International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced PRNGs based ACORN with Chaotic Map for Securing DICOM Image Encryption

T. Vijayakumar[1] and M. Y. Mohamed Parvees[2]

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: Due to technological advances, medical and non-medical services are needed to provide the best teleradiology services to secure medical images. Primary issue is medical image secrecy. Conventional block and stream ciphers can't encrypt large volumes of data because small files contain minimal data. The study aims in the direction of create a chaotic map based encryption algorithm to protect clinical images. The enhanced Pseudo Random Number Generators (PRNGs) Centered Additive Congruential Random Number [ACORN] generator, including the nonlinear dynamical method Logistic chaotic map, are utilized in this work to present a 24Bit colour DICOM image encryption technique. We use ACORN Generator to generate 8 (24Bit) random images in our recommended DICOM image encryption method. The equations of several Enhanced Chaotic Economic Maps are derived through replacing cosine and sine functions in the standard ECEM. High-reliability encryption is accomplished through careful analysis of the ECEMs' Lyapunov exponents (proponents) and bifurcate nature. To protect patient privacy, 8-bit DICOM image pixels generated using enhanced Chaotic maps are swapped, chaotically distributed, and diffused using a variety of chaotic sequences. Scrambling is followed by a battery of security tests to prove the algorithm is sound; these include entropy, statistical, differential, key sensitivity, key space, noise attack, decryption effectiveness, and cropping.

Keywords: *Chaotic map, ACORN, DICOM, Encryption Medical Images, ECEM, Patient confidentiality*.

1. Introduction

In the Teleradiology field, there is a rapid growth in Picture Archiving and Communications Systems and cloud services, together with the emergence of the radiological information system. Thus, the confidentiality of the patient has turned into a challenging factor in a common medium. In a virtual Picture Archiving and Communications Systems and cloud, the confidentiality of the patient is obtained by sharing the encrypted form of the data Zhouet al. [1]. The patient's data must be protected, and produce a technique to encrypt the data by the cloud service. The fundamental efficient encryption is the primary need to safeguard the data, even though many new techniques and services such as IoT and Cloud are available. Therefore, it is evident that the analysis of preventive encryption algorithms now becomes necessary to give security and confidentiality in cloud storage. DICOM pixels have a strong connection and minimal unnecessary resolution data. Large amounts of repeated data are encrypted using stereotypical block ciphers such as DES, EES, BLOWFISH, and IDEA. The traditional encryption algorithms lack computing time and competence Ravichandran et al. [2].Moreover, complex sizes are fixed by the process of the block ciphers. The surplus bits are padded with other excessive bits if the unencrypted text is devoid of firm blocks. Thus, the padding creates the system unreliable.Only a handful of encryption programs are studied in imaging informatics to safeguard the patient's data. This encryption also includes chaotic-based encryption [3- 8]. Simultaneously, [2] developed a Chaotic system to encrypt 16-bit Digital Imaging and Communications in Medicine images of integrating multiple one-dimensional chaotic maps, lowering the computational difficulty of the encryption algorithm.This approach needs as much key space as possible to avoid exhaustive searches. Author uses a combination of chaotic maps (chaotic maps) and DNA sequence operation to encrypt the DICOM data. The ACM -Arnold cat map is used for encryption, and the clinical image and pseudo-random number sizes were modified by Praveenkumar et al. [9, 5]. This analysis includes the excess computational capability to alter the size of the image. Cao et al. [10-14] excessive forces are required for pre-processing and encrypting an image. Thus, in the encryption DICOM images, only a few crypto mechanisms have been proposed [15-17].The authors gather various 1-Dimensional chaotic maps used for image encryption. Correspondingly, the large dimensional maps are involved in the encryption of the image to get great secret storage [18-20]. Therefore, the main design is to give larger keyspace and the best disarray property. These benefits are gained through enhancing a chaotic equation and utilizing them in various necessary functions like diffusion, chaotic, and substitution [21-26]. Moreover, DICOM security is an emerging field of study that requires facilitation in order to confront the difficulties and challenges of sharing DICOM. In the chaotic-based encryption method, the creation of chaotic sequences is crucial to providing effective encryption and ignoring various types of security threats. Yavuz et al. [27-30]. The objective is to offer efficient chaotic encryption. Changes would be made to the available chaotic maps in order to achieve excellent confused behavior. Due to this, a Enhanced chaotic economic map would

[1] *Department of Computer and Information Science, Faculty of Science, Annamalai University, Annamalainagar – 608 002, India.*
ORCID ID : 0000-3343-7165-777X
[2] *Department of Computer and Information Science, Faculty of Science, Annamalai University, Annamalainagar – 608 002, India.*
ORCID ID : 0000-3343-7165-777X

** Corresponding Author Email: vijimca17@gmail.com*

be elevated to achieve excellent confused behaviour as opposed to the norm regarding its positive Lyapunov exponents and bifurcation nature. Physicists have developed a new technique to improve the CEM and encrypt the DICOM pixels in an attempt to make them more difficult to read. The technique involves developing three innovative types of Enhanced chaotic economic maps which are used to generate a variety of masking, permutation, and confusion sequences for each pixel. Al-Maadee et al. [31-34] explain how image encryption is attained by employing a turbulent Lorenz structure and a novel crude polynomial. S-encloses computation that employs 16 distinct S-boxes based on 16 crude unchanged polynomials of Galois field of request 256 and projective universal gathering, and then combines these S-boxes to form a turbulent guide. To get an encoded image, a plain image is jumbled using XOR activity and turbulent combination k1. The significant downside of this type is it required some investment used for encryption.

2. Proposed Cryptosystem Algorithm

The idea move toward for decrypting and encrypting vast amounts of information is to use a symmetric cryptographic technique. The suggested cryptosystem technique is a symmetric arrangement that relies on the qualities of diffusion and chaotic. The two key steps in our suggested DICOM image encryption system are the creation of diffusion and chaotic arrangements. The random images that serve as the origins for diffusion and chaotic sequences are created utilizing arbitrary number generators. To create random images matrices in our suggested system, ACORN generator is deployed. Wikramaratna [35] defines the ACORN generator from equations (1), (2), (3) and (4). Gth order Additive Congruential Random Number Generators (ACORN) are generated from an integer modulus M, an integer seed Y_0^0 fulfilling 0<$Y_0^0$0 <M and a set of k integer values.

$$Y_n^0 = Y_{n-1}^0 \ , \ n \geq 1 \quad (1)$$

$$Y_n^m = Y_n^{m-1} + Y_{n-1}^m \bmod M, \ n \geq 1, \ m = 1,\ldots,k \quad (2)$$

Wherein by $(Y)_{\text{mod M}}$ denotes the remainder on separating Y by M. By dividing M, figures Y_n^k could be regularized to a unit interval.

$$X_n^k = Y_n^k / M, \ n \geq 1 \quad (3)$$

If few basic restrictions on a preliminary parameter figures are fulfilled, the numbers X_n^k is described by Eqs (1)–(3) estimated as consistently disseminated on unit interval up to k dimensions. In other words, the modulus M must act as a big integer (usually key power), and the seed Y_0^0 including the modulus must be comparatively crucial.This is a strategy we've used in most of our trials with ACORN generator and it looks to be quite effective.

3. Mathematical Background

The equation $x_{n+1} = x_n + g \times [e - h - \gamma f] \times x_n^{\gamma}$ represents the CEM.

Where e > 0 is market demand size, f > 0 is market price slope, h ≥0 is fixed marginal cost γ and γ = 3 is constant and g > 0 is adjustment parameter speed. x_0 is the initial parameter between and (0, 1). The bifurcated range of the Chaotic Economic Map indicates that chaotic behaviour exists between and (0, 0.38). As described by Parvees et al. [35], this study makes use of ECEM type-4 and kicks off the development of the other three ECEM variants. The chaos economics map can be adjusted by multiplying the initial parameter x_n by the sin and cos trigonometric functions shown in equations (4) and (5). (7). Equations (4) through (7) represent the ECEM type-4 and type-5.

$$x_{n+1} = \sin x_n + g * [e - h - (1f) * (\cos x_n)^1] \quad (4)$$

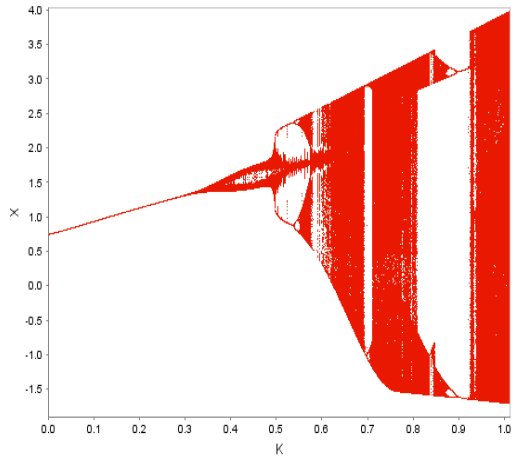
$$x_{n+1} = \cos x_n + g * [e - h - (4f) * (\cos x_n)^4] \quad (5)$$

$$x_{n+1} = \cos x_n + g * [e - h - (3f) * (\sin x_n)^3] \quad (6)$$

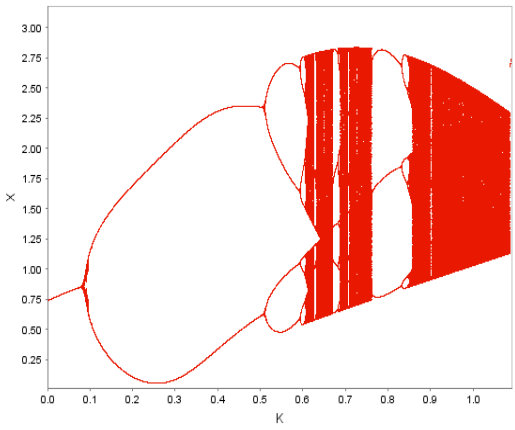
$$x_{n+1} = \sin x_n + g * [e - h - (2f) * (\sin x_n)^2] \quad (7)$$

Types 5, 6, and 7 of the ECEM exhibit chaotic behaviour between the ranges (0.63 and 1), (1.51 and 2.35), and (1.07 and 1.75) of g, illustrating the bifurcate range and Lyapunov exponent values for each. Here we have [Figures.1(A)–(F)]. The ECEM shows larger bifurcation range and positive Lyapunov exponents than the Chaotic economic map.

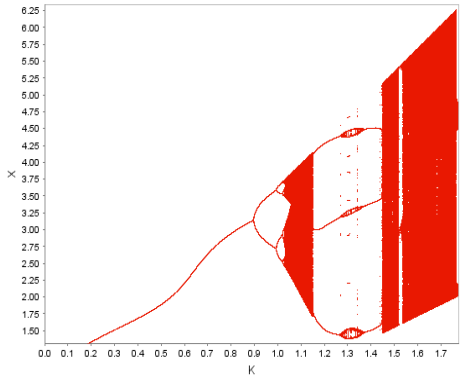
Figure 1. Bifurcate and LE -Lyapunov exponents diagram for CEM and ECEM by means of the control parameter (g), (A) bifurcation for ECEM Type[2], (B) LE for ECEM Type[1], (C) LE for ECEM types[2] and[3], (D) LE for ECEM Type[3], (E) LE for ECEM Type[4]



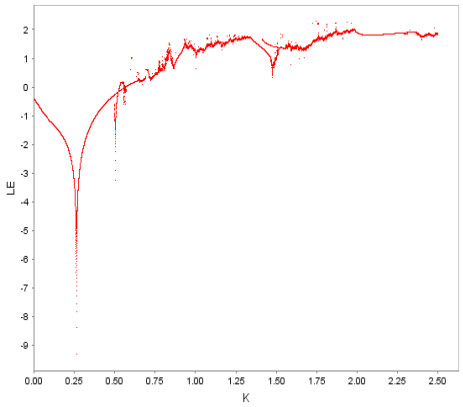
(A)



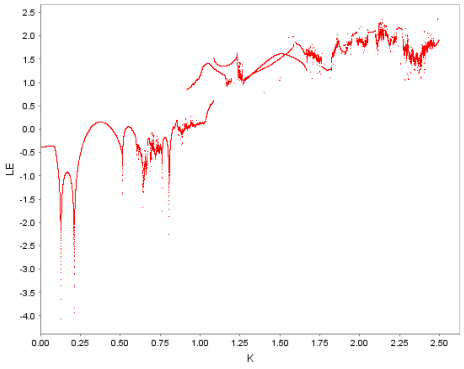
(B)



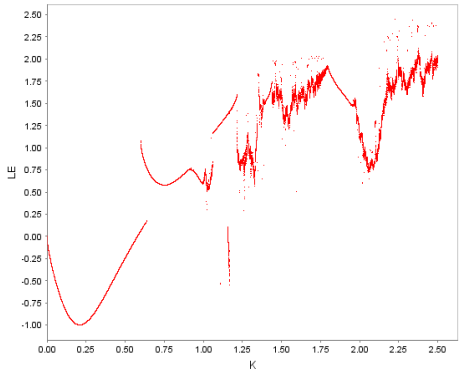
(C)



(D)



(E)



(F)

4. Methodology

The DICOM pixel data is encrypted by three processes they are diffusion, permutation, and swamping. The different types of sequences are generated from recapitalization of the four Enhanced chaotic maps, from which various input parameters are utilized to create the presented system complex and stronger. In the decryption process, the same input parameters known as encrypting keys which also used for decrypting.

4.1. Creation of permutation sequence

An ECEM of type -4 is used to generate the chaotic double-valued sequences that use all 64 bits. To obtain sorted sequences, the sequences are rearranged in either descending or ascending order. Permutation sequences are obtained by applying two ordered sequences. The pseudocode for creating the sequence of permutation is depicted in Pseudocode I. The positions of the DICOM pixels are scrambled through the eight permutation sequences in the presented algorithm.

Pseudocode I: Creating permutation sequence

BEGIN
Confusion seq $H = \{h_1, h_2, h_3, \ldots h_n\} \leftarrow SequenceGeneration(e, f, h, \gamma, g)$ from confusion Equation -2.
Choose confused sequence $H = \{h_{1000}, h_{1001}, h_{1002}, \ldots c_n\} Q = \{q_1, q_2, q_3, \ldots, q_n\}$ by sorting H.
Let $h1000$= e.$e1$ $e2$ $e3$ $e4$ $e5$ $e6$ $e7$ $e8$ $e9e10$ $e11e12$ $e13$ $e14$ $e15$ $e16$
Calculate $sum = ((100 - e_1e_2) * (100 - e_{11}e_{12})) - ((100 - e_8e_9) * (100 - e_{14}e_{15}))$
If sum =0 group confused elements into one dimensional array v_0
Repeat to get $v_1, v_2, v_3, \ldots, v_{10000}$ while sum=1,2,3,…,1000 for remain seq.
Permutation seq U= $\{u_1, u_2, u_3, \ldots, u_n\}$ is obtain by indexing $\{v_0, v_1, v_2, \ldots, v_{10000}\}$ with the elements of Q = $\{q_1, q_2, q_3, \ldots, q_n\}$.
END

4.2. Creation of diffusion sequence

The 64-bit double valued confused sequence is created from the ECEM type-6. Whereas the values between 0 and 65,535 of the 16-bitvalued DICOM pixels, the confused sequences are modified as numeric valued sequence and its values presents between 0 and 65,535. Altering the values of the DICOM pixels and they are covered by applying the eight types of diffusion sequences. The covered sequences are created by the Pseudocode II are shown bellow

Pseudocode :II

BEGIN
Chaotic seq $H = \{h_1, h_2, h_3, \ldots, h_n\} \leftarrow SequenceGeneration(e, f, h, \gamma, g)$ from chaotic Equation-3.
Select chaotic seq $X = \{x_{1000}, x_{1001}, \ldots, x_n\}$ from C.
Obtain masking seq $W = \{w_1, w_2, w_3, \ldots, w_n\}$ from $X = \{x_1, x_2, x_3, \ldots x_n\}$ by calculating
W_i= int $\{[abs(x_i) - [abs(x_i)] * 10^{16}] \bmod 65535\}$ where $W_i \in (0, 65535)$.
END

4.3. Creation of confused sequence

Using ECEM type-6 and type-7, the swapping sequence is generated. ECEM type-6 and type-7 sequences are encapsulated to obtain 64-bit double-valued sequences. Moreover, the 64-bit double valued sequences are used to obtain the numeric valued swapping sequences. When exchange the pixel values of the

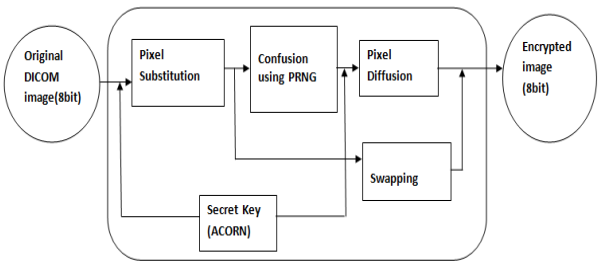
DICOM, sequence substitution is effective. From Pseudocode 3, nearly 16 distinct types of swapping sequences can be generated.
Pseudocode:III

BEGIN
Chaotic seq H= {h_1, h_2, h_3, …,h_n} ← *SequenceGeneration*(e, f, h, γ, g) from chaotic Equation-2.
Choose chaotic seq h = {h_{1000}, h_{1001}, h_{1002},…h_n}.
Q= {q_1, q_2,q_3, …,q_n} ← *Sort* (H) By sorting H.
Let $c1000$=$e.e1e2e3e4e5e6e7e8e9e10e11e12e13e14e15e16$
Calculate *sum* = ((100 – e_1e_2)*(100 – $e_{11}e_{12}$)) – ((100 – e_8e_9) *(100 – $e_{14}e_{15}$))
If *sum* =0 group seq into one-dimensional array v_0
Repeat to get while v_1, v_2, v_3,…,v_{10000}while *sum* = 1, 2, 3, …, 1000 for remaining chaotic seq.
Swapping seq T = {t_1, t_2, t_3, …,t_n} is obtained by indexing {v_0, v_1, v_2, …, v_{100}} with the elements of Q ={q_1,q_2, q_3, …,q_n}.
END

4.4. Creation of confused sequence

The entire algorithms are projected in Pseudocode 4 and they are more intricate, so that they become challenging to assume the run. Initiating the swapping procedure between the permutation and covering procedures demonstrates the significance of the presented algorithm (Figure 2). The pixels of DICOM are completely encrypted and they get highest random at the end of the eighth encapsulation. The reverse process of encryption is decryption.
Pseudocode:IV
BEGIN
READ DICOM img
SET r ← *img width*, SET m ← *img height*
COMPUTE $n = r * m$
READ16-bit grey values in 1-dimensional array K= {k_1,k_2,k_3,…,k_n}
CREATE 8 permutation (U_1, U_2, …,U_8), 8 masking (W_1, W_2, …, W_8) and 16 swapping (T_1,T_2,T_3, …,T_{16}) seq of length n using different ECEMs.
SET e ← 1, SET f ← 1, SET g ← 2
for n ← 1 to 8 do
CALCULATE permuted pixel U_e
CALCULATE confused pixels K ← $K \leftrightarrow T_f$
CALCULATE diffused pixels K ← $K \oplus W_e$
CALCULATE confused pixels K ← $K \leftrightarrow T_g$
SETi ← e+1, SETf ← j+2,SET g ← g+2
end for
RETURN Encrypt pixels K.

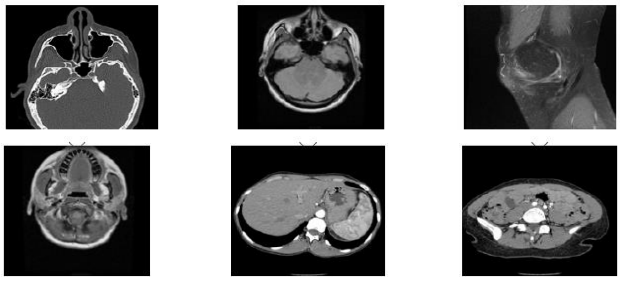
Figure 2. DICOM Encryption Scheme's Structure.



5. Results

Considering these six 16-bit DICOM images in sizes 512*512 and 256*256,this section analyses and displays the outcomes of the method shown in Figure 3. Differential, statistical, key space, key sensitivity, noise attack, cropping attack, and decipher efficiency analyses be used to evaluate the presented encryption scheme.

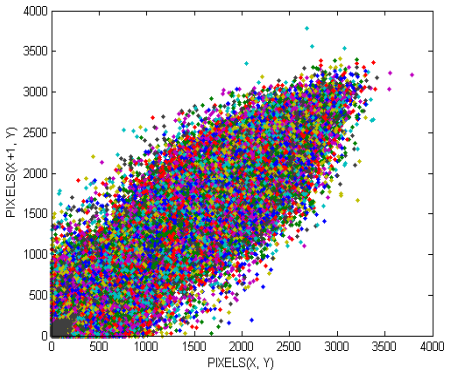
Figure 3. The test DICOM images, [1] MI-01[2] MI-02 [3] MI-03 [4] MI-04 [5] CT-01[6] CT-02



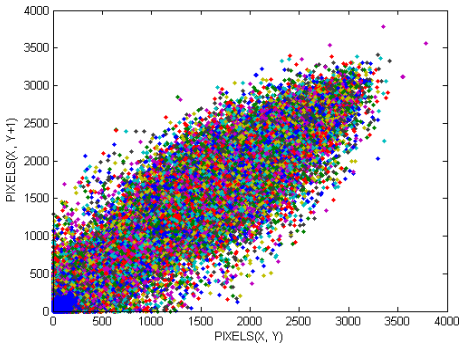
5.1. Statistical analysis

DICOM images can be encrypted using the presented algorithm by having their pixel data scrambled, swapped, and modified. This is why testing the proposed image encryption algorithm's robustness against statistical attacks is essential.

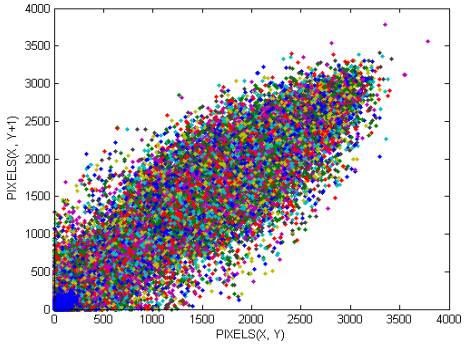
Figure 4. The correlation coefficient analysis of Plain and encrypted images (1) and (4) horizontal, (2) and (5) vertical and (3) and (6) diagonal



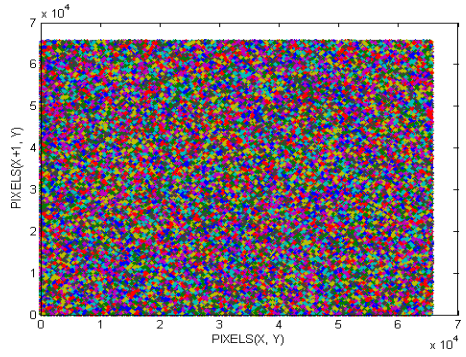
(1)



(2)



(3)



(4)

5.1.1. Correlation Coefficient Analysis

Correlation coefficients are used to study the correlation between any two given pixels. A correlation value is calculated by picking pixels at random from 10,000 adjustment positions and adding them into an equation (8). In order to create an encrypted image, a regular cryptosystem must obviously destroy the link between individual pixels. As a result, the value of the correlation coefficient for an encrypted image must be far from one (1), as this would indicate that the image's pixels are fixed and the encryption system is unable to decrypt the image. Correlation values between encrypted and unencrypted images are shown in Table 1. [37-39]. In the image each pixel is same to the others. Image encryption correlation coefficients are computed in the vertical, horizontal, and diagonal directions (Fig. 5).

$$\gamma_{gh} = \frac{Cov(g,h)}{\sqrt{F(g)\sqrt{F(h)}}} \tag{8}$$

where x and y values of adjacent pixels.

$$Cov(g,h) = \frac{1}{U \times V}\sum_{n=1}^{U}\sum_{m=1}^{V}[g(t,r) - E(g)][h(m,n - S(h)]$$

$$S(g) = \frac{1}{U \times V}\sum_{m=1}^{U}\sum_{n=1}^{V} g(m,n), F(g) = \frac{1}{U \times V}\sum_{m=1}^{U}\sum_{n=1}^{V}[g(m,n) - S(g)]^2$$

5.1.2. Histogram Analysis

The Histogram analysis is carried out by drawing pixel graphs of both the encrypted and original images. Everyone can understand the data and its significance because it is evenly distributed across the pixels, as figure shown 5(a).The encrypt algorithm also evenly disperses the 16-bit pixel data through transformation, swapping, and diffusion. Therefore, the contents of the encrypted image are secure from any would-be thieves. If you look at Figure 5(b), you can see the histogram of the encrypted image, and you can see that the flat allocation of pixels is enough to support the cipher image algorithm. That histogram analysis is used to protect the encrypted image from statistical attacks is now abundantly clear. Therefore, the presented encryption algorithm is effective, as shown by the histogram analysis.

5.1.3. Information Entropy

In 1949, Shannon proposed the concept of the information entropy uses statistical analysis towards quantify the quantity of uncertainty present in a system. This assessment is grounded in the randomness of the encrypted image. Information entropy analysis formula is,

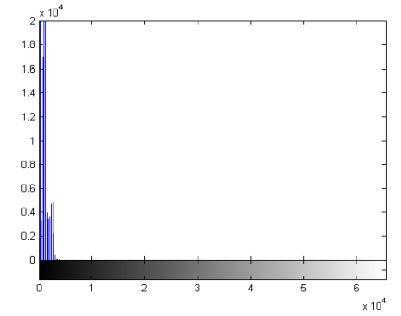
$$U(t) = \sum_{z=1}^{R} n(tz)\log\frac{1}{n(tz)} \tag{9}$$

Where, R is the pixels of the image, $tz \in t$ and $n(t_z)$ is the symbol of the probability of occurrence $'t_z'$.Therefore, the image displays the 8-bit data. If the entropy is calculated to be very close to its maximum value, the algorithm will produce extremely blurry results. Table 2 displays the entropy results. The fact that the cipher image and its values are so close to 16(15.8888 ≈16) indicates that the algorithm did a good job of encrypting the image and protecting it from entropy.

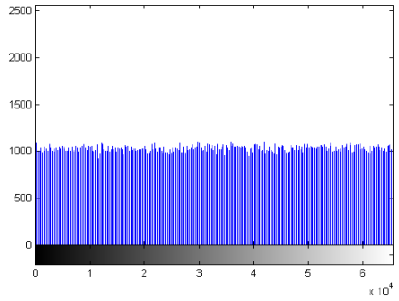
Table 1. The correlation coefficient analysis of test images

Test Image	*Image*	*Vertical*	*Horizontal*	*Diagonal*
MI–1	Plain Img	0.9676	0.9757	0.9548
	Cipher	0.0944	0.0057	0.0067
MI–2	Plain Img	0.97560	0.96639	0.94940
	Cipher	–0.00604	–0.00354	0.00068
MI–3	Plain Img	0.9719	0.9846	0.9641
	Cipher	0.0884	0.0061	0.0112
MI–4	Plain Img	0.98663	0.98353	0.95535
	Cipher	–0.00524	0.00452	0.00046
CT–1	Plain Img	0.998292	0.99658	0.99191
	Cipher	0.002600	–0.00411	0.00719
CT–2	Plain Img	0.98650	0.99752	0.99369
	Cipher	–0.00002	0.00002	–0.00161

Figure 5. The histogram analysis, (1) original DICOM (2) encrypted image of MRI-1 (color online version)



(1)



(2)

Table 2. The entropy values of test images nits for magnetic properties

Test Images	Original Image	Encrypted image
MI-1	8.91519	15.80932
MI-2	8.08822	15.17223
MI-3	8.44120	15.80740
MI-4	9.11792	15.17250
CT-1	9.06850	15.80675
CT-2	7.53473	15.80640

5.1.4. Mean-variance grey value analysis

The impact of the encryption on the image's pixels is measured using a mean-variance grey value analysis. The mean-variance value of the plain-image pixels is less than that of the encrypted-image pixels. Mean-variance analysis of gray-scale images is determined by the given equation:

$$k = \frac{1}{U \times V} \sum_{m=1}^{U} \sum_{n=1}^{V} \left(B(m,n) - \overline{B} \right) \tag{10}$$

THere, B is the mean value of pixels, and the size of the original image is $U \times V$.

Statistics comparing the encrypted and unencrypted images' means and standard deviations. When comparing the cipher and plain images, the plain image always has a lower value when calculating the difference between the two. The mean-variance of the cipher image would be higher because the muddled cryptosystem breaks down the connections between the pixels. The average dispersion of grey-scale images is shown in Table 3. The analysis is consistent with the results presented by Zhen et al. [36]. Large samples are required for the mean-variance grey value analysis.

Table 3. The entropy values of test images nits for magnetic properties

Test img	*Original img*	*Encrypted img*
MI-1	573.53720	16,497.24195
MI-2	184.39219	16,475.85243
MI-3	484.67239	16,476.88167
MI-4	177.60507	16,458.90618
CT-1	504.51829	16,484.28775
CT-2	501.18447	16,468.40775

5.1.5. Mean Square Error and Peak Signal to Noise Ratio

The algorithm's efficacy can be evaluated by comparing the enciphered image's degree of randomness to that of the original image using the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The MSE compares the encrypted and unencrypted image pixels. The formula for this is (11) and (12). Table 4. The future encryption algorithm will yield a secure cryptosystem as evidenced by the high MSE error value and low PSNR value.

$$MSE = \frac{1}{U \times V} \sum_{z=1}^{t} \sum_{x=1}^{r} \left| o(z, j) - ex(z, x) \right| \tag{11}$$

Here *o(z,x)* symbolizes the original image ; *ex(z, x)* depicts the cipher image; and the dimensions of the images are denoted by U×V.

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE} \right) \tag{12}$$

where MAX_i is the image highest feasible pixel value.

5.2. Key Space Analysis

Instances and probabilities of encryption with various key types are displayed in the key space analysis. The role of key space analysis is critical in protecting a cryptosystem from brute-force attacks. An analysis of the key space is required if attackers plan to use the key form discovered in the key space to break apart the cryptosystem. Both the first equation and the control parameters contribute to the muddled state of the key space. In order to shuffle, swap, and otherwise shuffle the pixels, the analysis makes use of 192 different parameters. It's possible to categorise them into four This investigation makes use of improved confused maps to better define the crucial domain. Input parameters are represented by the 64-bit value. In most cases, a power of 2 is used to denote the key space. Compared to the key spaces reported by Ravichandranet al. [2], Fu et al. [18], and Praveenkumar et al. [8], this system's key space of 212288 is significantly larger. It is so large that searching its key space by brute force has become the most difficult thing possible. When the key space is large, the cryptosystem becomes secure. Confusion in the cryptosystem typically provides a larger key space. The key space was a crucial metric in the development of the confused cryptosystem.

Table 4. The correlation coefficient analysis of test images

Metrics	*MI-1*	*MI-2*	*MI-3*
MSE	18,949.2928018	904.9927718	945.03066
PSNR	47.542803	48.54296	48.54378
Metrics	***MI-4***	***CT-1***	***CT-2***
MSE	18,991.32981	18,936.91040	18,927.30562
PSNR	48.54610	48.53793	47.56014

5.3. Key Sensitivity Analysis

The importance of key sensitivity in cryptosystem analysis cannot be overstated. For this analysis, we tweak the key and try to break the cryptosystem using the new version of the key. The key has been altered if there is even a single bit (or digit) difference between it and the original. There is a one-decimal-place difference in the key used to decode the cipher image. The encryption is analyzed by the usage of the original set of keys and have the value of a parameter x_0 = 4.500000000000001. In decrypt the altered value of the assigned parameter is x_0 = 4.5000000000000001. The following decrypted images are shown in the figures 6(a)-6(d). it is clear that the usage of lightly modified key for decryption gives variant image decrypt and it is different from the original. Therefore, the keys are having higher sensitivity in the presented algorithm.

5.4. Differential attack analysis

The information is extracted by the attackers through differential attack and they change the values of the pixel. Assuming a plain image is necessary because of the possibility of a shift in pixel value patterns during decrypt. As a result, this risk is analysed in terms of the confused cryptography by means of the metrics NPCR (Number of Pixels Change Rate) and UACI (User Adaptive Cryptographic Index) (Unified Average Changing Intensity). When compare two images decrypted with the same key, NCPR analyses the percentage of changed pixels, while UACI calculates the ratio of changed pixels. Then the algorithm of the encryption is effective in spite of differential attacks. The equations 13 and 14 are used for calculating NPCR and UACI.

$$NPCR = \frac{1}{U \times V} \sum_{m=1}^{U} \sum_{n=1}^{V} D(m,n) \times 100 \tag{13}$$

$$UACI = \frac{1}{U \times V} \sum_{m=1}^{U} \sum_{n=1}^{V} \frac{\left(S_1(m,n) - S_2(m,n)\right)}{255} \times 100 \tag{14}$$

Here $D(m,n)$depicts the variation among $S_1(m,n)$ and $S_2(m,n)$.In case, the $S_1(m,n) = S_2(m,n)$and F (m,n) =0,where else $F(m,n)$ =0.

The NPCR provides data on the least amount number of pixels that have changed, while the UACI details any shifts between the two cipher images. The encrypted image has the values 99.6721 and 33.3842. The values are computed, and the conclusion of the computation shows that the results are more effective than the results stated by Fu et al. [18] and Ravichandranet al. [2]. In Table 5, we can see how well a given cryptosystem has the potential to protect against differential attacks.

5.5. Encryption speed analysis

The creation of 64-bit double valued confused sequences incorporating four distinct types of improved CEM along with multiple steps of consecutive rounds. This analysis employs 2.6GHZ Intelcore-15 processor computer system and DICOM image of 512x512 with the depth of 16-bit is encrypted through the RAM of 4GB. The different algorithms are categorized on the basics of the encryption speed are enlisted in the Table number 8. It shows the presented algorithm speed is excelled than that of the results of Natesh et al. [14], and also Fu et al. [5] algorithm, Caoet al. [10], and Stoyanov et al. [40] receive less time in encryption, and also comparing with the presented algorithm these are have lower security level. There 192 types of keys are used in different rounds of the algorithms. Thus, it is an effective approach and furthermore it is hard to penetrate by the brute-force attack. The time of the encryption increases because of the involvement of computation in creating the various types of confused sequences and the process of permutation, swapping, and diffusion. Moreover, the algorithm applied the functions of cosine and sine in the equations delays the time a little slower in the presented algorithm when comparing with the other results.

On the whole, this algorithm ensures the security and safety in higher standard with in the period of the optimum time.

Table 5. The NPCR and UACI values of test images

	UACI		*NPCR*	
Test images	***Proposed***	***Ravichandranetal.(2016)***	***Proposed***	***Ravichandranetal.(2016)***
MI-1	49.08670	NA	99.98909	NA
MI-2	50.98732	33.373	99.98944	99.9970
MI-3	50.03991	33.342	99.98920	99.55
MI-4	49.94685	NA	99.98845	NA
CT-1	50.2665	33.396	99.99945	99.9982
CT-2	49.98823	33.387	99.99943	99.9963

6. Conclusion

The cryptosystem is a dynamic thing and therefore it utilizes various types of ECEM to create random sequences for encrypting the pixels of DICOM in adapting swapping – swapping pattern-permutation-diffusion. The color DICOM images of 24-bit are encrypted by the data pixels, this ensures that the crypto system gives confidentiality to the patient's images the approaches of enhanced PRNGS are ACORN applied in this study to maximize the random sequences than the original, then they are mingled with improved logistic two dimensional coupled chaotic map-CCM for providing efficient pixel scrambling.. This

study applied several kinds of procedures the various input parameters act as key for many rounds. Hence the presented cryptosystem is rigid and it is sufficient enough to give confidentiality for the clinical image. However, the emulsions of Enchanced Chaotic maps treat the largest key space so that they highly repel the attacks of brute force. There are several kinds of statistical protective examinations they grey value information entropy, MSE and PSNR, and run length statistics and also comparing these examinations with the known literature to show that this system has the potential to defeat different types of statistical attacks. As the same, the end result of differential analysis also ensure that the entire cryptosystem is fully protected from threats. The whole cryptosystem has the ability to provide the best protection and a greater key space and protect the entire cryptosystem from any type of threats having high potential attacks. This method is best suited to safeguard the communication and clinical images. Above all the presented encryption tool that offers a super standard security and authenticity of the clinical images because it applies several types of statistical approaches obviously increase the security and confidentiality of the data.

Acknowledgements

Would like to thank Department of Computer and Information Science, Annamalai University authorities for providing RUSA funded Computer Laboratory and Dr.C.P.Ramaswami Aiyar Library, Annamalai University.

Author contributions

Vijayakumar T: Conceptualization, Methodology, Software, Field study **Mohammed parvees M.Y:** Data curation, Writing-Original draft preparation, Software, Validation., Field study

Conflicts of interest

The authors declare no conflicts of interest.

References

L., Zhou, V. Varadharajan, and M. Hitchens, (2012) 'A flexible cryptographic approach for securedata storage in the cloud using role-based access control', *International Journal of CloudComputing*,Vol.1,Nos. 2/3, pp.201–220.

D. Ravichandran, P. Praveenkumar, J.B.B Rayappan and R. Amirtharajan,(2016)' Chaos based cross overandmutation for securing DICOMimage',*ComputesinBiologyandMedicine*,Vol.72, pp.170–184, DOI: 10.1016/j.compbiomed.2016.03.020.

L.O.M. Kobayashi and S.S. Fururie, (2009) 'Proposal for DICOM multi frame medical image integrity and authenticity', *Journal of Digital Imaging*, Vol. 22, No. 1, pp.71–83,DOI:10.1007/s10278-008-9103-6.

P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J.B.B.Rayappan, (2015) 'Triple chaotic image scrambling on RGB a random image encryption approach' ,*Security and Communications Networks*, Vol.8, No.18,pp.3335–3345, DOI: 10.1002/sec.1257.

C. Fu, W. Meng, Y.Zhan, Z. Zhu, F.C.M. Lau,C.K., Tse and Ma, H. (2013) 'An efficient andsecure medical image protection scheme based on chaotic maps', *Computers in Biology andMedicine*,Vol. 43,pp.1000–1010, DOI: 10.1016/j.compbiomed.2013.05.005.

A. Kanso and M. Ghebleh, (2015) 'An efficient and robust image encryption scheme for medical applications', *Communications in Nonlinear Science and Numerica lSimulation*, Vol.24,Nos.1–3, pp.98–116, DOI: 10.1016/j.cnsns.2014.12.005.

M,Y.M.Parvees, J.A.Samath, I.K.Raj and R.M.Nirmal, (2017) 'Chaos-based stegano cryptic approach to protect medical images with text data of patients', *Journa lof Medical Imaging and Health Informatics*, Vol.7, pp.1–8, DOI: 10.1166/jmihi.2017.1993.

P.Praveenkumar, N.Kerthana Devi, D.Ravichandran, J.Avila, K.Thenmozhi,J.B.B. Rayappan and R.Amirtharajan, (2017) 'Trans receiving of encrypted medical image – a cognitive approach', Multimedia Tools Applications, pp.1–26, DOI: 10.1007/s11042-017-4741-7.

C.Fu, W. Meng, Y. Zhan, Z. Zhu, F.C.M. Lau, C.K. Tse and H. Ma, (2013) 'An efficient and secure medical image protection scheme based on chaotic maps', Computers in Biology and Medicine, Vol. 43, pp.1000–1010, DOI: 10.1016/j.compbiomed.2013.05.005.

W. Cao, Y. Zh,ou ,C.L.P. Philip and L. Xia, (2017) 'Medical image encryption using edge maps',Signal Processing, Vol. 132, pp.96–109, DOI: 10.1016/j.sigpro.2016.10.003

M. Dzwonkowski , M. Papaj and R.Rykaczewski, (2015) 'A new quaternion-based encryption method for DICOM images', IEEE Transactions on Image Processing, DOI: 10.1109/TIP.2015.2467317.

J.Hu and F.Han, (2009) 'A pixel-based scrambling scheme for digital medical images protection', Journal of Network and Computer Applications, Vol. 32, pp.788–794, DOI: 10.1016/j.jnca.2009.02.009.

A.Al-Haj, G.Abandah and N.Hussein, (2015) 'Crypto-based algorithms for secured medical image transmission', IET Information Security, Vol. 9, pp.365–373, DOI: 10.1049/iet- ifs.2014.0245.

Q.N.Natsheh, B.Li and A.G.Gale, (2016) 'Security of multi-frame DICOM images using XOR encryption approach', International Conference on Medical Imaging Understanding and Analysis, Procedia Computer Science, Vol. 90, pp.175–181, DOI: 10.1016/ j.procs.2016.07.018.

C.Dong, (2014) 'Colour image encryption using one-time keys and coupled chaotic systems', Signal Processing: Image Communications, Vol. 29, pp.628–640, DOI: 10.1016/j.image. 2013.09.006

S.Behnia, A.Akhshani, H.Mahmodi, and A.Akhavan, (2008) 'A novel algorithm for image encryption based on mixture of chaotic maps', Chaos, Solitons and Fractals, Vol. 35, pp.408–419, DOI: 10.1016/j.chaos.2006.05.011.

S.Dhall , SK.Pal ,K.Sharma (2018) Cryptanalysis of image encryption scheme based on a new 1D chaotic system. Signal Process 146:22–32. https://doi.org/10.1016/J.SIGPRO.2017.12.021.

M.Dzwonkowski , R.Rykaczewski (2019) Secure quaternion feistel cipher for DICOM images. IEEE Trans Image Process 28:371–380. https://doi.org/10.1109/TIP.2018.2868388.

R.Enayatifar ,AH. Abdullah ,IF. Isnin et al (2017) Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Eng 90:146–154. https://doi.org/10.1016/J.OPTLASENG.2016.10.006.

D.Huo ,ZD Fu ,S Yuan et al (2019) Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding. Physics Letters, Section A: General, Atomic and Solid State Physics 383:915– 922. https://doi.org/10.1016/j.physleta.2018.12.011.

Q.Zhang, L.Guo and X.Wei, (2010) 'Image encryption using DNA addition combining with chaotic maps', Mathematical and Computer Modelling, Vol. 52, Nos. 11/12, pp.2028–2035, DOI: 10.1016/j.mcm.2010.06.005.

C.Fu, G.Zhang, O.Bian, W.Lei and H.Ma, (2014) 'A novel medical image protection scheme using a 3-dimensional chaotic system', PLoS One, Vol. 9, p.e115773 DOI: 10.1371/journal.pone.0115773.

A.Kanso and M.Ghebleh, (2012) 'A novel image encryption algorithm based on a 3D chaotic map', Communications in Nonlinear Science and Numerical Simulation, Vol. 17, pp.2943–2959, DOI: 10.1016/j.cnsns.2011.11.030.

S.M.Seyedzadeh, and S,Mirzakuchaki, (2012) 'A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map', Signal Processing, Vol. 92, pp.1202–1215, DOI: 10.1016/j.sigpro.2011.11.004.

S.Rajagopalan ,S. Poori ,M. Narasimhan et al (2020) Chua's diode and strange attractor: a three-layer hardware–software co-design for medical image confidentiality. IET Image Process 14:1248–1256. https://doi.org/10.1049/iet-ipr.2019.0562.

Y.Zhang , Y.Li ,W. Wen et al (2015) Deciphering an image cipher based on 3-cell chaotic map and biological operations. Nonlinear Dynamics 82:1831–1837. https://doi.org/10.1007/s11071-015-2280-1.

E.Yavuz, R.Yazici, M.C.Kasapbas and E.Yamac, (2016) 'A chaos-based image encryption algorithm with simple logical functions', Computers & Electrical Engineering, Vol. 54, pp.471–483, DOI: 10.1016/j.compeleceng.2015.11.008.

Hua, Zhongyun, Shuang Yi, and Yicong Zhou. "Medical image encryption using high-speed scrambling and pixel adaptive diffusion." *Signal Processing* 144 (2018): 134-144.

Kamal, T.Sara et al. "A new image encryption algorithm for grey and color medical images." *IEEE Access* 9 (2021): 37855-37865,DOI**:** 10.1109/ACCESS.2021.3063237.

Guesmi, Ramzi, and M. A. Farah. "A new efficient medical image cipher based on hybrid chaotic map and DNA code." *Multimedia tools and applications* 80.2 (2021): 1925-1944.Google Scholar.

TemadherAlassiry Al-Maadee, IqtadarHussain, Amir Anees, Muhammad Tahir Mustafa, "A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes", Multimedia Tools and Applications, 2021,Vol-80, pp-24801–24822, https://doi.org/10.1007/s11042-021-10695-5.

S.AashiqBanu and RengarajanAmirtharajan. "Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach." *Multimedia Tools and Applications* 79.39 (2020): 28807-28824.

A.Belazi , Abd El-Latif AA, S Belghith (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170. https://doi.org/10.1016/J.SIGPRO.2016.03.021.

JC Dagadu , J Li , EO Aboagye (2019) Medical image encryption based on hybrid chaotic DNA diffusion. WirelPersCommun 108:591–612. https://doi.org/10.1007/s11277-019-06420-z.

R.S. Wikramaratna, "Theoretical background for the ACORN random number generator", Report AEA-APS-0244, AEA Technology, Winfrith, Dorset, UK, 1992.

W.Zhen, H. Xia, L.Yu-Xia, and S.Xiao-Na, (2013) 'A new image encryption algorithm based on the fractional-order', Chinese Physics B, Vol. 010504, DOI: 10.1088/1674-1056/22/1/010504.

J.Liu, Y.Ma, S. Li, J.Lian & X.Zhang, (2018). A new simple chaotic system and its application in medical image encryption. *Multimedia Tools and Applications*, *77*(17), 22787-22808.

S.Kumar, B.Panna &R.K.Jha, (2019). Medical image encryption using fractional discrete cosine transform with chaotic function. *Medical & biological engineering & computing*, *57*(11), 2517-2533.

T.Wazi, Mayada et al. "A secure image cryptosystem via multiple chaotic maps." *Discrete Mathematics, Algorithms and Applications* (2021): 2150141.

B.Stoyanov, and K.Kordov, (2015) 'Image encryption using Chebyshev map and rotation equation', Entropy, Vol. 17, pp.2117–2139, DOI: 10.3390/e17042117.