JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A ENCRYPTION ALGORITHM FOR MEDICAL IMAGES USING IMAGE BLOCKS AND CHAOS

P. Sai Pavani[1], Dr. U.V. Ratna Kumari[2]
[1]Student, MTech, JNTUK, Andhra Pradesh, India
[2]Professor, JNTUK, Andhra Pradesh, India

Abstract :

Telehealth and technology adoption for diagnosing diseases have become crucial during pandemic. Remote diagnosing of diseases requires medical images and their transmission through network. So, securing these medical images is important for both correct diagnosis and confidentiality. This paper introduces a encryption algorithm designed to secure medical images. To achieve this, the medical image is split into blocks. Subsequently these images undergo series of transformations like data substitution and scrambling. The jumbled picture is then decoded using a key generated with the use of a chaotic logistic map and tent map. We do thorough analyses of the security and time complexity of our suggested encryption technology to ensure its efficacy. Security assessment employs various metrics, including entropy, correlation coefficient, histogram differential attacks, key sensitivity, key space, and Peak Signal-to-Noise Ratio (PSNR). These measurements collectively evaluate the security of a system. The findings show that medical picture encryption provides a significant boost to security. Furthermore, a comparative analysis is conducted with several existing methods, revealing that our proposed encryption algorithm surpasses the performance of these methods in safeguarding medical images.

Key words : Encryption, chaos, logistic map, tent map

Introduction:

With quick advancements in medical technology, diagnosing diseases using medical images became common. These medical images are transmitted over different networks, so they need high protection to avoid any unauthorized usage. As healthcare data consists of more sensitive data when compared to other types of data, if unauthorized sources are able to obtain the information of the medical images, it may lead to many severe problems like loss of privacy of patient. If the data in the medical images is prone to any little changes, it may threaten the patients life due to incorrect diagnosis. It may also lead to faulty usage of such confidential data. So, these images are to be transmitted securely. We can secure images using different methods like image steganography, image watermarking, image encryption. Image steganography [1], [2] and image watermarking [3], [4] are used in secure medical image transmission. But the most highly effective method in securing images is encryption.

Encryption algorithms primarily employ two key steps: confusion and diffusion. Image encryption is a procedure which converts plain image into cipher image by using secret key. To restore original plain image from encrypted image, we need that secret key without which original image cant be obtained. So, only the receiver with the secret key will be able to get the data in the image which leads to secure transmission. Medical images are usually characterised by high correlation between neighbouring pixels and high data redundancy. So, the encryption algorithm used for medical images must be able to reduce correlation and redundancy.

Many encryption algorithms for medical images were proposed earlier like [5] - [10] which helped in reducing correlation. To improve randomness and encryption efficiency, Kamal et al. introduced a method in [6] that makes use of logistic maps and scrambling. In [7], Shankar et al proposed algorithm which used chaos function to encrypt medical images. In their work cited as reference [10], Chen et al. introduced a comprehensive optical encryption

framework that utilizes Shearlets and double random phase encoding (DRPE) for the encryption of medical images. Hua et al. [9] developed a novel technique for encrypting medical images using a mixture of fast scrambling, pixel-versatile dissemination, and irregular information inclusion. These algorithms are able to reduce redundancy and correlation.

Yet some existing chaotic systems may exhibit discontinuous range of chaotic parameters and may be liable to attacks. So, the algorithm must be able to increase randomness and reduce correlation thereby increasing the encryption efficiency. This paper proposes a algorithm which helps reduce correlation by using data substitution using S-box which is generally used in traditional encryption techniques to improve randomness and scrambling technique which helps reduce correlation coefficient. To improve efficiency, this algorithm uses different chaotic maps like logistic map and tent map to produce key.

This paper contributions are summarized as

A simple image splitting technique is used. Data substitution using S-box which is a step involved in AES is used to generate randomness.
Both logistic map and tent map are used in key generation to make it robust against differential attacks.

In this paper, Section 2 explains the proposed method in detail. Section 3 discusses the analysis and simulation results. The conclusion is given in Section 4.

Proposed Method :

The proposed algorithm for secure medical image transmission consists of encryption and decryption steps. The plain image is encrypted using a secret key and it can be reobtained by decrypting the encrypted image using only that secret key.

Encryption :

In our algorithm, encryption consists of four steps. The first step is Image splitting into blocks. The second step consists of data substitution using S-box and scrambling. Key generation is the third step with diffusion as fourth step. The steps involved in encryption algorithm is given in Fig 2.

Image Splitting :

The plain image is split into non overlapped blocks of equal size. The block sizes can be selected by user. The block size can be 16,32,64. The plain image can be of any size. This step will split the image without losing data or quality of the image.

Confusion :

As the medical images have high correlation between neighbouring pixels, the pixels arrangement must be changed to reduce correlation and improve security. In this algorithm,
1.Data substitution using S-box is performed for all pixels for five rounds.
2.we change the pixels arrangement by applying zigzag pattern to the blocks. 3.Then the blocks are rotated by 90^{o} to produce scrambled image X . The zigzag pattern used in our algorithm is given below

The zigzag pattern used in our algorithm is given by the pattern [1,2,5,9,6,3,4,7,10,13,14,11,8,12,15,16] if the original array is [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16]

Key generation :

In our algorithm, two types of logistic maps are used to produce the key. The maps used are logistic map and tent map.

The logistic map is defined as

$$Y_{n+1} = aY_n(1-Y_n) \quad (1)$$

Where a is control parameter between $0 \leq a \leq 4$ and Yn is an output sequence between $0 < Y_n < 1$. When $a \in [3.57, 4]$ the map is in a state of disarray.

The initial value of logistic map Y_0 depends on our original plain image P.

$$Y_0 = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} P(i,j)}{M \times N \times 255} \quad (2)$$

Here, M, N refers to number of rows and columns of P respectively.

The logistic map (eq. 1) is iterated N_0+MN times and first N_0 elements are skipped to produce sequence S_1 of size MN.

The tent map is defined as

$$X_{n+1} = \begin{cases} rX_n, & X_n < 0.5 \\ r(1-X_n), & X_n \geq 0.5 \end{cases} \quad (3)$$

Here, r is control parameter, the tent map behaves as chaotic if $r \in [1.4, 2]$ and $X_0 \in [0,1]$. The tent map(eq. 3) is iterated $N_0 + MN$ times and first N_0 elements are skipped to get S_2 sequence of size MN.

The sequence S is generated by using alternate values from S_1 and S_2 which has a size of MN.

Then the key is generated by using

$$K(i) = \mathrm{mod}\left(\mathrm{floor}\left(S(i) \times 10^{14}\right), 256\right), \quad i = 1 : MN \quad (4)$$

Diffusion :

In this step, bit wise XOR operation is performed between key K obtained from eq 4 and scrambled image X obtained after confusion step to obtain our required encrypted image.

Decryption :

Decryption is applied to obtain the original plain image from encrypted image. The process involves

(i) Bit wise XOR operation between key and encrypted image.
(ii) The inverse operation of rotation is performed and un zigzag the pattern for all blocks. (iii) Inverse S-box is used to remove newly added data. Then the decrypted image is obtained.

Algorithm:

The proposed encryption algorithm is given as

Input: Plain image P with size M x N, parameter N_0, a for logistic map and parameters r, X_0 and N_0

1. Divide P into non overlapping blocks of equal size $h = 2^n$, where n values from 4,5,6.
2. Perform data substitution using S-box for five rounds for each pixel.
3. Perform Zigzag pattern and rotation of 90^0 for each and every block to obtain scrambled image X.
4. Generate initial condition of logistic map using eq 2.
5. Iterate the chaotic map (eq.1) $N_0 + MN$ times, and then discard first N_0 elements to get a new sequence S_1 with size MN.
6. For the given X_0 value, obtain tent map and iterate it (eq. 3) $N_0 + MN$ times, and then discard first N_0 elements to get a new sequence S_2 with size MN.
7. Obtain sequence S by using S_1 and S_2 which has size of MN.
8. For i = 1: MN do 9.
   K(i) = mod (floor (S(i) × 1014), 256)

10. End for
11. Make a 1D pixel vector Y out of the matrix X.
12. $E = Y \oplus K$
13. Convert E into 2D matrix Z

Output: Encrypted image Z

Steps:

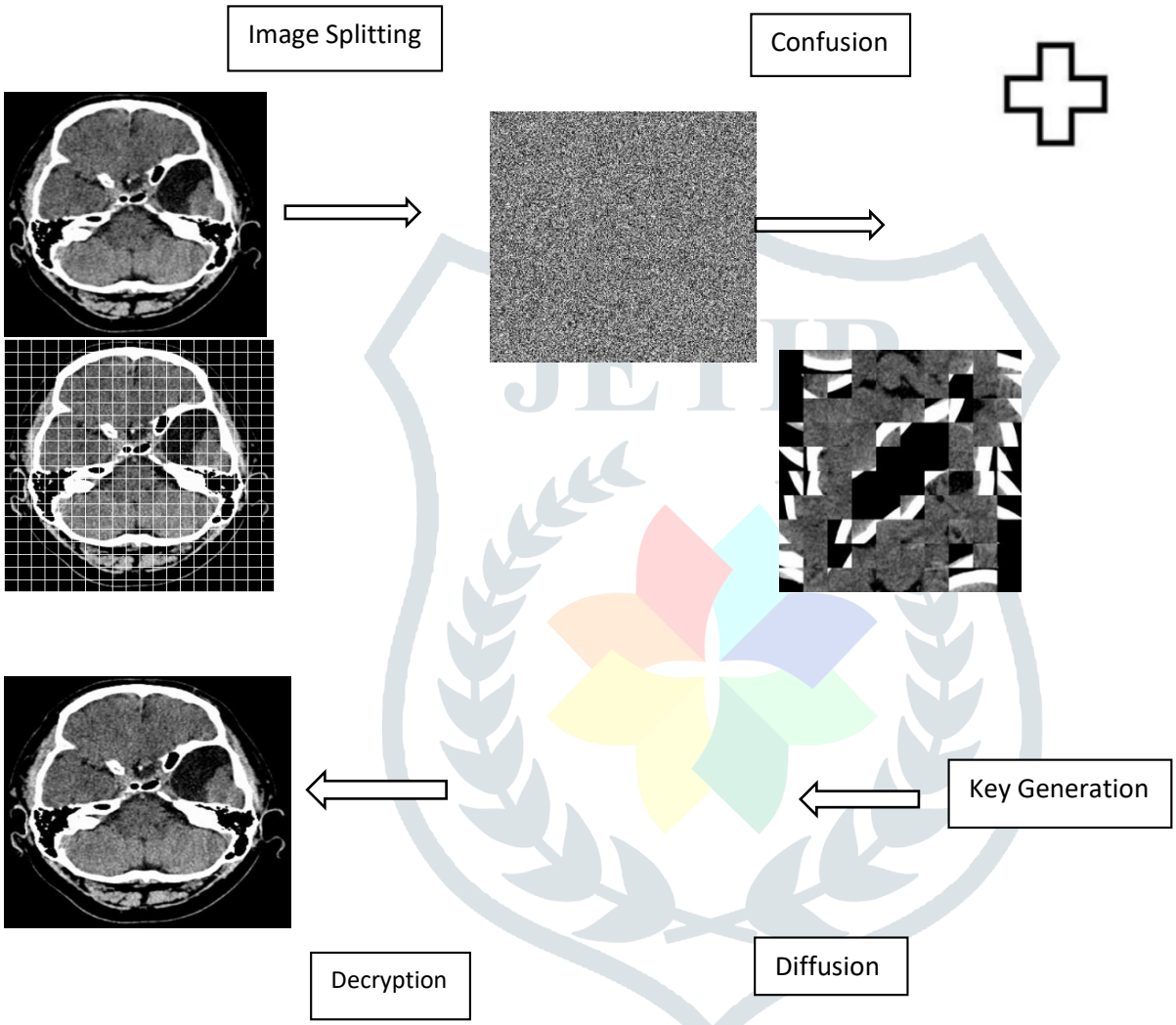
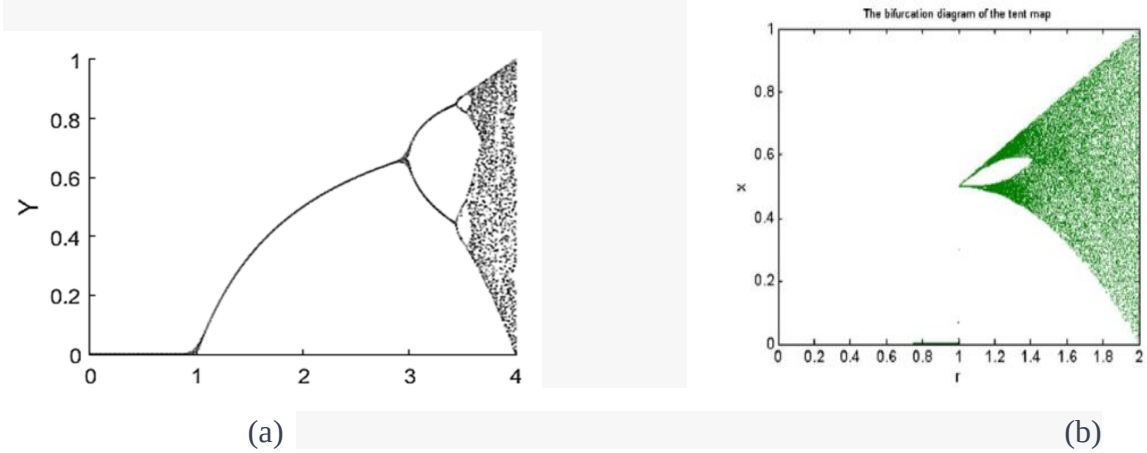


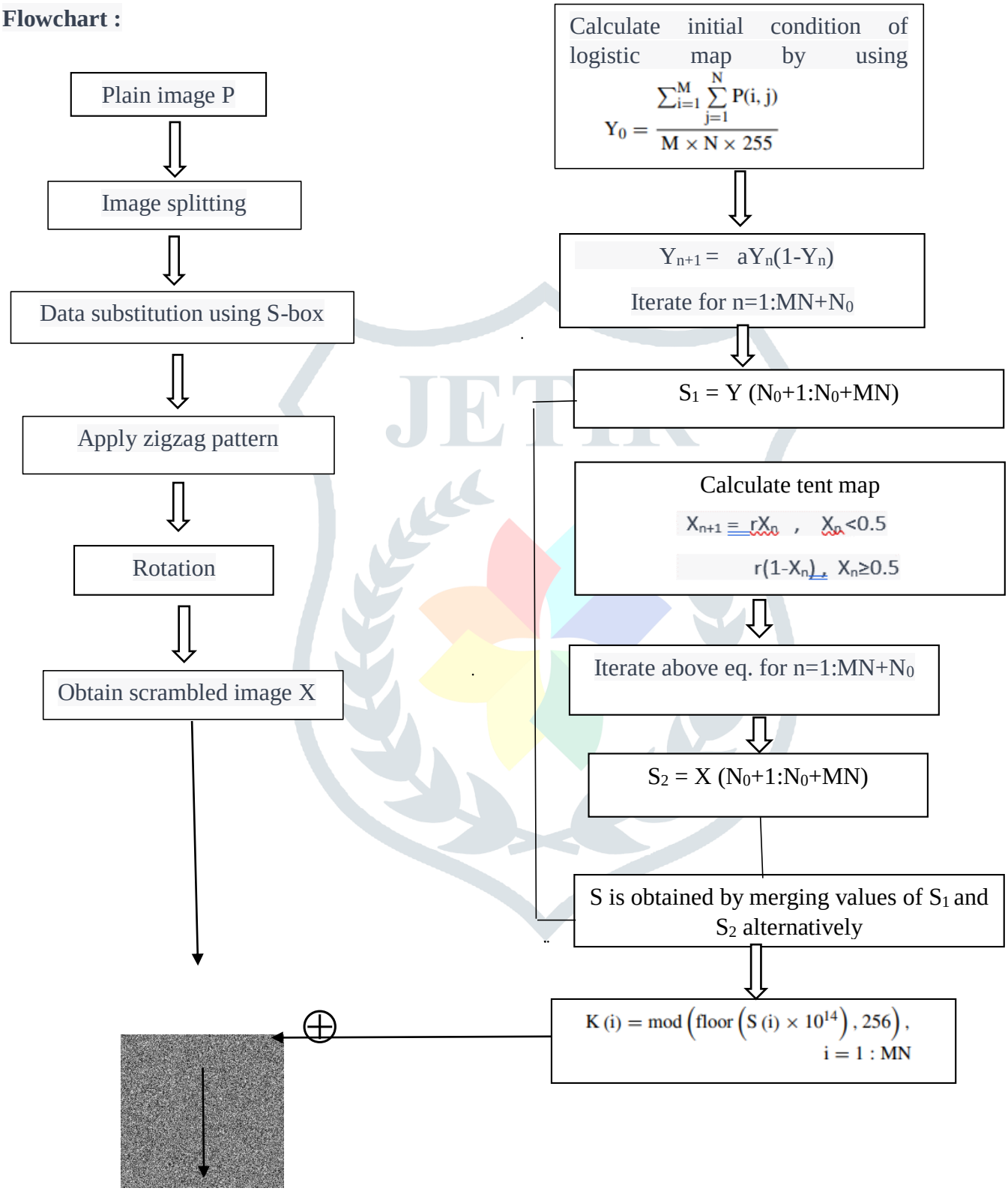
Fig 1: Encryption algorithm block diagram



(a) (b)

Fig 2: Bifurcation diagram of (a) Logistic map (b) Tent map

Flowchart :



Results :

The efficiency of the algorithm is tested using entropy, image histogram, correlation coefficient, differential attack, key sensitivity, PSNR which are used to test the security of algorithm and time complexity. The test images are obtained from [11], [12].

The algorithm is executed using Python with parameters as

Size of split block : 32x32

No. of rounds of data substitution :5

Logistic map values : a= 3.9 , N_0= random integer (1000 to 2000)

Tent map values : r= 1.5 , X_0=0.5, N_0 = random integer(1000 to 2000)

(a) (b) (c)

Fig 3:Test images **(a)** Img1 **(b)** Img2 **(c)** Img3

Entropy :

Information entropy is defined as the amount of randomness or uncertainty of an image. For greyscale images, the maximum value of entropy is 8. Higher the value of entropy, higher the randomness of image.

Entropy is given by

$$H(m) = \sum_{i=1}^{w} P(m_i)\log_2 \frac{1}{P(m_i)}$$

Where P(m) is probability of m.

The entropy values of encrypted images using our algorithm are given in Table1. The entropy values of encrypted images using other algorithms is given in Table2. As we can see, the proposed algorithm has higher entropy values compared to other algorithms. Here, OI- Original image and EI- Encrypted image

Table 1 : Encrypted images entropy

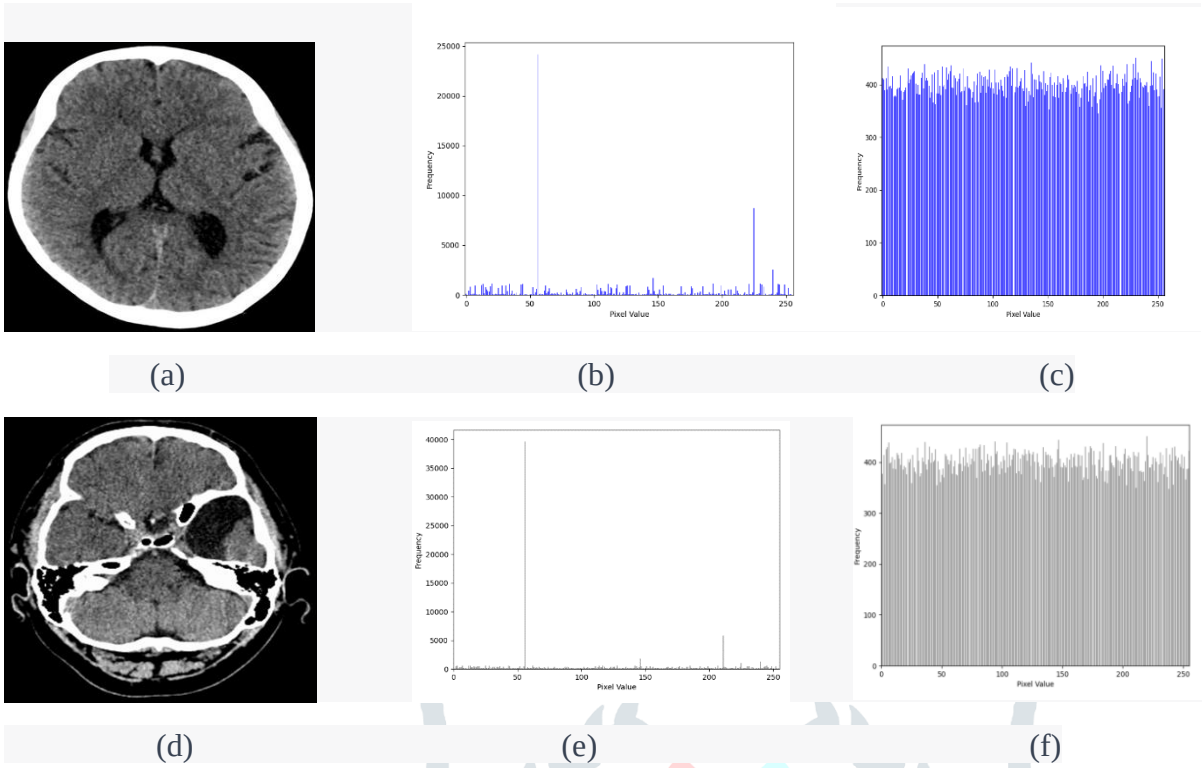
Test image	OI Entropy	EI Entropy
Img1	5.900	7.9991
Img2	5.438	7.9982
Img3	5.041	7.9990

Table 2 : Entropy of our algorithm and other algorithms

Method	Entropy
Proposed	7.999
[6]	7.999
[13]	7.909
[16]	4.475

Image histogram :

The image histogram is representation of pixels distribution in image. The histogram of an encrypted image should be flat and should not be similar to plain image. The histogram of the original plain images and encrypted images using our algorithm is shown in figure1. As we can see, the histogram of plain images and encrypted images are not similar to each other and encrypted image histogram is flat.



(a) (b) (c)

(d) (e) (f)

Fig 4: **(a)** Img1 **(b)**Histogram of (a) **(c)**Histogram of encrypted image of (a) **(d)** Img2 **(e)**Histogram of (d) **(f)**Histogram of encrypted image (d)

Correlation coefficient :

The encryption algorithm have to generate encrypted images with low correlation between neighbouring pixels to have more efficiency. As medical images have high correlation, our algorithm is using both scrambling and data substitution to reduce the correlation. The range of correlation coefficient is from -1 to 1. Correlation coefficient of 1 means that the neighbouring pixels are similar.

$$r_{A,B} = \frac{E((A - E(A))(B - E(B)))}{\sqrt{D(A)D(B)}}$$

$$E(A) = \frac{1}{s}\sum_{i=1}^{s} A_i$$

$$D(A) = \frac{1}{s}\sum_{i=1}^{s} (A_i - E(A))^2$$

Where A,B are grey values of two neighbouring pixels.

S is total number of selected pairs

The correlation coefficient values of plain and encrypted images in horizontal(H), vertical(V), diagonal(D) directions is given in Table3. The values of this algorithm is compared with other methods. The proposed algorithm values shows reduction in adjacent pixels correlation for encrypted images.

Table 3 : Correlation Coefficient values

Test image	Direction	Plain image	Encrypted image
Img1	H	0.9802	-0.018
	V	0.9780	0.0004
	D	0.963	-0.013
Img2	H	0.983	0.0002
	V	0.991	-0.0009
	D	0.997	-0.0005
Img3	H	0.970	-0.024
	V	0.963	0.0001
	D	0.940	-0.0014

Differential attack :

Differential attack is used to guess the information of a image by comparing variations in plain image and encrypted image and obtain the key. To assess the efficiency of algorithm, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) used. It gives how well the algorithm is able to resist differential attack. The NPCR and UACI values of our algorithm are also compared with other algorithm. The NPCR and UACI are calculated as

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100(\%)$$

$$D(i,j) = \begin{cases} 0 & \text{if } E_1(i,j) = E_2(i,j), \\ 1 & \text{if } E_1(i,j) \neq E_2(i,j), \end{cases}$$

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100(\%)$$

Where M,N are image width and height

E1,E2 are two encrypted images from plain image and modified plain image

The optimal values of NPCR is 99.6094% and UACI is 33.4635%

The values of NPCR and UACI is given in Table6. The values obtained are near to the ideal values.

Table 4: NPCR and UACI values

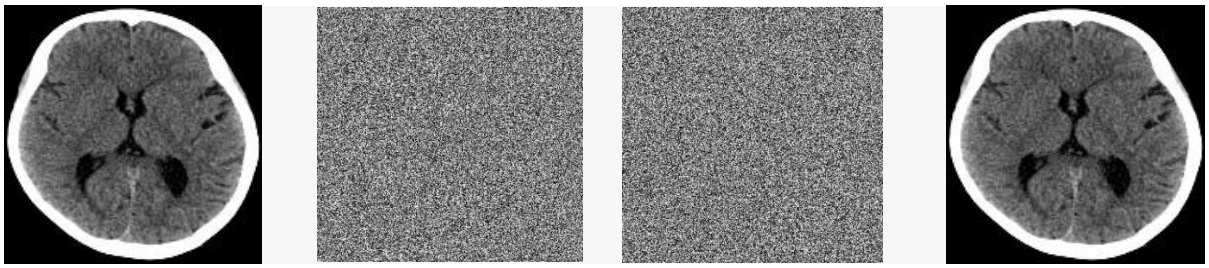
Test image	NPCR	UACI
Img1	99.6367	33.3526
Img2	99.6025	33.4058
Img3	99.593	33.450

Table 5: Comparison with other methods

Method	NPCR	UACI
Proposed	99.6367	33.4058
[6]	99.6010	33.4389
[14]	99.532	33.450
[9]	99.6067	33.4954

Key Sensitivity :

Any slight change in key must not be able to produce the original plain image from encrypted image or else attackers may obtain plain images with similar key. We generated a similar key by making slight change in Y_0 by making Y_0 as Y_0+10^(-10). The new key is used in decryption and results are shown in figure. As we can see, it wasn't able to reconstruct original image. While the original key is able to obtain original image.



(a) (b) (c) (d)

Fig 5: (a) Original image **(b)**Encrypted image with first key **(c)**Decrypted image with second key **(d)** Decrypted image with first key

Encryption efficiency :

The difference between original and encrypted image is given by Peak Signal to Noise ratio (PSNR). It is given by

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\text{MSE}}\right) \text{(db)}$$

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|\text{OI}(i,j) - \text{EI}(i,j)|^2$$

Where OI is original image

EI is encrypted image

The values of PSNR is given in Table. The lower values obtained show significant difference between original and encrypted image.

Table 6: PSNR values

Image	Img1	Img2	Img3
PSNR	5.991	5.679	5.284

Time Complexity :

The total time complexity of our encryption algorithm is estimated by using time complexity of each step in the encryption process. The time complexity of image splitting and scrambling is given as $O((M \times N)/k^2)$, where k is the block size of the original image. The time complexity of key generation and diffusions steps is given as O(M x N). So, the time complexity of overall algorithm is O(M x N).

Conclusion :

This paper introduced a medical image encryption algorithm which is based on image blocks and chaos. The performance and efficiency of the algorithm is tested for entropy, image histogram, correlation coefficient, differential attack, key sensitivity. The values are compared with existing methods. The results of this algorithm show that it has good efficiency in medical image encryption.

References :

[1] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, ''Medical JPEG image steganography based on preserving inter-block dependencies,'' Comput. Electr. Eng., vol. 67, pp. 320–329, Apr. 2018.

[2] M. A. Usman and M. R. Usman, ‘‘Using image steganography for providing enhanced medical data security,’’ in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018.

[3] K. M. Hosny, M. M. Darwish, K. Li, and A. Salah, ‘‘Parallel multi-core CPU and GPU for fast and robust medical image watermarking,’’ IEEE Access, vol. 6, pp. 77212–77225, Dec. 2018.

[4] K. M. Hosny and M. M. Darwish, ‘‘Resilient color image watermarking using accurate quaternion radial substituted chebyshev moments,’’ ACM Trans. Multimedia Comput., Commun., Appl., vol. 15, no. 2, pp. 1–25, Jun. 2019.

[5] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, ‘‘A new simple chaotic system and its application in medical image encryption,’’ Multimedia Tools Appl., vol. 77, no. 17, pp. 22787–22808, Sep. 2018.

[6] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," in *IEEE Access*, vol. 9, pp. 37855-37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[7] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, and W. Wu, ‘‘An efficient optimal key based chaos function for medical image security,’’ IEEE Access, vol. 6, pp. 77145–77154, 2018.

[8] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, ‘‘Novel medical image encryption scheme based on chaos and DNA encoding,’’ IEEE Access, vol. 7, pp. 36667–36681, 2019.

[9] Z. Hua, S. Yi, and Y. Zhou, ‘‘Medical image encryption using highspeed scrambling and pixel adaptive diffusion,’’ Signal Process., vol. 144, pp. 134–144, Mar. 2018.

[10] M. Chen, G. Ma, C. Tang, and Z. Lei, ‘‘Generalized optical encryption framework based on shearlets for medical image,’’ Opt. Lasers Eng., vol. 128, May 2020, Art. no. 106026.

[11] Category: Computed Tomography Images of Mikael Häggström’s Brain. Accessed: Feb. 9, 2021. [Online]. Available: https://commons.wikimedia.org/wiki/Category:Computed_tomography_images_of_Mikael_H%C3%A4ggstr%C3%B6m%27s_brain

[12] The Stanford Volume Data Archive. Accessed: Feb. 9, 2021. [Online]. Available: https://graphics.stanford.edu/data/voldata/

[13] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, ‘‘A novel image encryption scheme based on DNA sequence operations and chaotic systems,’’ Neural Comput. Appl., vol. 31, no. 1, pp. 219–237, Jan. 2019.

[14] J. Chandrasekaran and S. J. Thiruvengadam, ‘‘A hybrid chaotic and number theoretic approach for securing DICOM images,’’ Secur. Commun. Netw., vol. 2017, Jan. 2017, Art. no. 6729896.

[15] X. Wang and C. Liu, ‘‘A novel and effective image encryption algorithm based on chaos and DNA encoding,’’ Multimedia Tools Appl., vol. 76, no. 5, pp. 6229–6245, Mar. 2017.

[16] S. Kumar, B. Panna, and R. Kumar, ‘‘Medical image encryption using fractional discrete cosine transform with chaotic function,’’ Med. Biol. Eng. Comput., vol. 57, no. 11, pp. 2517–2533, 2019.

[17] A. Banu S and R. Amirtharajan, ‘‘A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach,’’ Med. Biol. Eng. Comput., vol. 58, no. 7, pp. 1445–1458, Jul. 2020.

[18] M. K. Hasan *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," in *IEEE Access*, vol. 9, pp. 47731-47742, 2021, doi: 10.1109/ACCESS.2021.3061710.