International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(9s) 2026 pp. 739-754
https://doi.org/10.70917/ijcisim-2026-3497
Article

NIST compliant Difference of Sine-Cosine based Non-linear Modulated Signal Chaotic Map Driven Medical Image Encryption Defender of Statistical and Differential Attacks

Suresh Nakum[1], Mehul Shah[2*]

[1]Gujarat Technological University, Ahmedabad, Electronics and Communication Engineering Department, GECR, Gujarat, India,
[2*]Charutar Vidhymandal. University, Electronics and Communication Engineering Department, GCET, Anand, 388001, Gujarat, India..
***Corresponding Author's Email**: drmehul.iitb@gmail.com

Abstract: This article proposes a Difference of Sine-Cosine based Non-linear Modulated Signal based chaotic map driven encryption technique designed for medical images, which are vital in disease diagnosis, treatment planning, and patient monitoring. Since medical images are classified as protected health information, they require strong encryption to ensure confidentiality and prevent unauthorized access. The proposed method uses a chaotic system sensitive to initial conditions, making small changes in the input image or key result in completely different encrypted outputs. This property significantly strengthens resistance against differential attacks. The chaotic map enhances confusion and diffusion, producing cipher images that pass all statistical randomness tests by National Institute of Standards and Technology (NIST) and exhibit no discernible patterns, thus protecting against cryptanalysis. In this approach, the image is first converted into a one-dimensional vector, which is then divided into two segments and diffusion is applied. The combined diffused data subsequently undergoes chaotic sequence based permutation, followed by six layers of diffusion both using chaotic and pseudo random sequences. The technique is evaluated using entropy analysis, correlation coefficients, key space analysis, and histogram uniformity with Number of Pixel Change Rate (NPCR) > 99.59% and Unified Average Change in Intensity (UACI) >33.33% but lower then derived theoretical upper bound limit, results confirm the schemes robustness and effectiveness in securing sensitive medical images, especially for telemedicine and cloud storage applications.
Keywords: Attack resistance, Bifurcation diagram, Chaotic map, Lyapunov exponent, Sine-Cosine Non-linear Modulated Signal.

1. INTRODUCTION

Medical imaging constitutes a cornerstone of modern healthcare, utilizing modalities such as Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET), Computed Tomography (CT), Ultrasound, and X-ray imaging to deliver critical diagnostic information Zhang et al. [1]. Strong encryption methods are required due to the sensitive nature of these images in order to preserve patient privacy and data integrity throughout transmission and storage. Several standards are used for this purpose. Health Information Protection and Accountability Act (HIPAA) gives guide lines for protection of medical images using encryption in United States Moore and Frye [2]. General Data Protection Regulation (GDPR) standard available in European Union, focusing on patient's sensitive information. It also allows users to delete personal data if require and offers consent based access method Greengard [3]. The universal protocol for managing, sending, and keeping medical images and associated information are called Digital Imaging and Communications in Medicine (DICOM). It supports several modalities, embeds patient data with images, and guarantees compatibility between imaging devices, widely used in the medical field DICOM Standards Committee [4]. While HIPAA, GDPR, and DICOM mandate strong protection mechanisms for medical images, they do not

prescribe specific encryption algorithms, allowing researchers and developers to employ suitable methods. A variety of medical image encryption approaches are available, such as transform-based methods, chaotic map-based methods, and traditional transposition and substitution-based methods.

Traditional Methods

Transposition encryption rearranges pixel positions without altering values, making it fast but less secure, as pixel patterns remain analysable while substitution encryption changes pixel values based on a key, offering better security, but can be compromised if the key or method lacks complexity Shannon [5].

Transform-Based Methods

These convert images into frequency domains encrypt coefficients, and then apply inverse transforms. Discrete cosine and other transforms based encryption hides visual details effectively but have low key space Li et al. [6].

Chaotic map-Based Methods

Due to their inherent sensitivity to initial conditions and the resulting unpredictability Naik and Singh [7], the sensitive nonlinear mapping in chaotic map is highly effective for image encryption. The proposed encryption framework employs a nonlinear chaotic dynamical system to generate highly complex and pseudo-random sequences suitable for secure image encryption. The chaotic sequence is mathematically represented by Equation [1].

$$X_{n+1} = f(X_n, \mu) \quad [1]$$

where X_n denotes the present state of the chaotic system at the n^{th} iteration, X_{n+1} represents the subsequent generated state, $f(\cdot)$ is a nonlinear mapping function, and μ is the control parameter governing the dynamical behavior of the system. For suitable values of μ, the map operates in the chaotic region, producing non-periodic and ergodic sequences with high randomness characteristics. A significant property of the chaotic system is its extreme sensitivity to initial conditions, mathematically expressed as $\delta r_n \rightarrow \delta r_{n+1} \gg \delta r_n$, ideal properties for cryptographic applications. which indicates that a very small variation in the initial state δr_n results in a substantially large deviation after several iterations. This property enhances cryptographic security because even a minute alteration in the secret key generates an entirely different chaotic sequence, thereby increasing resistance against brute-force, statistical, and differential attacks.

The generated chaotic sequence is subsequently utilized in both confusion and diffusion stages of the encryption process. Initially, the pixel positions of the plain image are shuffled using a permutation mechanism controlled by chaotic indices. Thereafter, diffusion is applied to modify pixel intensity values using the generated chaotic sequence. The overall encryption operation is represented by Equation [2]

$$I' = S(P(I), X_n) \quad [2]$$

where I represents the original plain image matrix and I' denotes the encrypted cipher image. The function $P(\cdot)$ corresponds to the permutation operation that rearranges pixel positions according to the chaotic ordering sequence, thereby reducing spatial correlation among adjacent pixels. The function $S(\cdot)$ denotes the substitution or diffusion process in which pixel intensity values are altered using the chaotic sequence X_n This combined permutation–diffusion architecture significantly improves the confusion and diffusion properties of the cryptosystem, resulting in enhanced randomness and stronger resistance to cryptanalytic attacks.

Recent development

Early advancements in chaos-based cryptography were primarily focused on the integration of intelligent frameworks and biological computing models to enhance structural preservation and unpredictability. Considerable efficacy in preserving vital structural information while resisting unauthorized cryptanalysis has been demonstrated by neural network-assisted encryption methods. Past researches indicate that a neural network-based chaotic framework achieved strong resistance against differential attacks, with a Number of Changing Pixel Rate (NPCR) of 99.75%, a Unified Average Changing Intensity (UACI) of 33.61%, and an information entropy of 7.984 being reported in Panigrahy et al. [8]. However, substantial computational overhead was imposed due to the inherent complexities associated with network training and parameter optimization.

To amplify confusion and diffusion characteristics, DNA encoding sequences have been combined with chaotic dynamics in several studies. Recent researches discuss that the application of biological sequence operations alongside

non-linear chaotic maps significantly improved pixel randomization, as reported in Elmanfaloty et al. [9]. Nevertheless, finite-precision degradation in digital hardware continued to remain a persistent limitation. To address this challenge, a chaotic neural network integrated with DNA computing was proposed in Maddodi et al. [10] to enhance dynamic key sensitivity. Although an NPCR of 99.67% and entropy of 7.9131 were achieved, the comparatively lower entropy value suggested the persistence of subtle statistical irregularities within the cipher-images.

The increasing deployment of resource-constrained IoT networks has intensified the demand for lightweight and computationally efficient encryption protocols. Several researches suggest that a multi-chaotic architecture optimized for IoT endpoints was introduced in Jain et al. [11]. Although an acceptable NPCR of 99.60% was demonstrated, a Peak Signal-to-Noise Ratio (PSNR) of 10.221 dB and entropy of 7.7083 were obtained, thereby indicating weaker statistical randomness and noticeable visual distortion trade-offs. Similarly, computational overhead was minimized in Choi et al. [12] by restricting operations to lightweight addition, rotation, and XOR logic combined with chaotic sequences. While execution speed was considerably accelerated, the absence of deep non-linear transformations reduced the overall system complexity, thereby increasing vulnerability to advanced cryptanalysis.

Past researches further indicate that a medical image encryption framework emphasizing high key sensitivity was presented in Shankar et al. [13]. However, an imbalanced diffusion profile was observed, where a highly elevated UACI of 48.22% was achieved alongside an insufficient NPCR of 82.78%, reflecting unstable diffusion dynamics. Conversely, a highly uniform neural network-assisted framework was developed in Thoms et al. [14] for its intended applications, where an NPCR of 99.63%, a UACI of 33.44%, and an exceptional entropy of 7.9972 were reported. Despite the strong statistical properties, stringent real-time synchronization between communication endpoints was required, significantly increasing implementation complexity.

To overcome the limitations associated with classical chaotic maps, optimization-driven and hardware-oriented architectures have recently been explored. Recent researches discuss that evolutionary optimization algorithms were leveraged in Toktas et al. [15] to stabilize chaotic map performance and directly enhance diffusion efficiency. Similarly, neural networks were utilized in Lin et al. [16] for adaptive and dynamic key generation in IoT environments, providing a key space of 2256. Furthermore, memristive Hopfield neural networks were investigated in Yu et al. [17] to facilitate real-time parallel processing in hardware, although the maintenance of non-linear stability required complex parameter tuning. Chaotic pseudo-random number generators (PRNGs) were deployed in Krishnamoorthi et al. [18] to improve unpredictability; however, the generated sequences remained highly susceptible to transmission bit errors and communication channel noise.

Recent state-of-the-art literature has predominantly emphasized hybrid frameworks in which multiple cryptographic principles are merged to maximize security. Several researches suggest that chaos theory has been integrated with advanced mathematical concepts, including elliptic curve cryptography, affine transformations, Hilbert matrices, and multi-stage diffusion layers, as presented in Previous works **[19–23]**. Balanced diffusion characteristics were achieved in Inam et al. [19], where an NPCR of 99.63%, a UACI of 33.47%, and an entropy of 7.9291 were reported. Enhanced statistical uniformity was further demonstrated in Kolivand et al. [21], with an NPCR of 99.69%, a UACI of 33.50%, and an entropy of 7.9872 being achieved. Importantly, the chaotic sequences proposed in **[21-23]** were validated using the NIST statistical test suite. In these studies, p-values exceeding the 0.01 significance threshold were consistently achieved across Frequency, Runs, Rank, DFT, Entropy, and Non-Overlapping Template Matching tests, although certain tests were reported to fail, thereby confirming low resistance against statistical attacks. Despite few advantages, hybrid frameworks inherently introduced severe penalties in terms of computational complexity, memory consumption, and execution latency.

Beyond the spatial domain, transform-domain and decentralized paradigms have also been investigated. Past researches indicate that Discrete Wavelet Transform (DWT)-based encryption was utilized in Kaur and Singh [24] to provide frequency-domain security and noise resilience, although real-time execution remained computationally prohibitive. A key space of 2256 was also reported. Alternatively, block chain technology was integrated in Inam et al. [25] to ensure tamper resistance and decentralized authentication for shared IoT images; however, storage overhead and network scalability continued to restrict large-scale practical deployment. Furthermore, a highly complex four-dimensional (4D) chaotic system was proposed in Wang et al. [26], providing an expansive key space of 2226 and pronounced non-linearity. Unfortunately, the physical hardware realization and parameter synchronization of such multidimensional maps remained highly challenging.

In proposed method Key space exceeds 2512 , fulfilling NIST recommendations for higher then 256 bit security against brute-force, while avalanche effects ensure greater than 50% bit flips per key change, further solidifying its

strength over existing lightweight encryption protocols. The proposed method delivers superior NPCR and UACI values, providing robust resistance to differential attacks. It achieves close-to-ideal entropy ≥7.99 bits/byte for 8-bit demonstrating exceptional resistance to entropy-based cryptanalysis. Adjacent pixel correlations are minimized horizontal, vertical and diagonal coefficients $|r| < 0.01$, eliminating exploitable patterns and outperforming 90% of compared schemes. The encryption passes all NIST SP 800-22 randomness tests with p-values >0.01, confirming high-quality key streams resilient to statistical attacks.

2. METHODOLOGY

The secret of using this strategy successfully is to make use of the chaotic space. By taking Difference of Sine-Cosine (DoSC) signal modulated by Non-linear term r^2 gives Sine-cosine Nonlinear Modulated signal (SNMS) based map is a novel designed one dimensional chaotic map having properties of the non-linear dynamic system, which is defined by Equation [3] and hybrid chaotic map Equation [4].

$$X_{n+1} = r^2 \cdot \sin\left(\pi \cdot {X_n}^2 - 4\right) - (1 - r) \cdot \cos\left(\pi \cdot {X_n}^2 - 3\right) \quad [3]$$

$$X_{n+1} = r \cdot X_n \cdot (1 - X_n) + k \cdot \sin(\pi \cdot X_n) \quad [4]$$

where $X_n \in (-1,1)$ represents the current chaotic state and $r \in (0,1)$ is the control parameter regulating the nonlinear dynamics of the system. The map combines quadratic nonlinearity, trigonometric modulation, and weighted parameter coupling to generate highly complex chaotic behaviour suitable for cryptographic applications. The constants -4 and -3 are intentionally introduced as nonlinear phase-shifting parameters inside the sine and cosine functions. These constants are not arbitrary offsets; rather, they significantly influence the dynamical evolution, distribution uniformity, bifurcation characteristics and randomness quality of the generated sequence. The argument of the trigonometric functions is given by $\theta_n = \pi X_n^2$. Since $X_n^2 > 0$, the term $\theta_n = \pi X_n^2$ alone produces a partially symmetric structure because positive and negative values of X_n generate identical squared outputs. Such symmetry may reduce randomness and create predictable orbit patterns. To destroy this structural symmetry, constant perturbation terms are introduced so $\theta 1 = \pi X_n^2 - 3$ and $\theta 2 = \pi X_n^2 - 4$. These phase offsets shift the sine and cosine trajectories into different nonlinear regions, preventing periodic overlap between successive iterations. The derivative of the proposed map determines its chaotic intensity. Differentiating Equation [1] with respect to X_n.

$$dX_{n+1}/dX_n = 2\pi * X_n[\, r^2 \cos(\pi X_n^2 - 4) + (1 - r) \sin(\pi X_n^2 - 3)] \quad [5]$$

The phase constants -4 and -3 ensure that the sine and cosine terms oscillate asynchronously, producing larger derivative fluctuations and increasing the probability that $|dX_{n+1}/dX_n| >> 1$ Equation [5]. This directly improves the Lyapunov exponent as it can be seen from definition below.

Lyapunov exponent

In the context of this map, the distance between two states changes relatively quickly. The parameter λ, also known as the Lyapunov exponent (LE), directly affects the sensitivity of the chaotic map. A positive LE exhibits chaotic behaviour, making long term forecasting challenging

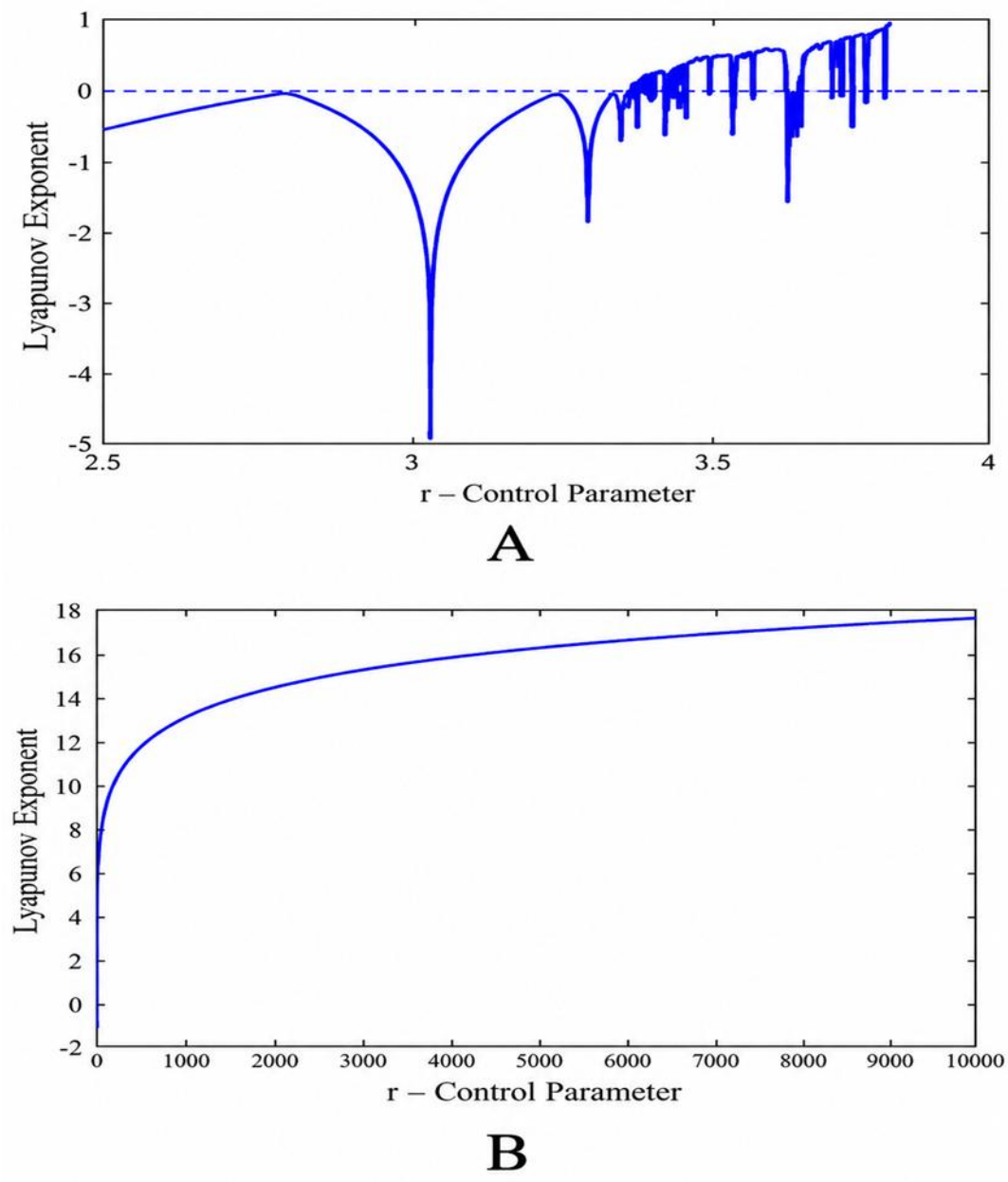

Figure 1: LE of (A) Hybrid chaotic map and (B) DoSC chaotic map (LE, r -Unit less)

since small changes in the initial conditions over time produce drastically different outcomes Eq. [6]. The Lyapunov exponent of the proposed chaotic map was computed using a numerical Jacobean-based approximation method. Jacobean defined as dX_{n+1}/dX_n for the one-dimensional nonlinear map. A characteristic of chaotic behaviour is that the chaotic map is more sensitive to initial conditions when the LE is higher.

$$\lambda = \lim_{(}N \to \infty_{)} (1/N) \Sigma_{n=1}{}^{N} \ln |dX_{n+1}/dX_n| \qquad [6]$$

The LE plot for the DoSC and Hybrid chaotic maps are shown in Figure 1. The graphic clearly shows that the LE is a non-decreasing function, which supports the dynamic sensitivity of the map and its possible uses in complex random number generating system. A larger positive Lyapunov exponent indicates stronger chaos, faster trajectory divergence, and higher unpredictability.

Bifurcation Diagram

A bifurcation diagram shows how changes in a system parameter affect its long term state or representation of the transition from order to chaos, as well as for depicting the dynamic behaviour of chaotic maps. Plotting the values of a system parameter, represented by the r control variable, on the horizontal axis and the associated asymptotic states of the system on the vertical axis creates the diagram for a chaotic map. For every r, plot the stable long-term values of Xn+1 from Xn.

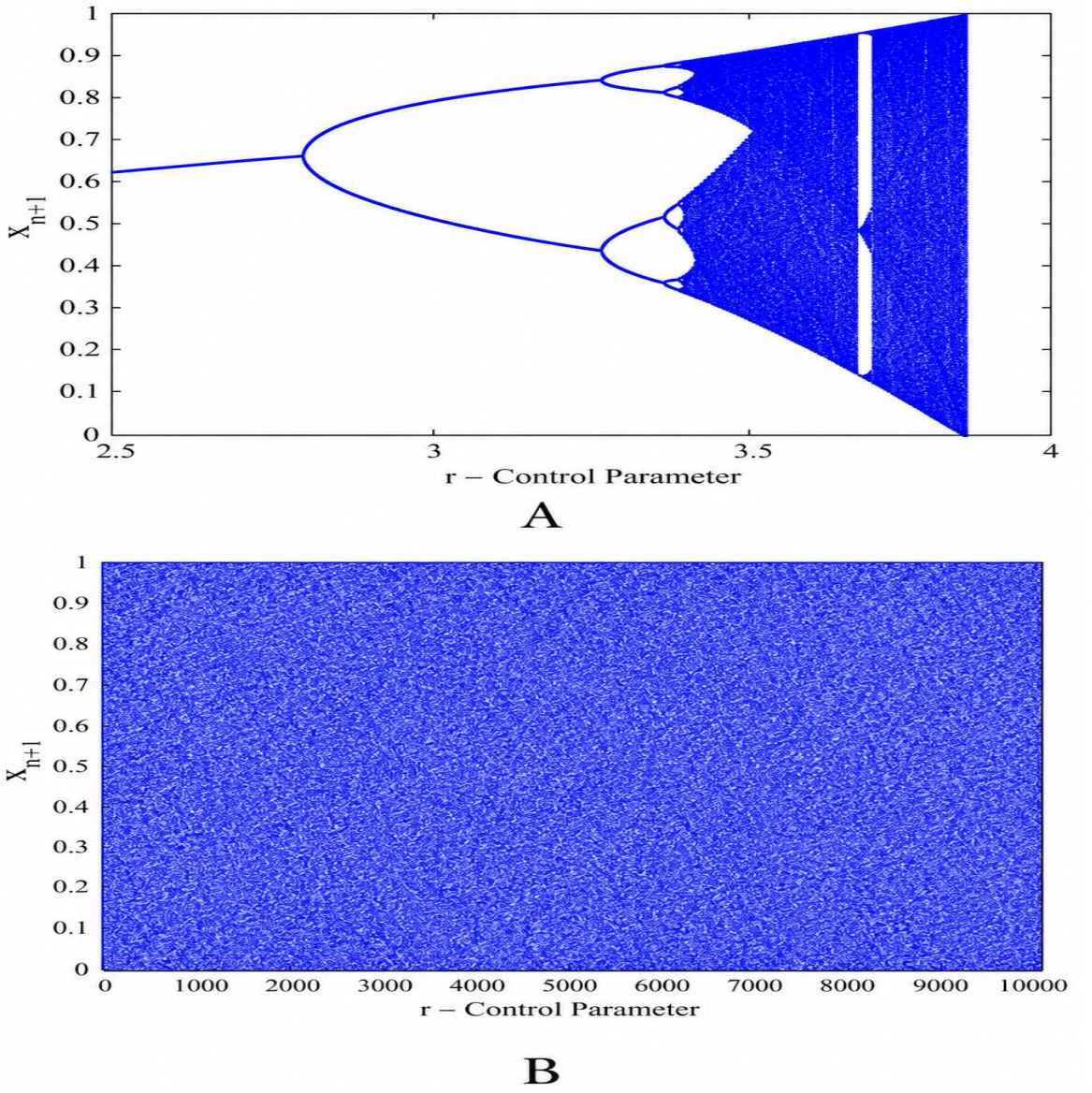

Figure 2: Bifurcation diagram of (A) Hybrid and (B) DoSC chaotic map (Xn+1, r-Unit less)

Figure 3 and Figure 4 shows bifurcation diagram of two chaotic maps used. For numerical computation, the control parameter r was varied within the range$0 < r < 10000$ and with a uniform step size. For each parameter value, the chaotic map was iterated for 5000 iterations. To eliminate transient effects and ensure convergence toward steady-state dynamics, the first 1000 iterations were discarded, while the remaining 4000 iterations were used for bifurcation and Lyapunov exponent analysis. The bifurcation diagram offers profound insights into the intricate dynamics of nonlinear systems. The system behaves chaotically above a critical value of r, when points densely occupy a region on the vertical axis, signifying an endless number of unstable periodic orbits.

The proposed map improves existing classical chaotic maps in several important ways. For the logistic map, the chaotic region exists only for limited parameter intervals near r≈3.57 to 4. The logistic map also suffers from non-

uniform output distribution, short periodic windows, and limited complexity under finite precision implementation. Similarly, the sine map provides smoother trajectories but exhibits weaker diffusion capability because of lower nonlinear dimensionality. The tent map has piecewise linear behavior, which simplifies implementation but reduces cryptographic complexity due to predictable linear segments. In contrast, the proposed map introduces several enhancements simultaneously.

a. Quadratic State Dependency: Map creates stronger nonlinear amplification than linear-state maps. Small changes in Xn produce amplified variations after squaring.

b. Hybrid Trigonometric Coupling: The coexistence of sine and cosine functions generates multi-directional oscillatory behavior, increasing entropy and sequence irregularity.

c. Phase Perturbation Constants: The constants −4and −3 destroy symmetry and avoid synchronization between trigonometric components.

d. Weighted Parameter Fusion: r2 and (1−r) allow dynamic balance between the sine and cosine components, increasing parameter sensitivity. Because of hybrid nonlinear interactions, the system maintains chaos over a wider parameter interval compared with conventional maps. The asynchronous phase shifts improve histogram uniformity and reduce statistical correlation among generated samples.

Consequently, the proposed hybrid chaotic map achieves superior randomness, stronger sensitivity to initial conditions, and enhanced suitability for secure image encryption applications.

Encryption method

Flowchart in Figure 5 depicts an image encryption process. First, the image is vectorized and divided into two parts, which are individually encrypted using XOR with two different keys. These encrypted halves are combined and subjected to further encryption using chaotic sequences generated via a DoSC and hybrid chaotic maps. Transposition and layered XOR operations using chaotic sequences and pseudo-noise (PN) sequences enhance security. Finally, the encrypted vector is reshaped back into an image format to complete the encryption.

Following the opposite procedure to that of encryption, decryption reconstructs the original image by reversing the encryption steps using the same pseudo-random sequences generated from 8-bit or 16-bit keys, along with identical chaotic map control parameters and initial conditions.

Experimental Setup

All simulations were performed on an HP workstation equipped with a 64-bit Windows operating system and an Intel(R) Core(TM) i7-6700HQ processor operating at 2.60 GHz. Medical test images obtained from online repositories, including MRI, CT, and PET scans, utilized to assess the performance of the proposed method Levoy **[27]** and Lister Hill National Centre for Biomedical Communications **[28]**.

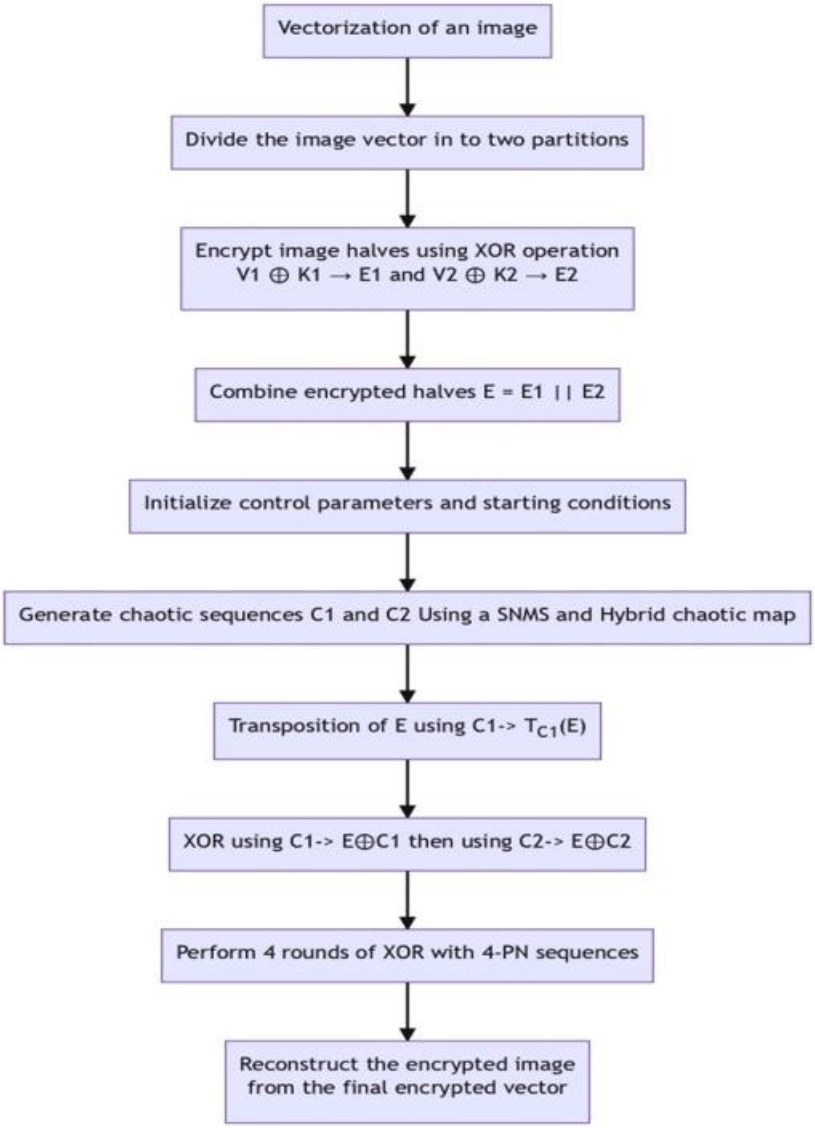

Figure 3: Schematic Representation of the Encryption Procedure

Performance Parameters

The parameters listed below are the primary tools used for performance evaluation.

a. Key Space: The set of all possible binary secret key combinations is known as the key space.

b. Peak Signal-to-Noise Ratio (PSNR): PSNR evaluates the quality of an image having Lmax maximum intensity in the presence of noise and is expressed by Equation [7].

$$\text{PSNR} = 10 \log_{10} \left[\frac{\text{Lmax}^2}{\text{MSE}} \right] \quad [7]$$

$$\text{MSE} = \left[\frac{1}{\text{H} \times \text{W}} \right] \sum\sum [\text{Je}(x, y) - \text{Jo}(x, y)]^2$$

for summation Σ, x range =0→H−1 and y range =0→W−1 Here, $J_o(x, y)$ and $J_e(x, y)$ denote the pixel intensity values of the original image and encrypted image, respectively.

c. NPCR: The NPCR measures the percentage of pixels that differ between two images and is calculated using Equation [8].

$$\text{NPCR} = \left[\frac{1}{H \times W}\right] \Sigma \Sigma\, C(x,y) \quad [8]$$

Where C(x,y) = 0, if $J_o(x,y) = J_e(x,y)$ else C(x,y) = 1.

Entropy: Entropy quantifies the randomness of pixel intensity values and is mathematically defined using probability in Equation [9].

$$H = -\Sigma\, P(\phi_k) \log_{10}[\, P(\phi_k)\,] \quad [9]$$

where ϕ_k represents the k^{th} intensity level of an image vector.

d. UACI: The UACI reflects the average intensity difference between the original and encrypted images, normalized by the maximum pixel value, as given in Equation [10].

$$\text{UACI} = \left[\frac{1}{H \times W}\right] \sum\sum \frac{|Je(x,y) - Jo(x,y)|}{255} \quad [10]$$

e. Correlation: The correlation coefficient between two images J_e and J_o is defined in terms of expectation μ and variance σ^2, as shown in Equation [11].

$$\rho(Je, Jo) = \frac{\mu[\,(J_e - \mu(J_e))\,(J_o - \mu(J_o))\,]}{(\,\sigma^2(J_e)\,\sigma^2(J_o)\,)^{1/2}} \quad [11]$$

For, k=0→N−1, $\mu(J_e) = \frac{1}{N}\Sigma J_e(k)$, $\sigma^2(J_e) = \frac{1}{N}\Sigma\big(J_e(k) - \mu(J_e)\big)^2$, $\mu(J_o) = \frac{1}{N}\Sigma J_o(k)$, $\sigma^2(J_o) = \frac{1}{N}\Sigma\big(J_o(k) - \mu(J_o)\big)^2$

f. Chi-Square Test: The chi-square statistic evaluates histogram uniformity of the encrypted image and is calculated using Equation [12].

$$\chi^2 = \sum \frac{(\,ge(i) - \bar{g})^2}{\bar{g}} \quad \text{with } i=0 \rightarrow 255 \quad [12]$$

where $g_e(i)$ denotes the observed frequency of observed intensity level i in the encrypted image and $\bar{g}$ represents the expected frequency.

g. Strict Avalanche Criterion (SAC): SAC is a fundamental cryptographic property. Let the encryption function be defined as $F: \{0,1\}^p \rightarrow \{0,1\}^q$, where p and q denote the input and output sizes, respectively. If changing any single input bit k causes each output bit l to change with a probability of 0.5, then SAC is satisfied if P (l | k is flipped) = 0.5 ∀ l.

3. RESULTS AND DISCUSSION

This method has high resistance to differential attacks, as it can be observed from various parameter values obtained. There is no visual clue from the encrypted image as it is observed from Figure 6, for significance level α=0.05 the corresponding critical chi-square value for df=255 is approximately χcritical2=293.24. The obtained experimental value χ2=258.16. is lower than the critical threshold 258.16<293.24 which indicates that the encrypted image histogram satisfies the statistical homogeneity criterion and exhibits an approximately uniform distribution. Hence, the null hypothesis of uniformity cannot be rejected at the 95% confidence level. This result confirms that the encrypted image possesses strong randomness characteristics and does not reveal significant statistical information about the original image, thereby strengthening resistance against statistical attacks.Bottom of Form

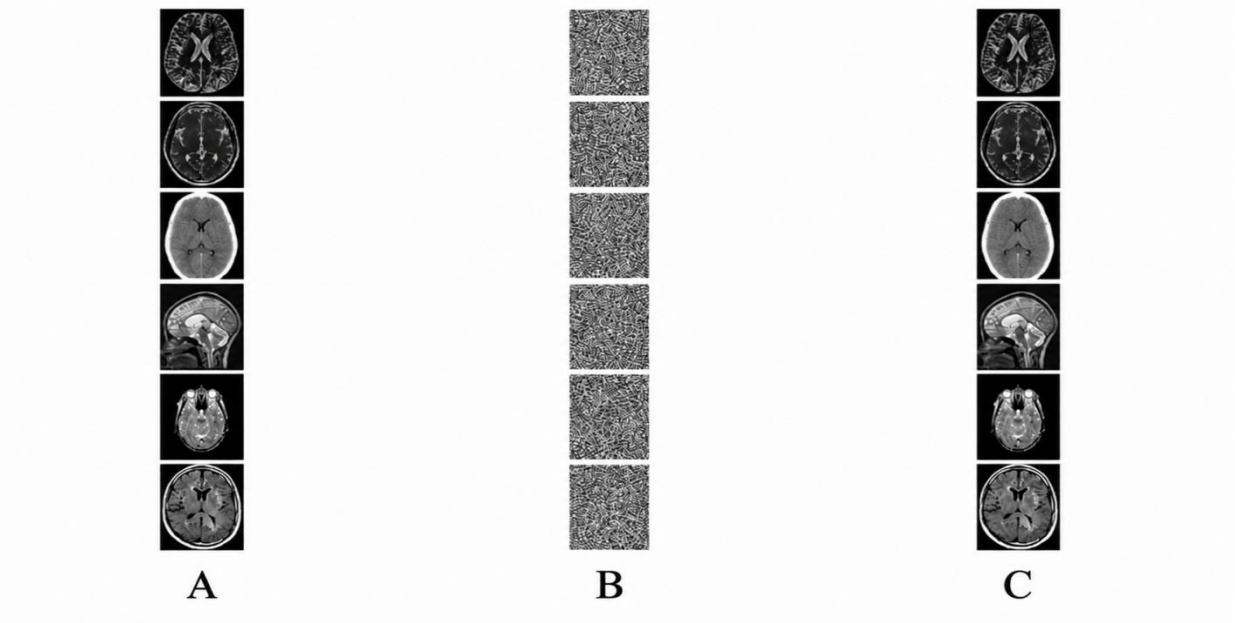

Figure 4: A. Original B. Encrypted and C. Decrypted images from top to bottom PET1, PET2, CT1, CT2, MRI1 and MRI2. The original images were taken from the **[27-28].**

Figure 7, flat probability density function means there is no leakage of information. In accordance with publicly available specifications recommendation that the NIST-SP-800-131A key length be at least 256 bits, we employ a technique in which 16 keys, each of which is 8 bits, are utilized for generations of a single PN sequence. Four of these and other sequences are K1, K2 then used for encryption, making the key length for this scheme 512 bits and key space is 2512.

The NIST SP 800-22 statistical test suite offers a comprehensive and standardized framework for assessing the statistical randomness of binary sequences generated from encrypted images. These tests are crucial in determining whether a sequence exhibits any statistical patterns that could undermine its unpredictability. The NIST statistical test suite was utilized to evaluate the randomness quality and cryptographic reliability of the generated chaotic sequences. The Frequency and Block Frequency tests verify the uniform distribution of binary bits globally and within fixed-size blocks, respectively, while the Runs and Longest Run tests examine the randomness behaviour of consecutive identical bits. The Rank test evaluates linear dependence among binary matrices, whereas the Discrete Fourier Transform (DFT) test detects periodic or repetitive structures within the sequence. The Non-Overlapping and Overlapping Template Matching tests analyse the occurrence frequency of predefined bit patterns to identify statistical irregularities. Furthermore, the Approximate Entropy and Serial tests measure sequence unpredictability and pattern uniformity, while the Linear Complexity test determines the difficulty of reproducing the sequence using linear feedback mechanisms. The Cumulative Sums (Cusum), Random Excursions, and Random Excursions Variant tests evaluate random walk behaviour and statistical fluctuation consistency. Additionally, the Universal Statistical test examines sequence compressibility to verify overall randomness characteristics. Successful performance in these tests confirms that the generated chaotic sequences possess strong statistical randomness and are suitable for secure cryptographic applications.

In this analysis, all the tests applied, and all yielded results in **Table** 1 that affirm the randomness of the sequence, while (8) reported the results which pass only 6 tests and (10), (21-23) has lower p-values. Proposed method with all p-values significantly above the 0.01 significance level, the statistical test results, demonstrate that the binary sequence exhibits strong unpredictability. This suggests that the sequence is highly entropied and unpredictable. Further other evaluation measures, demonstrate that the encryption technique has strong defence **Table** 2. Compared with schemes having lower key spaces, the proposed method achieves an exhaustive key space of 2512 offering strong resistance to brute-force attacks Figure 8. The PSNR shows how similar the encrypted and original images are. Greater discrepancies are indicated by lower PSNR, It's values range from 5.8248 to 7.3624, which means that the original image is effectively obscured by the encryption. The reported values, which are remarkably low, suggesting that the encryption procedure significantly distorted the images. Several existing methods report even poorer PSNR

performance. For instance, the fractal and block-chain scheme averages at 26.25 (25), indicating less degradation and hence very much reduced obfuscation. While the multi-chaos method for IoT applications exhibits a low PSNR of 10.21 (11).

The average intensity difference between two encrypted images produced from marginally different inputs is measured by UACI, obtained UACI> 33.33% Figure 9, UACI values show how sensitive the encryption technique is to small input changes. This sensitivity is essential for preventing differential attacks, in which adversaries try to deduce the encryption key by examining little variations in output. Let $J_o(i, j) = 0\ \forall(i, j)$ and assume the cipher image pixels $J_e(i, j)$ are Independent and Identically Distributed (i.i.d) random variables uniformly distributed over [0, 255]. The UACI is defined in Equation [9] Taking expectation and using linearity, $E[UACI] = \left(\left[\frac{1}{255}\right]\right) E[Je] = \left(\frac{1}{255}\right)\int_0^{255}\left(\frac{1}{255}\right) x\, dx$ Evaluating the integral yields E[UACI] =127.5/255=1/2.

Thus, for a fully dark plaintext image, the expected high UACI converges to 0.5, which constitutes the theoretical upper bound under ideal diffusion. UACI=50% is the upper limit can be catch by darker images. In the present work, multiple independent encryption experiments were conducted using different initial conditions, secret keys, and medical test images to evaluate the consistency and robustness of the proposed cryptosystem. Repeated experimental analysis demonstrated that the obtained entropy, NPCR, UACI, and correlation values remain highly consistent across different trials, confirming the robustness of the chaotic encryption framework. Furthermore, the low variance observed in the experimental outcomes validates the reliability of the proposed chaotic map and its resistance against statistical uncertainties.

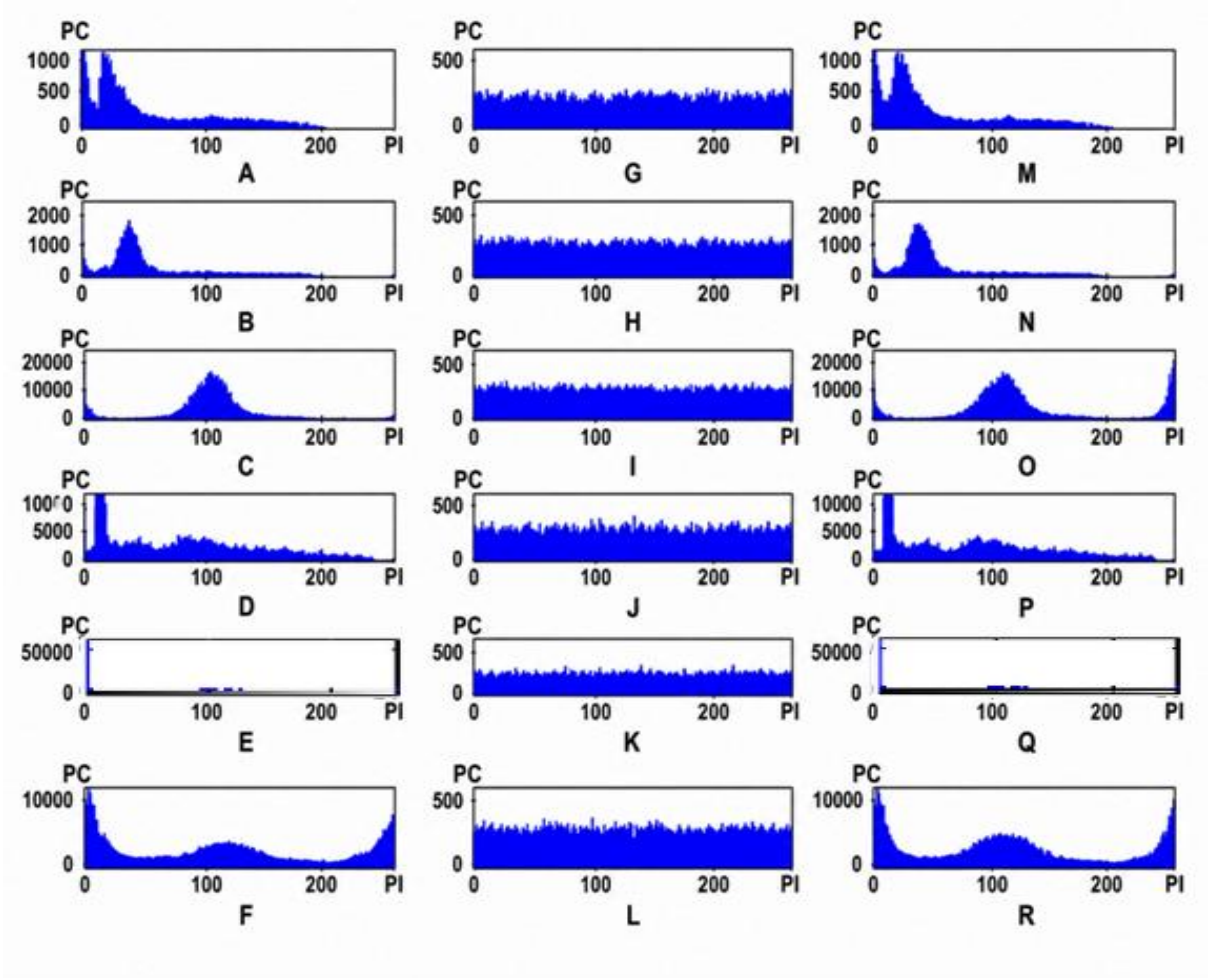

Figure 5: Histograms- Plot of pixel count (PC) with respect to pixel intensity (PI) for six medical images PET1, PET2, CT1, CT2, MRI1, and MRI2. (A–F) Original medical image histograms, (G–L) encrypted image histograms, and (M–R) decrypted image histograms.

When the input is slightly altered, NPCR calculates the proportion of pixel changes between two encrypted images. The given values, which fall between 99.5968% and 99.6254%, are close to the optimal value. Method with grasshopper optimization, which yields a poor NPCR of 85.48% (13). DNA-based methods (9) also have slightly lower average value. Entropy assesses how random the encrypted images are. The optimal entropy value for an 8-bit image is 8, which denotes total randomness. According to the reported entropy values Figure 10, which range from 7.9992 to 7.9995, the encrypted images are nearly perfectly random, since they are quite close to the ideal. Because no patterns can be seen in the encrypted data, this randomness guarantees that the cipher image is immune to statistical analysis attacks.

Table 1: NIST Statistical Validation of the Proposed Scheme

Test Name	Result	P-Value
Overlapping Template Matching	Pass	0.999989
REVLC Test*	Pass	0.990766, 0.941963, 0.888238, 0.742782, 0.469969, 0.406009, 0.268005, 0.089569
Frequency (Monobit)	Pass	0.922985
Discrete Fourier Transform(Spectral)	Pass	0.891130
Universal Statistical	Pass	0.886898
Non-overlapping Template Matching*	Pass	0.865069, 0.861583, 0.555254, 0.392639, 0.085962, 0.081584
Random Excursions*	Pass	0.831681, 0.560772
Serial Test*	Pass	0.760313, 0.673290, 0.669815, 0.654296, 0.612049, 0.476033, 0.455432
Cumulative Sums*	Pass	0.600529, 0.516936
Rank	Pass	0.554065
Approximate Entropy	Pass	0.395667
Longest Run of Ones in a Block	Pass	0.217370
Block Frequency	Pass	0.174380
Runs	Pass	0.107934

REVLC = Random Excursions Variant and Linear Complexity Test. *Multi-state/multi-dimension tests. The NIST test results presented in this table were obtained using the generated encrypted sequences. A (p)-value greater than 0.01 indicates that the sequence successfully passes the corresponding randomness test.

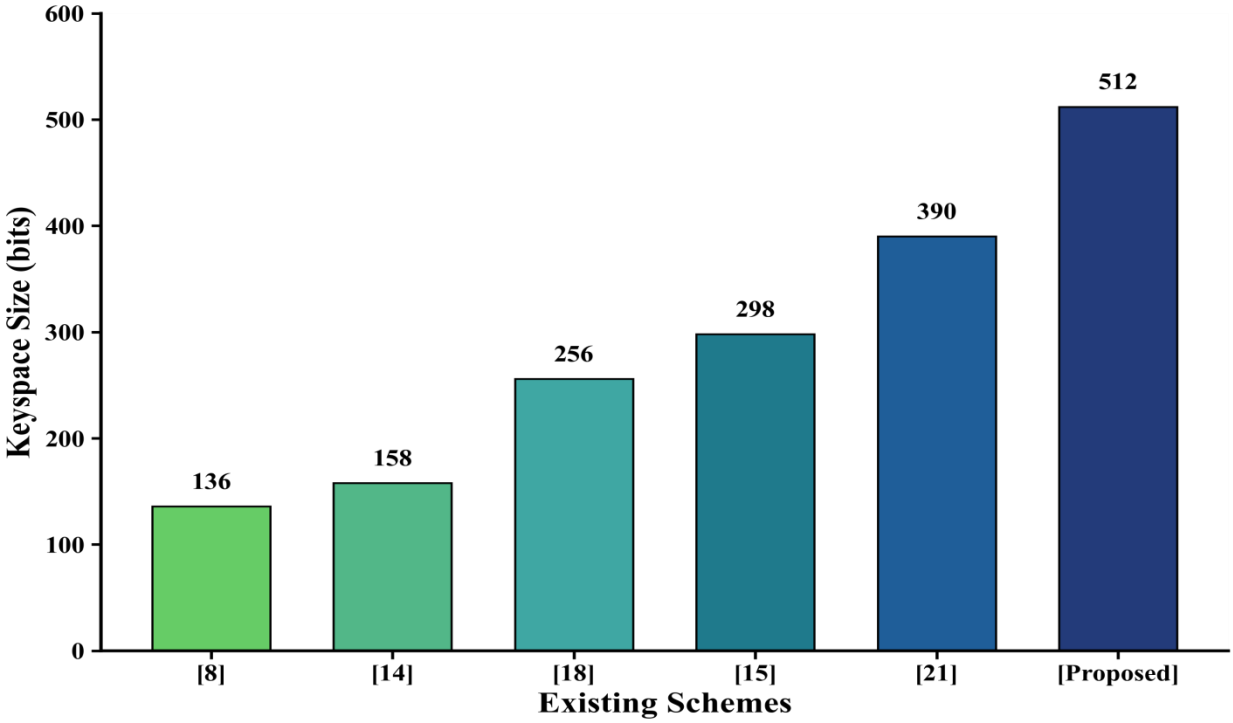

Figure 6: Key-space comparison of the proposed and existing schemes

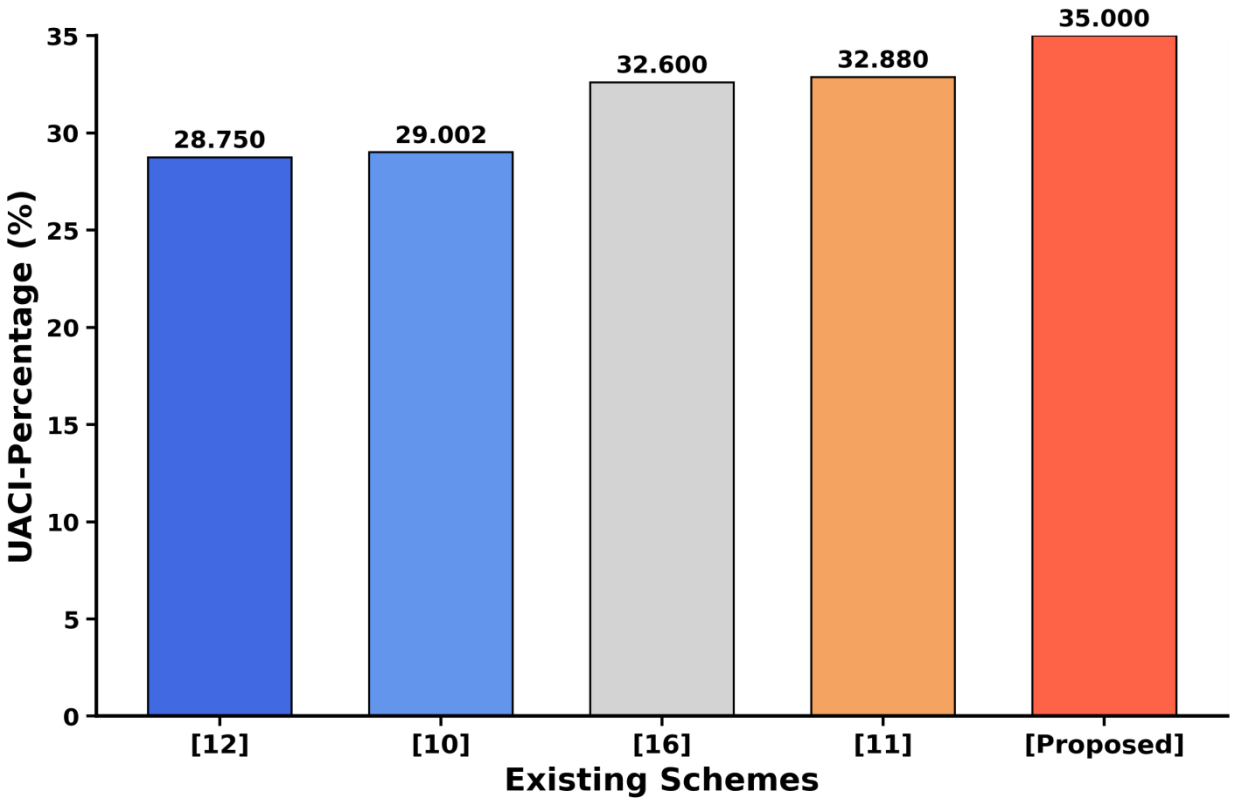

Figure 7: Comparative Analysis of UACI Values

Table 2: Quantitative Analysis of Image Encryption Performance

Parameters	PET-1	PET-2	CT-1	CT-2	MRI-1	MRI-2
PSNR	6.0139	6.0038	7.3624	7.1547	7.0586	5.8248
UACI	38.6154	38.6934	35.0114	35.9106	36.3487	42.7695
NPCR	99.6165	99.6174	99.6254	99.6086	99.5968	99.6140
Entropy	7.9994	7.9993	7.9992	7.9993	7.9994	7.9995
Correlation (H)	-0.0021	-0.0018	-0.0014	-0.0013	0.0017	0.0010
Correlation (V)	0.0019	0.0006	-0.0020	0.0005	-0.0015	-0.0008
Correlation (D)	-0.0021	-0.0090	0.0024	0.0002	-0.0008	-0.0021

The values presented in this table were obtained from experimental results.

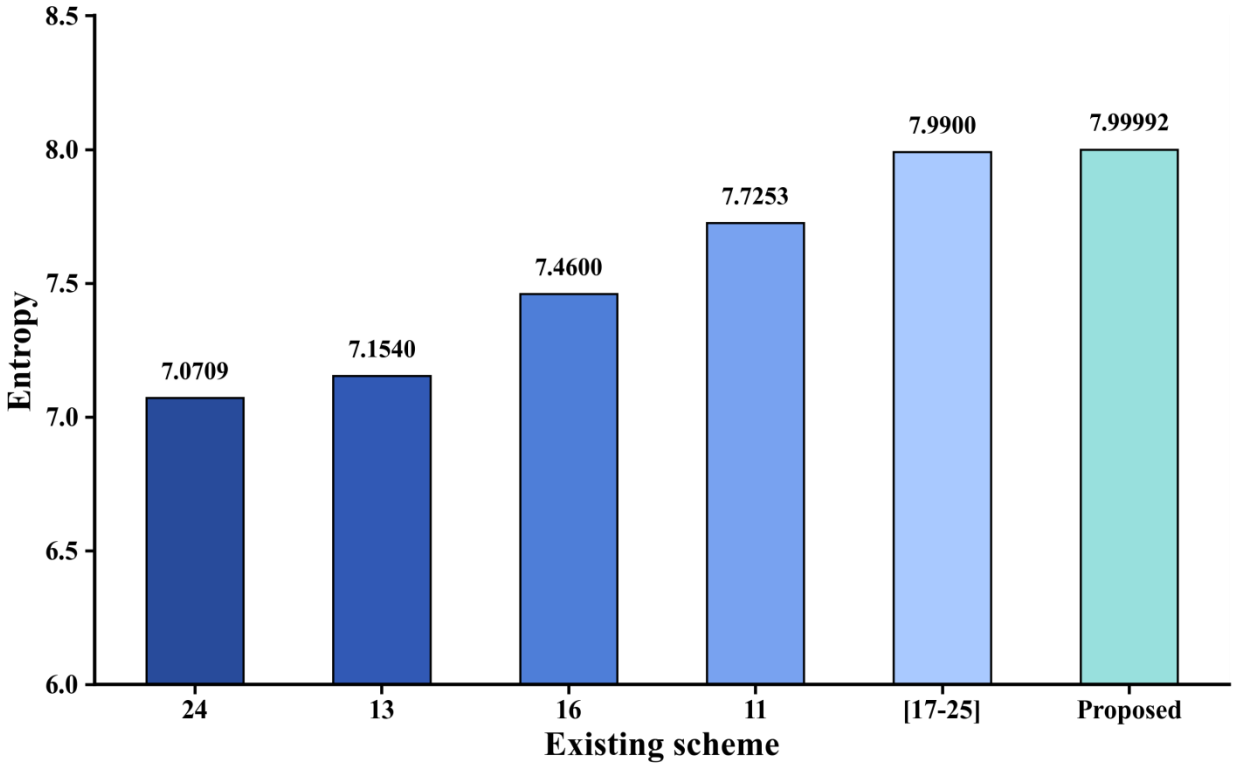

Figure 8: Entropy Performance Comparison of Encryption Methods

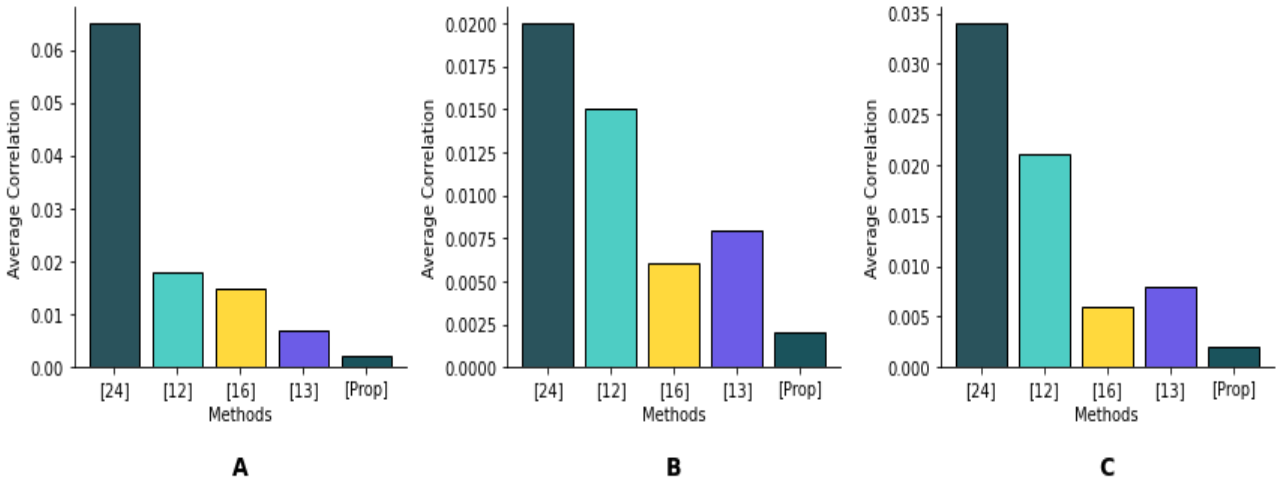

Figure 11: Correlation comparison for directions (A) Horizontal (B) Vertical and (C) Diagonal

Zero correlation, which shows that neighbouring pixels are totally de-correlated, is the ideal for encrypted images. It is confirmed that the encryption process effectively breaks pixel associations by the reported correlation values, which are all near zero -0.0021 to 0.0010 for Horizontal(H), -0.0020 to 0.0019 for Vertical(V), and -0.0021 to 0.0024 for Diagonal(D) while other has high correlation Figure 11. This guarantees that no structural patterns that an attacker could exploit are retained in encrypted images **Table** 2. A strict avalanche criterion (SAC) of 50.09% guarantees that there is a nearly equal chance of flipping the appropriate bit in the output for each bit in the input, indicating a very high resistance to differential attacks. Small changes in the input will inevitably result in significant changes in the output due to high degree of avalanche effect. These results confirm the proposed method's robustness against statistical and differential attacks and its suitability for secure medical image encryption.

4. CONCLUSION

The characterized DoSC signal's nonlinear modulation based chaotic map properties are proven to be significant and promising in general. To summarize, our extensive results convincingly establish the cryptographic security of the proposed construction and illustrate its explicit conformity to mainstream (NIST) standards for secure encryption practices. It has high-key space 2512, which strongly illustrates excellent front for any brute-force attack. In addition, parameters such very low PSNR and flat histograms even make original image lose its recognizability property from the receiver just after encryption seems completely different. A high NPCR and UACI values suggest strong opposition to small perturbations, hence provides an efficient equivalent diffusion of the input data variation throughout the cipher text. Near-ideal entropy values 7.9992 confirm the outstanding randomness and unpredictability of the encrypted images, while the negligible correlation coefficients successfully validate the complete de-correlation of adjacent pixel intensities in both horizontal and vertical directions. Collectively, these important metrics firmly establish the overall robustness of the encryption mechanism, rendering it highly resistant to various differential attacks as well as a wide range of statistical attacks. Image encryption time measured is 100µ second, for practical video applications, lightweight and high-speed implementations are necessary to satisfy real-time processing constraints. Future research may focus on developing lightweight and high-speed architectures suitable for real-time embedded systems. The proposed framework can also be extended toward secure video encryption by employing frame-wise dynamic chaotic key generation and temporal diffusion mechanisms. Future studies also investigate resistance against deep-learning-based cryptanalysis and chosen-cipher attacks.

References

1. Zhang Y, Dong Z. "Medical imaging and image processing", Technologies, 11(2), pp. 1–4, 2023. https://doi:10.3390/technologies11020054.
2. Moore W, Frye S. "Review of HIPAA, part 1: History, protected health information, and privacy and security rules", J Nucl Med Technol, 47(4), pp. 269–272, 2019. https://doi:10.2967/jnmt.119.227819.
3. Greengard S. "Weighing the impact of GDPR", Commun ACM, 61(11), pp. 16–18, 2018. https://doi:10.1145/3276744.
4. DICOM Standards Committee. "DICOM PS3.22-2024e: Real-time communication", 2024.
5. Shannon CE. "Communication theory of secrecy systems", Bell Syst Tech J, 28(4), pp. 656–715, 1949. https://doi:

10.1002/j.1538-7305.1949.tb00928.x.
6. Li S, Ma R, Zhang H. “Enhancing security for JPEG image against mosaic attack using inter-block shuffle encryption”, IEEE Access, 7, pp. 72463–72472, 2019. https://doi:10.1109/ACCESS.2019.2918860.
7. Naik RB, Singh U. “A review on applications of chaotic maps in pseudo-random number generators and encryption”, Ann Data Sci, 11, pp. 25–50, 2024. http://doi:10.1007/s40745-021-00364-7.
8. Panigrahy AK, Maniyath SR, Sathiyanarayanan M, et al. “A faster and robust artificial neural network-based image encryption technique with improved SSIM”, IEEE Access, 99, pp. 1-11, 2024. https://doi:10.1109/ACCESS.2024.3353294.
9. Elmanfaloty RA, Alnajim AM, AbouBakr E. “A finite-precision implementation of an image encryption scheme based on DNA encoding and binarized chaotic cores”, IEEE Access, 9, pp. 136905-136916, 2021. https://doi:10.1109/ACCESS.2021.3118050.
10. Maddodi G, Awad A, Awad D, Awad M, Lee B. “A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding”, Multimed Tools Appl, 77(21), pp. 28427–28456, 2018. https://doi:10.1007/s11042-018-5669-2.
11. Jain K, Titus B, Krishnan P, Sujeetha S, Prabu P, Alluhaidan AS. “A lightweight multi-chaos-based image encryption scheme for IoT networks”, IEEE Access, 12, pp. 62118–62148, 2024. https://doi:10.1109/ACCESS.2024.3377665.
12. Choi J, Seok S, Seo H, Kim H. “A fast ARX model-based image encryption scheme”, Multimed Tools Appl, 75(22), pp. 14685–14706, 2016. https://doi:10.1007/s11042-016-3274-9.
13. Shankar K, Elhoseny M, Chelvi ED, Lakshmanaprabu SK, Wu W. “An efficient optimal key-based chaos function for medical image security”, IEEE Access, 6, pp. 77145-77154, 2018. https://doi:10.1109/ACCESS.2018.2874026.
14. Thoms GRW, Muresan R, Al-Dweik A. “Chaotic encryption algorithm with key-controlled neural networks for intelligent transportation systems”, IEEE Access, 7, pp. 158697–158709, 2019. doi: 10.1109/ACCESS.2019.2950007.
15. Toktas A, Erkan U, Toktas F, Yetgin Z. “Chaotic map optimization for image encryption using triple-objective differential evolution algorithm”, IEEE Access, 9, pp. 127814–127832, 2021. https://doi:10.1109/ACCESS.2021.3111691.
16. Lin CH, Lai HY, Huang PT, Chen PY, Pai NS, Zhang FZ. “Combining Riemann–Lebesgue-based key generator and machine-learning-based intelligent encryption scheme for IoMT images infosecurity”, IEEE Internet Things J, 11(1), pp. 1344-1360, 2024.
17. Yu F, Kong X, Mokbel A, Yao W, Cai S. “Complex dynamics, hardware implementation and image encryption application of multiscroll memristive Hopfield neural network with a novel local active memristor”, IEEE Trans Circuits Syst II Exp Briefs, 70, pp. 326-330, 2023.
18. Krishnamoorthi S, Dhanaraj RK, Islam SH. “CCM-PRNG: Pseudorandom bit generator based on crossover chaotic map and its application in image encryption”, Multimed Tools Appl, 83(34), pp. 80823-80846, 2024. https://doi:10.1007/s11042-024-18668-0.
19. Inam S, Kanwal S, Rashid S, Hajjej F, Hamdi M. “A novel image encryption scheme based on elliptic curves, Hilbert matrices and chaotic maps for enhanced visual security in telecommunication systems”, Eur Phys J Plus, 29, pp. 1-21, 2025.
20. Rashidi B. “An image encryption method based on a high-performance and efficient block cipher”, J Signal Process Syst, 96, pp. 601-615, 2024. https://doi:10.1007/s11265-024-01937-4.
21. Kolivand H, Hamood SF, Asadianfam S, Rahim SM, Hurst W. “Image encryption framework based on multi-chaotic maps and equal pixel-value quantization”, Multimed Tools Appl, 84(17), pp. 17769-17804, 2024. https://doi:10.1007/s11042-024-19771-y.
22. Shafique A, Ahmed J, Rehman MU, Hazzazi MM. “Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain”, IEEE Access, 4, pp. 1-24, 2021. https://doi:10.1109/ACCESS.2021.3071535.
23. Sambas A, Zhang X, Moghrabi IAR, et al. “ANN-based chaotic PRNG in a novel jerk chaotic system and its application to image encryption via 2-D Hilbert curve”, Sci Rep, 14, p. 29602, 2024. https://doi:10.1038/s41598-024-80969-z.
24. Kaur R, Singh B. “Robust image encryption algorithm in DWT domain”, Multimed Tools Appl, 83(13), pp. 1-23, 2023.
25. Inam S, Kanwal S, Batool M, Al-Otaibi S, Jamjoom MM. “A blockchain-integrated chaotic fractal encryption scheme for secure medical imaging in industrial IoT settings”, Sci Rep, 15, p. 7652, 2023.
26. Wang Q, Sang H, Wang P, Yu X, Yang Z. “A novel 4-D chaotic system coupled with dual memristors and its application in image encryption”, Sci Rep, 14, p. 29615, 2023. https://doi.org/10.1038/s41598-024-80445-8.
27. Levoy M. “Medical images: The Stanford volume data archive”, Available at: https://graphics.stanford.edu/data/voldata/ (Accessed on date: 18 July 2026).
28. Lister Hill National Centre for Biomedical Communications. “MedPix: Open access medical image database”, Available at: https://medpix.nlm.nih.gov/home (Accessed on date: 18 July 2026).