Hindawi
Security and Communication Networks
Volume 2023, Article ID 9801983, 1 page
https://doi.org/10.1155/2023/9801983

*Retraction*

# Retracted: Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare

**Security and Communication Networks**

Received 13 September 2023; Accepted 13 September 2023; Published 14 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

## References

[1] P. Rashmi, M. C. Supriya, and Q. Hua, "Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare," *Security and Communication Networks*, vol. 2022, Article ID 9363377, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9363377, 9 pages
https://doi.org/10.1155/2022/9363377

*Research Article*

# Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare

**P. Rashmi**,[1] **M. C. Supriya**,[2] **and Qiaozhi Hua**[3]

[1] *Research Scholar Sri Siddhartha Academy of Higher Education, Tumakuru, India*
[2] *Professor Dept of ISE SSIT Tumakuru, Sri Siddhartha Academy of Higher Education, Tumakuru, India*
[3] *Computer School, Hubei University of Arts and Science, Xiangyang 441000, China*

Correspondence should be addressed to Qiaozhi Hua; 11722@hbuas.edu.cn

Received 23 August 2021; Revised 28 September 2021; Accepted 11 January 2022; Published 27 February 2022

Academic Editor: Chinmay Chakraborty

Image encryption is highly required in the big data healthcare cloud to improve the security of the medical image for remote access. Data hiding method is the process of storing the medical information of the patient in the medical image in the hidden format. Many existing data hiding methods are based on wavelet and chaotic map due to its effectiveness. Wavelet based methods have limitations of lack of phase information, poor directionality, and shift sensitivity. Chaotic map is applied to improve the security of the medical image and chaotic map has the limitation of low sensitive to control parameters and initial conditions. In this research, the Improved Chaos Encryption (ICE) is applied to improve the security based on randomness. The average energy is calculated in the images and compared with adaptive threshold to segment the Lorenz 96 model applied in the chaos encryption algorithm to improve the model security. Lorenz 96 increased the randomness of the chaos encryption method due to its high sensitivity. Medial images were used to test the performance of the ICE in the image encryption and image hiding. The proposed ICE model evaluated the quality of the recovered and decrypted image in the various embedding rate. The result shows that the proposed ICE model has the PSNR value of 104.7 dB compared to the LSB-ROI method which has 97.61 dB PSNR.

## 1. Introduction

In medical images stored in the cloud, the data hiding method is used to store the medical images of patient for remote access. Healthcare generates a bigger amount of data related to the patient for diagnosis purposes. The encoding method is used in the data hiding approach to store the medical record in the medical images. Decoding is performed in the client side to extract the hidden data and also find digital content that has been attacked. Two types of methods are present in data hiding, namely, steganography and watermarking [1–11]. In reversible data hiding (RDH), the original cover or the region of interest (ROI) is restored losslessly and the remaining part of the images is restored in lossy manner. The RDH plays an important role in medical image processing and in other applications such as big data healthcare, image transcoding, and multimedia archive management [12]. Image encryption method is applied to secure the image and the images can be restored based on authentication to protect the data from users or attackers. Image encryption is required in the medical images to store in cloud and to protect the privacy of the patients [13]. Electronic Patient Record (EPR) consists of patient ID's information, diagnostics reports, and vital signs. The EPR is hidden in the medical images to store in cloud for authenticated information [14]. Most of the RDH method aims to enhance the embedding rate and quality of the images for encryption.

The patient's sensitive information stored in the cloud has the chance to be leaked to hackers with malicious intent. In medical information systems, the protection of patient's privacy and medical images plays an important role and attained more attention [15–26]. Medical images transmission or storage in cloud is easily accessible by the hacker that creates privacy issue. Data hiding method prevents information from unauthorized access and protects the privacy of data. Medical images such as computed tomography (CT), ultrasound, X-ray, and magnetic resonance imaging (MRI) created by imaging devices are used as the cover image [27–32]. The chaotic method is used in the image encryption to improve the security based on the features of initial values of nonlinearity, pseudorandomness, and sensitivity. The chaotic encryption method is widely followed in the encryption process due to its features [33, 34]. The discrete chaotic maps are sensitive to control parameters and initial conditions that increase randomness being deterministic, unpredictable, and easily reproducible [35]. In this research, the ICE method is proposed to increase the privacy of the data in the cloud. Medical images were used to test the proposed model's efficiency in various embedding rate.

(1) This research aims to measure average energy in the images and, compared with adaptive threshold, to segment the image into ROI, RONI, and border area. The ROI is encrypted and decrypted in lossless manner and RONI is retrieved in lossy manner.

(2) The objective of this research is to apply Lorenz 96 model in chaos encryption method to increase the sensitivity to initial value and resilience against the various kinds of attacks. The random value is set in the chaotic sequence generator to enhance the ability in attack resistance.

(3) The PSNR value is measured for various embedding rate in the medical images to evaluate the quality of retrieved images. The proposed Lorenz-chaotic encryption method is compared with state-of-the-art method to evaluate the efficiency.

(4) The proposed ICE model has achieved the PSNR value of 104.7 dB and existing LSB-ROI method has 97.61 dB PSNR. The proposed method has achieved higher performance due to its sensitivity to initial condition.

The review of recent researches in the image encryption and data hiding methods is given in Section 2, the proposed ICE method, image embedding, and recovery were given in Section 3, results of the proposed ICE method are given in Section 4, and conclusion is given in Section 5.

## 2. Related Works

Medical information storing in cloud for remote access requires effective encryption method to protect the privacy of the medical data. Data hiding or embedding techniques were applied to store the sensitive information in the image. ROI-based methods show the considerable performance in encryption and preserve the quality of the image. Chaotic based encryption method increases the efficiency of the encryption.

Parah et al. [36] applied the Intermediate Significant Bit Substitution (ISBS) to embed the checksum data, watermark data, and EPR to eliminate commonly used Least Significant Bit (LSB) replacement/removal attacks. Chen and Chi [37] applied Block Truncation Coding (BTC) method for data hiding and compression method to reduce the image size and improve the security. The block classification method is applied to classify the blocks into three types such as smooth blocks, and two complex blocks. Applied separate method for three types of block for data hiding and encryption. Loan et al. [38] applied hybrid edge detection method and Pixel Repetition Method (PRM) for the data hiding in medical image. The PRM is applied to increase the small size image and hybrid edge detection method is applied to preserve the edge information. Geetha and Geetha [39] applied the Rhombus Mean Interpolation method to predict the interpolated points for data hiding method. Checksum is applied in the nonoverlapping method to embed for content authentication and tamper detection. The modified LSB based methods such as ISBS [36], BTC [37], PRM [38], and Rhombus Mean Interpolation [39] have limitations of high loss of information due to rearranging of image.

Yang et al. [40] applied adaptive threshold method to automatically segment ROI and RONI in the medical images. To enhance the ROI, the grayscale is stretched and data is embedded in the stretched histogram peak bins. Gao et al. [41] applied reversible data hiding (RDH) and contrast enhanced algorithm to improve the image quality and embedding capacity. The developed algorithm separates ROI and NROI in the medical images and stretches the ROI's gray level histogram. Balasamy and Suganyadevi [42] applied fuzzy based ROI selection method and wavelet transformation method to embed the encrypted watermark in medical images. Fuzzification method is applied to measure the critical points based on the final and central intensity with selected ROI. Wu et al. [43] applied Otsu's method for image segmentation to enhance the ROI in the medical images before contrast enhancing. The GrabCut interactive algorithm is used to accurately segment the ROI in medical images. The analysis of the proposed GrabCut method in medical images shows that the proposed method is effective in encryption and data hiding. Zhou et al. [44] proposed game theory with hidden ROI position and optimized ROI parameters for lossless medical image encryption. The Quantum Cell Neural Network (QCNN) hyperchaotic model generates random sequence to diffuse and scramble ROI. The result shows that the game theory provides optimal balance between the encryption speed and security performance. Priya and Santhi [45] proposed nonembedding image encryption to conceal the presence of the watermark in the medical image. The biometric authentication is applied to decrypt the information in the medical image. The developed method prevents the intentional and unintentional attacks. Ding et al. [46] applied Deep Learning based Encryption and Decryption Network (DLEDNet) method for the encryption and decryption in the medical images. Main learning network is applied in Cycle-GAN to transfer the medical images. The adaptive threshold methods [40, 41] have higher performance in the segmentation and has lower embedding rate in data hiding. The fuzzy [42] method is supervised method and manual features are required for segmentation in data hiding. Otsu's method [43] changes the modality of histogram due to global thresholding and degrades the images. The QCNN [44] and DLEDNet [46] model have limitation of overfitting and authentication method [45], which has lower sensitivity for data hiding.

Yin and Li [47] proposed modified quantum chaos system and Particle Swarm Optimization (PSO) with genetic simulated annealing method for the medical image encryption. The modified chaos system method is applied for key stream and genetic algorithm is applied for the selection and cross operation to process the plaintext images. Simulated annealing method is applied to scramble the image to generate the optimal sequence. The PSO method is applied to process the simulation annealing. Liu et al. [48] partition the ROI and NROI in the medical image using ROI-based reversible data hiding method. An encryption key is applied to encrypt ROI and NROI in the medical images. The LSB of the EPR and encrypted ROI is concatenate in the data hider. The LSB substitution method is applied to embed the concatenate data in the medical image. Zhang et al. [49] proposed hyperchaotic system for the encryption of medical images and embedded the patient private information in ROI based on reversible data hiding method. The developed method has low distortion and high embedding capacity in the data hiding process and also improves the security of the encryption phase. Anand and Singh [50] applied Singular Value Decomposition (SVD)-Discrete Wavelet Transform (DWT) to embed the multiwatermarks in medical images. Hamming code is applied to decrease the channel noise distortion in the text watermark. The chaotic-LZW has the higher efficiency in data hiding and security in the medical image. Kumar et al. [51] applied chaotic map on the fractional Discrete Cosine Transform (FrDCT) on the medical images. The result shows that the proposed model has the higher efficiency in improving the security in the data hiding. Ravichandran et al. [52] provided the hybrid encryption method based on chaotic map and deoxyribonucleic acid to be adaptable for selective and full medical image encryption. The result shows that the hybrid model has the higher efficiency in the security improvement. The PSO [47] method has lower convergence in the parameter settings and encryption method [49] has lower embedding performance. The SVD-DWT [50] method has limitation of lack of phase information, poor directionality, and shift sensitivity. The chaotic map [51, 52] methods have limitations of low sensitivity in initial conditions and control parameters.

## 3. Method

Medical images required image hiding and image encryption to increase the privacy of the patient data. In this research, the ICE method is applied to increase the security of the medical encryption. Medical images were used to test the efficiency of the proposed method in the encryption. The Lorenz 96 model is applied in the chaos encryption to increase the privacy of the image. The overview of ICE model in medical image encryption is shown in Figure 1.

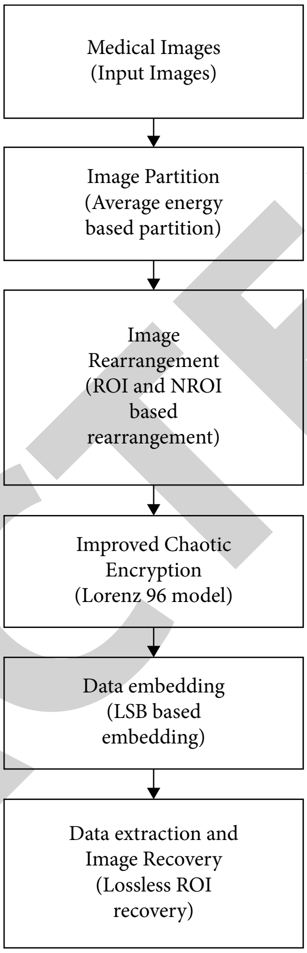
Medical Images (Input Images)
Image Partition (Average energy based partition)
Image Rearrangement (ROI and NROI based rearrangement)
Improved Chaotic Encryption (Lorenz 96 model)
Data embedding (LSB based embedding)
Data extraction and Image Recovery (Lossless ROI recovery)

Figure 1: The overview of the proposed ICE method.

## 4. Image Partition

The original input medical image $I$ is divided into three parts such as border area, ROI, and region of noninterest (RONI). In most cases, the ROI is irregular shape in medical images. The image bottom line is the border area and ROI vertices are used to describe ROI, denoted by $D_{\mathrm{roi}}$ with length $L_c$.

The size of input medical image is $N_1 \times N_2$ and is first divided into block size of $n_1 \times n_2$. The amount of blocks is $(N_1 \times N_2)/(n_1 \times n_2)$. Every block average energy is measured using the following formula:

$$\text{average energy}\,(m, n) = \frac{\sum_{i=1}^{n_1} \sum_{j=1}^{n_2} I\,(i, j)^2}{n_1 \times n_2}, \qquad (1)$$

where Average energy $(m, n)$ denotes the current block average energy, the image blocks position is denoted as $(m, n)$, and the pixel value is denoted as $I\,(i,\ j)$. Every block average energy value with an adaptive threshold $T$ determines the ROI. If average energy $(m,\ n) > T$, then it belongs to the ROI; otherwise, the blocks belong to RONI.

The ROI is carried out in lossless retrieval and RONI is carried out in lossy retrieval. The ROI is placed in front concatenated by border area and RONI. The rearrangement operation can improve the security.

*4.1. Chaotic Encryption Algorithm.* A chaotic system providing chaotic sequence is applied for the image encryption for medical images [53–55]. The encryption method robustness is important for the medical image encryption. Since chaotic encryption method is sensitive to initial value and resilience against various kinds of attacks, the chaotic encryption method is used for encryption.

The Chen system is applied to iterate out three chaotic sequences in the chaotic state that is applied in this encryption algorithm. The Chen system is defined in the following equation:

$$\begin{cases} x = 35(y - x), \\ y = -7x - xz + 28y, \\ z = xy - 3z. \end{cases} \tag{2}$$

The proposed encryption involves four steps; they are as follows.

Step 1: the image matrix is denoted as $P = [p]_{512\times512}$. Initial value is selected as $K' = [k_0', k_1', k_2', k_3']$, where $k_0' \leq 512 \times 512$; the scrambling algorithm iteration is set to 50; the chaotic Chen system initial value is denoted in triplet $[k_1', k_2', k_3']$, and it is randomly set to $[0.0663598, 0.45679, 0.9256]$. This random operation is applied to enhance the encryption algorithm ability to attack resistance.

Step 2: the Chen system and key group obtains the chaotic sequences of $C_1$, $C_2$, $C_3$ and three sequences consist of bits 1001 to $1000 + M \times N$ to chaos discard (secret image size is denoted as $M \times N$).

Step 3: the Helical scan sort matrix is denoted as $A$ and the scrambling iteration is used to calculate $A'$, as in the following equation:

$$A_i' \begin{cases} \text{rotation}(A, 90), & 0 < C_1(i) < 0.25, \\ \text{rotation}(A, 180), & 0.25 \leq C_1(i) < 0.5, \\ \text{rotation}(A, 270), & 0.5 \leq C_1(i) < 0.75, \\ \text{rotation}(A, 270), & 70.75 \leq C_1(i) < 1. \end{cases} \tag{3}$$

The simplest version of Lorenz 96 model based on periodic system of $K(k = 1, \ldots, K)$ is

$$\frac{\mathrm{d}X_k}{\mathrm{d}t} = -X_{k-1}\left(X_{k-2} - X_{k+1}\right) - X_k + F. \tag{4}$$

Advection term is first term on the right hand side, damping is represented as second term, and external forcing term is provided as $F$ that is set as 10.

Two-level version of Lorenz 96 model is applied for parameter estimation and this will add another periodic variable $Y$. The $X$ and $Y$ are linked in coupling term that is last term in equation. Each $X$ has $J$ $Y$ variables related with it.

$X$ is resolved, slow variables, and $Y$ is fast and unresolved variables. The task is to represent a parameterization on fast variables effect on $X$ and replace last term in $X$ equation for convenience.

Consider ignoring correlation in space and time, modelling $B_k$ as a local function of $X_k$, as given in

$$-hc\overline{Y}_k \coloneqq B_k \approx (X_k). \tag{5}$$

A linear regression is applied for simplest parameterization, as given in equation

$$B_k = aX_k + b. \tag{6}$$

Advantages of Lorenz 96 model are discussed as below:

Multiscale: Lorenz 96 model is applied for parameterization in chaotic map that is divided into resolved and unresolved processes.
Encryption complexity: as Lorenz 96 model increases the randomness and sensitivity of chaotic map parameter, the complexity of the model to decrypt is high which improves the security.

The Lorenz 96 model has been applied in the chaos encryption method to improve the security of the model.

$$L = (x_{m+1} - x_{m-2})x_{m-1} - x_m + F, \tag{7}$$

where $m = 1, \ldots, M$, $x = x_{M-1}$, $x_0 = x_M$, and $x_{M+1} = x_1$. This model mimics an meteorological quality of unspecified scalar time evolution, $x$, and latitude circle of equidistant grid $M$.

Let $P = [p]_{512\times512} = [p_0]_{512\times512}$, and get the chaotic sequence $C_2$ of index $S$ in order. Then, $P_i' = [p_i']_{512\times512}$ is determined, as in

$$p_i' = \left(A_i'(S(j))\right) = p_{i-1}(j), \quad j = 1, 2, \ldots, 512 \times 512, \tag{8}$$

where $i = 1, 2, \ldots, k_0'$, and the scrambling process is repeated $k_0^{\text{'}}$ times. Finally, $P' = P'k_0'$.

Step 4: $P' = [p']_{512\times512}$ and $C_3$ using the chaotic diffusion diffuse the matrix $P'' = [p'']_{512\times512}$ as shown in the following equation:

$$p''(j) = \begin{cases} p'(j) \oplus \left(\text{mod}\left(C_3(j) \times 1000, 256\right)\right), & j = 1, \\ p'(j) \oplus p'(j-1) \oplus \left(\text{mod}\left(C_3 \times 1000, 256\right)\right), \\ j = 2, 3, \ldots, M \times N. \end{cases} \tag{9}$$

Cipher secret image $P''$ is obtained in four steps with a key sequence $K'$. Original.

Four steps help to obtain a key sequence $K'$ and cipher secret image $P''$. The encryption and decryption are carried out based on key sequence and decryption is inverse of encryption.

*4.2. Data Embedding.* From the appointed position $L(x, y)$, $D_{\text{roi}}$ and $H$ are embedded into the LSBs border area and the key is used to control the position. Note that the data owner or third party cannot access the original image content without the encryption key; thus the owner content privacy is protected.

The data is embedded into the encrypted medical image.

Step 1: the LSB is read to obtain $D_{\mathrm{roi}}$ and embedded in the border area appointed position $L(x,y)$ and shared key is used to control the position.

Step 2: after vertex ROI information, the LSB-plane ROI is recorded by data hider, denoted as $D_{\mathrm{lsb}}$.

Step 3: the EPR and $D_{\mathrm{lsb}}$ are concatenated to form the embedded data $W$, as shown in

$$W = D_{\mathrm{lsb}} + \mathrm{EPR}. \tag{10}$$

Here, the concatenation operation is indicated using "+," the LSB substitution is used by data hider to embed W, and embedding process end position is pointed out by an ending label into encrypted image except for the border area.

Embedding is performed based on single LSB plane and more information is embedded based on two or more LSB planes.

*4.3. Data Extraction and Image Recovery.* In the image recovery and data extraction, three cases are analyzed, namely, receiver having (i) only data-hiding key, (ii) only the encryption key, and (iii) both encryption and data-hiding key.

*Case 1.* The receiver with the data-hiding key can read the embedded data and the original image cannot be obtained. From the border area given position $L(x,y)$, $D_{\mathrm{roi}}$ can be read, and then ROI size and vertex information can be obtained. From first pixel to ending label, the LSB-plane is read and embedded $W$ is extracted successfully. The $W$ is separated into EPR and $D_{\mathrm{lsb}}$, as given in (6).

*Case 2.* The receiver with encryption key roughly recovers the original image and embedded data is not obtained. From the border area of appointed position $L(x,y)$, $D_{\mathrm{roi}}$ is read, and then ROI size is obtained. The receiver decrypts the image with the encryption key except the LSB plane. The inverse of encryption process is decryption. The ROI is rearranged to its original position based on $D_{\mathrm{roi}}$. Encrypted image most significant bits (MSB) are not altered by the data embedding operation; the decrypted MSB is same as the original MSB. The decrypted image content is similar to the original image.

*Case 3.* If the receiver has both encryption key and data-hiding key, both embedded data and losslessly recovered ROI.

Step 1: based on the data hiding key, $D_{\mathrm{lsb}}$ and EPR can be obtained.

Step 2: the encrypted ROI LSB plane is recovered with $D_{\mathrm{lsb}}$.

Step 3: from the border area of appointed position $L(x,y)$, $D_{\mathrm{roi}}$ and $H$ can be read.

Step 4: the embedded data is calculated in decrypted version according to the encryption key.

Step 5: ROI is losslessly recovered and returns to its original position with $D_{\mathrm{roi}}$.

Step 6: integrity authentication: $H'$ denotes recovered ROI hash message. If $H$ is equal to $H'$, the image is authentic; otherwise ROI has been tampered.

## 5. Result

Data hiding and image encryption techniques are required in the medical images in the cloud for remote access. In this research, ICE method is proposed to encrypt the images with data hiding method. The 18 medical images from online available dataset (http://imaging.cancer.gov/) were used in this method to test the efficiency of the ICE method. Input medical images in the size of 512 × 512 (16 bits). Each vertex coordinates are represented by 20 bits. The test images used to test model performance are shown in Figure 2.

The proposed ICE method is applied for the data hiding and image encryption to transfer the image in the cloud. In the client side, the decryption is performed to retrieve the original images with hidden data. The input images, rearrange image, encrypted image, encrypted and embedded image, recovered image, and directly decrypted image are shown in Figure 3. The rearrange operation increases the security of the ROI. The embedding rate of each pixel is set as 0.5 and assume that ROI size is set as 5% in the image. The PSNR value of the decrypted image is achieved as 105.12 dB.

The proposed ICE method recovered images PSNR value for various embedding rate is shown in Table 1. The three images such as Im 1, Im 5, and Im 9 were selected for the PSNR analysis in three LSB planes. The average PSNR value of 18 images is presented in the table for three LSB planes and various embedding rate. The increases in embedding rate decrease the PSNR value of the image and single LSB plane has higher quality compared to 2 or 3 planes. The single LSB plane and lower embedding rate have higher quality of image in the analysis. The lower embedding rate has less data in RONI and less distortion in extracting embedded data. The proposed ICE method of recovered images average PSNR value of 18 medical images is given in Table 1.

The increases in the embedding rate decrease the PSNR value of the recovered images. The 1 LSB plane has the higher PSNR than 2 LSB planes and 3 LSB planes. The average PSNR values for 18 images for various embedding rate and LSB plane are presented in Table 2. The less embedding rate has less distortion in the data recovery and payload is less for single LSB plane. The quality of image is high for less embedding rate and single LSB plane in data recovery. The proposed ICE method has the considerable PSNR value for the 0.5 embedding rate in the analysis. The average PSNR value of the ICE method for 0.5 embedding rate is 104.21 and average PSNR value for 0.1 embedding rate is 114.42 dB in the analysis.

The proposed ICE method of directly decrypted images for various embedding rate is shown in Table 2. The increases

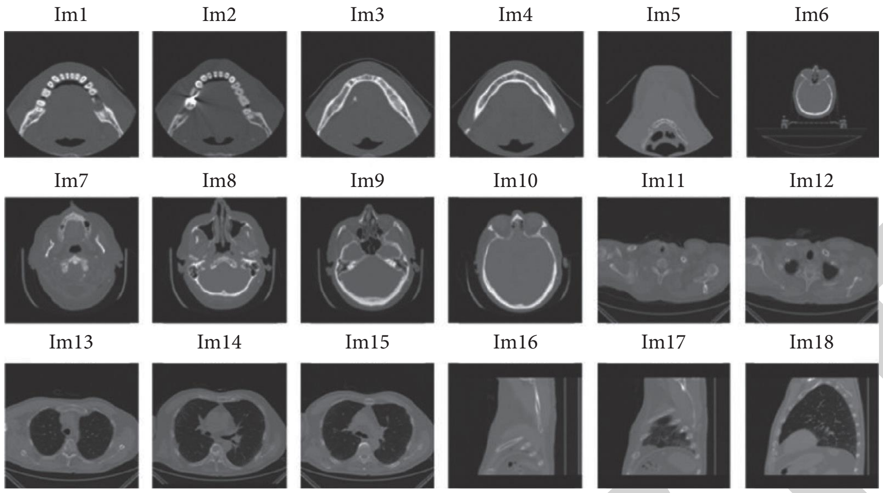

Figure 2: Test images for data hiding and image encryption.

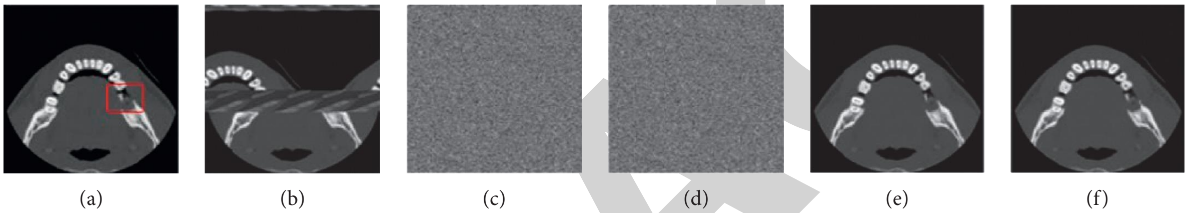

Figure 3: The proposed model: (a) input image, (b) rearranged image, (c) encrypted image, (d) encrypted and embedded image, and (e) directly decrypted image and (f) recovered image.

Table 1: Recovered image PSNR for the various embedding rate.

| Embedding rate | | PSNR | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 0.005 | 0.01 | 0.05 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
| Im 1 | 1 LSB plane | 132.41 | 132.14 | 118.1 | 113.06 | 110.06 | 107.08 | 105.6 | 104.07 |
| | 2 LSB planes | 115.1 | 114.87 | 110.2 | 105.07 | 103.12 | 101.26 | 100.12 | 99.76 |
| | 3 LSB planes | 106.15 | 105.47 | 101.76 | 99.43 | 97.42 | 95.41 | 94.32 | 93.13 |
| Im 5 | 1 LSB plane | 135.67 | 133.46 | 116.36 | 110.62 | 109.64 | 107.68 | 105.61 | 104.21 |
| | 2 LSB planes | 115.61 | 114.28 | 110.21 | 105.61 | 104.62 | 101.32 | 101.16 | 99.16 |
| | 3 LSB planes | 105.12 | 104.21 | 102.26 | 101.54 | 99.42 | 96.32 | 95.53 | 94.21 |
| Im 9 | 1 LSB plane | 134.51 | 133.43 | 116.87 | 113.26 | 110.43 | 107.62 | 106.32 | 106.42 |
| | 2 LSB planes | 115.62 | 114.32 | 110.72 | 107.24 | 105.34 | 103.16 | 102.12 | 101.53 |
| | 3 LSB planes | 106.21 | 105.54 | 103.31 | 101.41 | 97.62 | 96.37 | 95.21 | 94.17 |
| Average value | 1 LSB plane | 134.52 | 135.47 | 117.61 | 114.42 | 109.21 | 108.43 | 105.12 | 104.21 |
| | 2 LSB planes | 115.21 | 114.67 | 109.37 | 106.31 | 103.64 | 101.21 | 101.13 | 99.87 |
| | 3 LSB planes | 106.72 | 105.32 | 102.36 | 99.24 | 97.61 | 95.62 | 95.12 | 94.31 |

in the embedding rate and LSB plane decrease the PSNR value of the directly decrypted images. The ICE model has the considerable PSNR value for the 0.5 embedding rate. The ICE model average PSNR value for 0.5 embedding rate is 105.61 dB and average PSNR of 109.61 dB for 0.1 embedding rate.

The average PSNR values for the 18 medical images of the ICE and existing methods for various embedding rate are compared in Figure 4. The result shows that proposed ICE method has the higher PSNR value compared to existing methods in the image encryption and data hiding. The existing methods [48, 49, 51, 52] have created the error value in the recovery of the images and the proposed model has lower error value compared to the existing models, which improves the image quality.

The ICE model is evaluated in the data hiding and image encryption in terms of SSIM, NPCR, UACI, and Entropy, as shown in Table 3. The proposed ICE model has higher efficiency than existing methods. The ICE method has the advantage of lossless retrieval of image in ROI region and improved the security of the model. The existing model [52] has produced the error in the retrieval process which affects the image quality. The ICE has 99.62 NPCR and existing method [52] has 99.32 NPCR in the image encryption.

Table 2: Directly decrypted images of PSNR for various embedding rate.

| Embedding rate | | PSNR | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 0.005 | 0.01 | 0.05 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
| Im 1 | 1 LSB plane | 116.12 | 115.21 | 114.16 | 110.26 | 107.32 | 106.41 | 105.34 | 105.12 |
| | 2 LSB planes | 111.23 | 110.61 | 108.61 | 106.32 | 104.41 | 102.31 | 101.21 | 99.43 |
| | 3 LSB planes | 105.32 | 105.21 | 103.32 | 101.17 | 99.43 | 96.32 | 95.51 | 94.21 |
| Im 5 | 1 LSB plane | 115.61 | 114.32 | 113.24 | 110.41 | 107.64 | 106.32 | 105.33 | 106.43 |
| | 2 LSB planes | 110.62 | 109.14 | 106.62 | 104.61 | 102.44 | 101.47 | 99.71 | 98.12 |
| | 3 LSB planes | 105.61 | 104.21 | 103.14 | 98.42 | 97.64 | 95.52 | 94.61 | 93.16 |
| Im 9 | 1 LSB plane | 115.71 | 116.46 | 114.21 | 109.61 | 107.61 | 105.31 | 105.21 | 103.57 |
| | 2 LSB planes | 111.49 | 110.76 | 107.81 | 105.65 | 103.47 | 103.45 | 101.32 | 99.46 |
| | 3 LSB planes | 106.21 | 104.24 | 101.26 | 99.24 | 97.45 | 96.78 | 95.51 | 96.12 |
| Average value | 1 LSB plane | 116.45 | 115.52 | 113.24 | 109.61 | 107.61 | 106.61 | 105.52 | 105.61 |
| | 2 LSB planes | 111.26 | 110.17 | 106.42 | 105.52 | 103.32 | 101.12 | 101.31 | 98.16 |
| | 3 LSB planes | 105.52 | 103.41 | 103.31 | 101.31 | 98.43 | 95.51 | 94.51 | 94.45 |

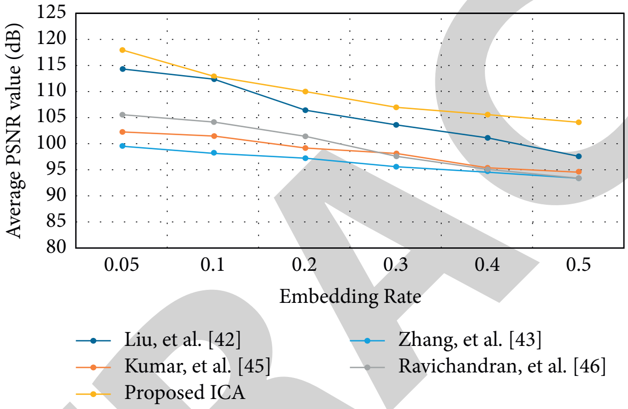

Figure 4: The average PSNR value of the proposed ICE method.

Table 3: Comparative analysis of the proposed model.

| Methods | SSIM | NPCR | UACI | Entropy |
|---|---|---|---|---|
| Liu et al. [48] | 0.9999 | 99.21 | 33.12 | 7.9922 |
| Zhang et al. [49] | 0.9941 | 99.24 | 33.17 | 7.9941 |
| Kumar et al. [51] | 0.9934 | 99.31 | 33.22 | 7.9953 |
| Ravichandran et al. [52] | 0.9972 | 99.32 | 33.24 | 7.9962 |
| Proposed ICE | 0.9999 | 99.62 | 33.41 | 7.9974 |

The proposed ICE method is compared with existing chaotic map and other encryption methods over plain-text attack, as shown in Table 4. The proposed ICE method has advantage of applying Lorenz 96 method to increase the sensitivity to initial conditions and control parameters. The existing chaotic map [41, 42] has limitation of lower sensitivity and periodic degradation on account of finite precision in the process. The wavelet transform [40] method has limitations of lack of phase information, poor directionality, and shift sensitivity. The fuzzy encryption [32] has required supervised features and PSO method [37] has lower convergence in parameter settings. The proposed ICE method has PSNR value of 134.52 and existing hybrid chaotic map has 117.3 PSNR value.

Table 4: Comparison of the proposed ICE with existing chaotic map and other encryption methods over plain-text attack.

| Methods | PSNR |
|---|---|
| Fuzzy [42] | 102.7 |
| PSO [47] | 106.5 |
| SVD-DWT [50] | 109.8 |
| FrDCT [51] | 115.1 |
| Hybrid chaotic map [52] | 117.3 |
| Proposed ICE method | 134.52 |

## 6. Conclusion

Medical images stored in the cloud require encryption to increase the security of the patient information. Data hiding method is applied to store the patient data in the medical image in the hidden format. In this research, the ICE method is applied to improve the security of the medical image and improves the quality of the image. The medical images were used to evaluate the performance of the proposed ICE and existing method. The proposed method is tested for quality in various embedding rate. The Lorenz 96 model is applied in the chaos method to improve the security based on increases of random value. The result shows that the proposed ICE method has 104.07 dB PSNR and the existing model has 97.61 dB PSNR value. The future work of the proposed model involves an effective data hiding technique to improve the embedding rate of the model.

## Data Availability

No data were used to support this study.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work was supported by the Hubei Natural Science Foundation under grant 2021CFB156.

## References

[1] C. Feng, B. Liu, K. Yu, S. K. Goudos, and S. Wan, "Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3582–3592, 2021.

[2] Z. Guo, K. Yu, A. Jolfaei, F. Ding, and N. Zhang, "Fuz-spam: label smoothing-based fuzzy detection of spammers in internet of things," *IEEE Transactions on Fuzzy Systems*, p. 1, 2021.

[3] K. Yu, L. Tan, S. Mumtaz et al., "Securing critical infrastructures: deep-learning-based threat detection in IIoT," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 76–82, 2021.

[4] D. Wang, Y. He, K. Yu, G. Srivastava, L. Nie, and R. Zhang, "Delay sensitive secure NOMA transmission for hierarchical HAP-LAP medical-care IoT networks," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[5] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: a blockchain-empowered approach," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 271–281, 2021.

[6] K. Yu, L. Tan, L. Lin, X. Cheng, Z. Yi, and T. Sato, "Deep-learning-empowered breast cancer auxiliary diagnosis for 5GB remote E-health," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 54–61, 2021.

[7] L. Yang, K. Yu, S. X. Yang, C. Chakraborty, Y. Lu, and T. Guo, "An intelligent trust cloud management method for secure clustering in 5G enabled internet of medical things," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[8] L. Zhen, Y. Zhang, K. Yu, N. Kumar, A. Barnawi, and Y. Xie, "Early collision detection for massive random access in satellite-based internet of things," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 5184–5189, 2021.

[9] T. Guo, K. Yu, M. Aloqaily, and S. Wan, "Constructing a prior-dependent graph for data clustering and dimension reduction in the edge of AIoT," *Future Generation Computer Systems*, vol. 128, pp. 381–394, 2022.

[10] L. Tan, K. Yu, F. Ming, X. Chen, and G. Srivastava, "Secure and resilient artificial intelligence of things: a HoneyNet approach for threat detection and situational awareness," *IEEE Consumer Electronics Magazine*, 2021.

[11] Q. Zhang, K. Yu, Z. Guo et al., "Graph neural networks-driven traffic forecasting for connected internet of vehicles," *IEEE Transactions on Network Science and Engineering*, p. 1, 2021.

[12] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Transactions on Multimedia*, vol. 22, no. 4, pp. 874–884, 2020.

[13] C. Qin, Z. He, X. Luo, and J. Dong, "Reversible data hiding in encrypted image with separable capability and high embedding capacity," *Information Sciences*, vol. 465, pp. 285–304, 2018.

[14] G. Gao, X. Wan, S. Yao, and Z. Cui, C. Zhou and C. Sun, "Reversible data hiding with contrast enhancement and tamper localization for medical images," *Information Sciences*, vol. 385-386, pp. 250–265, 2017.

[15] B. Ma, B. Li, X.-Y. Wang, C. P. Wang, J. Li, and Y.-Q. Shi, "A code division multiplexing and block classification-based real-time reversible data-hiding algorithm for medical images," *Journal of Real-Time Image Processing*, vol. 16, no. 4, pp. 857–869, 2019.

[16] K. A. Kumari, A. Sharma, C. Chakraborty, and M. Ananyaa, "Preserving health care data security and privacy using carmichael's theorem-based homomorphic encryption and modified enhanced homomorphic encryption schemes in edge computing systems," *Big Data*, 2021.

[17] H. H. Attar, A. A. Solyman, A. Alrosan, C. Chakraborty, and M. R. Khosravi, "Deterministic cooperative hybrid ring-mesh network coding for big data transmission over lossy channels in 5G networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–18, 2021.

[18] V. Ravi, H. Narasimhan, C. Chakraborty, and T. D. Pham, "Deep learning-based meta-classifier approach for COVID-19 classification using CT scan and chest X-ray images," *Multimedia Systems*, pp. 1–15, 2021.

[19] J. Amin, M. Sharif, N. Gul, S. Kadry, and C. Chakraborty, "Quantum machine learning architecture for COVID-19 classification based on synthetic data generation using conditional adversarial neural network," *Cognitive Computation*, pp. 1–12, 2021.

[20] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13784–13795, 2020.

[21] L. Tan, K. Yu, L. Lin et al., "Speech emotion recognition enhanced traffic efficiency solution for autonomous vehicles in a 5G-enabled space-air-ground integrated intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2021.

[22] Y. Sun, J. Liu, K. Yu, M. Alazab, and K. Lin, "PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1981–1990, 2022.

[23] Y. Gong, L. Zhang, R. Liu, K. Yu, and G. Srivastava, "Nonlinear MIMO for industrial internet of things in cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5533–5541, 2021.

[24] F. Ding, G. Zhu, M. Alazab, X. Li, and K. Yu, "Deep-learning-empowered digital forensics for edge consumer electronics in 5G HetNets," *IEEE Consumer Electronics Magazine*, p. 1, 2020.

[25] L. Liu, J. Feng, Q. Pei et al., "Blockchain-Enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor-critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.

[26] W.-L. Shang, J. Chen, H. Bi, Y. Sui, Y. Chen, and H. Yu, "Impacts of COVID-19 pandemic on user behaviors and

environmental benefits of bike sharing: a big-data analysis," *Applied Energy*, vol. 285, Article ID 116429, 2021.

[27] M. Z. Konyar and S. Öztürk, "Reed Solomon coding-based medical image data hiding method against salt and pepper noise," *Symmetry*, vol. 12, no. 6, p. 899, 2020.

[28] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet of Things Journal*, p. 1, 2021.

[29] K. Yu, L. Tan, C. Yang et al., "A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings," *IEEE Internet of Things Journal*, p. 1, 2021.

[30] F. Ding, G. Zhu, Y. Li, X. Zhang, P. K. Atrey, and S. Lyu, "Anti-forensics for face swapping videos via adversarial training," *IEEE Transactions on Multimedia*, p. 1, 2021.

[31] F. Ding, K. Yu, Z. Gu, X. Li, and Y. Shi, "Perceptual enhancement for autonomous vehicles: restoring visually degraded images for context prediction via adversarial training," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2021.

[32] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2021.

[33] X. Chen and C.-J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi Journal of Biological Sciences*, vol. 24, no. 8, pp. 1821–1827, 2017.

[34] 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.

[35] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption," *Journal of Advanced Research*, vol. 10, pp. 85–98, 2018.

[36] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique," *Journal of Biomedical Informatics*, vol. 66, pp. 214–230, 2017.

[37] Y.-Y. Chen and K.-Y. Chi, "Cloud image watermarking: high quality data hiding and blind decoding scheme based on block truncation coding," *Multimedia Systems*, vol. 25, no. 5, pp. 551–563, 2019.

[38] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoon, and G. M. Bhat, "Hiding electronic patient record (epr) in medical images: a high capacity and computationally efficient technique for e-healthcare applications," *Journal of Biomedical Informatics*, vol. 73, pp. 125–136, 2017.

[39] R. Geetha and S. Geetha, "Embedding electronic patient information in clinical images: an improved and efficient reversible data hiding technique," *Multimedia Tools and Applications*, vol. 79, no. 19, pp. 12869–12890, 2020.

[40] Y. Yang, W. Zhang, D. Liang, and N. Yu, "A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18043–18065, 2018.

[41] G. Gao, S. Tong, Z. Xia, B. Wu, L. Xu, and Z. Zhao, "Reversible data hiding with automatic contrast enhancement for medical images," *Signal Processing*, vol. 178, Article ID 107817, 2021.

[42] K Balasamy and S Suganyadevi, "A Fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7167–7186, 2021.

[43] H. T. Wu, Q. Huang, Y. Cheung, L. Xu, and S. Tang, "Reversible contrast enhancement for medical images with background segmentation," *IET Image Processing*, vol. 14, no. 2, pp. 327–336, 2019.

[44] J. Zhou, J. Li, and X. Di, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position," *IEEE Access*, vol. 8, pp. 122210–122228, 2020.

[45] S. Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images," *Mobile Networks and Applications*, pp. 1–8, 2019.

[46] Y. Ding, G. Wu, D. Chen et al., "DeepEDN: a deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1504–1518, 2021.

[47] S. Yin and H. Li, "GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system," *Evolutionary Intelligence*, pp. 1–13, 2020.

[48] Y. Liu, X. Qu, and G. Xin, "A ROI-based reversible data hiding scheme in encrypted medical images," *Journal of Visual Communication and Image Representation*, vol. 39pp. 51–57, C, 2016.

[49] S. Zhang, T. Gao, and L. Gao, "A novel encryption frame for medical image with watermark based on hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2014, Article ID 240749, 11 pages, 2014.

[50] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, 2020.

[51] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical, & Biological Engineering & Computing*, vol. 57, no. 11, pp. 2517–2533, 2019.

[52] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.

[53] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dynamics*, vol. 99, no. 4, pp. 3041–3064, 2019.

[54] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[55] Q. Li, X. Wang, X. Wang et al., "A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks," *IEEE Access*, vol. 8, pp. 168166–168176, 2020.