{D_0}{D(u,v)}\right]^{2m}} \qquad (1)$$

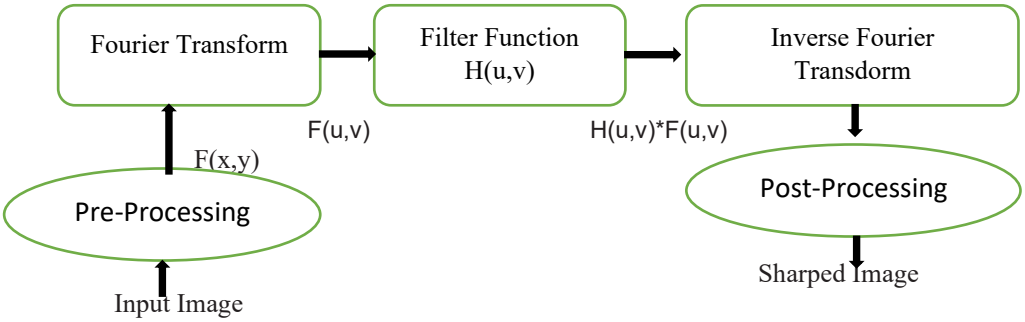
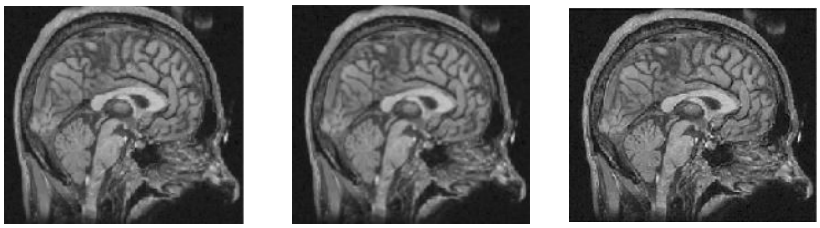


Figure. 2. Basic steps for filtering in the frequency domain [10]



(a) Original image (b) Without BHPF (c) With BHPF

Figure .3. *Comparison* between decrypted images using the proposed MARC4 scheme without BHPF and with BHPF

3.2 The modified Arnold's Cat Map

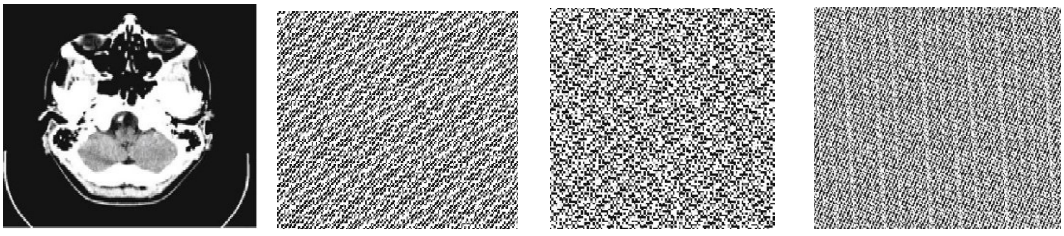
Vimali G and M. Senbagavalli [11] introduced an instance of chaos technique called Arnold's cat map in recognition of mathematicians Vladimir, who developed it by an image of a cat. An image is transformed into another one by changing the locations of the pixels randomly via a specific number of iterations. In [11], the equation (Equation. 2) is used to calculate the locations of the new pixels such that $\alpha_1 = 1, \alpha_2 = 1, \beta_1 = 1, \beta_2 = 2$. Using this equation and after a specific number of iterations I, the original image will be reconstructed as shown in Figure 4. Therefore, in the original Arnold's cat map technique, the encryption phase uses several iterations that are smaller than I. Then, in the decryption phase, the remaining number of iterations is used to reconstruct the original image.

$$If\ we\ let\ A = \begin{bmatrix} x \\ y \end{bmatrix}\ be\ \ a\ n * \ n\ matrix\ of\ image\ pixels, Arnold's\ cat\ map\ is\ the\ transformation.$$

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} \alpha_1 x + \beta_1 y \\ \alpha_2 x + \beta_2 y \end{bmatrix} mod\ n \qquad (2)$$

$$where\ mod\ is\ the\ \begin{bmatrix} \alpha_1 x + \beta_1 y \\ \alpha_2 x + \beta_2 y \end{bmatrix} and\ n$$

In the proposed MRC4 technique, the values of these parameters$\alpha_1 = 1, \alpha_2 = 1, \beta_1 = 1, \beta_2 = 2$ corresponding number of iterations needed to retrieve back the original image have been determined. The number of iterations for the brain CT images that have size 256*256 (192 iterations), and for the brain MRI images that have size 320*320 (240 iterations). These different numbers of iterations, for different image size values. It is proposed that the encryption phase employs "k_1"$(8\ bits)$ response to how many iterations in it and (total number of iteration - k_1) in the decryption phase. This experiment is 50% of the number of iterations in the encryption phase. And hence, the decryption phase employs another 50% of the iterations to recover the original image. By using the proposed approach, the strength of the encryption/decryption technique is increased by adding more bits for the encryption/decryption key.



(a) Iteration 0 (b) Iteration 17 (c) Iteration 80 (d) Iteration 88

(e) Iteration 90 (f) Iteration 144 (g) Iteration 192

Figure.4: Arnold's cat map applied to CT at certain iterations

3.3 Improved RC4

In [12] is given an Improved RC4, unlike traditional RC4 two S-boxes are used that more the randomness inside the state and enhanced the statistical properties of the cipher. The authors had meant that the proposed algorithm has removed serval weak factors of RC4. The key bytes and plaintext stream with apply X-OR operation. Figure 5.

Key-Generation Algorithm:

Two S-boxes state vector is initialized a 256-byte from A variable-length key of 1 to 256 bits, with elements Sbox1 [0] to Sbox1 [255] and Sbox2 [0] to Sbox2 [255]. The key1, 2 is generated from Sbox1 and Sbox2 by way of choosing certainly one of 255 entries systematically, then the entries in Sbox1, 2 are permuted again.

3.3.1. Key-Scheduling Algorithm(KSA)

In ascending order, Initialize: The values of Sbox1, Sbox2 are equal to the values from 0 to 255,

```
For x from zero to 255
y:= (y + Sbox1 [x] + key1 [x mod K]);
Swap (Sbox1 [x], Sbox1 [y]);
z:= (z + Sbox2 [x] + key2 [x mod K]);
Swap (Sbox2 [x], Sbox2 [z]);
End for
```

3.3.2. Pseudorandom generation algorithm (PRGA)

Once the vector Sbox1, 2 is initialized, the input key will not be used. In this step, for each Sbox1, the Sbox2[x] algorithm swap it with another byte in Sbox 1, Sbox2 as indicated by the current configuration of Sbox1, Sbox2. After achieving Sbox 1, Sbox2 [255] the process continues, starting from Sbox 1, 2 [0] again

```
While message
x:= x + 1;
y:= y + Sbox1 [x];
Swap (Sbox1 [x] and Sbox1 [y]);
z:= z+ Sbox2 [x];
Swap Sbox2 [x] and Sbox2 [z];
out1 Sbox1 [Sbox2 [x] + Sbox2 [z]];
out2 Sbox2 [Sbox1 [x] + Sbox1 [y]];
Swap (Sbox1 [Sbox2 [y]], Sbox1 [Sbox2 [z]]);
Swap (Sbox2 [Sbox1 [y]], Sbox2 [Sbox1 [z]]);
End while
```

3.3.3. Encrypt using X-Or

Figure 6 shows the implementation of the proposed system for brain CT image using $k_1 = 96$ for CT Brain image. It is seen that the sharpened image in Figure 6 (b) has better quality than the original image Figure 6(a). It is also seen that the retrieved image Figure 6(f) is similar to the original sharpened image Figure 6 (b).

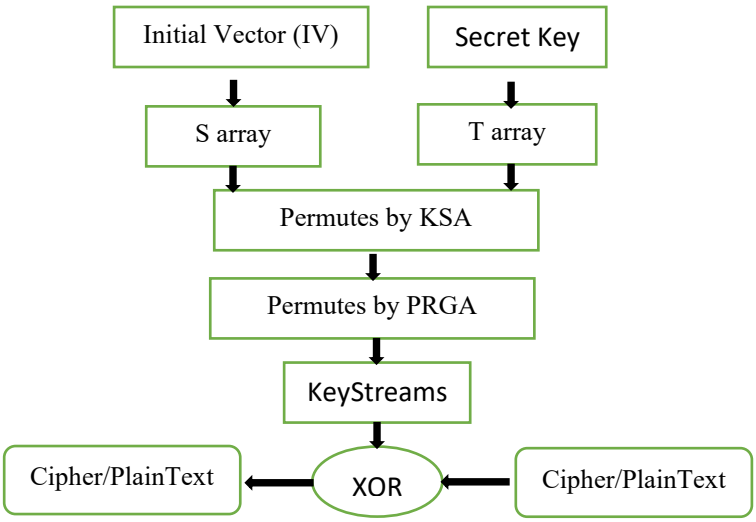


Figure.5. *RC4* algorithm [12]

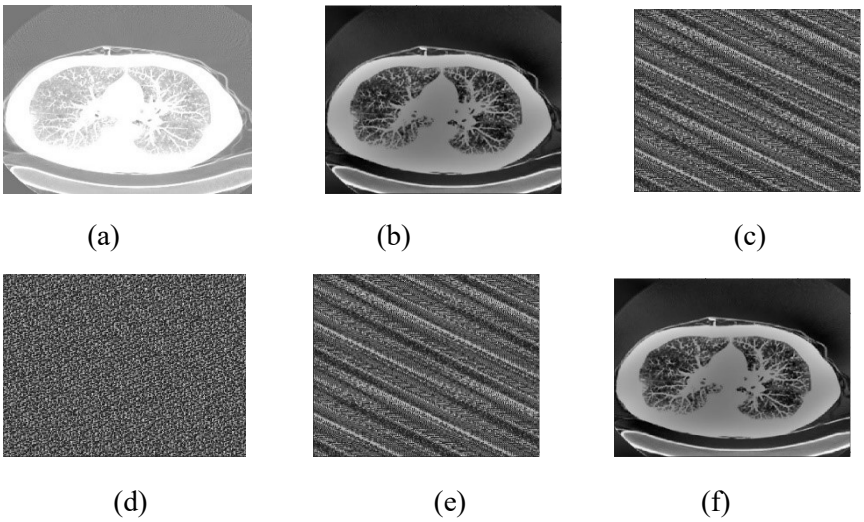


Figure .6: *The proposed* MARC4 technique (a) Original image, (b) sharpened image (c) Encryption using $k_1 = 96$, (d) modified RC4 encryption, (e) modified RC4 decryption, (f) retrieved image after decryption phase

4. Experimental Results and Analysis

Based on the previous section, the proposed technique proved its capability to protect medical images and delivered the decrypted images to the authorized person with high quality. In this section to show the strength of the proposed encryption technique, two medical image encryption techniques, namely, CAT-AES, and the proposed MARC4-264 are tested using two data sets of DICOM images. One set contains 20 brain CT images with dimensions of 256*256 [13] and the second one is a set of 100 brain MRI images with a 320*320-pixel dimension [14]. The experimental work is done using MATLAB on a Windows 8 machine (Intel i5).

4.1 Performance Metrics

The performance of the two encryption techniques is measured in terms of encryption strength and run-time encryption and decryption. Therefore, three performance metrics are first used to measure the encryption strength are correlation coefficient r [9], unified average changing intensity (UACI) [15], and a number of pixels change rate (NPCR) [15]. Based on the absolute correlation coefficient (r), as defined by Equation (3), the strength of an encryption algorithm is measured by comparing the pixels at the same position in the original image and encrypted image. The absolute correlation coefficient has values from 0 to +1. In case the correlation coefficient has a value closest to zero, it means uncorrelated to the original image. In our experimental work, the absolute correlation coefficient has been used to show the efficiency of the encryption algorithms. And thus, the absolute correlation coefficient should be able to achieve a lower value of the coefficient (r), ideally, it should be zero.

The absolute correlation coefficient is calculated as follows:

$$r = \left| \frac{\sum_m \sum_n (A_{mn} - A`)(B_{mn} - B`)}{\sqrt{\left(\sum_m \sum_n (A_{mn} - A`)^2\right)\left(\sum_m \sum_n (B_{mn} - B`)^2\right)}} \right| \quad (3)$$

,where A_{mn} is the pixel value of the original image A of size mxn pixels, B_{mn} is the pixel value of the encrypted image B of size mxn pixels, $A`$ is the mean value of the original image pixels, and $B`$ is the mean value of the encrypted image pixels [9].

In order to measure the strength of an encryption technique against the differential attacks the NPCR and UACI are used. Over the past decade the widely used performance metrics for medical image encryption techniques [15]. Suppose encrypted images before and after a one-pixel change in an original image are I^1 andI^2, respectively. The pixel values at the location (i, j) in I^1 and $I^2$are denoted as $I^1(i, j)$ and$I^2(i, j)$. Then, an array D is defined in Equation (4) as a bipolar array, i.e, an array of ones or zeros. Based on the calculated bipolar array D, the NPCR and UACI can be mathematically calculated by Equations. (5) and (6), respectively.

$$D(i,j) = \begin{cases} 0, if\ I(i,j) = I^2(i,j) \\ 1, if\ I^1(i,j) \neq I^2(i,j) \end{cases} \quad (4)$$

$$NPCR: N(I^1, I^2) = \sum_{i,j} \frac{D(i,j)}{T} * 100\% \quad (5)$$

$$UACI: U(I^1, I^2) = \sum_{i,j} \frac{|I^1(i,j) - I^2(i,j)|}{F * T} * 100\% \quad (6)$$

where T represents the total number of pixels in the encrypted image under consideration, and symbol F means the largest pixel value could be used for the encrypted image [15]. Therefore, for the gray medical images, the value of F equals 255.

The range of NPCR is [0, 1]. When $N(I^1, I^2) = 0$, it means that all pixels in the second image I^2 equal the values in the first imageI^1. In other words, the two images are identical with none of the pixels changed. On the other hand, when $N(I^1, I^2) = 1$, it means that all

pixels in the second image I^2 are not equal compared to the corresponding values in the first imageI^1. Similar to NPCR, the range of UACI is also [0, 1]. For two identical images, the value of UACI is also zero, i.e.$U(I^1, I^2) = 0$. Therefore, the NPCR and UACI, of an encryption technique with higher efficiency, should be as large as possible [15].

4.2 Comparative Study

As mentioned earlier, two medical image encryption techniques, namely, CAT-AES, and the proposed MARC4-264 are tested in our comparative study. To have fair comparisons, the number of iterations for CAT-AES and MARC4-264 are fixed to be 192 and 240 for both datasets, respectively. Hence, for the proposed MARC4-264 technique, the encryption is done using $k_1 = 96$ for Brain CT dataset and $k_1 = 120$ for Brain MRI Dataset.

The first comparison is held by calculating the absolute correlation coefficient (r) for each technique on the two datasets. Table 3 compares the two medical image encryption techniques in terms of the number of images for each technique based versus the absolute correlation coefficient for 20 Brain CT images from the first dataset. As indicated in Table 3, the resultant values of the calculated absolute correlation coefficient are grouped into ranges. For each range, Table 3 contains the number of images within such a range for each technique. It is seen from Table 3 that CAT-AES can achieve larger values of absolute correlation coefficient compared to the proposed technique. It is also seen from Table 3 that the majority of brain CT images, encrypted by the MARC4-264, have the absolute correlation coefficient equal to zero (13 out of 20 images) compared to Cat-AES (2 out of 20 images).

Figure. 7 and Figure. 8 presented the absolute correlation coefficient, between the original and encrypted images, for the two encryption techniques for both datasets. Figure. 7 shows that the absolute correlation coefficient, calculated on the first dataset, respectively. These results show that the proposed MARC4-264 technique has the best minimum correlation coefficient. Which corresponds uncorrelated between the original image and encrypted image. For the second dataset of 100 MRI images, Figure.8 shows also that the majority of images (81 out of 100) encrypted by the proposed technique have the absolute correlation coefficient equal to zero. It is seen also from this figure that the proposed technique is capable of achieving the lowest correlation coefficient in comparison to other techniques as well.

Table.3. *Number* of images for each technique based on correlation coefficient ranges for 20 Brain CT images

Absolute correlation coefficient range	Cat-AES	MARC4-264
0---0.005	2	13
0.005---0.01	3	0
0.01---0.05	4	4
0.05---0.1	6	3
0.1---0.2	2	0
0.2---0.3	2	0
0.3---0.4	1	0
0.4---0.5	0	0
0.5---0.6	0	0

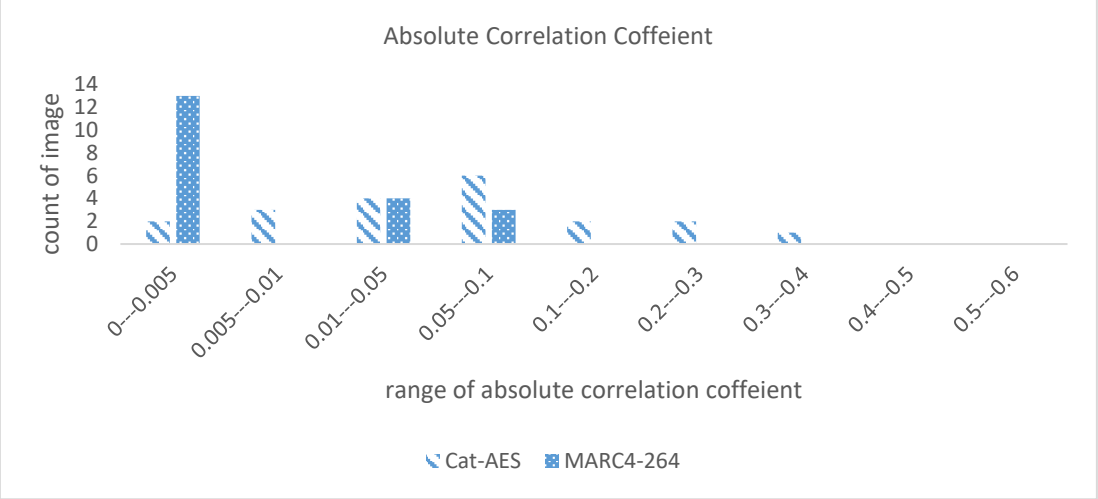


Figure .7. The absolute correlation coefficient on 20 256*256 brain CT

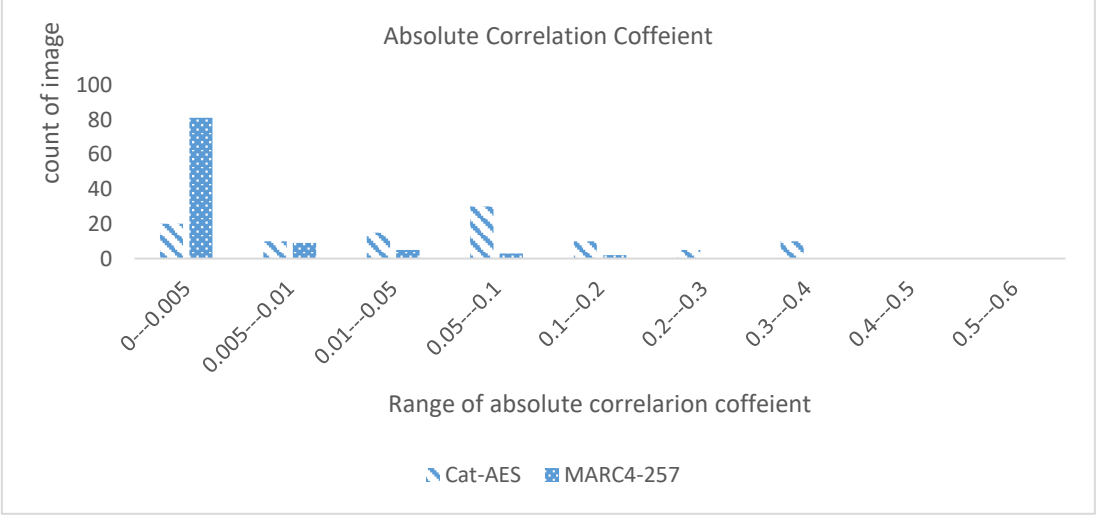


Figure .8. The absolute correlation coefficient on 100 320*320 brain MRI

Then, to show the robustness of the proposed technique against the differential attacks, the NPCR and UACI are calculated for both datasets. Table 4 contains the average values of NPCR and UACI achieved by the two encryption techniques, namely, CAT-AES, and the proposed MARC4-264. These values are calculated using the original image and the encrypted image. The results show the ability of the MARC4-264 technique to achieve better values of UACI and NPCR in comparison to the Cat-AES technique. This better performance is expected since both techniques depend on a chaos map to strengthen the encryption process. It is seen that the proposed MARC4-264 technique can achieve much larger values of the NPCR and UACI, which show the robustness of the proposed encryption technique in comparison to CAT-AES techniques.

It is seen from Tables 3, 4, Figures 7 and 8, that the proposed MARC4-264 technique shows a much higher level of encryption strength in comparison to the CAT-AES technique. This is mainly due to the preprocessing phase of the medical images by using a high pass

filter. As explained earlier, the BHPF is used to enhance the quality of the images concerning the medical information. In addition to such an enhancement, the image pixel values are normally changed by applying the filter, and therefore the encrypted image is much uncorrelated to the original image.

Table.4. average UACI and NPCR for two techniques of 20 Brain CT & 100 Brain MRI

	CAT-AES		**Proposed MARC4**	
	UACI	NPCR	UACI	NPCR
20 Brain CT	29.193%	89.448%	31.438%	99.718%
100 Brain MRI	30.251%	93.337%	33.218%	99.816%

As explained before in Section 3, the proposed MARC4-264 technique provides a smaller number of iterations that corresponds to a faster encryption/decryption process. Finally, the computational costs, in terms of average run times, of both CAT-AES and the proposed MARC4-264 are reported in Table 5. The average run times for the proposed MARC4-264 technique are calculated using the $k_1 = 96,120$ iterations for both datasets, respectively. The results reported in Table 5 show that the use of the BHPF preprocessing phase has a negligible effect on the overall computational cost of the proposed MARC4-264. It is also seen that the proposed MARC4-264 techniques have achieved a significant reduction of computational cost in comparison to the original CAT-AES technique.

Table.5. average of run time for two techniques of 20 Brain CT & 100 Brain MRI in seconds

	Cat-AES	**Proposed MARC4-264**
20 Brain CT	75,3729	35,2483
100 Brain MRI	435,8619	135.7762

The proposed technique is also compared with recent chaotic-based encryption techniques [16-18], according to Table .6. It becomes clear to medical image encryption techniques that our technique is better than among the three systems in terms of comparative factors (the correlation coefficient, NPCI, and UACI). Accordingly, we recommend using the proposed technique in addition to that NPCR is ∞.

Table.6: comparison for fourth techniques based on CC, NPCR, and UACI

	fractional DCT with chaotic function	**Hybrid Chaotic DNA Diffusion**	**fourth-order chaotic system**	**The Proposed technique**
The correlation coefficient	0.07856	0.05431	0.00321	0.00046
NPCR	99.04316%	99.00129%	99.05127%	99.98774%
UACI	33.2910%	32.3167%	32.1823%	33.67810%

5. Conclusion and Future Scope

CAT-AES and Proposed MARC4-264 were used in this paper. Their algorithms were applied on two datasets of DICOM images: 20 brain CT images, 100 brain MRI images. The images were evaluated by the absolute correlation coefficient, UACI, and NPCR. The absolute correlation coefficient was equal to zero when encrypting with Proposed MARC4-

264 on 13 out of 20 of the brain CT and 81 out of 100 of the brain MRI.it is mean high uncorrelated between the original images and encrypted images. The MARC4 appears high-intensity DICOM images and has shown enhancements to the encryption quality.

Arnold's cat map tests for images were only finished on square ones; however, it has been proposed in [11] to enlarge a non-square image into a square and use a pseudo-random number generator to pad the more pixels. A different dimensional cat map such as the one used in [8] could also be used for pre-encryption to see how this affects the encryption quality. Future work will test for images of different dimensions, color spectrum, bit intensity.

References

[1]. Dongare, Ashish S., A. S. Alvi, and N. M. Tarbani. "An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application [J]." *International Research Journal of Engineering and Technology (IRJET)* Vol: 04 no: 04 (2017).

[2]. Debbarma, Nikhil, Lalita Kumari, and Jagdish Lal Raheja. "2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation." *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* vol.2, no. 4 (2013).

[3]. Khadega Khaled, Mohamed A. Wahby Shalaby, and Khaled Mostafa El Sayed, "Automatic Fuzzy-based Hybrid Approach for Segmentation and Centerline Extraction of Main Coronary Arteries." International Journal of Advanced Computer Science and Applications, vol 8, no 6. pp. 258-264, 2017

[4]. Bhardwaj, Rupali, and Vaishalli Sharma. "Effective Image Encryption Technique through 2D Cellular Automata." In *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*, pp. 39-46. Springer, Singapore, (2018) https://doi.org/10.1007/978-981-10-3373-5_3.

[5]. Abood, May H. "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms." In Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp. 86-90. IEEE, (2017.)

[6]. Sunil Kumari1 and Kavita Kathuria, et al" A Review on Image Cryptography" International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 25, no. 01 (2015)

[7]. Ranjan, Kumar HS, Safeeriya SP Fathimath, Ganesh Aithal, and Surendra Shetty. "A Survey on Key (s) and Keyless Image Encryption Techniques." *Cybernetics and Information Technologies* vol. 17, no. 4, pp: 134-164 (2017) https://doi.org/10.1515/cait-2017-0046 .

[8]. AlZain, Mohammed A., and Osama S. Faragallah. "Efficient Chaotic Tent Map-based Image Cryptosystem." International Journal of Computer Applications 975 (2017).

[9]. Bhogal, Ranvir S., Baihua Li, Alastair G. Gale, and Yan Chen. "Medical image encryption using chaotic map improved advanced encryption standard." In I.J. Information Technology and Computer Science, vol 8, pp: 1-10(2018) https://doi.org/10.5815/ijitcs.2018.08.01

[10]. Dogra, Ayush, and Parvinder Bhalla. "Image sharpening by Gaussian and Butterworth high pass filter." *Biomedical & Pharmacology Journal* 7, no. 2, pp:707-713 (2014). https://doi.org/10.13005/bpj/545

[11]. Bhardwaj, Rupali, and Vaishalli Sharma. "Effective Image Encryption Technique through 2D Cellular Automata." In *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*, pp. 39-46. Springer, Singapore, (2018) https://doi.org/10.1007/978-981-10-3373-5_3.

[12]. JINDAL, Poonam; SINGH, Brahmjit. "Optimization of the security-performance tradeoff in the RC4 encryption algorithm." *Wireless Personal Communications*, no.92.3, pp: 1221-1250 (2017).

[13]. https://sourceforge.net/p/openil/svn/1603/tree/trunk/Test%20Images/DICOM/

[14]. https://zenodo.org/record/16956#.XWbSo-KxXIV

[15]. Wu, Yue, Joseph P. Noonan, and Sos Agaian. "NPCR and UACI randomness tests for image encryption." *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)* 1, no. 2, pp: 31-38 (2011).

[16]. KUMAR, Sumit; PANNA, Bhaskar; JHA, Rajib Kumar. "Medical image encryption using fractional discrete cosine transform with chaotic function." Medical & biological engineering & computing, vol.57, no.11, pp: 2517-2533(2019).

[17]. DAGADU, Joshua C.; LI, Jian-Ping; ABOAGYE, Emelia O. "Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion."Wireless Personal Communications, vol.108, no.1, pp: 591-612 (2019).

[18]. LIU, Jizhao, et al. "A novel fourth-order chaotic system and its algorithm for medical image encryption." Multidimensional Systems and Signal Processing, vol.30, no.4, pp: 1637-1657 (2019).