Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 218 (2023) 918–926

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering

2D Lorentz Chaotic Model Coupled with Logistic Chaotic Model for Medical Image Encryption: Towards Ensuring Security for Teleradiology

Siju John [a], S.N Kumar [b]

[a]*Lincoln University College,Kota Bharu, 15050*
[b]*Department of EEE, Amal Jyothi College of Engineering, Kanjirappally, 686518*

Abstract

Medical images play pivotal role in health care sector for disease diagnosis and therapeutic planning. Encryption algorithms are widely used in medical image processing for ensuring privacy in data transfer. This research work proposes a hybrid chaotic model, 2D Lorentz Chaotic model coupled with the Logistic chaotic model for the encryption/decryption of medical DICOM CT images. Prior to encryption, preprocessing was done by the median filter. The hybrid chaotic model scrambles the rows and columns of the image and bitwise XOR operation is carried out to generate the encrypted image. The performance metrics reveals the proficiency of the approach utilized in this research work, the mean PSNR value was 73.45, mean NPCR value was 99.99 and mean UACI value was 26.03. The hybrid encryption model outperforms the existing encryption techniques and paves the way towards the teleradiology applications. The encrypted image can be transferred through the cloud network and the receiver side node can decrypt the image. The decrypted image equality was found to be proficient for healthcare applications.

Keywords: encryption,image processing, teleradiology

1. Introduction

Image security play's vital role in the transmission of data from one node to another node. In chaotic system of digital image generation for encryption, the hash value is embedded during the process of chaotic key generation. As a result, the security level can be significantly improved from the initial state, dynamic changing of key values also improves the security [1]. In [2] also, the Lorentz chaotic system was applied for image encryption and for decorrelation of pixel values, noise was added. The computation time was found to be low, since there one round of substitution and permutation was applied. In [3], the secure hash algorithm (SHA-3) and adaptive differential evolution

10.1016/j.procs.2023.01.072

(ADE) are used for solving the challenges faced by classical encryption system. The optimization process was done by ADE on the input parameters, whereas SHA generates the secret key, can resist different security attacks [3]. A hybrid combination of Lorentz chaotic map and gingerbread-man chaotic map was employed in [4] for the image encryption. Lorentz chaotic map was initially applied to decorrelate the pixel values, after XOR operation of scrambled image with the random matrix, gingerbread-man chaotic map was applied to generate the cipher image. The encryption of RGB images using DNA cryptography model was proposed in [5]. Lorentz and Rosseler chaotic system were applied at the initial stage and for the refinement of encryption model, 2D logistic chaotic function was also applied. The performance metrics evaluation suggests the application of this encryption model for healthcare and forensic application. The hybrid combination of 3D Lorentz chaotic and Rossler chaotic function was employed in [6] for image encryption, the proposed encryption model resists classical attacks. 3D Lorentz chaotic function was utilized in [7] for the encryption of images, encryption process was based on shuffling method through fractals and 3D Lorenz chaotic map. A secured cryptography system was proposed in [8] utilizing the hyperchaotic Lorentz system, the key stream was related to the input plain text image apart from the key values, hence it resists against different classical attacks. The SCAN technique along with the chaotic tent map was deployed in [9] for the encryption of images, spiral SCAN model was used for higher order 4 bit planes and diagonal SCAN model was used for lower order four bit planes. In [10], the improved Lorentz chaotic model termed as Lorentz 96 was employed for the encryption of images. The fractional fourier transform along with the optical bit plane jig saw transform was utilized in [11] for ensuring the security of medical images. The block based encryption with multiple chaos are proposed in [12] for the encryption of images, focusing on region of interest. Partial image encryption focusing on the permutation and diffusion was put forward in [13] for image encryption, computation time was lowered. The security aspect of medical images for telemedicine application was highlighted in [14], the importance of watermarking in ensuring security for health care sector was proposed in [15]. The paper organization is as follows; section 2 highlights the hybrid chaotic algorithm for image encryption, the simulation results was put forward in section 3 with real time CT images as input, performance validation was done by appropriate metrics. Conclusion is finally drawn in section 4.

2. Materials and Methods

2.1. Hybrid Encryption Model-2D Lorentz Chaotic Algorithm Coupled with 2D Logistic Chaotic Algorithm

Chaotic models are utilized in many real-world applications. Chaotic systems are useful for image encryption methods because they have various parameters that affect the system's behaviour. In this research work for encryption 2-D Lorenz chaotic system coupled with the logistic chaotic model is used. The level of complexity in the chaotic mapping algorithm is low. The proposed encryption and decryption scheme in this research work improves the security.

$$y_{n+1} = \mu y_n(1 - y_n) \tag{1}$$

$$\begin{Bmatrix} y_{1,n+1} = (1 + ah)y_{1,n} - hy_{1,n}y_{2,n} \\ y_{2,n+1} = (1 - h)y_{1,n} + \mathrm{h}\left(y_{1,n}\right)^2 \end{Bmatrix} \tag{2}$$

Equation (1) is the Logistic mapping equation, when $3.569945672\cdot\cdot\cdot\cdot\cdot\cdot < \mu \leq 4$, the system is in a chaotic state. Equation (2) is the mapping equation of the two- dimensional discrete Lorentz chaotic system. When the parameters $a \in [0.9, 1]$ and $h \in [0.9, 1]$, the system complexity increases. In image encryption models, parameters are chosen in such a manner that, it is difficult to crack. The hybrid chaotic function generates key values for the input image, scrambling and bitwise XOR operation was performed to generate encrypted image.

2.2. Medical Image Encryption using Hybrid Chaotic Model

The step-by-step procedure in the proposed medical image encryption are as follows

Step 1: Convert the input color image R_{color} to a grayscale image R_{Gray} by reading the original image. R_{Gray} is written as Follows

$$R_{Gray} = \begin{pmatrix} R_{i1,j1} & R_{i1j2} & \cdots & R_{i1jn} \\ R_{i2,j1} & R_{i2j2} & \cdots & R_{i2jn} \\ \cdots & \cdots & \cdots & \cdots \\ R_{im,j1} & R_{im1j2} & \cdots & R_{im1jn} \end{pmatrix} \tag{3}$$

Step 2: Convert the grey image pixel value from decimal to binary form

Step 3: Create two group of sequences using hybrid encryption model, Y_H and Y_V,

$$Y_H = \{Y_{H1}, Y_{H2}, Y_{H3}, \dots, Y_{Hm}\} \tag{4}$$

$$Y_V = \{Y_{V1}, Y_{V2}, Y_{V3}, \dots, Y_{V8n}\} \tag{5}$$

Step 4: Scramble the rows and columns, utilizing the chaotic groups in step 2, the resultant image matrix are as follows

$$R_{\text{En1Dec}} = \begin{pmatrix} R_{h1,v1} & R_{h1,v2} & \cdots & R_{h1,v8n} \\ R_{i2,v1} & R_{i2,v2} & \cdots & R_{h2,v8n} \\ \cdots & \cdots & \cdots & \cdots \\ R_{hm,v1} & R_{hm,v2} & \cdots & R_{hm1v8n} \end{pmatrix} \tag{6}$$

$$R_{\text{En1Dec}} = \begin{pmatrix} R_{H1,V1} & R_{H1,V2} & \cdots & R_{H1,V8n} \\ R_{H2,V1} & R_{H2,V2} & \cdots & R_{H2,V8n} \\ \cdots & \cdots & \cdots & \cdots \\ R_{Hm,V1} & R_{Hm,V2} & \cdots & R_{Hm1V8n} \end{pmatrix} \tag{7}$$

Where,

$$R_{Hi,Vj} = bin2dec\left(R_{hi,j\times 8-7} R_{hi,j\times 8-6} R_{hi,j\times 8-5} R_{hi,j\times 8-4} R_{hi,j\times 8-3} R_{hi,j\times 8-2} R_{hi,j\times 8-1} R_{hi,j\times 8}\right) \tag{8}$$

Step 5: Convert R_{En1Bin} from 2D to a 1D sequence. $R_{En1Bin1D}$,

$$R_{En1Bin1D} = \{r_1, r_2, r_3, \dots, r_{mn}\} \tag{9}$$

Step 6: Create two-dimensional chaotic sequences Y_1 and Y_2 by using equation 2.

$$Y_1 = \{Y_{1,1}, Y_{1,2}, Y_{1,3}, \dots, Y_{1,mn}\} \tag{10}$$

$$Y_2 = \{Y_{2,1}, Y_{2,2}, Y_{2,3}, \dots, Y_{2,mn}\} \tag{11}$$

Step 7: Equation 3 is used to process Y_1 and Y_2:

$$Y_i = floor(mod(Y_i \times 10^{14}), 256) \tag{12}$$

where i = 1, 2.

Step 8: After step 7, convert Y_1 and Y_2 to binary form. B_1 and B_2 are the binary sequences.

Step 9: To get $K_1 = bitxor(R_{En1Bin1D}, B_1)$, perform bitwise XOR between R_{En1Bin} and B_1

Step 10: To create $K_2 = bitxor(K_1, B_2)$, perform bitwise XOR between the K_1 and B_2.

Step 11: Convert binary K_2 to decimal, then back to 2D form. The encrypted image is denoted by the letter K.

$$K = \begin{pmatrix} K_{i1,j1} & K_{i1,j2} & \cdots & K_{i1,jn} \\ K_{i2,j1} & K_{i2,j2} & \cdots & K_{i2,jn} \\ \cdots & \cdots & \cdots & \cdots \\ K_{jm,V1} & K_{im,j2} & \cdots & K_{im,jn} \end{pmatrix} \tag{13}$$

2.3. Medical Image Decryption using Hybrid Chaotic Model

The following are the steps deployed to generate the decrypted image in the receiver node side.

Step 1: Take encrypted image K and then convert K into a 1D sequence K_{decID}.

Step 2: K_{decID} is converted to K_{binID}, a binary 1D sequence.

Step 3: Create 2D chaotic sequences Y_1 and Y_2 using equation 2, where

$$Y_1 = \{Y_{1,1}, Y_{1,2}, Y_{1,3}, \dots, Y_{1,mn}\} \tag{14}$$

$$Y_2 = \{Y_{2,1}, Y_{2,2}, Y_{2,3}, \dots, Y_{2,mn}\} \tag{15}$$

Step 4: Equation 3 is used to process Y_1 and Y_2.

Step 5: After step 4, convert Y_1 and Y_2 to a binary form and then get B_1 and B_2 as the binary sequences.

Step 6: To get $C_1 = bitxor(K_{bin1D}, B_1)$, perform bitwise Xor between K_{bin1D} and B_2

Step 7: To create $C_2 = bitxor(C_1, B_2)$, perform bitwise Xor between C_1 and B_1
Step 8: Convert the 1D C2 sequence to 2D sequence.
Step 9: Use Lorentz model for creating two sets of chaotic sequences, YH and YV,

$$Y_H = \{Y_{H1}, Y_{H2}, Y_{H3}, \dots, Y_{Hm}\} \tag{16}$$

$$Y_V = \{Y_{V1}, Y_{V2}, Y_{V3}, \dots, Y_{V8n}\} \tag{17}$$

Step 10: Reverse scrambling is done and binary values are converted into decimal values (C), the C represents the decrypted image.

The two stage chaotic model was employed in this research work for the storage and transmission of medical data. The algorithms are tested on DICOM CT images and validated by the performance metrics. The proposed hybrid encryption model was found to generate proficient results for gray scale and color images. The two stage chaotic model improves the security and makes the robust against different types of attacks. Prior to encryption, the preprocessing was done by median filter, since the CT images are usually corrupted by the gaussian noise.

3. Results and Discussion

This research work proposes hybrid encryption Model for the encryption/decryption of medical images. The real time abdomen CT images utilized in this research work was obtained from Metro Scans and Research Laboratory, Trivandrum. The performance metrics [16][17] validation for the 2D Chaotic Lorentz Model coupled with Logistic Chaotic model are as follows; Histogram Deviation estimates the difference between the original and encrypted images. Encryption is efficient, when HD value is high. It relies on the input and encrypted image histograms. The Histogram deviation (HD) is expressed as follows

$$HD = \frac{\left(\frac{d_0 + \mathrm{d}_{255}}{2}\right) + \sum_1^{255} \mathrm{d_i}}{\mathrm{M\,X\,N}} \tag{18}$$

Where $\mathrm{d_i}$ = amplitude of the absolute difference at the ith Gray level.

The correlation coefficient is a vital metric that estimates the efficiency of the encryption model, lower the value of correlation measure better will be the encryption model. The Correlation coefficient (CC) measure is expressed as follows

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D}(x)\sqrt{D(y)}} \tag{19}$$

Where,

$$D(x) = \frac{1}{L}\sum_l^L = 1\left(x_l - \frac{1}{L}\sum_K^L = 1\,x_k\right)^2 \tag{20}$$

x= plain image, y= cipher image and L= Number of pixels involved in the calculation

$$cov(x,y) = \frac{1}{L}\sum_l^L = 1\left(x_l - \frac{1}{L}\sum_K^L = 1x_k\right)\left(y_l - \frac{1}{L}\sum_K^L = 1y_k\right) \tag{21}$$

The irregular deviation (ID) is a measure that describes how much there is a deviation between the input and encrypted images. The Irregular Deviation (ID) is expressed as follows

$$ID = \frac{\sum_{1=0}^{255}|H\,(i) - M_H|}{M \times N} \tag{22}$$

Where M_H = Mean value of histogram, H= Histogram of the difference image.

An ideal encrypted image's histogram should have a uniform distribution of all grey levels. The Deviation from Identity (DI) metric calculates the difference between the encrypted image's histogram and the ideal encrypted image's histogram. The lower the DI value, the greater the encryption quality.

$$DI = \frac{\sum_{1=0}^{255}|H\,(C_1) - H(C)|}{M \times N} \tag{23}$$

Where $H(C)$ = Histogram of encrypted image

$$H(C_1) = \begin{cases} \frac{M \times N}{256} & ,0\ C_l \leq 255 \\ 0, otherwise & \end{cases} \tag{24}$$

The UACI estimates the mean intensity variation between the two images, a high value of UACI is an indication of proficient encryption model. The UACI is expressed as follows

$$UACI = \frac{1}{M \times N}\left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{C_{1\,(i,j)} - C_{2\,(i,j)}}{255}\right] \times 100\% \tag{25}$$

Where CK= Ciphered images: k= {1,2}

The NPCR determines the measure of how much percentage difference is there in two images. Higher value of NPCR indicates the proficiency of the encryption model, the NPCR metric is expressed as follows

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j}^{N}=1\, D(i,j)}{M \times N} \times 100\% \tag{26}$$

Where'

$$D(i,j) = \begin{cases} 1, \text{if C1 (i, j)} = \text{C2 (i, j)} \\ \quad 0, Otherwise \end{cases} \tag{27}$$

The Peak Signal to Noise Ratio (PSNR) is expressed as follows

$$PSNR = 10 \times log_{10}\left[\frac{M \times N \times 255^2}{\sum_{m=1}^{M} \sum_{n=1}^{N} |(f\ (m,n) - f_d(m,n))|^2}\right] \tag{28}$$

Where f (m,n) = Original image and f d (m,n)= Decrypted image

The information entropy is a measure of uncertainty in an image, closer the value to 8 for a gray scale image indicates the proficiency of the encryption model. The Information Entropy (IE) is expressed as follows

$$IE = \sum_{i=0}^{2^j - 1} P\ (S_i). \log_2 \frac{1}{p(S_i)} \tag{29}$$

Where $p(S_i)$ = Probability of the symbol Si

The figure 1 and 2 depicts the outputs corresponding to the input images (D1, D2, D3 and D4).

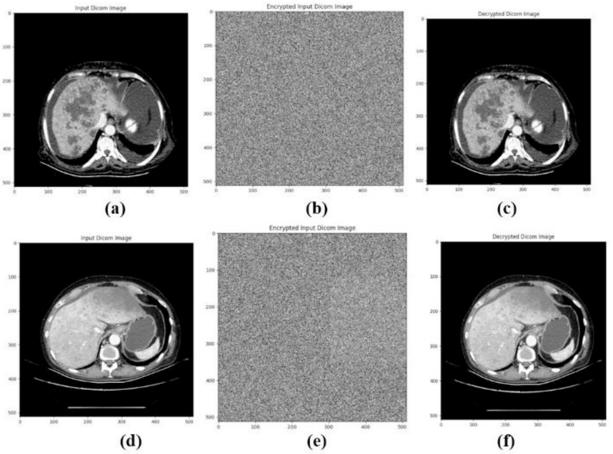

Fig. 1. (a,d) Input DICOM medical images (D1 and D2), (b,e) Encrypted medical images, (c,f) Decrypted medical images

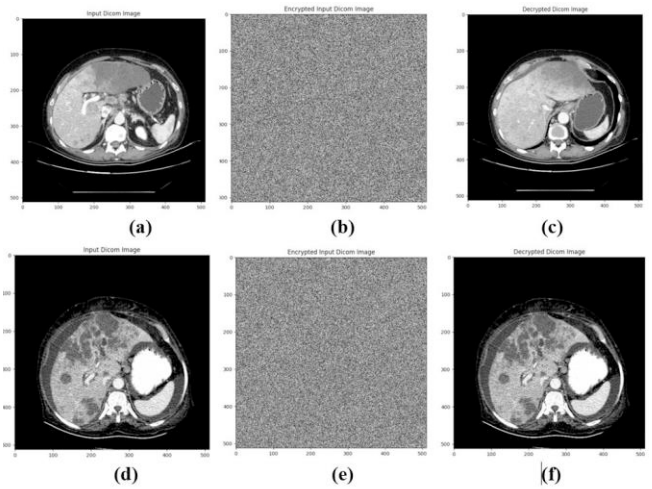

Fig. 2. (a,d) Input DICOM medical images (D3 and D4), (b,d) Encrypted medical images, (c,f) Decrypted medical images

Figure 3 depicts the histogram of the input image (D1) and the corresponding encrypted image. The flat histogram of the encrypted images reveals the proficiency of the encryption approach.

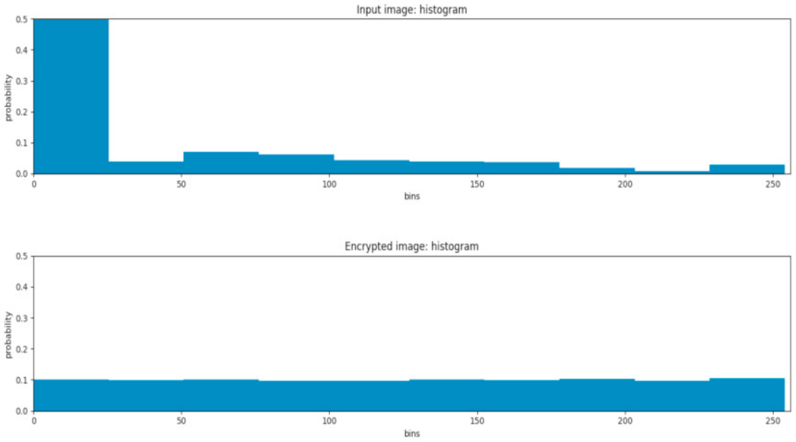

Fig. 3. Histogram of the input and encrypted image corresponding to D1

The table 1, 2 and 3 below depicts the performance metrics values corresponding to the encrypted image with respect to the input images.

Table 1. HD, IH, CC and DI values corresponding to the encryption model

Image details	Histogram deviation	Irregular Histogram	Correlation Coefficient	Deviation from Identity
D1	1.0060	0.02927	-0.0025	0.0292
D2	1.0059	0.02762	-0.0039	0.0276
D3	1.0060	0.02809	-0.0019	0.0280
D4	1.0059	0.02807	-0.0061	0.0280

The correlation plot corresponding to the input image D1 is depicted above in fig 4. The negative and low correlation values indicates the robustness of the encryption model.

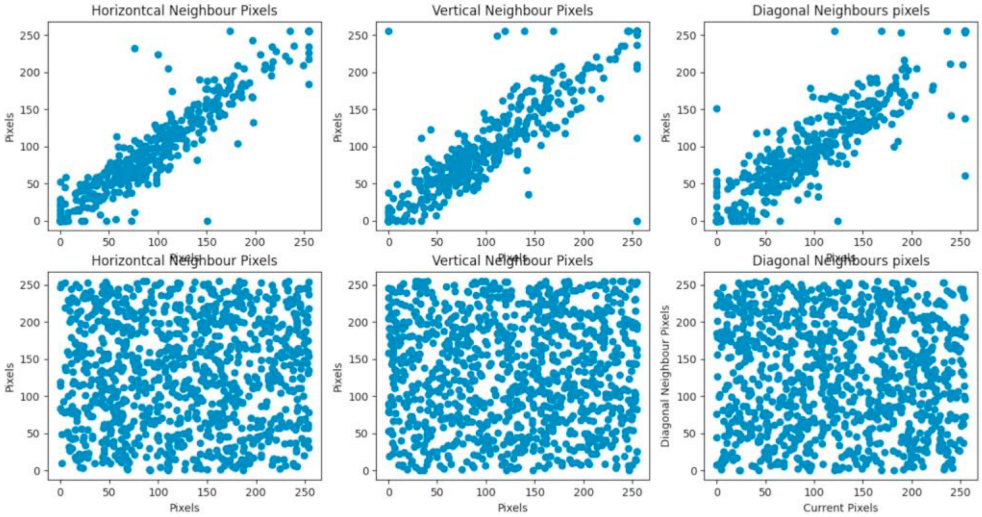

Fig. 4. Correlation plot corresponding to the input and encrypted image corresponding to the D1

The table 2 below depicts the UACI, NPCR and entropy values of proposed hybrid encryption model corresponding to the input DICOM images.

Table 2. UACI, NPCR and Entropy values corresponding to the encryption model

Image details	UACI	NPCR	Entropy
D1	25.33	99.99	7.991
D2	24.15	99.99	7.991
D3	26.34	99.99	7.991
D4	28.32	99.99	7.991

The table 3 below depicts the PSNR and MSE values of proposed hybrid encryption model corresponding to the input DICOM images.

Table 3. PSNR and MSE values corresponding to encryption model estimated between input and decrypted image

Image details	PSNR	MSE
D1	54.18	0.2480
D2	68.16	0.0099
D3	83.23	0.0003
D4	88.33	0.0009

The horizontal correlation (HC), vertical correlation (VC) and diagonal correlation (DC) values are represented in table 4.

Table 4. Correlation values corresponding to the input and encrypted images

Image Details	[HC , VC , DC]
D1	[0.9708, 0.9505, 0.9533], [0.0374,0.0007, -0.0377]
D2	[0.9829, 0.9549, 0.9412], [0.0038, 0.0427, -0.0003]
D3	[0.9837, 0.93383, 0.9493], [-0.0161, -0.0488, 0.0340]
D4	[0.9781, 0.9557, 0.9323], [-0.0455,0.0109,0.0228]

The performance metrics evaluation reveals the proficiency of the encryption model for secure data transfer in health care sector. The proposed algorithm was compared with the existing works in terms of entropy and the details are depicted in table 5. The entropy of proposed hybrid encryption was found to be in par with the existing approaches.

Table 5: Comparison of proposed hybrid encryption model with existing approaches in terms of entropy

Reference details of encryption model	Entropy
[18]	7.9995
[19]	7.9993
[20]	7.9995
[21]	7.9999
Proposed hybrid encryption model	7.9993

The PSNR values comparison with the existing works are depicted in table 6.

Table 6: Comparison of proposed hybrid encryption model with existing approaches in terms of PSNR values

Reference details of encryption model	PSNR values
[21] Lena	39.51
[21] Ultrasound	39.54
[21] MRI	39.75
[21] Endoscopy	39.67
[22] Medical Image	39.51
Proposed hybrid encryption model	73.47

The PSNR value of the proposed hybrid encryption model was found to be high, when compared with the existing approaches. The PSNR value reflects the quality of the decrypted image and higher value favors the precise diagnosis in the health care sector.

4. Conclusion

This research work proposes 2D hybrid encryption model for ensuring security of medical images during transmission through cloud network. Performance validation by the metrics reveals the proficiency of encryption model there by ensuring privacy. The proposed hybrid encryption model was compared with the existing approaches, a mean PSNR value of 73.475 and mean entropy value of 7.99. Security being an important aspect in the today's technology world, medical images should be protected for safeguarding the patient's details as per council of medical ethics. The outcome of this research work caters the needs of researchers working on medical image encryption for teleradiology application. The future work will be focusing on the compression with encryption for secure and fast data transfer through cloud network.

Acknowledgements

The authors would like to acknowledge the support from the Schmitt Center for Biomedical Instrumentation of Amal Jyothi College of Engineering and LUCMRC, Kuttikkanam for supporting this research work. The authors would also like to acknowledge the support from Metro Scans and Research Laboratory, Trivandrum in providing the real time medical images.

References

[1] Al-Hazaimeh, O. M., Al-Jamal, M. F., Alhindawi, N., & Omari, A. (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. Neural Computing and Applications, 31(7), 2395–2405.

[2] Anees, A. (2015). An image encryption scheme based on lorenz system for low profile applications. 3D Research, 6(3), 1–10.

[3] Kaur, M., & Kumar, V. (2018). Adaptive differential evolution-based lorenz chaotic system for image encryption. Arabian Journal for Science and Engineering, 43(12), 8127–8144.

[4] Khan, F. A., Ahmed, J., Khan, J. S., Ahmad, J., & Khan, M. A. (2017). A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation. Journal of Intelligent & Fuzzy Systems, 33(6), 3753–3765.

[5] Kumar, V., & Girdhar, A. (2021). A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach. Multimedia Tools and Applications, 80(3), 3749–3773.

[6] Malik, D. S., & Shah, T. (2020). Color multiple image encryption scheme based on 3D-chaotic maps. Mathematics and Computers in Simulation, 178, 646–666.

[7] Masood, F., Ahmad, J., Shah, S. A., Jamal, S. S., & Hussain, I. (2020). A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map. Entropy, 22(3), 274.

[8] Zhang, J. (2015). An image encryption scheme based on cat map and hyperchaotic lorenz system. 2015 IEEE International Conference on Computational Intelligence & Communication Technology, 78–82. Al-Hazaimeh, O. M., Al-Jamal, M. F., Alhindawi, N., & Omari, A. (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. Neural Computing and Applications, 31(7), 2395–2405.

[9] Parameshachari, B. D., & Panduranga, H. T. (2022). Medical image encryption using SCAN technique and chaotic tent map system. In *Recent Advances in Artificial Intelligence and Data Engineering* (pp. 181-193). Springer, Singapore.

[10] Rashmi, P., Supriya, M. C., & Hua, Q. (2022). Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare. Security and Communication Networks.

[11] Alqahtani, F., Amoon, M., & El-Shafai, W. (2022). A Fractional Fourier Based Medical Image Authentication Approach. CMC-COMPUTERS MATERIALS & CONTINUA, 70(2), 3133-3150.

[12] Kiran, P., & Parameshachari, B. D. (2022). Resource Optimized Selective Image Encryption of Medical Images Using Multiple Chaotic Systems. Microprocessors and Microsystems, 91, 104546.

[13] Parameshachari BD, Panduranga HT, de Prado RP. Partial image encryption of medical images based on various permutation techniques. InComputer Vision and Recognition Systems 2022 (pp. 223-238). Apple Academic Press.

[14] Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: a systematic review. Multimedia Tools and Applications, 1-45.

[15] Amine, K., Fares, K., Redouane, K. M., & Salah, E. (2022). Medical image watermarking for telemedicine application security. Journal of Circuits, Systems and Computers, 31(05), 2250097.

[16] Kaur, M., Singh, S., & Kaur, M. (2021). Computational image encryption techniques: a comprehensive review. Mathematical Problems in Engineering, 2021.

[17] Malik, A., Gupta, S., & Dhall, S. (2020). Analysis of traditional and modern image encryption algorithms under realistic ambience. Multimedia Tools and Applications, 79(37), 27941-27993.

[18] Dridi, M., Bouallegue, B., Hajjaji, M. A., & Mtibaa, A. (2016). An enhancement crypto-compression scheme for image based on chaotic system. International Journal of Applied Engineering Research, 11(7), 4718-4725.

[19] Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A. M., Hirota, K., & Abd EL-Latif, A. A. (2020). Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Information Sciences, 515, 191-217.

[20] Zhang, Y. (2020). The fast image encryption algorithm based on lifting scheme and chaos. Information sciences, 520, 177-194.

[21] Gafsi, M., Abbassi, N., Hajjaji, M. A., Malek, J., & Mtibaa, A. (2020). Improved chaos-based cryptosystem for medical image encryption and decryption. Scientific Programming, 2020.

[22] Rajendran, S., & Doraipandian, M. (2021). Chaos based secure medical image transmission model for IoT-powered healthcare systems. In IOP Conference Series: Materials Science and Engineering (Vol. 1022, No. 1, p. 012106). IOP Publishing.