International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/214504 Volume 9, Issue 4, July – August (2022)

RESEARCH ARTICLE

Enhanced Fractional Order Lorenz System for Medical Image Encryption in Cloud-Based Healthcare Administration

P. Suhasini
Department of Computer Science, College of Science and Humanities, SRM Institute of Science and Technology,
Kattankulathur, Chennai, Tamil Nadu, India
sp7695@srmist.edu.in

S. Kanchana
Department of Computer Science, College of Science and Humanities, SRM Institute of Science and Technology,
Kattankulathur, Chennai, Tamil Nadu, India
kanchans@srmist.edu.in

Received: 18 June 2022 / Revised: 21 July 2022 / Accepted: 24 July 2022 / Published: 30 August 2022

Abstract – Cloud technology is a new computing paradigm increasing at a frenetic pace. Recently, doctors have switched to cloud computing as it provides wide storage spaces. A medical image highlights the patient's physical condition. These medical images possess a stronger correlation and larger data volume than ordinary images. Moreover, the current image encryption methodologies have several limitations during the encryption of medical images. This paper enhances the Fractional Order Lorenz System and a Matrix Scrambling Method (FOLS-MSM) for achieving medical image encryption with maximized correlation, reliability, and high resolution. In particular, the Fractional Order Lorenz System is developed by integrating the potentialities of the Arnold map, Tent map, and Lorenz Map for attaining the image encryption process. Initially, the Arnold map is used for scrambling the initial value. Then, the tent map is used iteratively to determine the state values to locate the position of the plaintext pixel. Then, the fractional Lorenz system considers the moulded pixel as the input, and scrambling is attained using a matrix method to attain confusion. Moreover, it generates the pseudo-random sequence for performing the cross-diffusion process to obtain the encrypted image. The potentiality of the enhanced FOLS-MSM explored based on security analysis with respect to sensitivity, correlation, PSNR, key space, histogram, and entropy analysis confirmed its predominance over the baseline medical encryption schemes used for comparison.

Index Terms – Medical Images, Encryption, Fractional Order Lorenz System, Matrix Scrambling Method, Pseudo-Random Sequence, Tent Map, Arnold Map.

1. INTRODUCTION

The fast evolution of Web-based technology has driven the dramatic growth of numerous network-enabled technologies, including cloud computing, Internet-of-Things (loT), and fog computing [1]. The rapid development of information technology and communication networks has led to the widespread adoption of these new technologies in healthcare. The IoT has been offered as a promising way to enhance accuracy and provide better medical service.

Medical IoT devices, also known as the Internet of Medical Things (loMT), monitor the health status of a sick person and collect the information into medical records that are transferred to the cloud for connectivity and backup by doctors [2]. In real-world applications, the cloud storage system has been classified into five types personal, private, public, community, and hybrid.

The cloud reduces the communication costs associated with significant data transfer volumes [3]. In the modern world, telemedicine and its associated applications have revolutionized several dimensions of healthcare departments based on rapid administration and remote diagnosing processes [4].

1.1. Healthcare Cloud Service Models

The cloud provides various types of service models in the healthcare field

Platform as a Services (PaaS)

Infrastructure as a Services (IaaS)

Software as a Services (SaaS)

SaaS-based applications offer a variety of facilities to hospitals, patients, and pharmaceutical companies. Healthcare organizations prefer SaaS-based solutions.

1.1.1. Paas in Healthcare

Providing access to medical data through cloud apps through Paas gives users flexibility. To deliver medical records to the cloud, you can access them anytime, anywhere, from any computer or mobile device. Cloud offers several benefits to medical centers and patients for securely sharing medical data.

1.1.2. Iaas in Healthcare

In the healthcare industry, it's a challenging task to maintain a massive amount of medical data. Cloud-based Iaas provides a wide range of storage facilities for securely storing the patient's records and includes flexibility for maintaining the patient's data.

1.1.3. Saas in Healthcare

Applications of Saas in healthcare include electronic health records, telehealth data, and non-clinical information systems such as billing, CRM, and supply chain. In contrast to traditional computer software, it offers subscription-based services at a reasonable cost.

In the telemedicinal application, digital images play an anchor role in guaranteeing superior and rapid healthcare. The digital images used in this telemedicinal application comprise diagnostic and confidential information related to the patients' health. These digital images are transmitted using a public network for sharing information about the patients' healthcare during the requirement introduced between patients, doctors, and hospitals. As a result, it is essential to secure the medical images during their storage and transit to guarantee patient privacy [5]. But the distinct characteristics of digital medical image data possessing maximized correlation between pixels, large size, and high redundancy has the possibility of introducing challenges to the traditional cryptographic algorithms. This limitation is mainly due to the insufficient information to guarantee required security during data encryption [6]. Thus, the need for developing a dedicated, enhanced image encryption algorithm arises as the classical algorithms fail to deliver a consistent solution.

Despite the obvious benefits of cloud computing, the risk of adversarial behaviours remains, and security and privacy issues continue to limit its adoption. The dangers of accessing the internet are always attached to threats. Because of many factors, including multiple access and data transmissions without effective encryption, risks emerge as a serious issue in a cloud computing setting. As a result, the essential factors of cloud computing services are privacy and security. The owners of the data that can be processed on the platform cannot control it in the cloud [7]. Specifically, medical image pertains to the type of image information that highlights the patients' physical condition with confidential data associated with the patients. Such potential information can be determined from MRI, CT, and other medical images during their storage or transit whenever required in telemedical applications [8]. Further, these medical images possess a stronger correlation, larger data volume, and higher redundancy than normal images.

Generally, real-time requirements and encryption algorithm security are stringent [9]. The natural association with cryptography, internal randomness, the sensitivity of parameters, and sensitivity to initial value being the characteristic of chaos is ideal for encrypting medical images [10]. Adopting the chaotic map into the medical data encryption enhances the unpredictability associated with the algorithm. In general, chaotic maps are categorized into one-dimensional and multidimensional chaotic maps. Most researchers initially utilized one-dimensional chaotic maps, namely Logistic maps, for encryption due to their efficiency over underuse basic encryption algorithms [11]. Despite the efficiency inherent with the one-dimensional chaotic systems, they only facilitate small key space and have the possibility of being cracked using a brute-force attack. However, multidimensional chaotic maps are essential for increasing the key space, introducing maximized randomness during encryption, and increasing the randomness of the chaotic maps that help prevent violent attacks during the storage and transmission of medical images.

This paper enhances the Fractional Order Lorenz System and a Matrix Scrambling Method (FOLS-MSM) for achieving medical image encryption with maximized correlation, reliability, and high resolution. In particular, the Fractional Order Lorenz System is developed by integrating the potentialities of the Arnold map, Tent map, and Lorenz Map for attaining the image encryption process. Initially, the Arnold map is used for scrambling the initial value. Then the tent map is used iteratively to determine the values of the states to locate the position of the plaintext pixel. Then, the fractional Lorenz system considers the moulded pixel as the input, and scrambling is attained using a matrix method to achieve confusion. Moreover, it generates the pseudo-random sequence for performing the cross-diffusion process to obtain an encrypted image. The potentiality of the enhanced FOLS-MSM explored based on security analysis with respect to sensitivity, correlation, PSNR, key space, histogram, and entropy analysis confirmed its predominance over the baseline medical encryption schemes used for comparison.

1.2. Problem Statement

With the dramatic growth of information technologies, images like medical, color, and greyscale are increasingly being used, stored, and transmitted in the cloud. Safeguarding this kind of data has become a challenging issue. The medical records contain information about a patient’s critical diseases, medical diagnostic reports such as scan reports, X-rays, ECG reports, and payment details. Medical data includes diagnostic and confidential health information of the patients. Sharing medical data with hospitals, doctors, and patients is necessary for certain situations. Data security is a challenging issue when transmitting data into the public network. The existing encryption systems, primarily used for text-based encryption, may not be appropriate for medical data containing images. Most encryption methods have some security and performance issues. An efficient image encryption algorithm is needed to secure confidential data while transferring it into the public network.

1.3. Objective

The paper aims to develop an image encryption technique to conduct effective encryption. It has a high level of conflict with brute force attacks and provides enhanced security to confidential medical data.

1.4. Organization of the Paper

The current section of the paper describes image encryption, followed by the problem statement and objective. The remaining section of the paper is organized as follows. Section 2 shows the literature review on the existing hybrid chaotic maps-based medical image encryption methods contributed to the literature over the past few years. Section 3 illustrates the detailed view of the enhanced FOLS-MSM with the supportive flow diagram that explains the steps involved during its implementation process. Experimental results and discussion of FOLS-MSM are presented in Section 4, providing proper justification for its performance. In conclusion, Section 5 reviews significant contributions and potential enhancements in the future.

2. LITERATURE REVIEW

“2D chaotic map using bit-plane decomposition”[12] proposed chaotic image encryption techniques such as the 2D Logistic-Sine-Coupling Map and Arnold's Cat map to enhance the randomness and security of the encrypted medical image. This chaotic medical image encryption scheme was proposed using bit-plane decomposition. It initially partitioned the complete ciphertext image into an eight-bitmap, such that the first four-bit is considered for a large number of plaintexts. It included the permutation of Arnold using the first four-bit depending on the time of permutation imposed concerning the image order. It further diffused the scrambled image utilizing the application of Henon Maps.

“Chaotic image encryption with dynamic S-boxes” [13] is proposed iteratively using the logistic map for mapping the parameters of the Henon map, such that two sequences determined can be partitioned into four new sequences. It finally included XOR operation over the ciphertext images. It was identified to conform better results in terms of pixel correlation and resistance against differential attacks. Then, image encryption for the medical data framework was proposed based on the merits of chaotic maps and dynamic substitution boxes (S-boxes) in a more efficient way to resist attacks during transmission. It was identified to be resistant against chosen ciphertext and plaintext attacks as it adopted the arrangement of S-box substitution imposed before and after chaotic substitution. It was proposed to prevent the reset attack launched against pseudo-random number generators. It was formulated as a generic framework that utilized the key-dependent dynamic S-Box method. The experiment analysis of this medical image encryption scheme confirmed better correlation and sensitivity.

“Hybrid zigzag, Bernoulli shift map image encryption”[14] is proposed with DNA coding to resist a possible number of attacks launched during transmission. This DNA and hybrid chaotic map approach comprise phases including the generation of Chaotic key and diffusion using DNA. It initially adopted the message digest algorithm for generating a hash function that can be imposed over plain medical images. It generated initial conditions and control parameters depending on the hash value and input ASCII string. The chaotic systems generate two different key matrices, which enable the diffusion operation to be determined row-by-row within a plain image matrix. DNA XOR algebraic operations alternately generated two chaotic key matrices during the cipher image generation process. It also used a logistic map for DNA encoding and decoding selection rules for encryption. It was identified as predominant in statistical, deferential, and key analyses demonstrated with different possibilities of attacks.

“Chaos-based PRNG-inspired image segmentation”[15] is proposed to generate a high-quality key for high randomness behaviour. The proposed system provides a more secure chaos-based encryption system to encrypt and decrypt medical images. It included an improved architecture for encrypting the secret image using the properties of permutation, substitution, and diffusion. It initially randomly permuted image pixels using the matrix determined using the PRNG. It substituted pixels using two different S-boxes, with image diffusion occurring using XORing pixels. It achieved a large key space for resisting brute-force attacks.

“Logistic-Sine-Coupling, Arnold map” [16] is proposed for efficient medical image encryption. It facilitated the unpredictability and security of the encrypted image. It was designed as a steganography method using the chaotic map and an image to conceal confidential data in a grayscale cover image. It encrypted the undisclosed medical image before hiding, and the image is pre-processed to resist stage-analysis. This technique uses three-point safety to confidential data utilizing a strong arbitrary structure for encryption, a grayscale image, and pre-processing of the image. “Enhanced genetic operation in five dimensions" [17] is proposed to attain the required degree of randomness during the medical image encryption process. This IGO-FDTLCS approach used the DNA recombination principle that integrated the merits of chaotic maps that aid in chaotic matrix generation. It improved the impacts of diffusion and scrambling by including the bit-level DNA mutation operation. It offered better randomness and security as it confirmed minimized time performance. It was also confirmed to be resistant to attacks based on the security analysis conducted using sensitivity, correlation, PSNR, comparing the decrypted image to the original, calculating the histogram, information entropy, and determining the key space.

2.1. Analysis of Various Chaotic Map Encryption Techniques

The analysis of various chaotic map encryption techniques are illustrated in the Table 1.

Table 1 Analysis of Various Chaotic Map Encryption Techniques

S. No	Methodology	Objective	Outcome
1.	"Novel unidimensional chaotic map" [18]	In this work, the positions and values of the pixels are simultaneously modified by the substitution and permutation processes.	By combining these two stages and developing the novel one-dimensional chaotic map, security and speed can be effectively improved.
2.	"Image encryption combined Ikeda, logistic map." [19]	Multiple chaotic maps are used in this proposed work to encrypt a given grayscale image at the pixel and bit levels using the Ikeda map and logistic map.	To generate the encrypted image, perform the bit XOR process on the vertical and horizontal portion of the plain image and circular shift bitwise operations on all the pixel intensities in the confusing image.
3.	"Optimized encryption combined Arnold and logistic map." [20]	In this proposed work optimized framework model is used, which is a combination of double chaos encryption techniques, namely Arnold, and logistic maps	The lightweight image encryption algorithm takes less time and less key-value and guarantees minimal correlation coefficients between adjacent pixels in the cipher image.
4.	"Unidimensional twin chaotic map" [21]	In this proposed work, an adaptive image encryption technique. This scheme is designed on a one dimensional chaotic map such as Quadratic and Henon maps, and PRN sequences were determined.	Shuffling and diffusion take place on pixels instead of bits, decreasing the encryption time.
5.	"chaotic map with double S-box" [22]	The performance of 1D chaotic maps can be improved using a double-S-box encryption scheme.	The proposed cryptosystem is more resistant to the four classic attacks than the other double S-box-based schemes.
6.	"wavelet transform with 3D shuffling" [23]	A multi-image encryption scheme is proposed in this article that uses Haar wavelet transforms and 3D shuffling to scramble images.	Improve the performance of low dimensional chaotic maps against a brute force attack.
7.	"Multi dimension image encryption based on ROI" [24]	An algorithm for encrypting confidential information based on the region of interest (ROI) was proposed for multidimensional chaotic image encryption.	The proposed work is to separate the region of interest from the entire image using histogram-oriented gradients and a support vector machine algorithm.

8.	“Hybrid chaotic map and optimized substitution box”[25]	This work combines an optimized S-box encryption algorithm with a low-dimensional hyperchaotic map.	It increases the performance of the 1D chaotic maps and provides excellent randomness against different cyber-attacks.
9.	“Novel 1D sine-powered chaotic map” [26]	This proposed work is a new unidimensional sine-powered chaotic system (DSP) to improve the performance of traditional sine chaotic maps.	In this paper, row-wise, column-wise confusion, and diffusion are used to enhance the performance of the chaotic map.
10.	“Improved Lorenz System” [27]	This paper proposed a novel method for improving the fractional order Lorenz system. This scheme increases the nonlinear kinetic complexity and ergodicity of the traditional Lorenz system.	The improved Lorenz system has better dynamic characteristics than the Lorenz system based on autocorrelation, frequency distribution, and information entropy analysis.
11.	“Henon map with CBNT” [28]	This paper introduces a novel, “Conditional Butterfly Network Topology (CBNT),” and Henon chaotic map for performing the bit-level process.	It conducts bitwise confusion, pixel-level confusion, and diffusion processes to transmit images securely over an insecure channel such as a public network. Then, it performs XOR operations to secure the data transfer.
12.	“DCPG combined chaotic map.” [29]	This paper proposed a new scheme for encrypting images using a chaotic Double pseudo-random generator (DCPG) and XOR operations.	This paper combines tent maps and Chebyshev chaos maps with varying control parameters to increase the encryption algorithm's performance and compare the results with symmetric algorithms.
13.	“1D cosine fractional chaotic map” [30]	This paper proposes a novel unidimensional cosine fractional chaotic map (1DCF) with varying control parameters.	It is mainly helpful for real-time image processing. This novel chaos map exhibits extremely high-level chaotic behaviour over a wide scale of control parameters.
14.	“Combine different chaotic maps” [31]	The proposed work uses the confusion-diffusion technique for encrypting the images. The key is generated by different chaotic maps.	A shuffled image is generated by disarranging the image pixels and diffusing it by performing XOR operations on the pixels of the shuffled image with a secret key.

15.	“Novel hyper chaotic map” [32]	A fast and novel image encryption technique utilizing 3D Lorenz chaotic maps is proposed in this paper based on keystream-based pixel-level and bit-level permutations.	Pixel permutation is made more secure through this double-scrambling. The efficient permutations and substitution guarantee efficient diffusion and confusion.

3. PROPOSED FRACTIONAL ORDER LORENZ SYSTEM AND A MATRIX SCRAMBLING METHOD (FOLS-MSM)-BASED MEDICAL IMAGE ENCRYPTION

The term "cloud" refers to a collection of internet-based services and infrastructure. Nowadays, numerous users share the cloud infrastructure for performing distinct tasks. When picking a cloud solution, healthcare providers are most concerned about security and privacy. Data security is compromised when it is transmitted to the cloud. Thus, confidential information should be encrypted using a reliable encryption algorithm to guarantee cloud privacy.

Encryption is a useful tool for ensuring data protection. Encryption aims to convert data files or plain images into cipher images, a string of illegible code generated by algorithms. The fractional-order Lorenz system is adopted in this medical image encryption process by integrating Arnold Map, Tent Map, and Lorenz Map. Initially, the input medical image is partitioned into different layers for imposing the process of scrambling only the first three layers using the merits of the Arnold Map.

3.1. Generalized Arnold Map

The generalized Arnold map, often called the “cat map,” is a nonlinear two-dimensional map based on equation (1).

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ \lambda & \mu\lambda + 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \, mod \; N \qquad (1)$$

where μ and λ are system parameters that indicate the real numbers, x_n, $y_n \in (0,1)$ N represents the height or width of the image. This Arnold map is frequently utilized in the process of image encryption for the objective of scrambling, during which x_n, y_n indicates the original image pixel position, x_{n+1}, y_{n+1} indicates the scrambled image's pixel position. However, the Arnold Map in its generalized form does not provide maximum efficiency. Thus, Arnold Map with optimization is used for the objective of scrambling as specified in equation (2).

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ \lambda & \mu\lambda + 1 \end{pmatrix} \begin{pmatrix} 1 \\ j \end{pmatrix} \qquad (2)$$

In an aforementioned manner, the pixel position concerning pixel (1, b) and pixel (1, j) can be interchanged. In the proposed mechanism, the input medical image divided into multiple layers can be introduced to scrambling. But only the first three layers are scrambled through Arnold Map. Moreover, the initial value used for the first scrambling process can be considered as the Arnold Map. In addition, the remaining two layers also contribute to the initial value of the remaining scrambling process. Figure 1 Here is a visual representation of the fractional-order Lorenz system proposed.

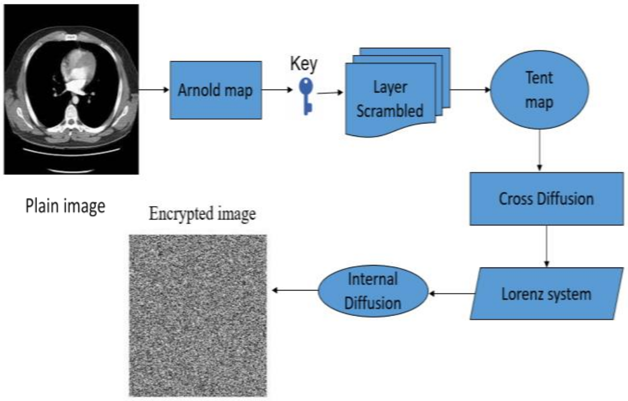


Figure 1 Proposed Model Diagram of Fractional-Order Lorenz System

3.1.1. Proposed Image Encryption Scheme Containing the Following Steps for Arnold Cat Map

Step 1. Choose any grayscale image M (m, n)

Where m and n denote the number of columns and rows in a plain image.

Step 2. for each pixel, M (m, n) do

Step 3. $\begin{pmatrix} M \\ N \end{pmatrix} \leftarrow \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$

Step 4. $M'(M,N) \leftarrow M(m,n)$

Step 5. end for loop

Step 6. Iteratively, all the pixel positions in the image are changed

Step 7. Finally, $M'(m,n)$, we get the scrambled image using Arnold's cat map.

3.2. Generalized Tent Map

The Tent Map imposes the second level of scrambling. The generalized form of tent map is defined based on equation (3)

$$x_{n+1} = \begin{cases} \mu x_n & 0 \leq x_n < 0.5 \\ \mu(1 - x_n) & 0.5 \leq x_n \leq 1 \end{cases} \qquad (3)$$

In this equation (3), the value of $x_n \in (0,1)$, and the control parameter value is $1 \leq \mu \leq 2$, the system is chaos. An interval [0, 1] is transformed onto itself using this map, which has only a single control parameter μ, where $\mu \in [0,2]$. The initial value of the map is x_0. The orbit of the system refers to a group of values such as $x_0, x_1, \dots, x_n$. The tent maps each value of x_0 such an orbit is obtained.

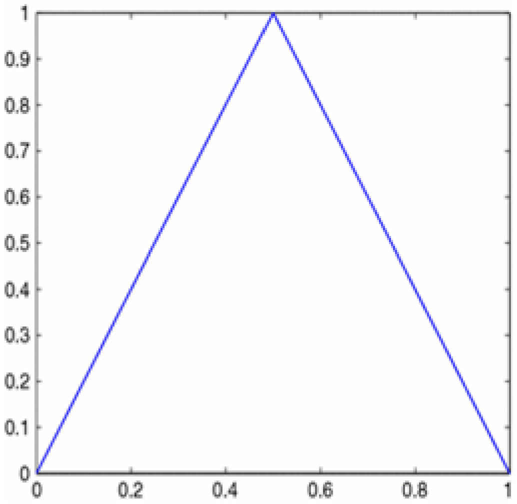


Figure 2 Graphical Representation of Tent Map

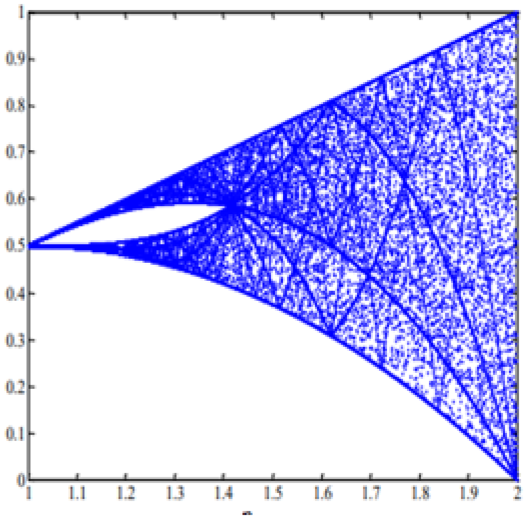


Figure 3 Tent Map Bifurcation Diagram

Depending on the control parameter value of p, the tent map with respect to (Eq.3) shows the range of dynamic characteristics ranging from predictable to chaotic behaviour. The construction of the chaos tent map utilized two straight lines to simplify the analysis compared to truly nonlinear systems. The formation of the chaotic tent map is simple, the equation is linear for specific parameter values, and the tent map exhibits complex behaviour and even chaotic phenomena. The value of $x_0 = 0.000001$,the value of p=1.999999, for i=0, 1…,20,000. Figure 2 shows the graphical representation of the chaotic tent map. A bifurcation diagram demonstrates the relationship between the values of one parameter and the system's behaviour is measured. Figure 3 illustrates a bifurcation diagram representing a tent map.

3.3. Fractional-Order Lorenz System

In 1963 E.N Lorenz proposed the Lorenz system [33]. The design of ordinary differential equations is known as the Lorenz system. It represents a system of chaotic behaviour derived from the Lorenz system. The enhanced FOLS-MSM scheme is adopted the fractional-order Lorenz scheme is defined as equation (4)

$$x_{n+1} = \begin{cases} \dfrac{d^{\alpha}x}{dt^{\alpha}} = \mu(y - x) \\ \dfrac{d^{\beta}x}{dt^{\beta}} = rx - xz + sy \\ \dfrac{d^{\gamma}x}{dt^{\gamma}} = xy - \lambda z \end{cases} \qquad (4)$$

Where $\mu, \lambda, r\ and\ s$ represents the system parameters with $\alpha, \beta\ and\ \gamma$ indicating the fractional order. Specifically, the value of $\mu, \lambda, r\ and\ s$ is assigned to 40, 3, 10, and 25, and the value of $\alpha, \beta\ and\ \gamma$ is set to 0.95, respectively.

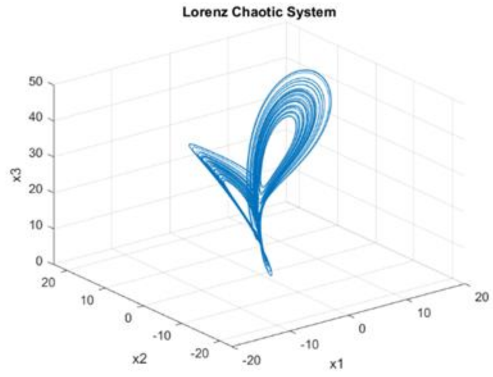


Figure 4 Phase Diagram of Lorenz System

"Butterfly effect" is a term that has originated from the Lorenz attractor, a theory proposing that chaos is a natural outcome in chaotic systems, regardless of our knowledge of the initial conditions. Figure 4 depicts the phase diagram of the Lorenz system. It is mainly used in the stage of plaintext selection and iterates for the objective of determining double sets of state values which are ideal for estimating the position of the plaintext pixel. The grey value of the pixel is modified in such a way that the initial value is generated for feeding it as input to the fractional Lorenz system. The fractional Lorenz system uses a portion of the pseudo-random sequence produced during the diffusion stage. It was used for cross-diffusion operation in the determined layers of medical images. Specifically, the process of diffusion is introduced in each layer using the add-mode strategy.

3.4. Matrix-Based Scrambling Strategy

This Matrix-based Scrambling Strategy represents the method of transformation that can be generated based on equation (5)

$$P_{X(k)} = S_M P_{X(k-1)} \, mod \, N \qquad (5)$$

Where,'S_M 'indicates the matrix of scrambling with the size of $N \times N$ with 'k 'representing the positive integer that depicts the frequency of scrambling imposed over the image. In particular, all the elements of S_M are integers such that the condition $det\ (S_M) \neq 0$ is satisfied. Hence, the transformation based on matrix scrambling is attained through equation (6)

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ b_{11} & b_{11} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \qquad (6)$$

Where $(x_n,\ y_n)$ and $(x_{n+1},\ y_{n+1})$ represents the old and new pixel positions of the plain and permutated images. In this process, the matrix (S_M) defined in equation (7) acts as the operator of scrambling to permutate the plain image.

$$S_M = \begin{pmatrix} a & a^2+1 \\ 1-a^2 & a^3 \end{pmatrix} \qquad (7)$$

Here, 'a' represents the positive integer, and at all the values of a, the condition $det\ (S_M) = 1$ needs to be satisfied to facilitate the reversible scrambling operation. Hence, the matrix used for inverse scrambling is defined using equation (8).

$$S_M = \begin{pmatrix} a^3 & -a^2-1 \\ 1-a^2 & a \end{pmatrix} \qquad (8)$$

The equation mentioned above (8) aids in determining the original input medical image from the permutated image. This value of 'a' is the varying coefficient that is completely identified based on the preference of the users and the permutation degree imposed over an image.

Furthermore, the utilization of the term a^2 and a^3 in the 'S_M' matrix is considered to minimize the difference in value estimated between the elements. This difference minimization between values increases the possibility of effectively changing the positions of the pixel even during small iterations. Thus, repetitive iteration of the matrix scrambling process can be significantly prevented.

In addition, the complete steps involved in the implementation of the proposed scheme are detailed as follows.

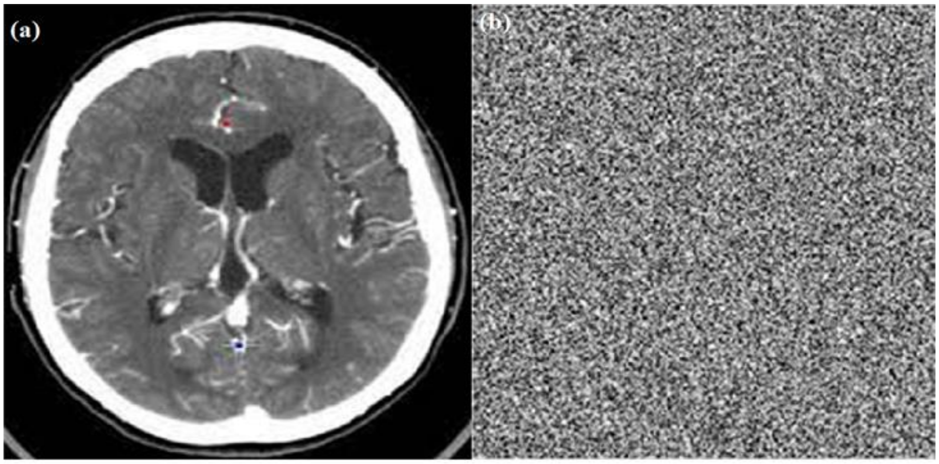
4. EXPERIMENTAL RESULTS

Enhanced FOLS-MSM experiments, benchmarking approaches, and system specifications are demonstrated in Table 2. The experimental image used to explore the proposed algorithm's predominance is a lung CT image of size 512x512.

Table 2 Hardware Specification of Enhanced FOLS-MSM

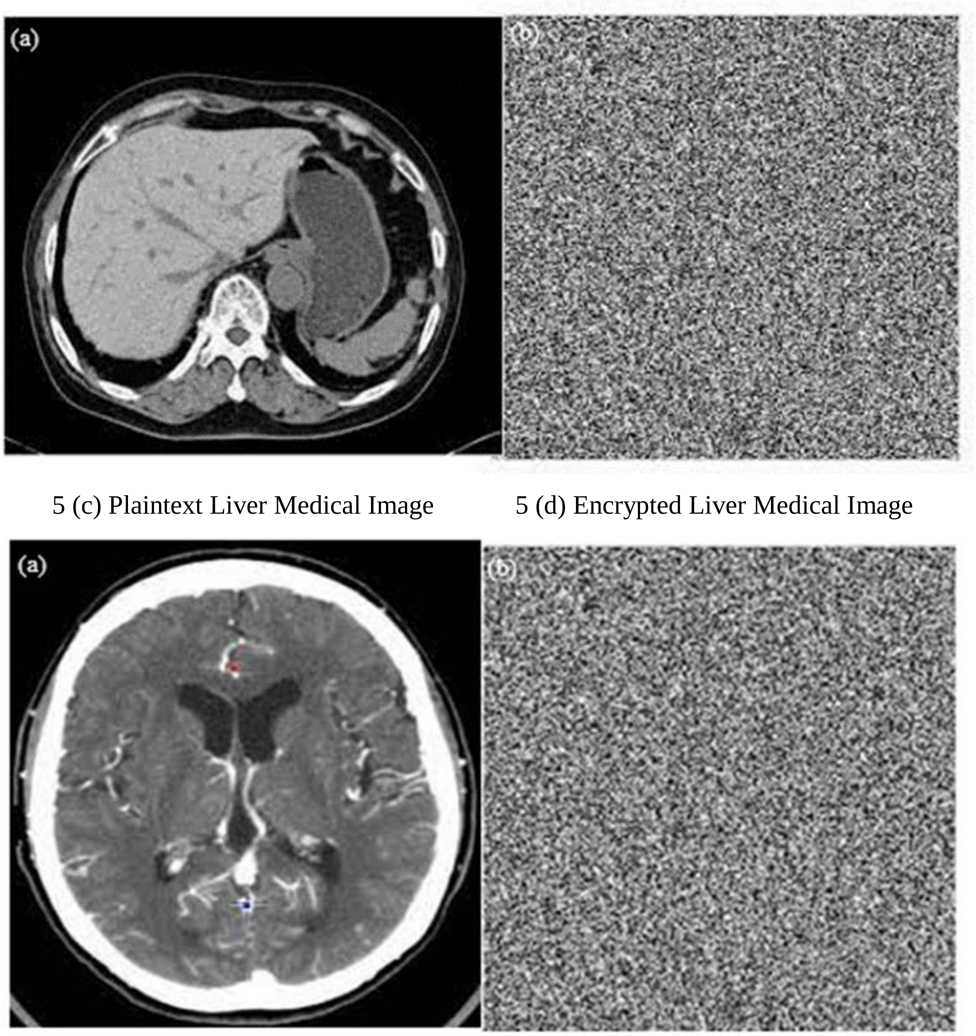
S.No	Hardware	Specification
1.	Matlab	R2021a
2.	Processor	Intel Core i5
3.	System Speed	2.40 GHz
4.	RAM	8 GB
5.	Disk size	250 GB SSD
6.	Operating system	Windows 11

4.1. Security Analysis Based on Key Space



5 (a) Plaintext Lung Medical Image 5 (b) Encrypted Lung Medical Image

RESEARCH ARTICLE



5 (c) Plaintext Liver Medical Image 5 (d) Encrypted Liver Medical Image

5 (e) Plaintext Brain Medical Image 5 (f) Encrypted Brain Medical Image

Figure 5 (a)-(f) Plaintext Image and its Encrypted Image during FOLS-MSM Implementation

The key space size is considered the potential reference value used for the potentiality of the results determined by the chaotic encryption algorithms. In specific, encryption algorithms that possess a large and sufficient key space are identified to resist exhaustive attacks comparatively well. The decrypted image is completely different when little changes are modifying the key. The results confirmed that the algorithmic key space is 10^{85} as specified in Figure 5. In particular, an image encryption algorithm is secure when the key space of the encryption algorithm is greater than 2^{128}. The proposed algorithm facilitates the key space of $10^{85} \approx 2^{280}$ which is better than the security value considered for theoretical validation. Hence, compared with the other literature works, this proposed encryption algorithm confirmed its effectiveness in resisting exhaustive attacks, as specified in Table 3.

Table 3 Comparison of Key Space for Medical Image Encryption Algorithms

Algorithms compared	Key space
Gafsi et al. [11]	2^{226}
Jain et al. [12]	2^{254}
Liang [17]	2^{249}
Li et al. [34]	2^{256}
Masood et al. [35]	2^{242}
FOLS-MSM (Proposed)	$10^{85} \approx 2^{280}$

4.2. Analysis of the Histogram

Histograms display the distribution of gray levels in an image and calculate the occurrences of each gray value. It is easy to determine information from the medical image when an image's histogram possesses a prominent distribution property. On the other hand, medical images do not provide maximized amount of valuable information when the image possesses a messy and evenly distributed histogram. Thus, the analysis of medical image encryption using a histogram is essential for quantifying the significance of the encryption process. A comparison of plaintext and ciphertext medical image histograms is described in Figure 6. It quantitatively illustrates that the image encoded by the algorithm differs only in terms of minimized pixel values. The encrypted histogram no longer provided clear characteristics.

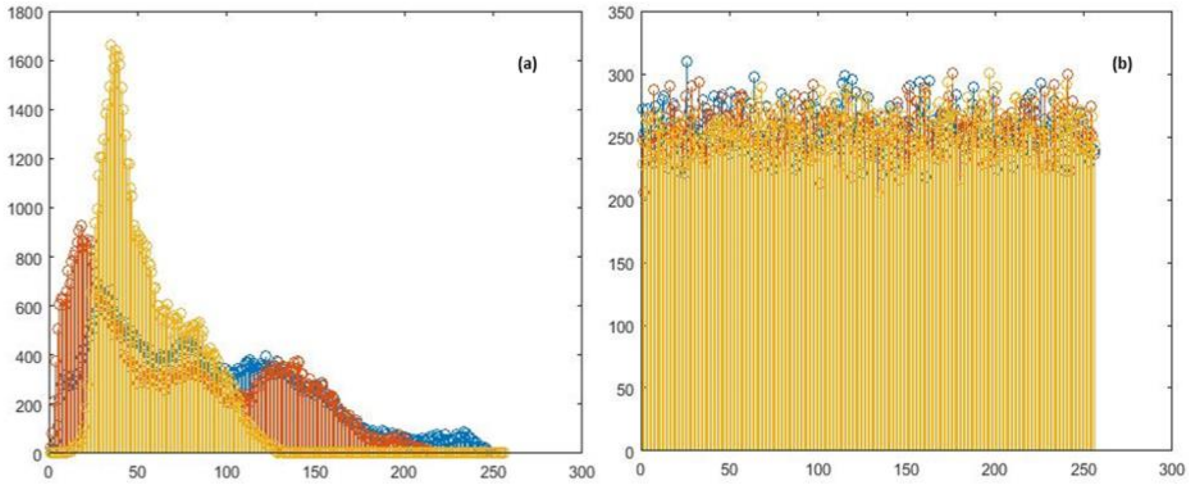


Figure 6 Proposed FOLS-MSM-Histogram of Plaintext and Encrypted Image

4.3. Investigation Based on Information Entropy

Table 4 Comparison of Medical Image Encryption using Information Entropy

Algorithms compared	Plain Image	Encrypted medical image
Gafsi et al. [11]	7.421878	7.518413
Jain et al. [12]	7.546812	7.611234
Liang [17]	7.611812	7.722118
Li et al. [34]	7.621216	7.818186
Masood et al. [35]	7.688721	7.812234
FOLS-MSM(Proposed)	7.325544	7.999413

The information entropy is a statistical measure to estimate the randomness and unpredictability of the image. Information entropy is a vital indicator for evaluating the impact of encryption. It is defined by equation (9).

$$H(E) = -\sum_{i=1}^{le} Pr(E_i) log_2 Pr(E_i) \quad (9)$$

Where H is information entropy, Pr is a probability distribution function. Table 4 clearly demonstrates that the information entropy achieved while implementing the enhanced FOLS-MSM is significantly improved. The range of values for pixels is 0 to 255, so the entropy value may be 8. The information entropy attained by the enhanced FOLS-MSM (closer to 8) is comparatively more significant than the baseline approaches used for evaluation. Thus, the enhanced FOLS-MSM is slightly superior to the algorithms used for benchmarking in terms of information entropy.

4.4. Investigation Based on Correlation Coefficient

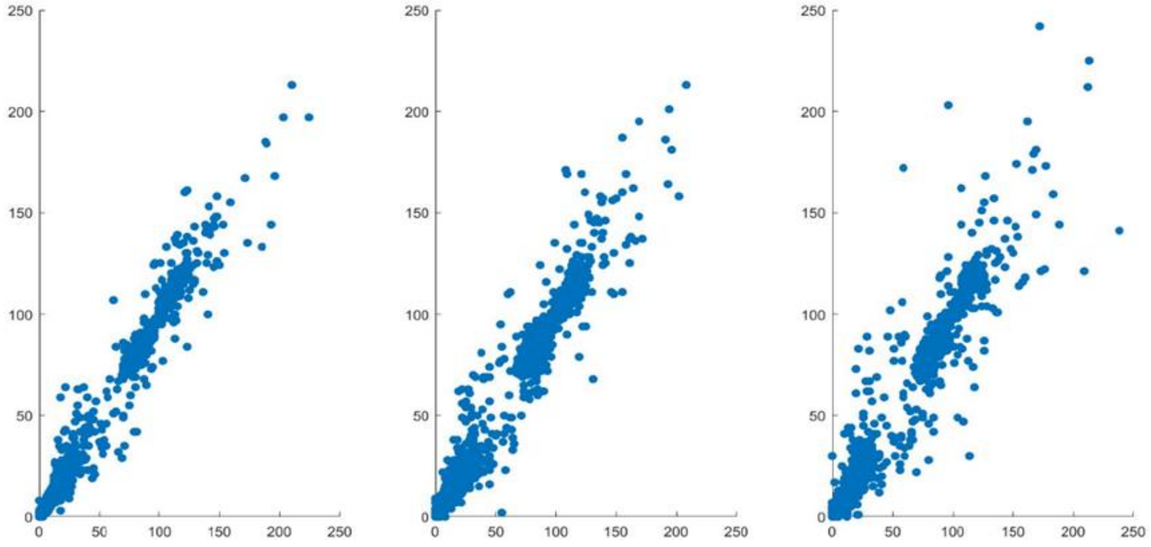
Table 5 Comparison of Medical Image Encryption Schemes using Correlation Coefficient

Compared Algorithms	Plain Image	Encrypted Medical Image
Horizontal	0.9963	-0.0031
Vertical	0.9944	0.0018
Diagonal	0.9939	0.0028
Liang [17]	0.98142	0.0026542
Li et al. [34]	0.9941	0.00841
Masood et al. [35]	0.93486	0.004472

An analysis of correlation coefficients is a technique for determining the probability of correlated adjacent pixels. The values between pixels in a plain image are very close so that it will present redundant information. A correlation coefficient near the value of 1 is a sign of greater redundancy otherwise, the value approaches 0. It is defined by equation (10).

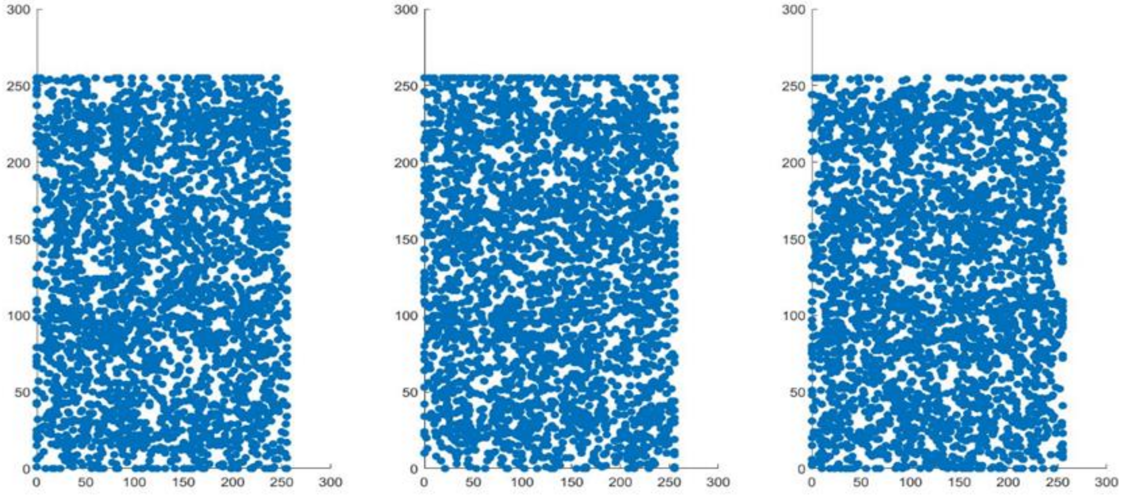
$$Correlation\ coefficent\ CC_{i,j} = \frac{cov(i,j)}{\sqrt{D_{xi}}\times\sqrt{D_{yj}}} \qquad (10)$$

Where cc is a correlation coefficient, $cov(i,j)$ is the covariance, D is the variance, and xi and yj are the grey values of two adjacent pixels in the image. In the original input medical image, the correlation coefficient between neighborhood pixels is comparatively high. This correlation coefficient is minimized after the application of the enhanced FOLS-MSM approach. Figure 7 illustrates the Correlation distribution of the plain image. The results of the correlation coefficient between neighborhood pixels (presented in Table 5) during the employment of the FOLS-MSM approach are closer to 0. Figure 8 shows the Correlation distribution of the encrypted image.



a) Horizontal b) Vertical c) Diagonal

Figure 7 (a)-(c) Correlation Distribution of the Plain Image



a) Horizontal b) Vertical c) Diagonal

Figure 8 (a)-(c) Correlation Distribution of the Encrypted Image

4.5. Investigation Based on NPCR and UACI Values

Differential attacks are based on changing the plain image while encrypting both with the same algorithm, and it is used to guess information about an image. Comparing the plain image to the encrypted image allows us to detect a correlation between the two images. To evaluate the algorithm's performance using the Number of Pixel Changing Rate, unified averaged changed intensity is measured by equations (11) and (12).

$$NPCR = \frac{1}{p\times q}\sum_{i=1}^{p}\sum_{j=1}^{q} C(i,j) \times 100\ \% \qquad (11)$$

$$UACI = \frac{1}{p\times q}\sum_{i=1}^{p}\sum_{j=1}^{q}\frac{|PI(i,j)-SI(i,j)|}{255} \times 100\ \% \qquad (12)$$

$$Where\ C(i,j) = \begin{cases} 0\ if\ PI(i,j)\ = SI(i,j) \\ 1\ if\ PI(i,j) \neq\ SI(i,j) \end{cases}$$

Where p, q represents the height and width of the image, let's take "PI" as the plain image and "SI" as the corresponding scrambled image. Table 6 below presents the comparative table of the NPCR and UACI facilitated by the enhanced FOLS-MSM approach by randomly changing the pixel value by 1- and 2-pixel values. The ideal value of NPCR is 99.6096 %, and the UACI value is 33.4649. In both cases, the enhanced FOLS-MSM approach is comparatively higher than the ideal value. This table shows that the enhanced algorithm provides better plaintext sensitivity.

Table 5 Comparison of NPCR and UACI Values with Respect to Medical Image Encryption

Pixel value changed	NPCR	UACI
(25,12)	99.6112%	33.5824%
(152,110)	99.6562%	33.6493%
(511,464)	99.8395%	33.6142%

4.6. Avalanche Effect

Avalanche Effect (AE) measures the modifications in the encryption key or changing the plaintext image and significantly changes the cipher image. Encryption techniques require randomness as a key prerequisite. It calculates the difference between plaintext images and cipher image modifications. With overwhelming probability, even the slight change in the plain image will change many bits due to the cipher image's avalanche effect. Figure 9 demonstrates the average avalanche effect values. By calculating hamming distance, we can measure the avalanche effect. It is desirable to have a high avalanche effect if the diffusion is high. Thus, the enhanced algorithm achieved the desired criteria. Table 7 presents the average avalanche effect values. It is defined by equation (13).

$$Avalanche = \frac{Total\ number\ of\ bits - number\ of\ flip\ bits}{Total\ number\ of\ bits} X100 \qquad (13)$$

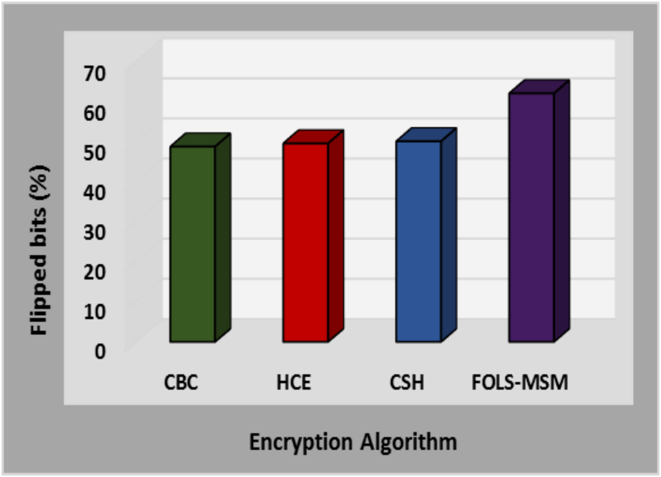


Figure 9 Avalanche Effect

Table 7 Average Avalanche Effect

Encryption Algorithm	Average Avalanche Effect (%)
Chaotic block cipher(CBC) [36]	48.7
Hybrid Chaotic Encryption (HCE) [37]	49.5
Chaotic hash scrambling(CSH) [38]	50.03
Enhanced FOLS-MSM(proposed)	62

5. CONCLUSION

The enhanced FOLS-MSM achieved better medical image encryption with maximized correlation, reliability, and high resolution. This work provides high data security while transmitting confidential data in the cloud network. The combination of Arnold Map, Tent Map, and Lorenz Map forms a fractional-order Lorenz System, facilitating better encryption. It ensured the process of initial value scrambling by incorporating the Arnold map, which also adopted a tent map for estimating the state values of the states to localize the plaintext pixel position. It used a specialized matrix scrambling method with the generation of pseudo-random sequences and attained a better cross-diffusion process while encrypting the medical image. The experimental results confirmed the information entropy of the enhanced FOLS-MSM is significantly improved, which is closer to 8 and comparatively greater than the baseline approaches used for evaluation. For further study, it has been decided to formulate a unified fractional map-based chaotic system and explore its capability over the proposed medical image encryption scheme.

REFERENCES

[1] Y. Gong, C. Zhang, Y. Fang, and J. Sun, “Protecting Location Privacy for Task Allocation in Ad Hoc Mobile Cloud Computing,” IEEE Trans. Emerg. Top. Comput., vol. 6, no. 1, pp. 110–121, 2018, doi: 10.1109/TETC.2015.2490021.

[2] W. Li et al., “Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing,” IEEE J. Biomed. Heal. Informatics, vol. 23, no. 3, pp. 1278–1289, 2019, doi: 10.1109/JBHI.2018.2850304.

[3] X. Li, J. Yuan, H. Ma, and W. Yao, “Fast and Parallel Trust Computing Scheme Based on Big Data Analysis for Collaboration Cloud Service,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 8, pp. 1917–1931, 2018, doi: 10.1109/TIFS.2018.2806925.

[4] D. S. Laiphrakpam and M. S. Khumanthem, “Medical image encryption based on improved ElGamal encryption technique,” Optik (Stuttg)., vol. 147, pp. 88–102, 2017, doi: 10.1016/j.ijleo.2017.08.028.

[5] R. Enayatifar, A. H. Abdullah, and M. Lee, “A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption,” Opt. Lasers Eng., vol. 51, no. 9, pp. 1066–1077, 2013, doi: 10.1016/j.optlaseng.2013.03.010.

[6] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, “Chaos based crossover and mutation for securing DICOM image,” Comput. Biol. Med., vol. 72, pp. 170–184, 2016, doi: 10.1016/j.compbiomed.2016.03.020.

[7] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, “Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services,” IEEE Syst. J., vol. 12, no. 2, pp. 1621–1631, 2018, doi: 10.1109/JSYST.2016.2633809.

[8] Z. Deng and S. Zhong, “A digital image encryption algorithm based on chaotic mapping,” J. Algorithms Comput. Technol., vol. 13, pp. 1–11, 2019, doi: 10.1177/1748302619853470.

[9] J. Zhao, S. Wang, Y. Chang, and X. Li, “A novel image encryption scheme based on an improper fractional-order chaotic system,” Nonlinear Dyn., vol. 80, no. 4, pp. 1721–1729, 2015, doi: 10.1007/s11071-015-1911-x.

[10] 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, doi: 10.1109/ACCESS.2020.2970806.

[11] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos, Solitons and Fractals, vol. 21, no. 3, pp. 749–761, 2004, doi: 10.1016/j.chaos.2003.12.022.

[12] Y. Dai, H. Wang, and Y. Wang, “Chaotic Medical Image Encryption Algorithm Based on Bit-Plane Decomposition,” Int. J. Pattern Recognit. Artif. Intell., vol. 30, no. 4, pp. 1–15, 2016, doi: 10.1142/S0218001416570019.

[13] S. Ibrahim et al., “Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps,” IEEE Access, vol. 8, pp. 160433–160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[14] J. C. Dagadu, J. P. Li, and E. O. Aboagye, “Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion,” Wirel. Pers. Commun., vol. 108, no. 1, pp. 591–612, 2019, doi: 10.1007/s11277-019-06420-z.

[15] M. Gafsi, N. Abbassi, M. A. Hajjaji, J. Malek, and A. Mtibaa, “Improved chaos-based cryptosystem for medical image encryption and decryption,” Sci. Program., vol. 2020, 2020, doi: 10.1155/2020/6612390.

[16] K. Jain, A. Aji, and P. Krishnan, “Medical Image Encryption Scheme Using Multiple Chaotic Maps,” Pattern Recognit. Lett., vol. 152, pp. 356–364, 2021, doi: 10.1016/j.patrec.2021.10.033.

[17] Z. Liang, Q. Qin, C. Zhou, N. Wang, Y. Xu, and W. Zhou, Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation, vol. 16, no. 11 November. 2021.

[18] M. Z. Talhaoui and X. Wang, “A new fractional one dimensional chaotic map and its application in high-speed image encryption,” Inf. Sci. (Ny)., vol. 550, pp. 13–26, 2021, doi: https://doi.org/10.1016/j.ins.2020.10.048.

[19] A. Girdhar, H. Kapur, and V. Kumar, “A novel grayscale image encryption approach based on chaotic maps and image blocks,” Appl. Phys. B Lasers Opt., vol. 127, no. 3, 2021, doi: 10.1007/S00340-021-07585-X.

[20] J. Ferdush, M. Begum, and M. S. Uddin, “Chaotic Lightweight Cryptosystem for Image Encryption,” Adv. Multimed., vol. 2021, p. 5527295, 2021, doi: 10.1155/2021/5527295.

[21] M. Lyle, P. Sarosh, and S. A. Parah, “Adaptive image encryption based on twin chaotic maps,” Multimed. Tools Appl., vol. 81, no. 6, pp. 8179–8198, 2022, doi: 10.1007/s11042-022-11917-0.

[22] S. Zhu, G. Wang, and C. Zhu, “A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes,” Entropy , vol. 21, no. 8. 2019, doi: 10.3390/e21080790.

[23] H. Zhong and G. Li, “Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling,” Multimed. Tools Appl., 2022, doi: 10.1007/s11042-022-12479-x.

[24] Y. Liu, J. Zhang, D. Han, P. Wu, Y. Sun, and Y. S. Moon, “A multidimensional chaotic image encryption algorithm based on the region of interest,” Multimed. Tools Appl., vol. 79, no. 25, pp. 17669–17705, 2020, doi: 10.1007/s11042-020-08645-8.

[25] M. A. Ben Farah, A. Farah, and T. Farah, “An image encryption scheme based on a new hybrid chaotic map and optimized substitution box,” Nonlinear Dyn., vol. 99, no. 4, pp. 3041–3064, 2020, doi: 10.1007/s11071-019-05413-8.

[26] A. Mansouri and X. Wang, “A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme,” Inf. Sci. (Ny)., vol. 520, pp. 46–62, 2020, doi: https://doi.org/10.1016/j.ins.2020.02.008.

[27] C. Zou, Q. Zhang, X. Wei, and C. Liu, “Image Encryption Based on Improved Lorenz System,” IEEE Access, vol. 8, pp. 75728–75740, 2020, doi: 10.1109/ACCESS.2020.2988880.

[28] R. Vidhya and M. Brindha, “A novel conditional Butterfly Network Topology based chaotic image encryption,” J. Inf. Secur. Appl., vol. 52, p. 102484, 2020, doi: https://doi.org/10.1016/j.jisa.2020.102484.

[29] R. I. Abdelfatah, “A new fast double-chaotic based Image encryption scheme,” Multimed. Tools Appl., vol. 79, no. 1, pp. 1241–1259, 2020, doi: 10.1007/s11042-019-08234-4.

[30] M. Z. Talhaoui, X. Wang, and A. Talhaoui, “A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme,” Vis. Comput., vol. 37, no. 7, pp. 1757–1768, 2021, doi: 10.1007/s00371-020-01936-z.

[31] M. T. Elkandoz and W. Alexan, “Image encryption based on a combination of multiple chaotic maps,” Multimed. Tools Appl., 2022, doi: 10.1007/s11042-022-12595-8.

[32] S. K.U. and A. Mohamed, “Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion,” Signal Process. Image Commun., vol. 99, p. 116495, 2021, doi: https://doi.org/10.1016/j.image.2021.116495.

[33] “E. N. Lorenz, ‘“Deterministic nonperiodic flow,”’J. Atmos. Sci., vol. 20,no. 2, pp. 130–141, 1963.”

[34] S. Li, L. Zhao, and N. Yang, “Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion,” Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/6624809.

[35] F. Masood et al., “A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations,” Wirel. Pers. Commun., no. 0123456789, 2021, doi: 10.1007/s11277-021-08584-z.

[36] S. Dhall, S. K. Pal, and K. Sharma, “A chaos-based probabilistic block cipher for image encryption,” J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 1, pp. 1533–1543, 2022, doi: https://doi.org/10.1016/j.jksuci.2018.09.015.

[37] M. Alawida, A. Samsudin, J. Sen Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” Signal Processing, vol. 160, pp. 45–58, 2019, doi: https://doi.org/10.1016/j.sigpro.2019.02.016.

[38] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, “Medical

Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling," J. King Saud Univ. - Comput. Inf. Sci., 2022, doi: https://doi.org/10.1016/j.jksuci.2022.04.002.

Authors

P. Suhasini received her Master of Information Technology from Bharathidasan University. She received her M.Phil., in Computer Science from Bharathidasan University. She has presented papers at National and International Conferences. She is doing her Ph.D., at SRM Institute of Science and Technology, Chennai. Her research interests are Cloud Computing & Machine Learning.

Dr. S. Kanchana Working as an Assistant Professor in the Department of Computer Science at SRM Institute of Science and Technology, Chennai. She obtained her Ph.D., a degree from Bharathiar University. She has published more than 15 research papers in National and International Journals and Conferences. She has received the Best poster Presentation Award in ISCA-2015. Her research interest includes Data Mining, IoT, and Cloud Computing.

How to cite this article:

P. Suhasini, S. Kanchana, "Enhanced Fractional Order Lorenz System for Medical Image Encryption in Cloud-Based Healthcare Administration", International Journal of Computer Networks and Applications (IJCNA), 9(4), PP: 424-437, 2022, DOI: 10.22247/ijcna/2022/214504.