Biomedical & Pharmacology Journal, June 2018. Vol. **11**(2), p. 897-906

3D Lorenz Map Governs DNA Rule in Encrypting DICOM Images

K. Abinaya Kumari[1], B. Akshaya[1], B.Umamaheswari[2], K.Thenmozhi[1], Rengarajan Amirtharajan[1] and Padmapriya Praveenkumar[1]

[1]ECE department, SASTRA Deemed University, Thanjavur, India.
[2]JECRC, Jaipur, India.

http://dx.doi.org/10.13005/bpj/1446

(Received: 18 April 2018; accepted: 09 June 2018)

This paper introduces a framework for the secure encryption of healthcare images. The objective of this paper is to encrypt medical images based on Deoxyribo Nucleic Acid (DNA), 3D Lorenz chaotic map, BITXOR operations. The different keys are employed to provide confusion, permutation, encoding and diffusion operations in the encryption procedure to provide uncorrelated image pixels. The proposed algorithm uses 3D Lorenz attractor as chaotic system for encrypting colour Digital Imaging and Communication in Medicine (DICOM) images. Further the encrypted image will be validated using encryption quality to evaluate the security analysis.

Keywords: DICOM, DNA, Lorenz map, NPCR, UACI.

With the fast advancement in technology and its usage in the field of high speed networks, the security prospective the encryption is essential to keep the health information safe. When transmitted through public channel, this sensitive medical records needs to be secured to prevent damage from attackers. Image encryption plays a key role in protecting those images and hence provides information security in the field of medical imaging. Kanso *et al*. [1] proposed an algorithm scheme based on traditional encryption scheme with increase in algorithm rounds to encrypt the digital image but these schemes are not appropriate for encrypting the DICOM images owed to their characteristics like, the size of the data is huge, correlation between the pixels is much stronger and redundancy of the data is high. To provide more uncorrelated pixels on encrypted image chaotic map is used for efficient encryption. The main aim of migrating towards the chaos system is, due to its high ergodicity , chaotic system is completely deterministic, its initial seeds are extremely sensitive hence small changes in initial seeds will forever alter the future of chaos system and so on, therefore it has been suggested for encrypting the medical images as considered in[2-5]. Because of this characteristics, analysing and predicting the chaos is difficult. Ravichandran *et al*[6] discussed that recently DNA computing plays a major role in the domain of cryptography for encrypting the digital images and more random keys are generated using multiple chaotic maps . Li *et al*[7] developed an algorithm that uses DNA based computation, it's advantage are massive parallelism, power consumption is extremely low, capacity for storing the data is large and offers unbreakable cryptosystem. Niyat[8] and kalpana[9] proposed a scheme with basic idea of encryption based on

DNA rule set. In the first stage is to encode the pixels of plain image into DNA sequence. Second stage is to encode using DNA rules like addition, subtraction or XOR operations to form the pixels of encrypted image.

Wang *et al*[10] and Enayatifar *et al*[11]. discussed about DNA encoding rule with algebraic operations like addition operation for encrypting images. Liu *et al*[12] proposed an algorithm to yield better entropy for the colour images. Fan *et al*[13] uses bit- level permutation and diffusion to boost the protection of the images while ensuring integrity. To ensure the robustness of algorithm, the ideal value of NPCR and UACI is discussed in[14, 15]. Jangid *et al*[16] algorithm gives the cryptographic approach using DNA rule set between plain and cipher output. To highly increase the security of encryption and to minimise BER of data an algorithm is proposed by Dang *et al*[17].

The proposed algorithm has the advantage of achieving good Quality metrics compared with available literature and also the algorithm results shows that the projected algorithm is proficient of resisting a variety of known attacks therefore, appropriate for enhancing security. The content of this paper is discussed as follows; in Section II the related work is discussed. Section III gives the design information of the proposed image encryption algorithm. In Section IV, simulation results are illustrated and in Section V, security features of the algorithm is analyzed. Finally, Section VI is ended with the conclusion part.

Related work

Lorenz chaotic system

3D – Lorenz map equations is as follows,

$$\begin{cases} dx1/dt = \alpha * (y1 - x1) & (1) \\ dy1/dt = x1 * (\beta - z1) - y1 & (2) \\ dz1/dt = (x1 * y1) - (\mu * z1) & (3) \end{cases}$$

In equations (1), (2) and (3) : α , β and μ are the control parameters whereas x1, y1 and z1 are the initial parameters. α , β and μ equals to 10, 28 and 8 /3 respectively and initial values are equal to 1, then 3D Lorenz map is in the chaotic state as in Fig 1a, hence it produces three different chaotic sequences.

DNA Encoding

DNA encoding is the process of encoding the binary pixel values into sequences. It has four nucleic acid bases such as Adenine ("A"), Cytosine ("C"), Guanine ("G") and Thymine ("T"). Here, "A" is complement to "T" and "G" is complement to "C" because in 2^1 binary combination, "0" and "1" are complement to each other and in 2^2 binary combinations "00" and "11" are complement to each other, "01" and "10" are also complement to each other. In general rule, "A" corresponds to "00", "C" corresponds to "01", "G" corresponds to "10" and "T" corresponds to "11" then the coding schemes can be of 24 kinds, still only 8 satisfies the complementary rule as shown in table.1 [10]. For easy understanding an example is considered, if pixel value is "255" its binary representation is" 11100001" then using general rule this binary value is encoded as "TGAC" each alphabets representing 2-bit respectively.

Addition operation for dna sequence

With the rapid development of computations in DNA, the algebraic operations like Addition operation is done. Once the pixels are DNA encoded then addition is done between the DNA encoded data and DNA encoded key sequence as shown in table.2 .

Proposed image encryption algorithm

Section III gives the details of designing the proposed image encryption. The procedure of algorithm includes 4 stages namely confusing, permuting, encoding and diffusing the image in order to enhance the security as in Fig 1b.

The encryption steps are described as follows,

Step1: First, 8-bit RGB DICOM image is used as the plain image IM and it is of size IM(M, N, 3) and S=M*N where M = no. of rows in input image and N = no. of columns in input image i.e. plain image

Step2: Split the colour DICOM image IM of size (M, N, 3) into three colour planes as IM_red, IM_green and IM_blue. Separated three colour planes each of size (M,N,1).

IM_ red = {R1, R_2, ..., R_{M*N} }
IM_ green = {G1, G_2, ..., G_{M*N} }
IM_ blue = {B1, B_2, ..., B_{M*N} }

Step3: Now, three sequences namely X sequence, Y sequence and Z sequence are generated using 3D Lorenz map. s=rows*columns of plain image and generating sequences as follows,

X= {Xi, Xi+1, Xi+2,....., Xi+(s-1) }
Y= {Yi, Yi+1, Yi+2,....., Yi+(s-1) }
Z= {Zi, Zi+1, Zi+2,....., Zi+(s-1) } ,
where i =1

Now, quantize the X sequence as Key1 = floor(mod (X*10^14, 256)) and similarly quantize Y and Z to generate other keys i.e. Key2 and Key3.

Step4: Sorting the elements of X, Y and Z sequences in ascending order and taking the Index values as Index1, Index2 and Index3 as in Fig 2a and b.

Step5: Confusing three colour planes IM_red, IM_green and IM_blue with corresponding Index1, Index2 and Index3.

Step6: By using the confused image, Permutation is done for three R, G and B planes as follows[16],

• Let IM = { IM(ii, jj) } denote the grayscale plain image, where ii=1 to M and jj=i to N.

aq(ii, jj) = de2bi (IM(ii, jj)

where function de2bi converts decimal values to binary values.

b = aq(ii , :)

where aq(ii , :) = {aq(ii , 1), aq(ii , 2),.....,aq(ii , M)} be the i^{th} row of aq, then

c=sum (b)

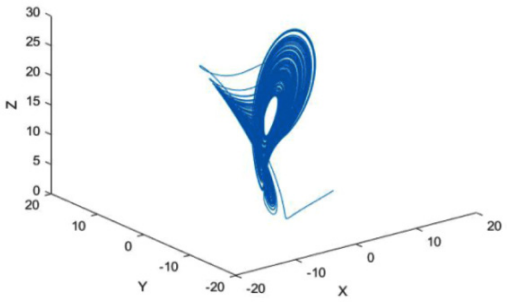


Fig.1a. 3D-Lorenz chaotic map

• Taking mod,

P_{mod} = mod (c, 2).

•Now, if $P_{mod} = 0$,

a(ii , :) is circular shifted towards right with Key steps

If $P_{mod} = 1$,

a(ii , :) is circular shifted towards left with same Key steps.

• Each group with 8-bits of vector is converted back into binary values, thus permuted image

PR_{img} = { PR_{img}(ii, jj) } is obtained as,

PR_{img} (ii , :) = bi2de (a(ii , :)

where ii=1 to M and jj=1 to N.

NOTE: Key1 is used for red plane, Key2 is used for green plane and Key3 is used for blue plane respectively.

Step7: BIT- XORing is performed for each R, G and B planes by using permuted image and corresponding key.

$$q(1) = PR_{img}(1) \oplus key(1) \quad ...(4)$$

where $\oplus$ symbol represents Bit-wise XOR operation.

$$q(k) = \sum_{k=2}^{S} q(k-1) \oplus PR_{img}(k) \quad ...(5)$$

and

$$X_R(k) = q(k) \oplus key(k) \quad ...(6)$$

where k= {1, 2, 3, 4,.....,S } and S=rows*columns of image.

Step8: BITXORed image of R, G and B planes and 3 keys are individually encoded using DNA encoding and added using addition rule.

Table 1. 8- Sets Of Encoding Rules For DNA

	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
00	A	A	T	T	C	C	G	G
011011	CGT	GCT	GCA	CGA	ATG	TAG	ATC	TAC

Table 2. Addition Rule For DNA

+	A	T	G	C
A	A	T	G	C
T	T	C	A	G
G	G	A	C	T
C	C	G	T	A

Step 9: Then it is decoded using DNA decoding rule.

Step 10: Finally, Diffusion is performed for each RGB planes to get cipher image as in Fig 3.

Each RGB planes is first bitxored with Key1 [row-wise],

P_{dif} = { P_{dif} (ii, jj) } , where ii=1 to M and jj=1 to N

...(7)

and

P_{dif} (ii , :) =DNA_{out} (ii , :) ⊕ key1 (ii , :)

...(8)

• Now, bitxoring the results of first stage with another key i.e Key2 [column-wise] is written as,

P_{dif} (: , jj) =P_{dif} (: , jj) ⊕ key2 (: , jj)

...(9)

Simulation results and security analysis

For experimental analysis, 3 colour DICOM images were considered. Encryption metrics like NPCR, UACI, and correlation were estimated to prove the strength of the proposed encryption scheme. Fig 4(a-e) and 5(a-e) shows the various stages output of the proposed algorithm. The proposed encryption algorithm is said to be superior, if it is indestructible in any cases and it should resist towards common attacks as discussed in this section and also this section demonstrates a security analysis on proposed encryption scheme.

Statistical attack analysis

It can be estimated by analyzing the pixels in the encrypted histogram, global entropy and correlation coefficients of encrypted image.

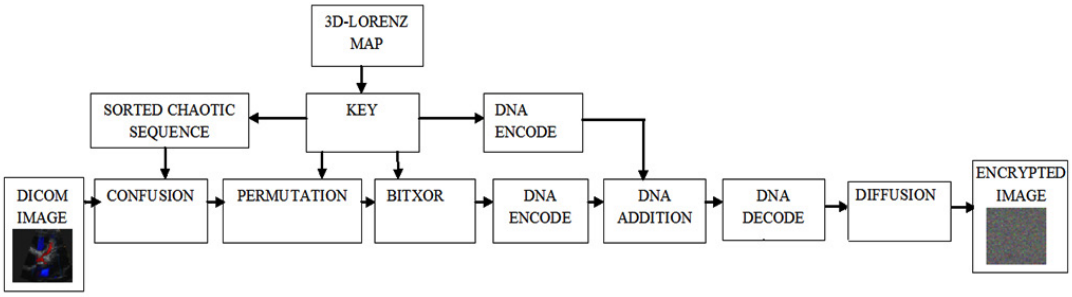


Fig. 1(b). Block description of the proposed Encryption scheme

0.2554	0.5989	0.9763	0.3855	0.8244	0.2909	0.7829	0.2985	0.8358
1	2	3	4	5	6	7	8	9

(a)

0.2554	0.2909	0.2985	0.3855	0.5989	0.7829	0.8244	0.8358	0.9763
1	6	8	4	2	7	5	9	3

(b)

Fig. 2. (a). Chaotic sequence with index; (b). Sorted chaotic sequence with index

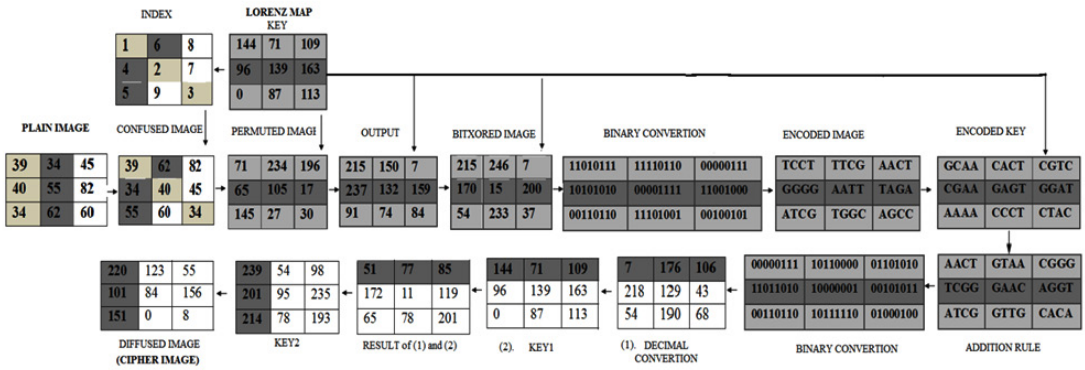


Fig. 3. Flowchart representation of the proposed algorithm

Entropy analysis

The Shannon entropy is adopted, in this case the randomness of random variable XX is measured as follows,

$$H(XX) = -\sum_{i=1}^{q} P(xx_i)\log(Pxx_i) \quad ...(10)$$

where each *Pxxi* is the possible value of *XX*. For M=8-bit data and q levels [q=2M], the range of entropy will lies in range [0,M]. If the entropy is little in the input data then the resultant key will have higher entropy. In general, entropy of the encrypted image should have value close to M, else if entropy value is lesser then there is a possibility of attack which can reduce the security of image transmission. Table.3 shows that all the values of each RGB planes for 3 test images are more closer to M and hence algorithm which is proposed is much efficient.

Image correlation analysis

Correlation analysis gives the similarities between two images (i.e).plain image and cipher image. In general, correlation lies in the range -1 to 1. If the value of correlation is close to negative values then algorithm has stronger ability of resisting statistical attack which is shown in Table.4. The following formulas are used to calculate the horizontal, vertical and diagonal correlations[13],

$$E_x(XX) = \frac{1}{N}\sum_{i=1}^{N} XX_i \quad ...(11)$$

$$Var(XX) = \frac{1}{N}\sum_{i=1}^{N} (XX_i - E_x(XX))^2 \quad ...(12)$$

$$Cov(XX, YY) = \frac{1}{N}\sum_{i=1}^{N} (XX_i - E_x(XX))(YY_i - E_x(YY)) \quad ...(13)$$

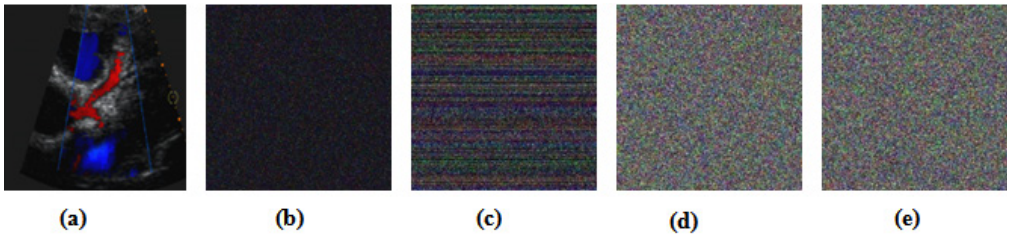


Fig. 4. Encryption results ;(a).Plain image(256x256) (b).Confused image (c).Permuted image (d).Bitxored image (e).Diffused image(Encrypted image)

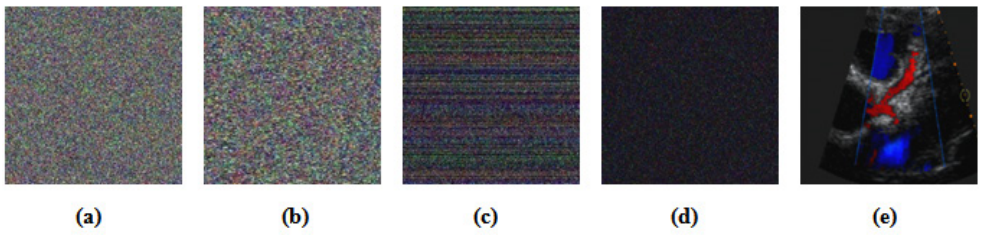


Fig. 5. Decryption results; (a).Encrypted image (b).Decrypt-Diffused image (c).Decrypt-Bitxored image (d).Decrypt-Permuted image (e).Decrypt-Confused image

Table 3. Entropy Analysis of 3 Test Images

Images		Plain Image	Cipher Image
Image1	R	4.7665	7.9966
	G	4.4863	7.9974
	B	5.0796	7.9972
Image2	R	3.1078	7.9970
	G	3.4056	7.9974
	B	2.6673	7.9973
Image3	R	5.8124	7.9974
	G	6.1789	7.9973
	B	5.5982	7.9971

$$R_{xy} = \frac{COV(XX,YY)}{\sqrt{Var(XX) * Var(YY)}} \quad ...(14)$$

where XX and YY are the pixels in the cipher image, E_x(XX) is the Mean, Var(XX) is the variance and Cov(XX, YY) is the co-variance of the given data.

Image histogram

Histogram shows how the image changes with respect to different intensity of pixel values of image. The Fig.6(a-c) represents the histogram

Table 4. Correlation of 3 test images

Images			Horizontal	Vertical	Diagonal
Image1	R	Plain image	0.9577	0.9642	0.9276
		Cipher image	-0.1507	0.0042	0.0114
	G	Plain image	0.9497	0.9585	0.9148
		Cipher image	-0.0032	-0.0060	0.0133
	B	Plain image	0.9436	0.9770	0.9254
		Cipher image	-0.0013	-0.1135	0.0101
Image2	R	Plain image	0.9518	0.9600	0.9310
		Cipher image	-0.0056	0.0016	0.0111
	G	Plain image	0.9257	0.9347	0.8933
		Cipher image	0.0024	0.0014	0.0112
	B	Plain image	0.8625	0.8755	0.8009
		Cipher image	0.0040	0.0021	0.0117
Image3	R	Plain image	0.9526	0.9620	0.9212
		Cipher image	0.1476	-0.0016	0.0083
	G	Plain image	0.9139	0.9314	0.8540
		Cipher image	-0.0016	0.0010	0.0154
	B	Plain image	0.9649	0.9727	0.9406
		Cipher image	-0.0017	0.0034	0.0141

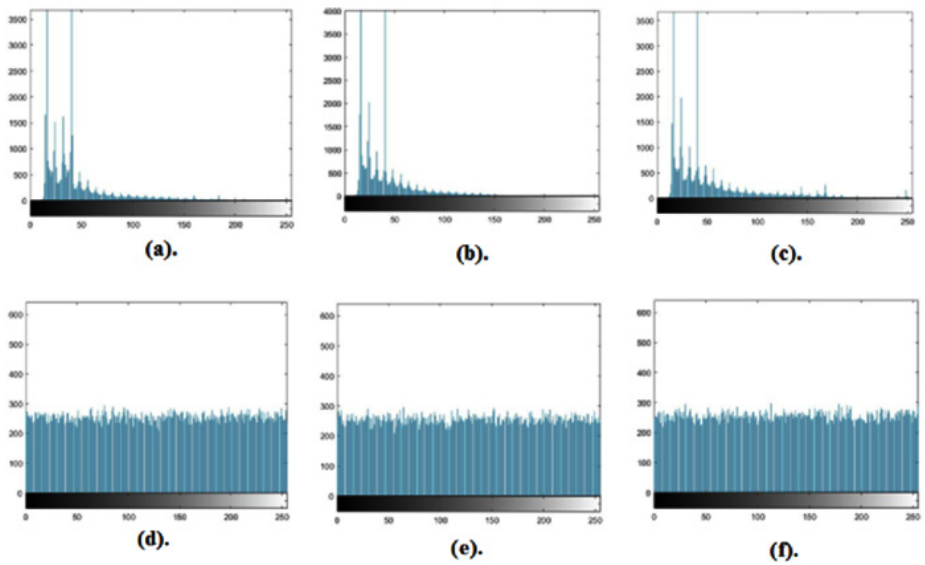


Fig. 6. Histogram; (a). Red plane of plain image (b).Green plane of plain image (c).Blue plane of plain image (d). Red plane of cipher image;(e).Green plane of cipher image (f). Blue plane of cipher image

of the original image and Fig.6(d-f) represents the histogram of the encrypted image. From the figures, it is found that the pixel values of RGB planes from plain image has irregular peaks, but the corresponding histograms of RGB planes of the cipher image has uniformly flat pixel distribution which makes statistical attacks difficult.

Differential attack

This attack includes NPCR(Number of pixel changing rate) and UACI(Unified average changing intensity) to analyse how the pixels at the output are uncorrelated and how it is resistant towards this attack. NPCR and UACI metrics is calculated for the proposed algorithm which is

Table 5. NPCR Analysis For 3 Test Images

Images		Npcr (%)	NPCR Critical Values N*0.05=99.5693%	N*0.01=99.5527%	N*0.001=99.5341%
Image1	R	99.6155	Pass	Pass	Pass
	G	99.5682	Pass	Pass	Pass
	B	99.6323	Pass	Pass	Pass
Image2	R	99.6094	Pass	Pass	Pass
	G	99.6124	Pass	Pass	Pass
	B	99.6384	Pass	Pass	Pass
Image3	R	99.6017	Pass	Pass	Pass
	G	99.5880	Pass	Pass	Pass
	B	99.6246	Pass	Pass	Pass

Table 6. UACI Analysis For 3 Test Images

Images		UACI (%)	U*0.05=33.2824% U*+0.05=33.6447%	U*- 0.01=33.2255% U*+0.01=33.7016%	U*0.001=33.1594% U*+0.001=33.767%
Image1	R	33.5181	Pass	Pass	Pass
	G	33.5296	Pass	Pass	Pass
	B	33.4709	Pass	Pass	Pass
Image2	R	33.4307	Pass	Pass	Pass
	G	33.3079	Pass	Pass	Pass
	B	33.3771	Pass	Pass	Pass
Image3	R	33.5562	Pass	Pass	Pass
	G	33.4987	Pass	Pass	Pass
	B	33.3784	Pass	Pass	Pass

Table 7. Performance Comparison With Existing Algorithms

Metrics	Entropy	Correlation			NPCR	UACI
		Horizontal	Vertical	Diagonal		
Fu et al.[2]	7.9992	NA	NA	NA	99.60	33.48
Fu et al.[3]	7.9993	0.0122	-0.0061	-0.0197	NA	NA
Praveenkumar et al.[4]	NA	0.0014	-0.0059	0.0042	99.63	31.22
Chandrasekaran et al.[5]	7.9976	0.0030	0.0017	0.0010	99.60	33.47
Li et al.[7]	7.9954	0.0046	0.0043	0.00315	NA	NA
Wang et al.[10]	7.9974	-0.0016	-0.0011	0.0012	99.61	33.44
Ravichandran et al.[13]	7.9972	-0.0016	-0.0025	0.0116	99.5982	33.4399
Proposed	7.9971	-0.0011	-0.0119	0.0118	99.6100	33.4519

shown in Table.5 and Table.6.

For calculating this metrics following formulas is used ,

$$NPCR = \frac{\sum_{n=1}^{K}\sum_{m=1}^{L} S(n,m)}{K*L} \times 100\% \quad ...(15)$$

$$\text{Where } S(n,m) = \begin{cases} 0, & \text{if } PV1(n,m) = PV2(n,m) \\ 1, & \text{if } PV1(n,m) \neq PV2(n,m) \end{cases} \quad ...(16)$$

$$UACI = \frac{\sum_{n=1}^{K}\sum_{m=1}^{L} |PV1(n,m) - PV2(n,m)|}{255*K*L} \times 100\% \quad ...(17)$$

where K=rows and L=columns in the image. PV1 is the directly obtained encrypted image and PV2 is the encrypted image by changing one pixel in the original image. The ideal values for NPCR and UACI is (NPCR > 99% and UACI > 33%) shown in Table.5 and Table.6[17, 18].

Quality of encryption

Mean square error (MSE)

The MSE gives the squared error between plain image and cipher image. Both MSE and PSNR are inversely proportional to each other. If MSE is higher, lower the PSNR. High MSE results in highly secured encryption. It can be calculated as[19],

$$MSE = \frac{\sum_{n=1}^{K}\sum_{m=1}^{L} (F(n,m) - \hat{F}(n,m))^2}{K*L} \quad ...(18)$$

where K and L = rows*columns in image and F(n, m) is the original image and $\hat{F}$ (n, m) is the encrypted image.

Peak signal to noise ratio (PSNR)

The PSNR is defined via the MSE. To measure the quality of output image PSNR is used. It is the ratio of maximum signal power and the corrupted noise power. If PSNR<10 db, then it is good. It can be calculated as,

$$PSNR = 10 \log_{10} \frac{((2^p - 1))^2}{MSE} \quad ...(19)$$

where p=8 since image used in the proposed algorithm is 8-bit.

Normalized absolute error (NAE)

The quality of reconstructed image can be measured using this NAE metric. It is defined as the ratio of difference between the original I (n, m) and the reconstructed image $\hat{I}$ (n, m) to the magnitude of original image. Lower the NAE, better the reconstruction of image. In the proposed algorithm NAE=0 hence exact reconstruction. It is given by,

$$NAE = \frac{\sum_{n=1}^{K}\sum_{m=1}^{L} |I(n,m) - \hat{I}(n,m)|}{\sum_{n=1}^{K}\sum_{m=1}^{L} |I(n,m)|} \quad ...(20)$$

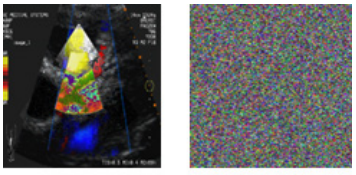
Chosen plaintext attack

In this analysis the XOR operation based diffusion algorithm is done hence it makes the algorithm efficient and makes plaintext attack difficult. It is calculated by using following equation,

$$E1(n,m) \oplus E2(n,m) = R1(n,m) \oplus R2(n,m) \quad ...(21)$$

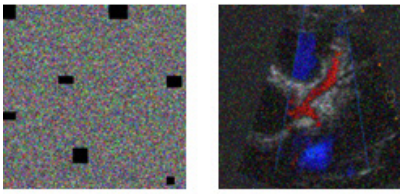
Table 8. MSE and PSNR calculation for 3 test images

Image	MSE	PSNR(db)
Image1	74.990	6.7524
Image2	106.788	5.2173
Image3	89.207	5.9986



(a) (b)

Fig.7. Chosen plaintext attack**;** (a). R1 (n, m) •" R2 (n, m) (b) . E1 (n, m) •" E2 (n, m)



(a) (b)

Fig. 8. a)Encrypted image after cropping b)Decrypted image of (a)

where R1 and R2 are two plain images that produces two cipher images E1 and E2. If Equation (21) is satisfied then the algorithm is vulnerable to this given attack. In this proposed algorithm Equation (21) is not satisfied, hence it has more ability of resisting towards chosen plaintext attack which is shown in Fig.7 a and b.

Cropping attack

During transmission of data, the data loss is the common issue. Cropping attack analysis is performed to find how the algorithm is stronger against a loss of data when an image is sent over the public channel[6].

Fig. 8 a and b shows the cropping of the encrypted images and corresponding decrypted image. Cropping is done at the left corner of encrypted image and at different areas respectively. Even after cropping, the intended receiver will be able to retrieve the plain image to some extent, hence against this cropping its robustness is been proved.

CONCLUSION

In this paper, DICOM images are encrypted using DNA key set enhanced from 3D Lorenz chaotic maps. Operations like confusion, permutation, encoding and diffusion operations were carried out to prove the robustness of the proposed encryption scheme. All the image quality metrics for the encrypted image was estimated and compared with available literature.

REFERENCES

1. Kanso, A. and Ghebleh, M. "An efficient and robust image encryption scheme for medical applications", *Communications in Nonlinear Science and Numerical Simulation*, **24**(1-3), pp. 98-116 (2015).
2. Fu, C. , Zhang, G., Bian, O. , Lei, W. and Ma, H. "A Novel Medical Image Protection Scheme Using a 3-Dimensional Chaotic System", *PLoS ONE*, **9**(12), p. e115773 (2014).
3. Fu, C., Meng, W., Zhan, Y., Zhu, Z., Lau, F., Tse, C. and Ma, H. "An efficient and secure medical image protection scheme based on chaotic maps", *Computers in Biology and Medicine*, **43**(8): pp. 1000-1010 (2013).
4. Praveenkumar, P., Amirtharajan, R., Thenmozhi, K. and Rayappan, J. "Fusion of confusion and diffusion: a novel image encryption approach", *Telecommunication Systems*, **65**(1), pp. 65-78 (2016).
5. Chandrasekaran, J. and Thiruvengadam, S. "A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images", *Security and Communication Networks*, vol. 2017, pp. 1-12 (2017).
6. Ravichandran, D., Praveenkumar, P., Rayappan, J. and Amirtharajan, R. "DNA Chaos Blend to Secure Medical Privacy", *IEEE Transactions on NanoBioscience*, **16**(8), pp. 850-858 (2017).
7. Li, X., Wang, L., Yan, Y. and Liu, P. "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems", *Optik - International Journal for Light and Electron Optics*, **127**(5), pp. 2558-2565 (2016).
8. Niyat, A. Y, Hei, R. M. H. and Jahan, M. V. " A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system", Oct 2015.
9. Kalpana and Murali, P. "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos", *Optik - International Journal for Light and Electron Optics*, **126**(24): pp. 5703-5709 (2015).
10. Wang, X. and Liu, C. "A novel and effective image encryption algorithm based on chaos and DNA encoding", *Multimedia Tools and Applications*, **76**(5), pp. 6229-6245 (2016).
11. Enayatifar, R., Abdullah, A. and Isnin, I. "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence", *Optics and Lasers in Engineering*, **56**: pp. 83-93 (2014).
12. Liu, L., Zhang, Q. and Wei, X. "A RGB image encryption algorithm based on DNA encoding and chaos map", *Computers & Electrical Engineering*, **38**(5): pp. 1240-1248 (2012).
13. Fan, H. and Li, M. "Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter- Intra-Pixels Bit-Level Permutation", *Mathematical Problems in Engineering*, 2017: pp. 1-11 (2017).
14. Wu, Y., Noonan, J. P. and Agaian, S. "NPCR and UACI randomness tests for image encryption", *Cyber J. Multidiscipl. J. Sci. Technol. J. Sel. Areas Telecommun.*, pp. 31-38 (2011).
15. Diaconu, A. - V. "Circular inter–intra pixels bit-level permutation and chaos-based image encryption", *Inf. Sci.*, **355**: pp. 314-327 (2016).
16. Jangid, R. K., Mohmmad, N., Didel, A. and Taterh, S. "Hybrid Approach of Image

Encryption Using DNA Cryptography and TF Hill Cipher Algorithm", (2014).

17. Dang, P. and Chau, P. "Robust image transmission over CDMA channels", *IEEE Transactions on Consumer Electronics*, **46**(3), pp. 664-672 (2000).