IoT based medical image encryption using linear feedback shift register – Towards ensuring security for teleradiology applications

Article *in* Measurement Sensors · January 2023

DOI: 10.1016/j.measen.2023.100676

CITATIONS
4

READS
58

2 authors:

Siju John
Amal Jyothi College of Engineering
7 PUBLICATIONS **8** CITATIONS
SEE PROFILE

S N Kumar
Amal Jyothi College of Engineering
94 PUBLICATIONS **546** CITATIONS
SEE PROFILE

Measurement: Sensors 25 (2023) 100676

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

IoT based medical image encryption using linear feedback shift register – Towards ensuring security for teleradiology applications

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

[a] Lincoln University College,Kota Bharu, 15050, Malaysia
[b] Department of CSE, Amal Jyothi College of Engineering, Kanjirappally, 686518, Kerala, India
[c] Department of EEE, Amal Jyothi College of Engineering, Kanjirappally, 686518, Kerala, India

ARTICLE INFO

Keywords:
IoT
Encryption
Teleradiology
Image processing
Computed tomography

ABSTRACT

Telemedicine gains prominence in today's scenario and image security plays a vital role in the healthcare sector for authenticating data transfer. Medical data, when transferred through a cloud network should be encrypted to ensure security, this research work proposes a medical image encryption scheme using a linear feedback shift register (LFSR). The LFSR generates pseudo-random numbers and shuffles the pixel position. The encrypted image was transferred through a cloud platform, receiver side node decrypts the data to recover the original image. The Digital Imaging and Communications in Medicine (DICOM) computed tomography images are utilized in this research work and for IoT implementation, a Raspberry Pi B+ processor was used. The IoT implementation facilitates data transfer through the cloud network. The performance validation was done by metrics and the results reveal the proficiency of the encryption/decryption model. The decrypted image quality was evaluated in terms of the Peak to Signal Noise Ratio (PSNR) and Means Square Error (MSE), low value of the correlation coefficient proves the robustness of the encryption. The outcome of the research work paves the way for the researchers in the secure transfer of medical data through the cloud platform.

1. Introduction

In our modern world, an expanding measure of data is being sent each and every moment over the Internet, including text as well as sound, pictures, and other interactive media documents. Images are broadly utilized in everyday life, and, subsequently, the security of image information is a significant prerequisite. Medical image encryption role is inevitable in teleradiology, since it involves the transfer of medical images from one node to another node. Noninvasive medical imaging modalities such as CT, MRI and US data are utilized in teleradiology for interpretation of diseases. The components of the teleradiology system are image sending node, transmission framework and receiving node. The teleradiology system data are transferred through cloud network and security, privacy aspect gains much prominence.

Encryption is additionally performed when it is important to secure client protection [1]. The process of encoding a message so that only authorized parties can access it is called encryption. The process of encrypting an image is called image encryption. Encryption can be characterized as a strategy by which data is changed over into secret code that conceals the data's actual significance [2]. In the encryption process, the input is called plain text, and the scrambled data is called as cipher text. Image encryption can be characterized so that it is the way toward encoding a secret image with the assistance of some encryption calculation so that unapproved clients can't get to it. Image and video encryption gains prominence in health care, web, and military applications [3,4]. Medical image encryption gains prominence in the healthcare sector with respect to teleradiology applications for data transfer, encryption, and compression technology was deployed in Ref. [5] for data transfer in telemedicine.

The hyperchaotic cellular neural network architecture along with DNA technology was utilized for encryption in Ref. [6] for teleradiology applications. Telehealth gains prominence in the COVID-19 scenario and helps patients in rural areas [7]. Security of medical data is ensured through encryption for transfer through the cloud network. The security aspect of telehealth is discussed in Refs. [8,9]. The ethical issues in teleradiology are highlighted in Ref. [9]. The advantages and limitations of telemedicine and its role in the COVID-19 scenario were highlighted in Ref. [10]. Video telehealth was found to be proficient for psychotherapy treatment [11]. The role of telehealth in cancer treatment during the COVID-19 scenario was discussed in Ref. [12]. In Ref. [13], a

* Corresponding author.
E-mail addresses: sjohn@lincoln.edu.my (S. John), appu123kumar@gmail.com (S.N. Kumar).

https://doi.org/10.1016/j.measen.2023.100676
Received 28 September 2022; Received in revised form 4 January 2023; Accepted 10 January 2023
Available online 12 January 2023

detailed review of telehealth guidelines was discussed, implementation of telehealth in the COVID-19 scenario was an aid for patients in rural areas to discuss with physicians. The objective of the proposed research work is to develop a proficient encryption model for transferring medical images with low computational complexity. Section 2 focuses on the related works, and Section 3 focuses on the medical image encryption/decryption based on the linear feedback shift register algorithm. Section 4 describes the simulation results and discussion and finally, a conclusion is drawn in section 5.

2. Related works

In [14], compressive sensing with a 1D chaotic system was put forward for the encryption of images, and the linear feedback shift register-based state sequence was employed in this work for the minimization of computational complexity. The secure Linear Feedback Shift Register (LFSR) framework is deployed in Ref. [15] for the encryption of images. The discrete Fourier transform based watermarking along with the LFSR was proposed in Ref. [16] for ensuring the security authentication of images. The chaotic encryption strategy coupled with the nonlinear filtering based on LFSR was put forward in Ref. [17] and validated in terms of the performance metrics. The LFSR coupled with the multi-ant cellular automation was highlighted in Ref. [18] for image encryption. The cellular automata with LFSR strategy were proposed in Ref. [19] for the encryption of images, implemented in Cyclone II Field Programmable Gate Array (FPGA), and tested on RGB and DICOM images. LFSR generates the pseudo-random sequence numbers, the chaotic functions are utilized to formulate the ciphered image, and the proposed algorithm in Ref. [20] withstands the statistical attacks.

The article [21] highlights the chaotic-based LFSR strategy for the encryption of images. The image encryption utilizing LFSR, and key generation by RC4 key generator was proposed in Ref. [21]. The random keys generated by the stream generator and pixels of the intermediate cipher image are subjected to XOR operation for the generation of the final cipher image. The crypto compression scheme was proposed in Ref. [22], and the AES algorithm along with the hybrid chaotic model comprising of Arnold and Henon map was utilized in this work. The 4D chaotic circuit was deployed in Ref. [23] for the encryption of images, and a fast image encryption scheme-based lifting wavelet and chaotic function was proposed in Ref. [24]. An improved chaotic system comprising hybrid chaotic functions was deployed in Ref. [25] for the encryption of medical images. The chaotic function-based medical image encryption was proposed in Ref. [26], IoT based implementation was found to be proficient for healthcare applications. A novel sine tangent chaotic function-based medical image encryption was proposed in Ref. [27], and a systematic review focusing on the security of medical images for telemedicine applications was highlighted in Ref. [28]. Novel chaotic function-based medical image encryption was proposed in Ref. [29], and region of interest based encryption for multiple medical images was put forward in Ref. [30]. Two stage scrambling and one stage diffusion was utilized in this work [30], Logistic-Tent chaotic system (LTS) was used for the generation of chaotic sequences. Most of the related works focus on the software implementation of encryption models and computational complexity is also high. The proposed research work focus on the IoT based implementation of encryption model and time complexity is also low.

3. Materials and methods

In the healthcare sector, medical images play a pivotal role, and especially in the current scenario, telemedicine gains prominence. Teleradiology refers to the transfer of medical images from one node to another node for disease diagnosis and prediction. Security aspects have to be considered while transferring the data even through the cloud network. The proposed research work paves the way toward the proficient transfer of medical data through the cloud network. The linear feedback shift register-based cryptography model was utilized in this research work for ensuring secured data transfer. Fig. 1 represents the IoT-based cryptography framework for teleradiology application.

The encryption was performed row-wise and column-wise by shuffling the pixel values with random numbers. The hardware implementation of the proposed encryption model was implemented in a Raspberry Pi B+ processor with a graphical user interface for the users, Python language was used for the development of the algorithm. The encrypted image was transferred through the cloud network. The inverse of the encryption process was carried out in the receiver node and the encrypted image was reconstructed to generate the original image.

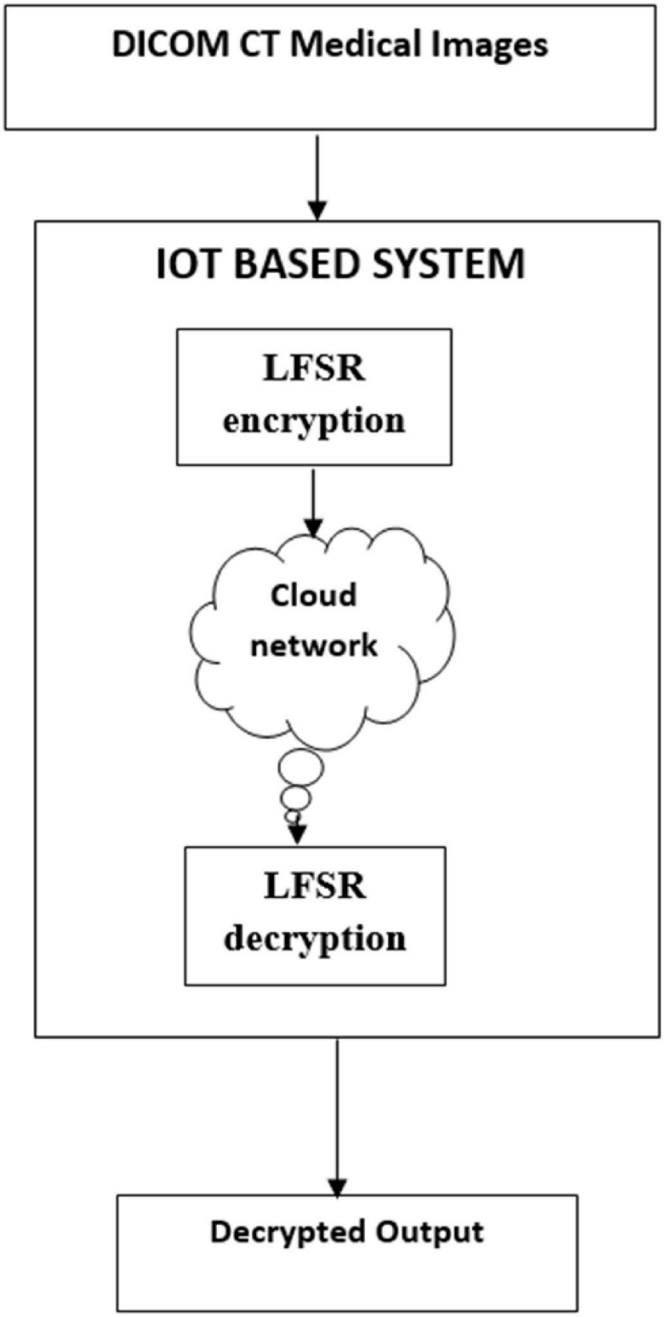


Fig. 1. IoT-based cryptography framework for teleradiology application.

3.1. Medical image encryption/decryption-based linear feedback shift register algorithm

The Linear Feedback Shift Register algorithm is used for the encryption of images by introducing random numbers used in the restructure pixel positions. The LFSR encryption framework is depicted in Fig. 2.

The different steps in the encryption phase of the LFSR algorithm are represented below.

Step 1: Load Input medical image

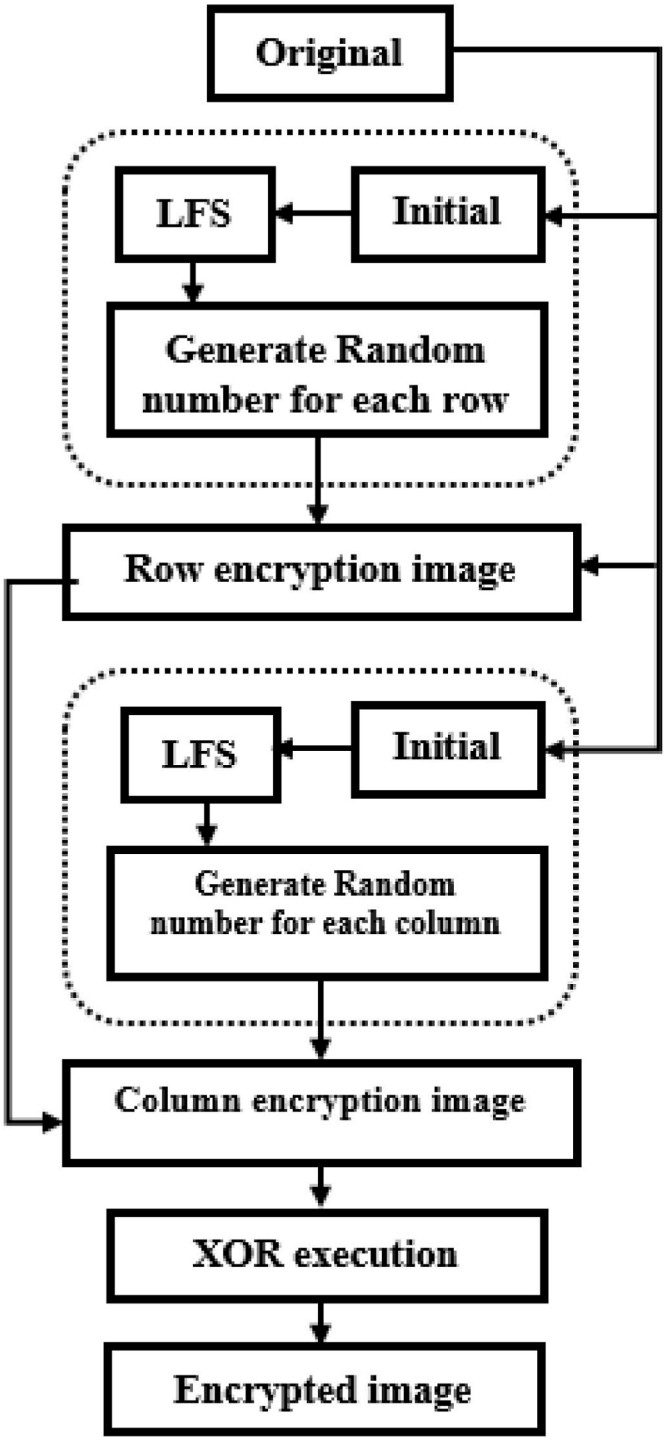


Fig. 2. LFSR Encryption flow diagram.

Step 2: Initialise LFSR
Step 3: Generate a random number for each row
Step 4: Perform encryption of medical image row-wise
Step 5: Generate a random number for each column
Step 6: Perform encryption of medical image column wise
Step 7: Perform XOR operation
Step 8: Get an encrypted medical image

The mathematical model of the LFSR in the theorem. The LFSR depends only on its feedback rather than its initial state. The characteristics of the LFSR polynomial based on feedback are represented as follows.

$$P(x) = \sum_{i=0}^{m} f_i x_i = x_m + f_{m-1}x^{m-1} + f_i x + 1$$

Where $f_m = f_0 = 0$

The $P(x)$ produce the longest sequence for the necessary and sufficient respect to m-level LFSR. equation (1) is complicated. Non existence $k < 2^{n-1}$ makes $x^k + 1$ is evenly divisible by $P(x)$.

LFSR consists of n tandem dual registers and a feedback function. The feedback function is given as input at each timestamp for state of shift registers, and its output feedbacks to the first level shift register and is used as the next state. The function of shift register depends on its state transition.

Encryption Phase: The encryption and decryption of the image in LFSR are done in two phases. In the encryption phase the input image row, column and size are initialized in LFSR. The random number is generated for each row to reorder the pixel position and the row of the image is encrypted. Then the random number is again generated for each column to reorder column pixel position and the column is encrypted. And finally, an XOR function is performed for all the pixels.

Decryption Phase: In the decryption phase, initially the XOR function is performed for all pixels of the encrypted image. Then the row, column, and size are initialized in LFSR with the information required to generate the random number in the LFSR for processing row and column. The generated random number is processed with the column of the encrypted image and then with the row of the encrypted image to obtain the decrypted original image.

Fig. 3 depicts the LFSR decryption flow diagram. The different steps in the decryption phase of the LFSR algorithm are represented below.

Step1: Load encrypted image
Step 2: Perform XOR operation
Step 3: Initialise LFSR values
Step 4: Generate a random number for each column
Step 4: Perform decryption of encrypted image column wise
Step 5: Generate a random number for each row
Step 6: Perform decryption of encrypted image row-wise
Step 7: Get decrypted image

The LFSR-based cryptography model was tested on DICOM CT images, no pre-processing was carried out, prior to encryption/decryption. The LFS in Fig. 3 stands for linear feedback shift, filtering algorithm may be employed prior to encryption/decryption, based on the medical imaging modality.

4. Results and discussion

The LFSR encryption/decryption algorithm was written in python language and executed through Google Colab. The IoT implementation of the LFSR algorithm was done in a Raspberry Pi B+ processor that facilitates the transfer of medical data through a cloud network. The real-time DICOM abdomen CT images are utilized in this research work for the validation of algorithms. The encryption/decryption framework was found to be efficient for DICOM images of any medical imaging

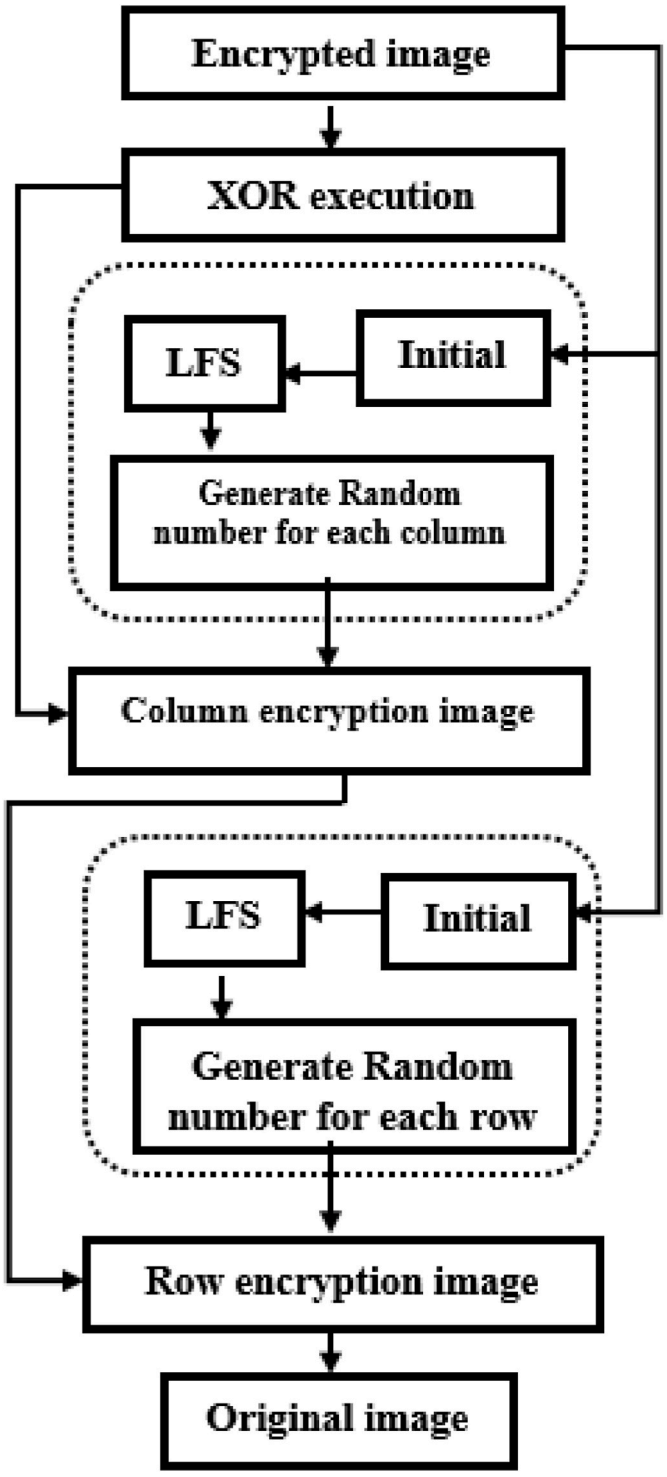


Fig. 3. LFSR Decryption flow diagram.

modality. The performance metrics are used for the validation of results and the simulation results of 5 DICOM input images are presented here. Fig. 4 depicts the LFSR algorithm results corresponding to the first three DICOM inputs (D1, D2, and D3). The first column in Fig. 4 depicts the input images. The second column depicts the encrypted images and the third column depicts the decrypted images.

Fig. 5 depicts the LFSR algorithm results corresponding to DICOM inputs (D4 and D5). The first column in Fig. 5 depicts the input images. The second column depicts the encrypted images and the third column depicts the decrypted images. Prior to the encryption/decryption process, no pre-processing was carried out. In the case of medical imaging modalities, based on the nature of noise, an appropriate filtering algorithm or enhancement algorithm can be used. The input images are subjected to encryption without any resizing. The encrypted image is stored in the cloud and can be transferred to any other node. On the receiver side, the decryption is carried out. Only the authenticated node users can decrypt the scrambled images.

In general, encryption generates an image which is often called a scrambled image, the histogram results depicted in Fig. 6 clearly depict the robustness of the cryptography algorithm. In Fig. 6, (a) depict the input image histogram and (b) represents the encrypted image histogram.

This research work proposes LFSR based 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. Histogram Deviation calculates the difference between the input image and encrypted images. Encryption is efficient when the HD value is high. It depends on the histogram of input and encrypted images.

The Histogram deviation (HD) is given as follows

$$HD = \frac{\left(\frac{d_0 + d_{255}}{2}\right) + \sum_{1}^{255} d_i}{M \times N} \tag{1}$$

Where d_i = amplitude of the absolute difference at the ith grey level.

The effectiveness of the encryption model is evaluated with the correlation coefficient, the encryption is effective only if the correlation coefficient is low. The Correlation coefficient (CC) measure is given as follows

$$r_{xy} = \frac{cov\,(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2}$$

Where,

$$D(x) = \frac{1}{L}\sum_{l}^{L} = 1\left(x_l - \frac{1}{L}\sum_{K}^{L} = 1\,x_k\right)^2 \tag{3}$$

x = input image, y = encrypted image and L = Number of pixels involved in the calculation

$$cov(x, y) = \frac{1}{L}\sum_{l}^{L} = 1\left(x_l - \frac{1}{L}\sum_{K}^{L} = 1x_k\right)\left(y_l - \frac{1}{L}\sum_{K}^{L} = 1y_k\right) \tag{4}$$

The irregular deviation (ID) measures the deviation between the input images and encrypted images. The Irregular Deviation (ID) is expressed as follows

$$ID = \frac{\sum_{1=0}^{255} |HD\,(i) - M_H|}{M \times N} \tag{5}$$

Where M_H = Mean of Histogram, HD= Histogram Deviation

The grey level histogram is uniformly distributed for ideal encrypted image.

The Deviation from Identity (DI) metric estimates the difference between the histograms of encrypted image and ideal encrypted image. The encryption quality better for lower the Deviation from Identity

$$DI = \frac{\sum_{1=0}^{255} |H\,(C_1) - H(C)|}{M \times N} \tag{6}$$

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

$$H(C_1) = \begin{cases} \dfrac{M \times N}{256} & ,0\ C_l \le 255 \\ 0, otherwise \end{cases} \tag{7}$$

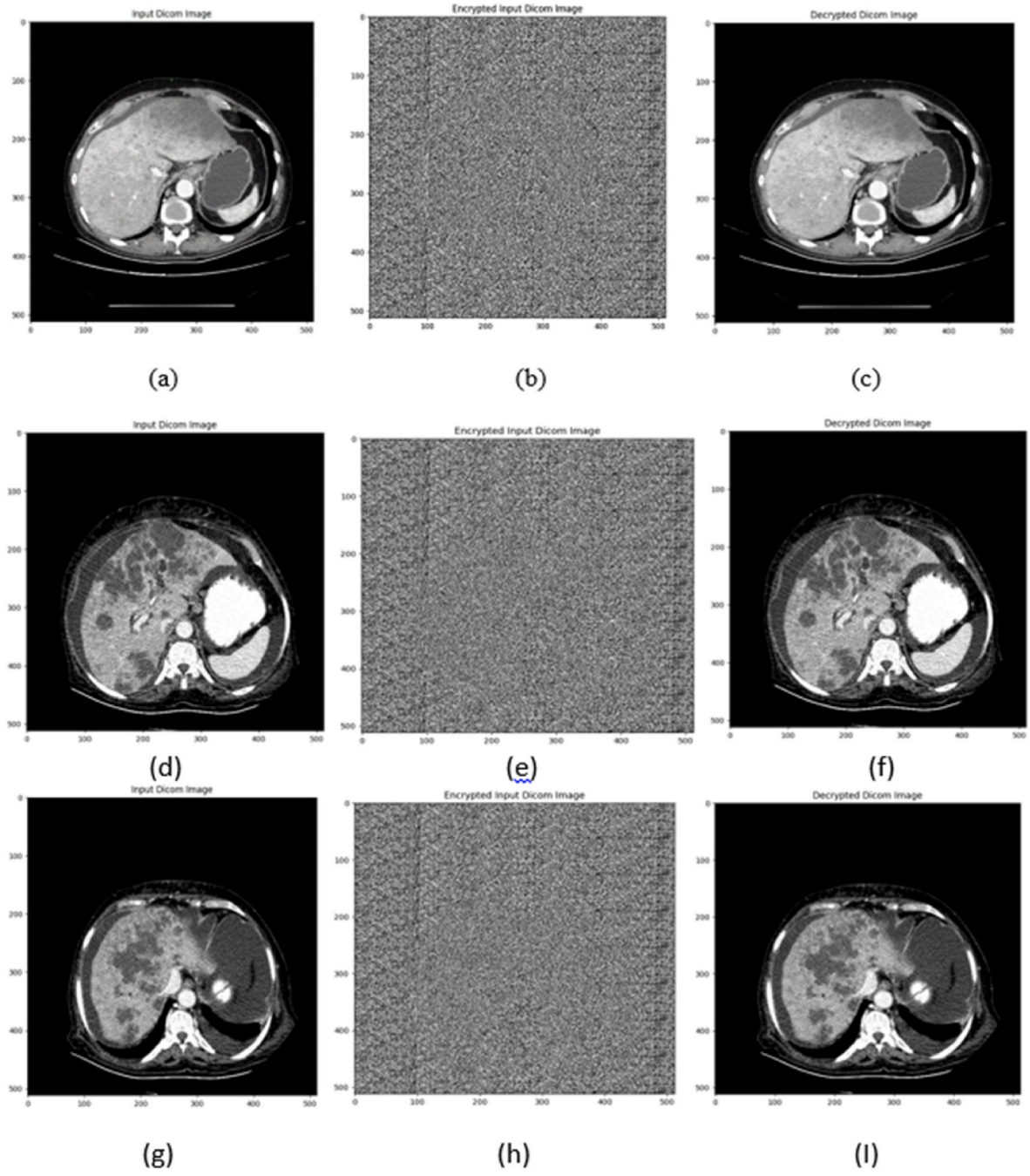


Fig. 4. The first column represents the input DICOM images (D1, D2, and D3), the second column represents the encrypted images, and the third column represents the decrypted images.

The unified average changing intensity (UACI) estimates the mean intensity variation between the two images, high efficiency of encryption for high value of UACI. The UACI is given as follows

$$UACI = \frac{1}{M \times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{C_{1\,(i,j)} - C_{2\,(i,j)}}{255}\right] \times 100\% \tag{8}$$

Where CK = Encrypted images: k = $\{1, 2\}$

The NPCR calculates 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

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j}^{N} = 1\, D(i,j)}{M \times N} \times 100\% \tag{9}$$

Where'

$$D(i,j) = \begin{cases} 1, \text{if C1 (i, j)} = \text{C2 (i, j)} \\ 0, Otherwise \end{cases} \tag{10}$$

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

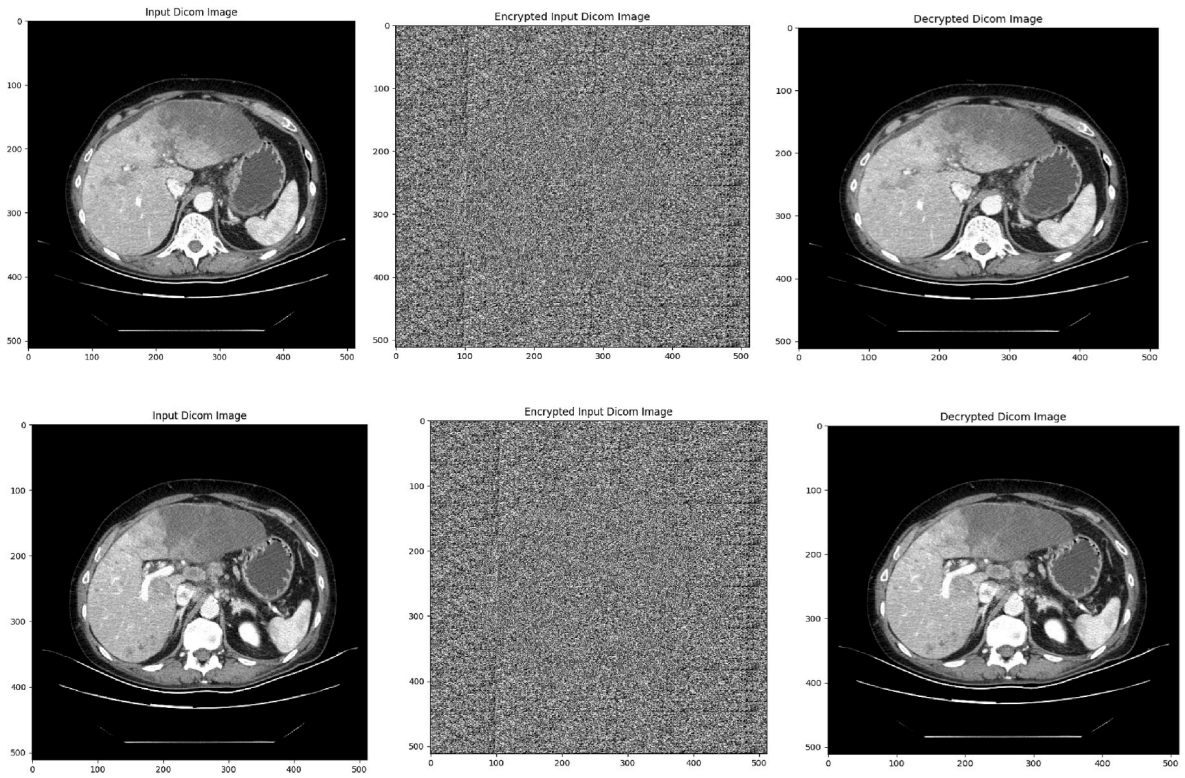


Fig. 5. The first column represents the input DICOM images (D4, D5), the second column represents the encrypted images, and the third column represents the decrypted images.

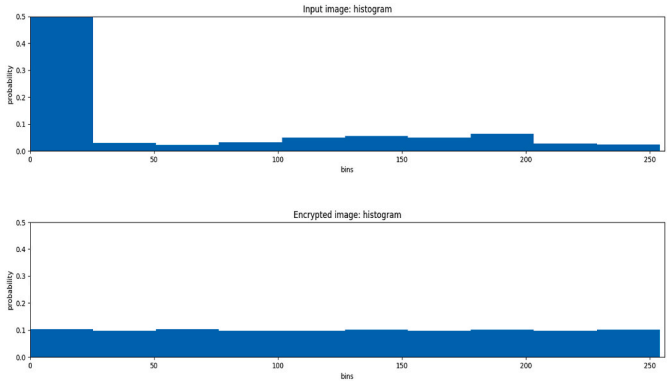


Fig. 6. Input image histogram and its encrypted version histogram corresponding to D1.

$$PSNR = 10 \times log_{10}\left[\frac{M \times N \times 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}|(f\ (m,n) - f_d(m,n))|^2}\right] \tag{11}$$

Where $f\ (m,n) =$ Original image and $f_d(m,n) =$ Decrypted image

The information entropy is a measure of uncertainty in an image, the effective encryption has grey scale value greater than 8. The Information Entropy (IE) is given as follows

$$IE = \sum_{i=0}^{2^j - 1} P\ (S_i).\ \log_2 \frac{1}{p(S_i)} \tag{12}$$

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

Tables 1–3 below depict the performance metrics values corresponding to the encrypted image with respect to the input images.

The correlation plot corresponding to the input image D1 is depicted in Fig. 7. The negative and low correlation values show the robustness of the encryption model.

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

Table 3 below depict the PSNR and MSE values of proposed hybrid encryption model corresponding to the input DICOM images. The high value of PSNR indicates the proficiency.

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

The performance metrics evaluation reveals the proficiency of the encryption model for secure data transfer in health care sector (see Table 5). For comparative analysis, the proposed LFSR encryption model was compared with the existing works [13–16], represented in Table 6. The hardware implementation of the proposed encryption model was done in Raspberry Pi B+ model processor, programming was done using python. Raspberry Pi B+ model was found to be efficient for the medical image processing applications. Raspberry Pi B+ model embedded processor comprises of 1.4 GHz 64-bit quad-core processor with Ethernet facility for cloud computing application. The Raspberry Pi B+ processor was found to be proficient for telemedicine application, depicted in Fig. 8.

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
D5	1.00462	0.02647	0.00667	0.0264

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

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
D5	54.18	0.2480

Pi B+ processor based system was found to be proficient for telemedicine application, depicted in Fig. 8.

The comparison of proposed LFSR cryptography model with the existing works reveals its proficiency in secure data transfer through the cloud network.

5. Conclusion

Medical image encryption gains prominence in the transfer of medical data and the big data handling is a crucial task in the today's digital environment. The proposed research work employs LFSR based algorithm for the encryption/decryption of medical images. The encrypted data was fed to the cloud platform and receiver side node decrypts the data. The performance validation was done by metrics such as correlation coefficient, PSNR, MSE, UACI, NPCR and entropy measures. The IoT implementation paves a way towards the efficient secure data transfer through the cloud network for telemedicine application. The comparison of the proposed LFSR algorithm with the existing approaches reveals its efficiency in terms of the performance metrics. The future work will be focusing on the implementation of hyper chaotic encryption algorithms on the real time medical images.

Contributions

The author Siju John performs the algorithm development and coding

The author S.N Kumar performs the IoT implementation and helps in the overall preparation of the manuscript.

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]
D5	[0.97981, 0.9653, 0.9592], [0.1334,0.0580, −0.0156]

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

Reference details of encryption model	Entropy
[13]	7.9995
[14]	7.9993
[15]	7.9995
[16] Proposed hybrid encryption model	7.9999 7.9991

The PSNR value comparison of proposed encryption model 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 (dB)
[16] Lena	39.51
[16] Ultrasound	39.54
[16] MRI	39.75
[16] Endoscopy	39.67
[17] Medical Image	39.51
Proposed hybrid encryption model	>50

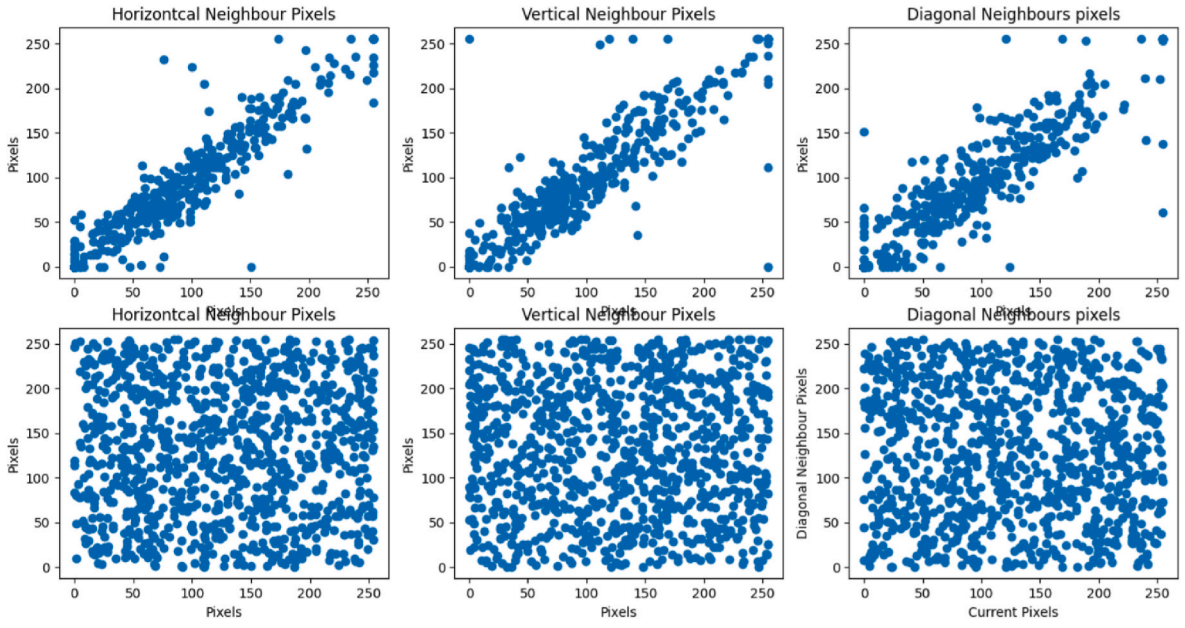
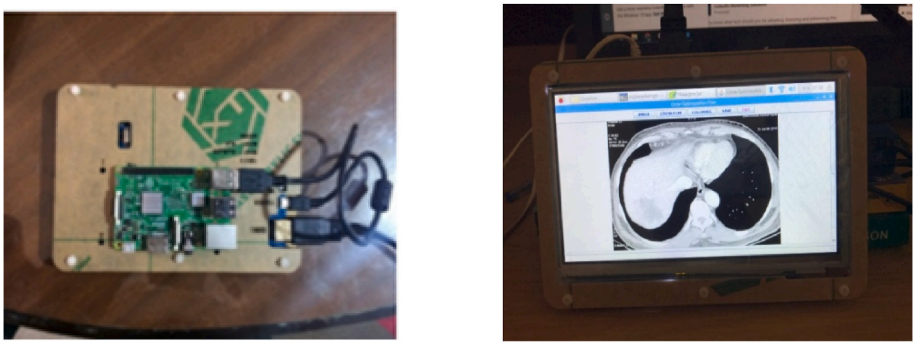


Fig. 7. Correlation plot corresponding to the input and encrypted image corresponding to the D1.



(a) (b)

Fig. 8. (a) Back view of the portable system, (b) Front view of the portable system.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgement

The author Mr Siju John would like to acknowledge the support from the LUC Marian Research Center (LUC MRC), a joint Research Centre of Marian College Kuttikkanam (Autonomous) Kerala, India and the Lincoln University College (LUC) Malaysia.

References

[1] P.R. Sankpal, P.A. Vijaya, Image encryption using chaotic maps: a survey, Proc. - 2014 5th Int. Conf. Signal Image Process. ICSIP 2014 (2014) 102–107, https://doi.org/10.1109/ICSIP.2014.80.
[2] A.A.P. Ratna, et al., Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion, Adv. Sci. Technol. Eng. Syst. 6 (1) (2021) 316–326, https://doi.org/10.25046/aj060136.
[3] G.B. Suresh, V. Mathivanan, Chaos based image encryption, Indones. J. Electr. Eng. Comput. Sci. 9 (1) (2018) 97–100, https://doi.org/10.11591/ijeecs.v9.i1.pp97-100.
[4] N. Mekki, M. Hamdi, T. Aguili, T.H. Kim, A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system, Proc. - 2018 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2018 (May) (2018) 1–10, https://doi.org/10.1109/COMMNET.2018.8360271.
[5] P. Puech, E. Chazard, L. Lemaitre, R. Beuscart, DicomWorks Teleradiology: secure transmission of medical images over the Internet at low cost, in: 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, IEEE, 2007, pp. 6705–6708. Aug 22.
[6] S.J. Sheela, K.V. Suresh, D. Tandur, A. Sanjay, Cellular neural network-based medical image encryption, Nov, SN Computer Science 1 (6) (2020), 1-1.
[7] B. Bose, D. Dey, A. Sengupta, N. Mulchandani, A. Patra, A novel medical image encryption using cyclic coding in covid-19 pandemic situation, in: Journal of Physics: Conference Series, vol. 1797, IOP Publishing, 2021 Feb 1, 012035. No. 1.
[8] L. Zhou, R. Thieret, V. Watzlaf, D. DeAlmeida, B. Parmanto, A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and validation, Int. J. Telerehabilitation 11 (1) (2019) 3.
[9] J.D. Young, S.A. Borgetti, P.J. Clapham, Telehealth: exploring the ethical issues, DePaul J. health care law 19 (3) (2018) 2.
[10] Y.Z. Almallah, D.J. Doyle, Telehealth in the time of Corona:'doctor in the house, Intern. Med. J. 50 (12) (2020 Dec) 1578–1583.
[11] D.F. Gros, L.A. Morland, C.J. Greene, R. Acierno, M. Strachan, L.E. Egede, P. W. Tuerk, H. Myrick, B.C. Frueh, Delivery of evidence-based psychotherapy via video telehealth, J. Psychopathol. Behav. Assess. 35 (4) (2013 Dec) 506–521.
[12] K. Burbury, Z.W. Wong, D. Yip, H. Thomas, P. Brooks, L. Gilham, A. Piper, I. Solo, C. Underhill, Telehealth in cancer care: during and beyond the COVID-19 pandemic, Intern. Med. J. 51 (1) (2021 Jan) 125–133.
[13] S.A. Powers, K.N. Perry, A.J. Ashdown, M. Pacailler, M.W. Scerbo, Human factors considerations for patients: a cursory review of telehealth guidelines, No. 1, in: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 65SAGE Publications, Los Angeles, CA, 2021 Sep, pp. 943–947. Sage CA.
[14] Y. Dou, M. Li, An image encryption algorithm based on compressive sensing and M Sequence, IEEE Access 8 (2020 Dec 8) 220646–220657.
[15] S. Saha, R.K. Karsh, M. Amrohi, Encryption and decryption of images using secure linear feedback shift registers, in: International Conference on Communication and Signal Processing (ICCSP) 2018 Apr 3, IEEE, 2018, 0295-0298.
[16] C. Dong, Y.W. Chen, J. Li, Y. Bai, Zero watermarking for medical images based on DFT and LFSR, in: 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), vol. 1, IEEE, 2012 May 25, pp. 22–26.
[17] S. Deb, B. Bhuyan, Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR, Multimed. Tool. Appl. 80 (13) (2021 May) 19803–19826.
[18] D. Dey, D. Giri, B. Jana, T. Maitra, R.N. Mohapatra, Linear-feedback shift register-based multi-ant cellular automation and chaotic map-based image encryption, Security and Privacy 1 (6) (2018 Nov) e52.
[19] S. Rajagopalan, S. Rethinam, S. Janakiraman, H.N. Upadhyay, R. Amirtharajan, Cellular automata+ LFSR+ synthetic image: a trio approach to image encryption, in: 2017 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2017 Jan 5, pp. 1–6.
[20] Y. Lv, X. Tong, A novel method of chaotic image encryption based on LFSR, in: 2009 International Conference on Management and Service Science, IEEE, 2009 Sep 20, pp. 1–4.
[21] B. Mondal, N. Sinha, T. Mandal, A secure image encryption algorithm using lfsr and rc4 key stream generator, in: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Springer, New Delhi, 2016, pp. 227–237.
[22] M. Dridi, B. Bouallegue, M.A. Hajjaji, A. Mtibaa, An enhancement crypto-compression scheme for image based on chaotic system, Int. J. Appl. Eng. Res. 11 (7) (2016) 4718–4725.
[23] N. Tsafack, J. Kengne, B. Abd-El-Atty, A.M. Iliyasu, K. Hirota, A.A. Abd EL-Latif, Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption, Inf. Sci. 515 (2020) 191–217.
[24] Y. Zhang, The fast image encryption algorithm based on lifting scheme and chaos, Inf. Sci. 520 (2020) 177–194.
[25] M. Gafsi, N. Abbassi, M.A. Hajjaji, J. Malek, A. Mtibaa, Improved Chaos-Based Cryptosystem for Medical Image Encryption and Decryption, Scientific Programming, 2020, 2020.
[26] S. Rajendran, M. Doraipandian, Chaos based secure medical image transmission model for IoT-powered healthcare systems, in: IOP Conference Series: Materials Science and Engineering, vol. 1022, IOP Publishing, 2021, 012106. No. 1.
[27] A. Belazi, S. Kharbech, M.N. Aslam, M. Talha, W. Xiang, A.M. Iliyasu, A.A. Abd El-Latif, Improved Sine-Tangent chaotic map with application in medical images encryption, J. Inf. Secur. Appl. 66 (2022 May 1), 103131.
[28] V. Saliba, H. Legido-Quigley, R. Hallik, A. Aaviksoo, J. Car, M. McKee, Telemedicine across borders: a systematic review of factors that hinder or support implementation, Int. J. Med. Inf. 81 (12) (2012) 793–809.
[29] K. Amara Korba, A. Djamel, F. Mohamed, B. Djalil, New chaotic map for real-time medical imaging system in e-Health, J. Ambient Intell. Hum. Comput. (2022 Sep 6), 1-11.
[30] X. Wang, Y. Wang, Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points, Expert Syst. Appl. 213 (2023), 118924.