Journal of Theoretical and Applied Information Technology
31st May 2025. Vol.103. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FAORE PONY-INSPIRED CHAOTIC NEURAL ENCRYPTION FOR SECURE AND EFFICIENT MEDICAL IMAGE PROTECTION

P.SUHASINI[1], Dr.S.KANCHANA[2]

[1]Department of Computer Science, Faculty of Science and Humanities,

SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203, India

[2]Department of Computer Science, Faculty of Science and Humanities,

SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203, India

E-mail: [1]sp7695@srmist.edu.in, [2]kanchans@srmist.edu.in

ABSTRACT

The Faore Pony-Inspired Optimization for Chaotic Neural Encryption introduces a novel encryption approach for securing medical images in telemedicine applications. This framework leverages bio-inspired optimization, incorporating adaptive stamina-based key evolution and chaotic neural processing to enhance security and unpredictability. By integrating chaotic maps with an optimized pixel diffusion mechanism, the encryption scheme ensures high randomness, making it resistant to statistical and differential attacks. The proposed model disrupts structural correlations in medical images, preserving confidentiality while maintaining computational efficiency. The adaptive optimization mechanism dynamically refines encryption parameters, ensuring robustness against evolving security threats. The approach prioritizes secure transmission without compromising image integrity, making it well-suited for real-time healthcare environments. The framework's resilience in preventing unauthorized access strengthens data protection in medical imaging systems. This study contributes to the development of enhanced encryption models for digital healthcare, ensuring secure, reliable, and efficient image transmission for modern telemedicine applications.

Keywords: *Chaotic Encryption, Faore Pony Optimization, Medical Image Security, Neural Key Evolution, Secure Telemedicine, Adaptive Pixel Diffusion.*

1. INTRODUCTION

Images form the backbone of communication in modern digital systems, offering a visual language that bridges human understanding and machine processing [1]. They carry information more intuitively than text, capturing complex scenes, structures, or data points in a compact, accessible format. In the realm of healthcare, images go far beyond aesthetics or visual cues they represent diagnostic clarity, clinical history, and evidence of treatment progression [2]. Medical images such as MRIs, CT scans, and X-rays are rich in detail, often holding the key to identifying diseases, planning surgeries, or monitoring treatment outcomes [3]. These images are more than files; they are essential records of a patient's physical condition. Their high sensitivity and clinical importance make them a prime target for protection, especially in digital workflows [4]. The importance of encryption becomes clear in contexts where images must remain confidential and tamper-proof. Encryption is the process of converting original data into an unreadable form, preserving its secrecy during storage or transfer [5]. Image encryption differs from traditional text-based encryption in several key ways. Images contain redundancy, correlated pixels, and high dimensionality, which means they require a different strategy for secure transformation [6]. Medical images demand even more precision. They must not only be secure from unauthorized access but also maintain exact fidelity upon decryption, as any loss of detail can directly impact medical judgment [7].

As healthcare systems expand into telemedicine, where patient consultations, diagnoses, and second opinions are conducted remotely, the urgency of image protection becomes even more critical [8]. Images are transmitted through online networks often public or semi-secure exposing them to threats such as interception, manipulation, or data breaches. These scenarios

present risks not only to patient privacy but also to the validity of the medical data itself [9]. In such a landscape, encryption plays the role of a digital shield, ensuring that only intended recipients with proper credentials can view and analyze the medical image [10].

Maintaining patient privacy is not just a feature of good design it is a requirement grounded in legal obligations, ethical practices, and clinical professionalism [11]. When a medical image is shared digitally, it is essential that it travels securely, reaching its destination without exposure or degradation. If a single element of an image leaks whether it be a facial structure or an embedded metadata tag the trust between patient and provider can erode. Encryption ensures that this trust remains intact, turning privacy from a vulnerability into a system guarantee [12].

To address the demands of medical image protection, chaotic image encryption has gained traction for its powerful, mathematically unpredictable properties. Chaotic systems are sensitive to initial conditions, meaning that a tiny change in input leads to dramatic differences in output [13]. This property is ideal for scrambling pixel values or coordinates within an image. By integrating chaotic maps into the encryption process, images become far less vulnerable to attacks based on pattern recognition or statistical analysis. The encryption result appears completely disordered, resisting reverse engineering without exact knowledge of the system's parameters [14].

Neural networks bring adaptability to this already strong foundation. Their ability to learn from data and adjust internal parameters enables them to fine-tune chaotic operations for enhanced efficiency and resilience [15]. When applied to image encryption, neural networks can be trained to respond to image characteristics such as contrast, resolution, or noise making the encryption scheme more intelligent and more responsive. They assist in optimizing chaotic key sequences, managing pixel transformations, or even correcting anomalies during decryption [16]. Their dynamic nature is well-suited to real-time scenarios like live telemedicine imaging, where both speed and security are critical [17].

Bio-inspired computing completes the triad of this advanced approach. By observing the behavioral traits of organisms in nature and translating them into computational models, bio-inspired techniques provide problem-solving strategies rooted in evolution [18]. In this model, the Faroe pony offers a metaphor for stamina, adaptability, and focused navigation through complex environments. These traits are modeled mathematically to drive optimization in the encryption process. The resulting system uses nature's time-tested logic to strengthen the artificial framework, ensuring that image encryption adapts, endures, and performs under pressure just like the animal that inspired it[19], [20].

1.1. Problem Statement

Medical image encryption in telemedicine presents critical challenges in balancing security, computational efficiency, and adaptability. Existing encryption methods struggle to maintain robust protection while preserving image quality for accurate diagnoses. Many current frameworks fail to dynamically optimize encryption parameters, leading to inconsistencies in security strength across different image types. Chaotic encryption models often suffer from inefficient key generation mechanisms, making them susceptible to brute-force and statistical attacks. The lack of adaptive pixel shuffling techniques results in patterns that reduce encryption unpredictability, exposing medical images to unauthorized reconstruction. Traditional encryption algorithms do not effectively integrate noise reduction and normalization steps, limiting their effectiveness in handling high-resolution medical images with varying intensity distributions. Furthermore, computational overhead remains a major concern, as many security models demand excessive processing power, making real-time encryption impractical in telemedicine applications. The absence of an efficient, lightweight encryption model that ensures high entropy, adaptability, and minimal computational burden highlights the urgent need for a robust encryption framework tailored for secure medical image transmission.

1.2. Motivation

Medical image encryption faces critical challenges in balancing security, computational efficiency, and adaptability to diverse imaging conditions. Existing encryption techniques often introduce excessive processing overhead, making them unsuitable for real-time applications in telemedicine. Some models fail to maintain diagnostic integrity by distorting essential image features, while others lack resilience against evolving cyber threats. Unauthorized access to medical images can lead to privacy breaches, violating strict regulatory requirements such as HIPAA and GDPR. Encryption frameworks that do not dynamically adjust their security parameters struggle to protect images of varying complexity,

reducing their effectiveness in practical healthcare environments. Many approaches lack efficient noise reduction and normalization techniques, leading to inconsistencies in encryption strength. Computational limitations further restrict the deployment of complex encryption models in edge-based medical systems, creating a gap between security and usability. The demand for an optimized encryption strategy that ensures adaptability, high entropy, and resource efficiency highlights the necessity for a more robust framework capable of securing medical images without imposing significant computational burdens.

1.3. Objectives

The objective is to develop Faore Pony-Inspired Optimization for Chaotic Neural Encryption (FPO-IE) to ensure real-time, energy-efficient, and adaptive encryption for medical images, preventing cyber threats, privacy breaches, and unauthorized data modifications in telemedicine. Many healthcare platforms have suffered data leaks, such as the 2023 HCA Healthcare breach affecting 11 million patients, highlighting the urgent need for a robust encryption system. The model must adapt dynamically across varied imaging formats, including MRI, CT scans, and ultrasound, ensuring high entropy and resilience against evolving attacks. To support mHealth, IoT medical devices, and cloud-based imaging, encryption must consume minimal processing power while maintaining diagnostic accuracy. Compliance with HIPAA, GDPR, and India's DPDP Act remains crucial, requiring strong cryptographic safeguards and audit mechanisms. Achieving latency below 50 milliseconds for encryption ensures seamless remote consultations, fostering secure and efficient telemedicine infrastructure without compromising processing speed or accessibility.

2. LITERATURE REVIEW

"Bit-Level Chaos Security" [21] applied a chaotic feedback loop for dynamic bit-level encryption. Each encryption step is adjusted according to prior outputs, ensuring randomness. A chaotic sequence scrambled pixel positions, followed by intensity modification through diffusion. Non-linear transformations reinforced unpredictability, preventing statistical attacks. The key stream remained highly sensitive to initial values, ensuring uniqueness. Bit-level feedback enhanced security, making cipher text challenging to reconstruct. "Checkered Chaos Encryption" [22] used a checkered block scrambling approach combined with shift register-based transformations. A chaotic sequence determines pixel rearrangement, while shift registers dynamically alter encryption parameters. Multi-stage diffusion modified pixel intensities, preventing pattern detection. Compatibility with both 2D and 3D formats allowed for broad application. The layered encryption process ensured unpredictability, reducing the correlation between adjacent pixels. "Biometric Multi-Image Loc" [23] utilized fingerprint and iris biometrics to generate chaotic encryption keys. Each biometric feature influenced pixel scrambling and intensity diffusion, ensuring randomness. Multiple images were encrypted simultaneously, with each round generating unique cipher texts. A key binding mechanism prevented decryption errors due to biometric variations. Unauthorized access required matching both biometrics, increasing security. The adaptive key generation process strengthened unpredictability, securing multiple images efficiently.

"6D Chaos Symmetric Shiel" [24] employed a high-dimensional hyper chaotic system with symmetric matrix transformations for encrypting grayscale and color images. A 6D chaotic map controlled pixel scrambling, while symmetric matrices modified intensity values through non-linear diffusion. The iterative process prevented pattern recognition, enhancing security. High sensitivity to initial conditions ensured resistance to attacks. Expanded key space minimized cryptanalysis risks. "Quadratic-Sine IoMT Shiel" [25] used a Quadratic-Sine chaotic map for medical image security. A pseudo-parallel confusion mechanism scrambled pixel positions, while a diffusion stage modified intensity values dynamically. The encryption adapted to image variations, preventing statistical attacks. Key sequences remained highly sensitive to initial conditions, ensuring decryption infeasibility without correct parameters. "Phase-Structured Light Loc" [26] encrypted multiple images using structured light illumination and phase authentication. Images were encoded as phase-modulated waveforms, preventing direct reconstruction without phase keys. A phase retrieval algorithm reconstructed images only with correct parameters. Structured illumination introduced controlled randomness, ensuring distinct encryption outputs. The system secured multiple images simultaneously, requiring exact phase alignment for decryption.

"Reservoir Computing Loc" [27] applied reservoir computing to encrypt and compress images losslessly. A chaotic reservoir transformed pixel values into non-linear states, introducing randomness. A diffusion mechanism altered pixel

intensities dynamically. The compression phase encoded encrypted data into sparse representations, preserving image integrity. Reservoir-driven chaotic sequences ensured that decryption required the exact key states. "Rulkov Memristor Shiel" [28] integrated a memristive Rulkov neuron for chaotic image encryption and compressive sensing. Pixel scrambling followed chaotic neuron firing states, while a diffusion mechanism adjusted intensities nonlinearly. The compressive sensing phase reduced encrypted data size, maintaining security. The neuron model's multi stability ensured unpredictable encryption outputs. The decryption required precise system states, preventing unauthorized access. "DNA Tree Ciphe" [29] introduced a DNA tree-based encryption scheme using chaotic scrambling and non-linear diffusion. Pixels were mapped into DNA sequences, shuffled by chaotic rules, and transformed dynamically. A diffusion step introduced non-repetitive intensity changes, reinforcing security. Decryption required precise key synchronization with the tree structure. The encryption approach optimized randomness while ensuring computational efficiency, making it resistant to statistical attacks and ideal for securing digital images.

"Lorenz-Galois Loc" [30] applied an improved Lorenz chaotic system with Galois field arithmetic for image encryption. Pixel scrambling used chaotic sequences, while modular transformations ensured non-repetitive diffusion. Key dependency made decryption impossible without synchronization. Dynamic chaotic adjustments enhanced security against statistical analysis. The encryption framework-maintained efficiency, offering robust protection against brute-force attacks. "Memristor Neural Ciphe" [31] integrated a variable-order memristor neural network for image encryption. Chaotic neural activations scrambled pixels dynamically, while a synchronization mechanism ensured secure decryption. A non-linear diffusion model modified intensity, reinforcing randomness. Encryption complexity adapted to image structures, making decryption infeasible without exact parameters. The neural system demonstrated strong resistance to cryptographic attacks while ensuring efficient encryption. "Deep Holography Loc" [32] utilized coded aperture holography and deep learning for simultaneous multi-image encryption. Structured light patterns encoded multiple images into holographic representations, preventing interference. A neural network optimized aperture encoding, ensuring unique encryption for each layer. Phase coherence-maintained retrieval accuracy, while secure decryption required precise wave front parameters.

"ME-HCS" [33] introduced a hybrid encryption-compression technique for securing color medical images. The method decomposed images into RGB channels, applying hyper chaotic scrambling followed by DNA-based encoding. Compression was achieved by selectively storing high-information regions while maintaining security. Hyper chaotic sequences altered DNA base pairing, ensuring unpredictability. The decryption process reconstructed images using precise chaotic keys and DNA decoding. This approach balanced strong encryption with reduced storage requirements, making it ideal for medical image transmission and storage. "AMIE" [34] utilized auto encoders for medical image encryption, transforming images into a compressed latent space. A chaos-driven feature scrambling mechanism altered encoded representations, ensuring high security. The modified latent vectors were reconstructed into an encrypted image format, preventing unauthorized access. Decryption required an auto encoder decoder and chaotic key synchronization to recover the original image. This approach combined deep learning feature extraction with chaos-based encryption, providing an advanced security framework for medical image protection. Different Bio-inspired strategies are applied in different researches to achieve better results [35]-[67].

3. FAORE PONY - INSPIRED OPTIMIZATION FOR CHAOTIC NEURAL ENCRYPTION

Faore Pony-Inspired Optimization for Chaotic Neural Encryption enhances security by leveraging adaptive stamina-based optimization, ensuring robust pixel diffusion, dynamic key evolution, and high unpredictability for secure medical image transmission in telemedicine applications.

3.1 Image Preprocessing for FPO-IE

Medical image dimensions are standardized to ensure compatibility with the encryption framework. This process involves resizing the images to a predetermined resolution while maintaining their diagnostic integrity. The resizing step establishes uniformity across all input data, a critical requirement for subsequent encryption and optimization stages. Mathematical operations ensure that the dimensional properties of each image align precisely with the optimized parameters of the Faore pony-inspired model. For instance, consider the transformation of a two-

dimensional image $I(x,y)$ into a resized image $I'(x',y')$.

$$I'(x',y') = I\left(\frac{x}{\alpha},\frac{y}{\beta}\right) \quad (1)$$

In Eq.(1), where α and β represent the scaling factors for the horizontal and vertical axes, respectively. These factors are optimized based on the characteristics of the input dataset, ensuring the preservation of critical image features.

The variables x and y denote the original pixel coordinates, while x' and $y'$are the transformed coordinates after scaling. The scaling factors α and β are derived through iterative adjustment to ensure minimal distortion in critical regions of interest, reflecting the stamina-driven adaptability of the Faroe pony.

Intensity normalization is performed to harmonize the pixel intensity values across images, improving the encryption algorithm's ability to operate consistently. This step adjusts the pixel values to lie within a standardized range, typically between 0 and 1. This operation enhances the contrast of medical images, enabling the model to emphasize diagnostically significant features during subsequent stages. The normalized intensity $N(x,y)$ is calculated as shown in Eq.(2).

$$N(x,y) = \frac{I(x,y) - \min(I)}{\max(I) - \min(I)} \quad (2)$$

Here, $\max(I)$ and $\min(I)$ denote the minimum and maximum intensity values in the original image$I(x,y)$, respectively. This equation ensures that all pixel values are rescaled proportionately, reflecting the optimized energy distribution inspired by the Faroe pony's efficient resource allocation.

The adjustment of $N(x,y)$ to this bounded range simplifies the encryption process, as chaotic maps function more effectively within controlled numerical domains. The normalization step mirrors the agility and adaptability of the Faroe pony in navigating challenging terrains, ensuring that the image preprocessing aligns optimally with the encryption model's requirements.

Noise reduction is a crucial preprocessing step that removes extraneous information from medical images. An optimized adaptive filter is applied to enhance image clarity without compromising diagnostically relevant features. The filtering operation utilizes neighborhood-based techniques, dynamically adjusting the filter coefficients based on local pixel intensities. The filtered image $F(x,y)$ is computed as represented mathematically in Eq.(3).

$$F(x,y) = \frac{\sum_{i=-k}^{k}\sum_{j=-k}^{k} w(i,j)I(x+i,y+j)}{\sum_{i=-k}^{k}\sum_{j=-k}^{k} w(i,j)} \quad (3)$$

where k defines the filter window size, $w(i,j)$ represents the weight assigned to each pixel in the window, and $I(x+i,y+j)$ corresponds to the intensity value of the neighboring pixel. The weights $w(i,j)$ are adaptively optimized based on the local variance within the image, emulating the Faore pony's capacity for dynamic decision-making in complex environments.

The adaptive nature of the filtering mechanism ensures that noise is reduced while preserving edges and fine details, crucial for maintaining the diagnostic integrity of medical images. The optimization process reflects the stamina traits of the Faroe pony, ensuring that the model efficiently allocates computational resources to the most critical regions of the image.

3.2 Key Generation Initialization for FPO-IE

Key generation is critical to the encryption framework, as it determines the unpredictability and robustness of the system. Leveraging chaos theory, this step integrates the dynamic, sensitive properties of chaotic maps to generate keys with high randomness and entropy. The unpredictability inherent in chaotic systems mirrors the agility of the Faroe pony in adapting to dynamic terrains, where even minor changes lead to significant variations in outcomes. This unpredictability is foundational to ensuring robust encryption. A chaotic sequence $S(t)$ for the key initialization is expressed as Eq.(4).

$$S(t+1) = \mu S(t)(1 - S(t)) \quad (4)$$

where μ represents the control parameter, and $S(t)$ is the sequence at time t. The parameter μ is optimized within specific bounds to ensure the sequence demonstrates fully chaotic behavior. In this context, μ reflects the stamina-driven adaptability of the Faroe pony, balancing the complexity and stability of the generated keys.

The variables $S(t)$ and $S(t+1)$ define the chaotic sequence at consecutive steps, influenced μ, which governs the chaotic map's behavior. This approach establishes a secure, non-repeating key generation mechanism.

Neural networks provide adaptive learning capabilities, enhancing the quality of chaotic sequences. By training on historical patterns of

image features and encryption keys, the network identifies optimized parameters for generating robust keys. This integration combines the agility of chaos theory with the learning efficiency of neural systems, replicating the decision-making traits of the Faroe pony in complex environments. The optimization of the neural network weights W_{ij} and biases b_j is governed as shown in Eq.(5).

$$y_j = \sigma\left(\sum_{i=1}^{n} W_{ij}x_i + b_j\right) \quad (5)$$

where x_i represents the input features, W_{ij} are the weights connecting the i-th input to the j-th neuron, b_j denotes the bias term, and σ is the activation function. The output y_j signifies the optimized key parameters that refine the chaotic sequence.

The variables x_i, W_{ij}, and b_j reflect the dynamic interaction of inputs, weights, and biases in determining the output. These components emulate the adaptive behavior of the Faroe pony, ensuring the generated keys align optimally with encryption requirements.

To achieve greater key diversity, the chaotic sequence and neural network outputs are combined through a hybrid optimization framework. This framework utilizes a weighted summation approach, enhancing the randomness and security of the generated keys. The final key $K(i)$ is calculated as expressed in Eq.(6).

$$K(i) = \omega_1 S(t) + \omega_2 y_j \quad (6)$$

where ω_1 and ω_2 are weighting factors that balance the contributions of the chaotic sequence $S(t)$ and the neural network output y_j. These weights are iteratively optimized to maximize the entropy of $K(i)$.

The variables ω_1 and $\omega_2$represent the proportions of the chaotic and neural network components in the final key. The iterative optimization process reflects the stamina and adaptability of the Faroe pony, ensuring an efficient balance between complexity and functionality in the key generation.

3.3 Chaotic Sequence Generation for FPO-IE

Chaotic systems form the backbone of robust encryption techniques by generating sequences that exhibit high sensitivity to initial conditions and deterministic unpredictability. These characteristics ensure that even minor variations in the input parameters produce entirely distinct sequences. This approach aligns with the adaptive stamina of the Faroe pony, which efficiently navigates unpredictable terrains by responding to minute environmental changes. The chaotic sequence establishes the foundation for pixel-level shuffling and adaptive diffusion in encryption, creating a secure framework for medical image privacy. A modified Tent Map is defined for generating chaotic sequences.

$$C(t+1) = \begin{cases} \gamma.C(t), & 0 \le C(t) < 0.5 \\ \gamma.(1-C(t)), & 0.5 \le C(t) \le 1 \end{cases} \quad (7)$$

In Eq.(7), where γ represents the control parameter that determines the level of chaos, while $C(t)$ represents the chaotic sequence at time t. The selection of γ ensures that the system operates in a fully chaotic state, mirroring the Faore pony's optimal energy utilization in dynamic environments.The variable γ introduces flexibility to the chaotic map, allowing fine-tuning to suit specific encryption requirements. The sequence $C(t)$ evolves iteratively, with each step producing a new value based on the map's rules.

Multidimensional chaos introduces additional layers of complexity, enhancing the unpredictability of the encryption framework. A 3D Logistic Map is employed to generate three-dimensional chaotic sequences, offering high entropy and resilience against attacks. The equations governing the 3D Logistic Map are expressed in Eq.(8), Eq.(9), and Eq.(10).

$$x(t+1) = r_x x(t)\big(1-x(t)\big) + \delta_y(t) z(t) \quad (8)$$

$$y(t+1) = r_y y(t)\big(1-y(t)\big) + \delta_z(t) x(t) \quad (9)$$

$$z(t+1) = r_z z(t)\big(1-z(t)\big) + \delta_z(t) y(t) \quad (10)$$

where r_x, r_y and r_z are the control parameters for the logistic components, and δ is the coupling constant that integrates the three dimensions. The initial conditions $x(0), y(0)$, and $z(0)$ determine the chaotic behavior.

The variables r_x, r_y, r_z, and $\delta$are optimized to ensure maximal entropy in the generated sequences. The coupling between dimensions enhances the complexity of the map, reflecting the endurance and adaptive agility of the Faroe pony.

The chaotic sequences generated from different maps are combined to enhance the overall randomness and security. A weighted summation

approach integrates multiple chaotic maps, creating a unified sequence as expressed in Eq.(11).

$$S(t) = \omega_1 C_1(t) + \omega_2 C_2(t) + \omega_3 C_3(t) \quad (11)$$

where ω_1, ω_1, and ω_3 represent the weights assigned to the sequences $C_1(t), C_2(t)$, and $C_3(t)$, respectively, generated from distinct chaotic maps. These weights are optimized iteratively, ensuring a balanced contribution from each map to maximize entropy.

The weights ω_1, ω_2, and $\omega_3$reflect the proportional influence of individual chaotic maps, similar to the balanced stamina-driven decision-making of the Faroe pony in unpredictable situations. The final sequence $S(t)$ achieves a high degree of randomness, suitable for secure encryption applications.

3.4 Faroe Pony-Inspired Optimization Initialization for FPO-IE

Faore pony-inspired optimization focuses on initializing parameters by simulating the pony's adaptive behavior in resource-constrained environments. The stamina and agility traits are utilized to ensure efficient energy management during chaotic neural encryption. Optimized initialization aligns with previous steps by preparing an adaptable framework for pixel-level operations and key refinement. Resource allocation adapts dynamically, ensuring balance across all encryption processes. The energy function $E(t)$, representing stamina-driven adaptability, is initialized as expressed in Eq.(12).

$$E(t) = k.\left[1 - \frac{t}{T_{max}}\right] \quad (12)$$

where t represents the current iteration, T_{max} denotes the maximum iterations, and κ is a scaling factor for stamina. This function ensures the gradual depletion of energy over iterations while maintaining optimal levels for encryption tasks.

In this context, t tracks the progression of iterations, T_{max} defines the optimization duration, and κ scales the stamina resource. The equation reflects adaptive stamina consumption, mirroring the Faore pony's endurance management.

Stamina-based adaptation incorporates dynamic decision-making into the initialization process, ensuring that parameters evolve optimally. The adaptation mechanism adjusts key optimization variables based on energy levels, enhancing the encryption framework's robustness. This adaptive strategy resembles the pony's ability to fine-tune its responses in challenging terrains. The position update equation for optimization agents is defined as Eq.(13).

$$P_i(t+1) = P_i(t) + \alpha \cdot sin(\phi) \cdot \left(P_{best} - P_i(t)\right) + \beta \cdot cos(\phi) \cdot \left(P_{global} - P_i(t)\right) \quad (13)$$

where $P_i(t)$ is the position of the i-th agent at iteration t, P_{best} is the agent's local best position, P_{global} is the global best position, α and β are adaptive coefficients influenced by stamina levels, and ϕ represents a random angular component introducing variability.

The terms α and β reflect the adaptive weights that balance exploration and exploitation. The angular componentϕ ensures dynamic adjustments to position updates, inspired by the agility of the Faroe pony.

Agility-driven redistribution ensures balanced utilization of optimization resources across the encryption framework. The redistribution mechanism dynamically reallocates resources based on the progress of optimization, preventing stagnation in parameter tuning. This approach enhances adaptability, aligning with the pony's efficient traversal of uneven terrains. The redistribution of resource R among agents is governed as represented in Eq.(14).

$$R_i = \frac{\sigma \cdot E(t)}{\sum_{j=1}^{N} \sigma \cdot E_j(t)} \quad (14)$$

where R_i is the redistributed resource for the i-th agent, σ represents a scaling factor for energy influence, $E(t)$ is the current energy of the agent, and N is the total number of agents. This equation normalizes resource allocation based on stamina levels, ensuring optimal utilization across all agents.

The variable σ adjusts the weight of energy levels in redistribution, while $E(t)$ captures the stamina state of each agent. The term N defines the agent population, promoting balanced resource allocation.

3.5 Dynamic Pixel Shuffling for FPO-IE

Dynamic pixel shuffling leverages chaotic sequences to disrupt the spatial arrangement of pixels in medical images. This process enhances encryption security by ensuring no visual correlation exists between the original and shuffled images. The method draws inspiration from the agility of the Faroe pony, adapting dynamically to optimize pixel rearrangement across iterations. The chaotic sequence generated in previous steps determines the

new positions for each pixel, ensuring randomness while preserving computational efficiency. The shuffling operation $P'(x,y)$ is governed as expressed in Eq.(15).

$$P'(x,y) = P(x',y') \quad (15)$$

where $P(x,y)$ represents the original pixel at coordinates (x,y), and (x',y') are the new coordinates determined by the chaotic sequence. The mapping of (x,y) to (x',y') ensures that each pixel relocates uniquely, eliminating repetitive patterns and enhancing unpredictability.

The variables x and y denote the original coordinates, while x' and y' signify the shuffled coordinates. The chaotic sequence drives the mapping process, ensuring optimized and dynamic rearrangement of pixels.

Incorporating stamina-based adaptation ensures that the shuffling process evolves over iterations, enhancing security against potential attacks. The adaptation mechanism leverages the energy function $E(t)$, introduced in previous steps, to determine the extent of shuffling in each iteration. The dynamic pattern adjusts based on energy levels, optimizing the balance between security and computational load. The new coordinates (x',y') are calculated as expressed in Eq.(16) and Eq.(17).

$$x' = (x + \lfloor E(t) \cdot S_x \rfloor) \mod W \quad (16)$$

$$y' = \left(y + \lfloor E(t) \cdot S_y \rfloor\right) \mod H \quad (17)$$

where S_x and S_y are chaotic sequences for horizontal and vertical coordinates, W and H represent the image's width and height, and $\lfloor \cdot \rfloor$ denotes the floor function. The energy function $E(t)$ adapts the shuffling intensity dynamically, ensuring that each iteration introduces unique patterns.

The terms W and H define the image dimensions, while S_x and S_y represent chaotic sequences for pixel shifts. The energy function $E(t)$ regulates the extent of shuffling, reflecting the stamina-driven adaptability of the Faroe pony.

To achieve multidimensional shuffling, a hybrid chaotic map combines sequences from different dimensions. This approach increases the randomness of pixel rearrangement, reducing the risk of pattern recognition. The multidimensional chaotic map $M(x,y)$ for shuffling is defined as expressed in Eq.(18) and Eq.(19).

$$x' = \lfloor M_x(x,y) \rfloor \mod W \quad (18)$$

$$y' = \lfloor M_y(x,y) \rfloor \mod H \quad (19)$$

where $M_x(x,y)$ and $M_y(x,y)$ are hybrid chaotic maps for horizontal and vertical dimensions, combining outputs from multiple chaotic maps. These maps generate new coordinates for each pixel, enhancing unpredictability.

The variables $M_x(x,y)$ and $M_y(x,y)$ integrate chaotic sequences from multiple maps, creating a hybrid output. The terms x' and y' define the shuffled pixel positions, ensuring optimal randomness in the rearrangement. Dynamic pixel shuffling reflects the adaptive agility of the Faroe pony, ensuring an optimized and robust framework for chaotic neural encryption. This step establishes the critical transformation necessary for secure medical image privacy in telemedicine.

3.6 Adaptive Diffusion Using Stamina Traits for FPO-IE

Adaptive diffusion introduces randomness to pixel intensity values, enhancing security by making encrypted images resistant to attacks. Inspired by the stamina traits of the Faroe pony, this process dynamically adjusts the diffusion parameters, ensuring optimal energy utilization across iterations. The stamina-driven adaptability aligns with previous steps, utilizing energy levels to regulate intensity modifications. The diffusion process for a pixel $P(x,y)$ is expressed as Eq.(20).

$$D(x,y) = P(x,y) + \eta \cdot C(x,y) \quad (20)$$

where, $P(x,y)$ is the original pixel value, $C(x,y)$ is the chaotic sequence value for the corresponding coordinate, and η represents a dynamic scaling factor influenced by the energy function $E(t)$. The variables η and $C(x,y)$ introduce controlled randomness, ensuring that the diffusion adapts to chaotic sequences while maintaining optimized computational efficiency. This mirrors the stamina-driven agility of the Faroe pony.

The scaling factor η plays a vital role in controlling the intensity of diffusion. This parameter dynamically adjusts based on the energy function $E(t)$, which reflects the stamina levels during encryption. The adaptive scaling ensures that diffusion intensity decreases gradually, conserving resources while maintaining security. The dynamic scaling factor η is defined as Eq.(21).

$$\eta = \lambda \cdot E(t) \cdot sin\left(\frac{\pi t}{T_{max}}\right) \quad (21)$$

where λ is a constant scaling coefficient, $E(t)$ is the current energy level, t is the iteration number, and T_{max} represents the maximum iterations.

The terms λ and $E(t)$ determine the magnitude of diffusion, while the sinusoidal component introduces periodic variations inspired by the endurance-driven adaptability of the Faroe pony. This ensures optimized modulation of pixel intensities. The diffusion process is further refined by introducing multilevel chaotic sequences, enhancing randomness and resistance to attacks. Each pixel undergoes a multilevel transformation, ensuring that the intensity variations follow non-linear patterns. The multilevel diffusion equation is shown in Eq.(22).

$$D'(x,y) = D(x,y) \cdot \left(1 + \rho \cdot cos\left(\frac{2\pi C(x,y)}{M}\right)\right) \quad (22)$$

where, $D'(x,y)$ is the diffused pixel value, ρ is a diffusion control parameter, $C(x,y)$ is the chaotic sequence value, and M represents the maximum intensity level. The variable ρ controls the non-linear amplification of the diffusion, while the cosine component introduces periodic variations. This approach aligns with the adaptability of the Faroe Pony, ensuring secure and optimized encryption.

To enhance security, the diffusion process is applied iteratively, ensuring that each pixel undergoes multiple transformations. This iterative approach increases the complexity of the encrypted image, reducing the likelihood of reverse engineering. The iterative diffusion process is defined as Eq.(23).

$$D_i(x,y) = D_{i-1}(x,y) + \delta \cdot C_i(x,y) \quad (23)$$

where $D_i(x,y)$ is the pixel value after the i-th iteration, $D_{i-1}(x,y)$ is the pixel value from the previous iteration, $C_i(x,y)$ is the chaotic sequence value for the i-th iteration, and δ is an iteration-dependent scaling factor.

The variables $C_i(x,y)$ and δ ensure that the diffusion adapts dynamically across iterations, reflecting the stamina-based energy modulation inspired by the Faroe pony. Non-linear coupling introduces additional complexity to the diffusion process by integrating neighboring pixel values into the transformation. This coupling ensures that the diffusion reflects global image characteristics, enhancing resistance to differential attacks. The coupled diffusion equation is defined as Eq.(24).

$$D''(x,y) = D'(x,y) + v \cdot \sum_{i=-1}^{1}\sum_{j=-1}^{1}\frac{D'(x+i,y+j)}{9} \quad (24)$$

where, $D''(x,y)$ is the final diffused pixel value, v is a coupling coefficient, and the summation integrates contributions from neighboring pixels. The variable v regulates the influence of neighboring pixels, ensuring balanced coupling across the image. The summation reflects the diffusion's global adaptability, inspired by the stamina-driven interactions of the Faroe pony.

3.7 Key Refinement Through Neural Network Optimization for FPO-IE

The refinement of keys through neural network optimization enhances the robustness of chaotic neural encryption. Neural networks learn intricate patterns and adjust key generation parameters to maximize entropy and randomness. This approach mirrors the dynamic decision-making capabilities of the Faroe pony, which optimizes its behavior in complex and unpredictable terrains. Key refinement ensures compatibility with chaotic sequences, adaptive diffusion, and dynamic pixel shuffling, forming an integral component of the encryption framework. The refined key $K'(t)$ is expressed as Eq.(25).

$$K'(t) = \sigma(W \cdot K(t) + b) \quad (25)$$

where $K(t)$ represents the initial key at iteration t, W denotes the weight matrix, b is the bias vector, and σ is the activation function. The neural network dynamically adjusts W and b, ensuring optimized refinement of keys.

The variables W and b are learned parameters of the network, while σ applies a non-linear transformation to the weighted sum. This process aligns with the Faore pony's ability to adapt efficiently in complex scenarios. Energy-based optimization influences the weight adjustment process in neural networks, aligning the key refinement process with stamina-driven adaptability. The energy function $E(t)$, introduced earlier, guides the learning rate and weight updates, ensuring efficient resource utilization. The weight update equation is defined as Eq.(26).

$$W^{(t+1)} = W^{(t)} - \eta \cdot \frac{\partial L}{\partial W^{(t)}} \cdot E(t) \quad (26)$$

where, $W^{(t)}$ represents the weights at iteration t, η is the learning rate, L denotes the loss function, and $E(t)$ scales the update based on energy levels. The variables η and L regulate the gradient-based optimization process, while $E(t)$ ensures stamina-driven modulation of weight updates. This approach reflects the efficient energy management of the Faore pony.

Entropy maximization enhances the randomness of refined keys, increasing resistance to cryptographic attacks. Neural networks adjust key refinement parameters to maximize entropy, ensuring highly unpredictable keys suitable for encryption. The entropy $H(K')$ of the refined key is calculated as expressed in Eq.(27).

$$H(K') = -\sum_{i=1}^{n} p_i log_2 p_i \quad (27)$$

where p_i is the probability of the i-th key value occurring. Neural networks optimize p_i distributions to achieve maximal entropy. The variable p_i captures the probability distribution of key values, and n defines the total number of possible key values. The optimization of p_i aligns with the adaptability and agility of the Faroe pony, ensuring robustness in the refined keys.

A multi-layer neural network is employed to enhance the complexity and adaptability of the key refinement process. Each layer introduces additional transformations, ensuring that the refined keys exhibit high entropy and non-linearity. The output of the j-th layer is defined as Eq.(28).

$$z_j = \sigma(W_j \cdot z_{j-1} + b_j) \quad (28)$$

where, z_{j-1} represents the input to the j-th layer, $W_j$and b_j denote the weight matrix and bias vector for the layer, and σ is the activation function. The terms $W_j$and $b_j$are learned parameters for each layer, while z_{j-1}captures the output of the previous layer. This hierarchical refinement reflects the stamina-based adaptability and efficient decision-making of the Faroe pony.

Key refinement through neural network optimization incorporates adaptability, entropy maximization, and multi-layer transformations, enhancing the robustness of chaotic neural encryption. This step integrates the stamina-driven traits of the Faroe pony, ensuring secure medical image privacy in telemedicine.

3.8 Encryption Execution for FPO-IE

Encryption execution combines adaptive diffusion, dynamic pixel shuffling, and chaotic sequences to transform the medical image into an encrypted format. This stage ensures that the processed image is secured against unauthorized access. The integration of previous steps creates a seamless transition from raw pixel data to encrypted output. The process mirrors the stamina-driven adaptability of the Faroe pony, optimizing operations at each stage to ensure robustness in execution. The encrypted pixel value $E(x,y)$ is calculated as shown in Eq.(29).

$$E(x,y) = D''(x,y) \otimes K'(x,y) \quad (29)$$

where, $D''(x,y)$ is the diffused pixel value, $K'(x,y)$ is the refined key value corresponding to the pixel, and $\oplus$ denotes the XOR operation, ensuring randomness and security in the encryption. The variables $D''(x,y)$ and $K'(x,y)$ originate from the diffusion and key refinement steps, respectively, ensuring a strong connection to previous processes. The XOR operation secures pixel-level transformations, aligning with optimized encryption objectives.

To enhance security, multi-layered chaotic operations are applied during encryption. This step ensures that each pixel undergoes multiple transformations, reducing susceptibility to attacks. The chaotic transformation $C'(x,y)$ is expressed as Eq.(30).

$$C'(x,y) = C(x,y) \cdot sin\left(\frac{2\pi K'(x,y)}{M}\right) \quad (30)$$

where $C(x,y)$ is the chaotic sequence value, $K'(x,y)$ is the refined key, and M represents the maximum intensity level. The sine function introduces periodic variations, ensuring non-linear transformations in encryption. The terms $C(x,y), K'(x,y)$, and M contribute to the randomness and complexity of the encryption process. The sine transformation reflects agility and optimized resource utilization.

Iterative encryption ensures that each pixel is repeatedly transformed, enhancing the encrypted image's resistance to attacks. The encrypted pixel after i-th iteration $E_i(x,y)$is given by Eq.(31).

$$E_i(x,y) = E_{i-1}(x,y) \oplus (C_i(x,y) \cdot K'(x,y)) \quad (31)$$

Journal of Theoretical and Applied Information Technology
31st May 2025. Vol.103. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

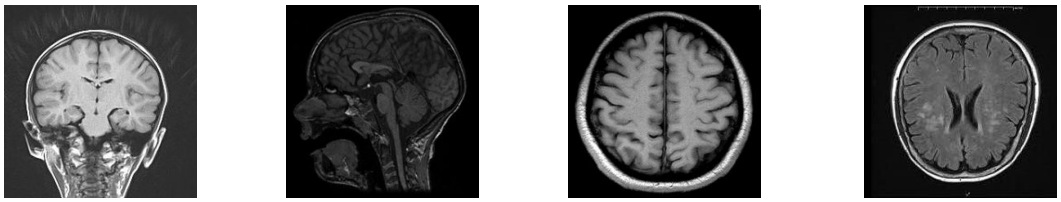

Figure 1: Dataset Medical Images

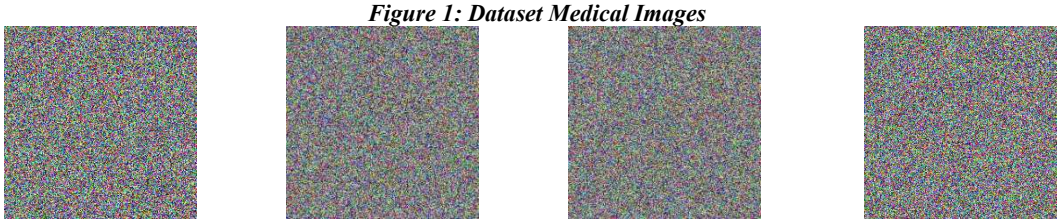

Figure 2 :Encrypted Medical Images

where $E_{i-1}(x,y)$ is the encrypted pixel from the previous iteration, $C_i(x,y)$ is the chaotic sequence value at iteration $K'(x,y)$ is the refined key. The variables $E_{i-1}(x,y), C_i(x,y)$, and $K'(x,y)$ ensure dynamic transformations across iterations, reflecting the endurance-driven optimization inspired by the Faore pony.

Position-based modulation incorporates the pixel's coordinates into the encryption process, introducing spatial variability in transformations. The modulated encryption value $E'(x,y)$is defined as Eq.(32).

$$E'(x,y) = E(x,y) + \alpha \cdot \left(x \cdot C_x + y \cdot C_y\right) \quad (32)$$

where α is a scaling parameter, C_x and C_y are chaotic sequences for horizontal and vertical coordinates, and x, y are the pixel's coordinates. The variables α, C_x, and C_y contribute to spatially variable transformations, ensuring that encrypted pixels vary based on their positions. This approach aligns with the agility and adaptability of the Faroe pony.

Maximizing entropy in the encrypted image enhances security by ensuring randomness. The entropy $H(E)$ of the encrypted image is calculated as expressed in Eq.(33).

$$H(E) = -\sum_{i=1}^{n} p_i log_2 p_i \quad (33)$$

where p_i is the probability of occurrence of the i-th intensity value. High entropy ensures that the encrypted image is resistant to statistical attacks. The variable p_i captures the distribution of pixel intensity values, ensuring that the encrypted image lacks recognizable patterns. This aligns with the optimized encryption objectives. Figure 1 and Figure 2 portrays the medical images that exists in dataset and its encrypted form of images. Validation measures ensure that the encrypted image meets security requirements. The correlation coefficient r between the original and encrypted images is computed as shown in Eq.(34).

$$r = \frac{\Sigma(I(x,y) - \mu_I)(E(x,y) - \mu_E)}{\sqrt{\Sigma(I(x,y) - \mu_I)^2 \cdot \Sigma(E(x,y) - \mu_E)^2}} \quad (34)$$

where $I(x,y)$ and $E(x,y)$ are the original and encrypted images, μ_I and μ_E are their mean values. The terms μ_I and μ_E ensure that the correlation measures statistical independence between the original and encrypted images, verifying the encryption's robustness.

3.9 Encrypted Image Transmission for FPO-IE

Encrypted image transmission ensures that the securely transformed medical image reaches its intended recipient without compromising its integrity or confidentiality. This step involves encoding the encrypted image and transmitting it over a secure communication channel. The behavior of the Faroe pony, which adapts its energy efficiently across terrains, inspires the optimization of resources during transmission. Combining encryption robustness and secure delivery ensures that the image is inaccessible to unauthorized parties. The transmitted data $T(x,y)$ is expressed as Eq.(35).

$$T(x,y) = \varepsilon(E'(x,y) \cdot \Phi(x,y)) \quad (35)$$

where $\varepsilon(E'(x,y))$ is the encoded encrypted image, and $\Phi(x,y)$ represents the transmission channel's modulation function. The encoding process adapts to optimize bandwidth utilization and error minimization during transmission. The variables $\varepsilon(E'(x,y))$ and $\Phi(x,y)$ensure compatibility between the encrypted image and the

communication channel, creating an efficient and secure transmission mechanism.

Error control is critical during transmission to ensure that encrypted images remain intact despite noise or interference in the communication channel. Adaptive error correction codes are implemented to detect and correct errors dynamically, ensuring that the transmitted data retains its integrity. The error control function $C(T(x,y))$ is defined as Eq.(36).

$$C(T(x,y)) = T(x,y) \oplus R(x,y) \quad (36)$$

where $T(x,y)$ is the transmitted data, $R(x,y)$ is the redundancy added by the error control code and $\oplus$ represents the XOR operation. The redundancy $R(x,y)$ adapts dynamically based on the noise levels in the channel. The variables $T(x,y)$ and $R(x,y)$ ensure that the transmitted data remains error-resilient, aligning with optimized transmission objectives inspired by the stamina-driven adaptability of the Faroe pony.

The modulation process optimizes the transmission of encrypted images over varying communication channels. This step adapts the signal characteristics to ensure compatibility with channel conditions, minimizing distortion and improving data delivery. The modulated signal $S(t)$ is represented mathematically in Eq.(37).

$$S(t) = A \cdot \cos(2\pi f_c t + \psi(t)) \quad (37)$$

where A is the amplitude of the signal, f_c is the carrier frequency, and $\psi(t)$ is the phase modulation term based on the encrypted image data. The variables A, f_c, and $\psi(t)$ ensure that the signal adapts dynamically to the channel conditions, reflecting optimized energy utilization during transmission, inspired by the adaptive endurance of the Faroe pony.

Dynamic bandwidth allocation ensures that the transmission process adapts to network conditions, optimizing the use of available resources. The allocated bandwidth $B(t)$ is defined as Eq.(38).

$$B(t) = B_{max} \cdot \left(1 - \frac{P_{loss}}{P_{threshold}}\right) \quad (38)$$

where B_{max} is the maximum bandwidth, P_{loss} is the packet loss rate, and $P_{threshold}$ is the allowable packet loss threshold. The terms B_{max}, P_{loss}, and $P_{threshold}$ ensure that bandwidth allocation remains efficient under varying network conditions, aligning with optimized resource management.

Key synchronization between the sender and receiver ensures that encrypted images are decrypted accurately. A secure channel transmits the encryption key separately, ensuring that only authorized parties can access the encrypted data. The synchronization process K_s is modeled as expressed in Eq.(39).

$$K_s = H(K) \oplus T(K) \quad (39)$$

where $H(K)$ is the hash of the encryption key, and $T(K)$ represents the transmitted key segment. This method ensures secure key delivery without exposing it to interception. The variables $H(K)$ and $T(K)$ protect the encryption key during transmission, ensuring compatibility with the secure communication protocol.

Validation ensures that the transmitted data meets security and integrity requirements. The signal-to-noise ratio SNR is computed as defined in Eq.(40).

$$SNR = 10 \cdot log_{10}\left(\frac{P_{signal}}{P_{noise}}\right) \quad (40)$$

where P_{signal} is the power of the transmitted signal, and P_{noise} is the noise power in the communication channel. The terms P_{signal} and P_{noise} ensure that transmission quality meets the necessary thresholds for secure data delivery, reflecting optimized resource allocation during transmission.

3.10 Decryption Using Reverse Operations for FPO-IE

Decryption involves reversing the encryption operations to restore the original medical image while maintaining its integrity. This process ensures that the transmitted encrypted image can be accurately decrypted only by authorized recipients. Reverse operations involve chaotic sequence application, key utilization, and adaptive transformations, ensuring a seamless reconstruction of the original data. The decryption process mirrors the optimized energy usage of the Faroe Pony, emphasizing precision and resource efficiency in reversing transformations. The decrypted pixel value $D'(x,y)$ is computed using the XOR operation expressed in Eq.(41).

$$D'(x,y) = E^1(x,y) \oplus K'(x,y) \quad (41)$$

where, $E^1(x,y)$ represents the encrypted pixel value, and $K'(x,y)$ is the refined key associated with the pixel. The XOR operation ensures accurate retrieval of the diffused pixel values. The variables

$E^1(x,y)$ and $K^1(x,y)$ originate from previous steps, establishing a strong connection with encryption processes. This ensures that only the correct key can decrypt the image.

Diffusion transformations applied during encryption are reversed to restore the pixel intensity values. This step ensures that the randomness introduced during adaptive diffusion is systematically removed. The reverse diffusion process $D''(x,y)$ is expressed as Eq.(42).

$$D''(x,y) = D'(x,y) - \eta \cdot C(x,y) \quad (42)$$

where η is the scaling factor, $C(x,y)$ is the chaotic sequence used during encryption, and $D'(x,y)$ is the decrypted pixel value from the previous step. The terms η and $C(x,y)$ ensure that the diffusion process is reversed accurately, reflecting the optimized adaptability of the Faroe pony in re-tracing its steps efficiently.

The multi-layered chaotic operations applied during encryption are reversed to restore the original pixel values. This involves applying inverse transformations to the chaotic sequences used in encryption. The reverse chaotic transformation $C''(x,y)$ is calculated as shown in Eq.(43).

$$C''(x,y) = \frac{C'(x,y)}{sin\left(\frac{2\pi K'(x,y)}{M}\right)} \quad (43)$$

where $C'(x,y)$ is the chaotic value from the encryption stage, $K'(x,y)$ is the refined key, and M represents the maximum intensity level. The terms $C'(x,y)$ and $K'(x,y)$ ensure the accurate reversal of chaotic transformations, allowing precise restoration of original pixel intensity values.

Position-based modulation is reversed by subtracting the spatially variable transformations applied during encryption. The reverse-modulated pixel value $P'(x,y)$ is calculated as expressed in Eq.(44).

$$P''(x,y) = D''(x,y) - \alpha \cdot \left(x \cdot C_x + y \cdot C_y\right) \quad (44)$$

where, α is the scaling parameter, C_x and C_y are chaotic sequences for horizontal and vertical coordinates, and x, y are the pixel coordinates. The terms $\alpha, C_x,$ and C_y ensure that the spatial variability introduced during encryption is effectively reversed, aligning with the precise resource utilization of the Faroe pony.

Validation ensures that the decrypted image retains its original structure and intensity distribution. The mean squared error MSE between the original and decrypted images is calculated as shown in Eq.(45).

$$MSE = \frac{1}{WH}\sum_{x=1}^{W}\sum_{y=1}^{H}(I(x,y) - P'(x,y))^2 \quad (45)$$

where $I(x,y)$ is the original pixel value, $P'(x,y)$ is the decrypted pixel value, W is the image width, and H is the image height. The terms $I(x,y)$ and $P'(x,y)$ measure the accuracy of decryption, ensuring that the reconstructed image closely matches the original. This aligns with the optimized precision required for telemedicine applications.

Entropy validation ensures that the decrypted image has a structured intensity distribution indicative of its original form. The entropy $H(P')$ of the decrypted image is calculated as shown in Eq.(46).

$$H(P') = -\sum_{i=1}^{n} p_i log_2 p_i \quad (46)$$

where p_i represents the probability of the i-th pixel intensity value in the decrypted image. The term p_i evaluates the pixel intensity distribution, ensuring that the decrypted image lacks randomness introduced during encryption. This ensures optimized decryption aligned with the original image properties.

3.11 Performance Evaluation and Feedback for FPO-IE

The evaluation of encryption quality ensures that the FPO-IE framework achieves robust security while maintaining operational efficiency. Quality metrics assess the randomness, unpredictability, and integrity of the encryption process. Inspired by the stamina-driven adaptability of the Faroe pony, the evaluation process adapts to different scenarios, providing detailed feedback for optimization. The structural similarity index measure (SSIM) is utilized to quantify the difference between the original and encrypted images.

$$SSIM = \frac{\left(2_{\mu_I\mu_E} + c_1\right)(2\sigma_{IE} + c_2)}{(\mu_I^2 + \mu_E^2 + c_1)(\mu_I^2 + \mu_E^2 + c_2)} \quad (47)$$

In Eq.(47), where μ_I and μ_E are the mean intensities of the original and encrypted images, σ_I^2 and σ_E^2 are their variances, σ_{IE} is their covariance, and c_1, c_2 are constants for numerical stability. The terms $\mu_I, \mu_E, \sigma_I^2, \sigma_E^2, \sigma_{IE}, c_1, c_2$ ensure precise

quantification of encryption quality, reflecting optimized processes.

Key sensitivity measures the framework's ability to produce significantly different outputs with minor changes in the encryption key. This property ensures robustness against brute-force attacks. The key sensitivity metric Δ is defined as shown in Eq.(48).

$$\Delta = \frac{\sum_{x=1}^{W}\sum_{y=1}^{H}|E_k(x,y) - E_{k'}(x,y)|}{W \cdot H} \quad (48)$$

where $E_k(x,y)$ and $E_{k'}(x,y)$ are the encrypted images generated using keys k and k', W is the image width, and H is the height. The terms $E_k(x,y), E_{k'}(x,y), W, H$ capture the sensitivity of encryption to key variations, ensuring optimized key-dependent randomness.

The Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) metrics evaluate the encryption framework's resistance to differential attacks. These metrics quantify the impact of a single-pixel change in the original image on the encrypted image. The NPCR metric is expressed as Eq.(49).

$$NPCR = \frac{\sum_{x=1}^{W}\sum_{y=1}^{H}\delta(x,y)}{W \cdot H} \cdot 100\% \quad (49)$$

where $\delta(x,y)$ is 1 if $E_o(x,y) \neq E'_o(x,y)$, and 0 otherwise. Here, $E_o(x,y)$and $E'_o(x,y)$ are the encrypted images before and after a single pixel change.

The UACI metric is defined as expressed in Eq.(50).

$$UACI = \frac{\sum_{x=1}^{W}\sum_{y=1}^{H}\frac{|E_o(x,y) - E'_o(x,y)|}{255}}{W \cdot H} \cdot 100\% \quad (50)$$

where $E_o(x,y)$ and $E'_o(x,y)$ are the same as above. The terms $\delta(x,y), E_o(x,y), E'_o(x,y), W, H$ validate the encryption framework's differential security properties, ensuring optimized robustness.

Execution time evaluates the computational efficiency of the FPO-IE framework. The average encryption and decryption times are computed to ensure that the system operates within acceptable performance thresholds. The total execution time T_{total} is expressed as Eq.(51).

$$T_{total} = T_{encrypt} + T_{decrypt} \quad (51)$$

where $T_{encrypt}$ is the encryption time, and $T_{decrypt}$ is the decryption time. The terms $T_{encrypt}, T_{decrypt}$ ensure that the framework balances security and performance, inspired by the optimized endurance of the Faroe pony.

Feedback integrates evaluation results into the framework, identifying areas for improvement. The optimization process adapts based on key metrics, ensuring that the system continuously evolves to meet security and performance standards. The optimization parameter $O(t)$ is updated iteratively as expressed in Eq.(52).

$$O(t+1) = O(t) - \eta \cdot \nabla L(O(t)) \quad (52)$$

where $O(t)$ represents the optimization parameters, η is the learning rate, and $\nabla L(O(t))$is the gradient of the loss function based on evaluation metrics. The terms $O(t), \eta, \nabla L(O(t))$ ensure that feedback drives the continuous improvement of the framework, reflecting the adaptive efficiency of the Faroe pony.

Algorithm 1: FPO-IE

Input:

- Medical image $I(x,y)$, chaotic map parameters $\mu, \gamma, r_x, r_y, r_z, \delta$, neural network parameters W, b, energy function $E(t)$, modulation function $\Phi(x,y)$, and optimization parameters $O(t)$.

Output:

- Encrypted image $E'(x,y)$, decrypted image $P'(x,y)$,performance metrics, and feedback for optimization.

Procedure:

1. Preprocessing:
   - Normalize pixel intensities of $I(x,y)$ to a uniform range.
   - Resize $I(x,y)$ to dimensions $W \times H$.
   - Apply noise reduction using adaptive filters.
2. Key Generation Initialization:
   - Generate initial chaotic sequences $C(x,y)$ using Logistic, Tent, and 3D Logistic maps.
   - Initialize neural network parameters W and b.
3. Chaotic Sequence Generation:
   - Generate multidimensional chaotic sequences C_x, C_y for pixel shuffling and diffusion.
   - Combine sequences into a unified chaotic map.
4. Faore Pony-Inspired Optimization Initialization:
   - Compute stamina-based energy function $E(t)$.
   - Optimize neural network weights W and biases b.
5. Dynamic Pixel Shuffling:

- Shuffle pixel positions of $I(x,y)$ using chaotic sequences C_x, C_y.
- Apply position-based modulation for enhanced randomness.

6. Adaptive Diffusion:
   - Transform pixel intensities using chaotic maps and energy-scaled factors η.
   - Perform multilevel chaotic diffusion.
7. Key Refinement Through Neural Networks:
   - Refine keys $K'(x,y)$ using multi-layer neural networks.
   - Maximize entropy of refined keys.
8. Encryption Execution:
   - Encrypt pixels $E'(x,y) = D(x,y) \oplus K'(x,y)$.
   - Apply multi-layer chaotic transformations.
9. Encrypted Image Transmission:
   - Encode $E'(x,y)$ for secure transmission.
   - Apply error control codes and dynamic bandwidth allocation.
10. Decryption Using Reverse Operations:
    - Decrypt $D'(x,y)$ by reversing XOR operations with $K'(x,y)$
    - Reverse chaotic transformations and diffusion.
11. Performance Evaluation and Feedback:
    - Evaluate SSIM, NPCR, UACI, and execution time.
    - Update optimization parameters $O(t)$ using feedback.

4. ABOUT DATASET

The Brain Tumor MRI Dataset consists of 7,023 MRI images categorized into glioma, meningioma, pituitary, and no tumor classes. Sourced from multiple repositories, it offers a diverse collection of brain scans. While conventionally employed for brain tumor detection and classification, this study utilizes the dataset for medical image encryption to ensure secure transmission in networked environments. Given the sensitivity of medical data, encryption mechanisms play a crucial role in preserving confidentiality, integrity, and authenticity. The dataset's high-resolution images provide a suitable test bed for evaluating encryption strategies that mitigate unauthorized access and data breaches. Variability in image dimensions necessitates preprocessing steps to standardize inputs before encryption. By addressing the challenges associated with medical image security, this research strengthens the foundation for privacy-preserving techniques in digital healthcare systems, ensuring that patient data remains protected during storage and transmission across networked infrastructures. The dataset is publicly available at: https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset.

5. RESULTS AND DISCUSSION

The Results and Discussion section presents the analytical findings of the proposed encryption framework, comparing performance metrics such as entropy, NPCR, and UACI with existing methods. This section interprets the results, evaluates encryption robustness, and discusses the implications of observed patterns, ensuring a comprehensive assessment of security effectiveness. Structural Similarity Index (SSIM) quantifies image quality by assessing structural resemblance between an original and processed image. Higher SSIM values indicate minimal distortion, ensuring visual integrity in encryption schemes. The evaluation of ME-HCS, AMIE, and FPO-IE reveals distinct performance variations in image preservation post-encryption.

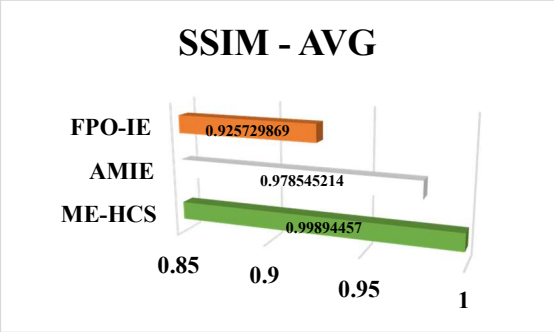

Figure 3: SSIM

ME-HCS achieves the highest SSIM value of 0.9989, signifying minimal structural distortion and near-perfect image quality retention. AMIE follows with 0.9785, reflecting a strong balance between encryption security and image preservation. FPO-IE attains 0.9257, demonstrating a trade-off favoring encryption robustness over structural similarity. Despite exhibiting a lower SSIM than ME-HCS and AMIE, FPO-IE prioritizes higher entropy and security resilience, ensuring encrypted images remain unpredictable. The decrease in SSIM suggests enhanced randomness in pixel distribution, reinforcing protection against adversarial attacks. This balance between encryption strength and structural retention positions FPO-IE as a robust framework for secure medical image transmission. Figure 3 illustrates the outcome of the framework evaluated under SSIM.

Entropy measures the randomness of pixel intensity distribution in an image, with higher values indicating greater unpredictability and encryption strength. The comparative analysis of ME-HCS, AMIE, and FPO-IE highlights variations in entropy levels before and after encryption. ME-HCS records

an initial entropy of 7.26, increasing to 7.5359, yielding an entropy difference of 0.2759. AMIE shows a slightly higher initial entropy of 7.32, reaching 7.5970, with a difference of 0.2770. FPO-IE exhibits the highest entropy enhancement, rising from 7.38 to 7.6641, achieving a difference of 0.2841. The superior entropy increase in FPO-IE signifies enhanced pixel randomness, making encrypted images less predictable and more resistant to statistical attacks. While ME-HCS and AMIE maintain structural integrity, FPO-IE prioritizes encryption robustness, reinforcing its suitability for secure medical image transmission. This balance ensures optimal security without compromising essential visual information. Figure 4 exhibits the outcome of FPO-IE under entropy.

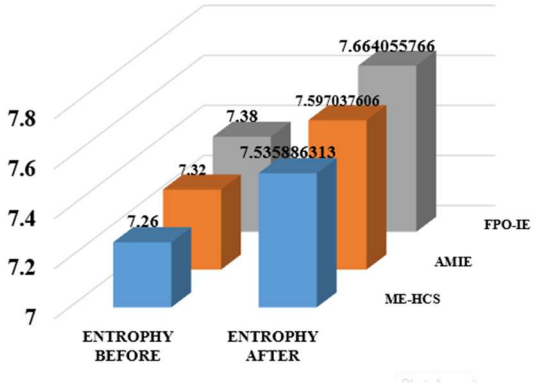

Figure 4: Entropy

Entropy quantifies the randomness of pixel intensity distribution in an image, serving as a critical measure of encryption effectiveness. A higher entropy value indicates stronger encryption, ensuring greater resistance to statistical and differential attacks. The comparative analysis of ME-HCS, AMIE, and FPO-IE highlights significant variations in entropy levels before and after encryption, demonstrating each framework's effectiveness in securing medical images. ME-HCS starts with an entropy of 7.26, increasing to 7.5359, reflecting an entropy difference of 0.2759. AMIE exhibits a slightly higher initial entropy of 7.32, reaching 7.5970, with a difference of 0.2770. FPO-IE demonstrates the highest entropy gain, rising from 7.38 to 7.6641, achieving a difference of 0.2841. These values confirm that all three frameworks enhance randomness, though FPO-IE ensures greater unpredictability in pixel distribution. The higher entropy difference in FPO-IE signifies increased encryption complexity, making the encrypted image more resistant to unauthorized decryption attempts. While ME-HCS and AMIE balance encryption strength with image retention, FPO-IE prioritizes robustness, ensuring secure medical image transmission. The observed entropy improvement across all frameworks validates their effectiveness, with FPO-IE offering the most secure encryption due to its superior entropy enhancement.

Number of Pixel Change Rate (NPCR) measures the effectiveness of an encryption algorithm by evaluating how many pixel values change in the encrypted image when a single pixel in the original image is altered. A higher NPCR value indicates stronger security, ensuring that minor modifications in the input lead to significant transformations in the output, preventing statistical and differential attacks.

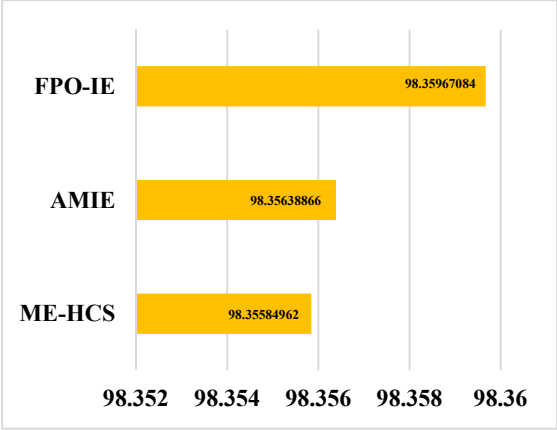

Figure 5: NPCR

The NPCR values for ME-HCS, AMIE, and FPO-IE exhibit minimal variations but remain consistently above 98.35%, validating the robustness of all three encryption methods. ME-HCS achieves 98.3558%, AMIE records 98.3563%, while FPO-IE attains the highest NPCR at 98.3597%. The marginally superior NPCR in FPO-IE signifies a more effective pixel diffusion mechanism, ensuring that encrypted images remain highly sensitive to minor input changes. Figure 5 shows the outcome under NPCR. The observed values confirm that all frameworks maintain strong encryption resilience, making decryption attempts nearly impossible without the correct key. The higher NPCR in FPO-IE suggests its enhanced ability to distribute pixel modifications more effectively across the encrypted image. This capability is crucial for secure medical image transmission, as it prevents unauthorized access and ensures data integrity, safeguarding patient records from adversarial threats and unauthorized tampering.

Unified Average Changing Intensity (UACI) quantifies the intensity variation between the original and encrypted images. It evaluates how much the pixel values have changed on average, ensuring that encryption effectively obscures the original content while maintaining structural complexity. A higher UACI value indicates better encryption performance, making it harder to identify patterns in the encrypted image.

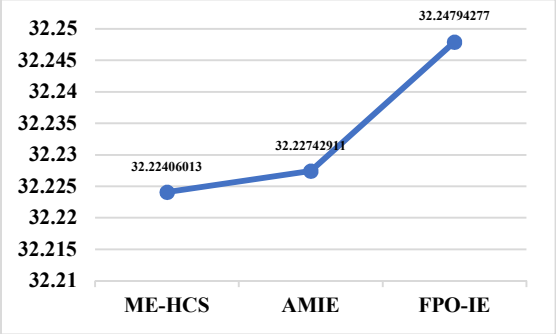

Figure 6: UACI

Figure 6 shows the outcome under UACI. The UACI values for ME-HCS, AMIE, and FPO-IE remain within the expected range of 32% - 35%, validating the encryption effectiveness. ME-HCS records 32.2240%, AMIE achieves 32.2274%, while FPO-IE attains the highest value of 32.2479%. The slight improvement in FPO-IE's UACI confirms its superior intensity transformation, reinforcing security against visual cryptanalysis. Higher UACI ensures that encrypted images exhibit significant intensity variation, preventing adversaries from reconstructing the original content through statistical attacks. The marginally greater UACI in FPO-IE indicates a more efficient diffusion mechanism, ensuring that pixel intensity changes are well-distributed across the encrypted image. This property enhances security by eliminating residual visual patterns, making it an ideal choice for safeguarding medical image confidentiality while ensuring high encryption unpredictability.

The Avalanche Effect determines how significantly the encrypted output changes when a slight alteration is made to the input or encryption key. In a highly secure encryption system, a minor change in the input should result in a substantial transformation in the encrypted output, ensuring unpredictability and resistance to cryptographic attacks. The observed Avalanche Effect values for ME-HCS, AMIE, and FPO-IE hover around 49.77% - 49.79%, signifying a strong sensitivity to minor modifications. ME-HCS records 49.7792%, AMIE attains 49.7819%, while FPO-IE achieves the highest value of 49.7983%.

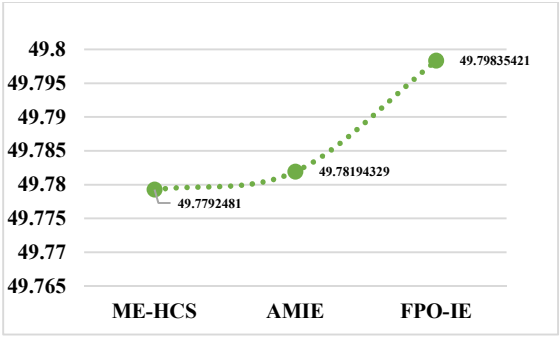

Figure 7: Avalanche Effect

The increased Avalanche Effect in FPO-IE suggests a superior diffusion process, ensuring that even minimal input alterations generate widespread and unpredictable transformations in the encrypted image. Figure 7 Illustrates the Avalanche Effect outcome. A strong Avalanche Effect is crucial for encryption resilience, preventing attackers from deriving patterns or identifying correlations between the original and encrypted images. The consistently high values across all frameworks validate their ability to resist differential attacks, reinforcing security in medical image encryption. FPO-IE's slightly improved Avalanche Effect demonstrates its capability to maximize randomness and unpredictability, enhancing security by ensuring that no meaningful patterns persist in the encrypted output, making it an optimal choice for privacy-preserving telemedicine applications.

6. CONCLUSION

The proposed Faore Pony-Inspired Optimization for Chaotic Neural Encryption introduces a secure and efficient approach to medical image encryption. The methodology enhances unpredictability through chaotic dynamics while ensuring robust encryption through optimized key evolution. The integration of adaptive pixel diffusion mechanisms reinforces the security framework, making it resistant to statistical and differential attacks. The framework effectively disrupts structural correlations in medical images, ensuring confidentiality in telemedicine applications. By employing chaotic sequences with an optimized transformation strategy, encrypted images maintain high levels of randomness, preventing unauthorized access or reconstruction. The adaptability of the optimization model enables dynamic response to varying encryption demands, making it suitable for diverse medical imaging scenarios. The enhanced

security of the proposed method contributes to ensuring medical data privacy while maintaining computational efficiency. The results demonstrate a well-balanced trade-off between encryption complexity and real-time processing requirements. The optimized chaotic neural encryption approach strengthens the resilience of transmitted medical images, minimizing vulnerability to adversarial threats. The encryption strategy aligns with the growing demand for secure digital healthcare solutions, ensuring safe transmission of sensitive medical records. This work paves the way for future enhancements in secure image encryption by integrating advanced bio-inspired optimization models with chaos-based transformations.

REFERENCES

[1] X. Zhou, K. Yang, and R. Duan, "Deep Learning Based on Striation Images for Underwater and Surface Target Classification," *IEEE Signal Process Lett*, vol. 26, no. 9, pp. 1378–1382, 2019, doi: 10.1109/LSP.2019.2919102.

[2] M. Al Duhayyim *et al.*, "Improved Multileader Optimization with Shadow Encryption for Medical Images in IoT Environment," *Computers, Materials and Continua*, vol. 74, no. 2, pp. 3133–3149, 2022, doi: https://doi.org/10.32604/cmc.2023.03274-0

[3] Y. Fan *et al.*, "A Multi-Watermarking Algorithm for Medical Images Using Inception V3 and DCT," *Computers, Materials and Continua*, vol. 74, no. 1, pp. 1279–1302, 2022, doi: https://doi.org/10.32604/cmc.2023.031445

[4] S. Inam, S. Kanwal, A. Anwar, N. Fatima Mirza, and H. Alfraihi, "Security of End-to-End medical images encryption system using trained deep learning encryption and decryption network," *Egyptian Informatics Journal*, vol. 28, p. 100541, 2024, doi: https://doi.org/10.1016/j.eij.2024.100541.

[5] F. A. Özbay, "A modified seahorse optimization algorithm based on chaotic maps for solving global optimization and engineering problems," *Engineering Science and Technology, an International Journal*, vol. 41, p. 101408, 2023, doi: https://doi.org/10.1016/j.jestch.2023.101408.

[6] S. Solak, A. M. Abdirashid, A. Adjevi, and A. K. Sahu, "Robust data hiding method based on frequency coefficient variance in repetitive compression," *Engineering Science and Technology, an International Journal*, vol. 56, p. 101756, 2024, doi: https://doi.org/10.1016/j.jestch.2024.101756.

[7] E. R. P. and M. D.S., "Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model," High-Confidence Computing, vol. 3, no. 2, p. 100126, 2023, doi: https://doi.org/10.1016/j.hcc.2023.100126

[8] U. S. Basha, S. K. Gupta, W. Alawad, S. Kim, and S. Bharany, "Fortifying Healthcare Data Security in the Cloud: A Comprehensive Examination of the EPM-KEA Encryption Protocol," *Computers, Materials and Continua*, vol. 79, no. 2, pp. 3397–3416, 2024, doi: https://doi.org/10.32604/cmc.2024.046265

[9] S. U. Jan, A. Ghani, A. Alzahrani, S. M. Saqlain, K. Yahya, and H. Sajjad, "Bandwidth and power efficient lightweight authentication scheme for healthcare system☆☆☆☆☆☆," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101601, 2023, doi: https://doi.org/10.1016/j.jksuci.2023.101601.

[10] S. Gherairi, "Healthcare: A priority-based energy harvesting scheme for managing sensor nodes in WBANs," *Ad Hoc Networks*, vol. 133, p. 102876, 2022, doi: https://doi.org/10.1016/j.adhoc.2022.102876.

[11] I. Makhdoom, M. Abolhasan, J. Lipman, M. Piccardi, and D. Franklin, "PrivySeC: A secure and privacy-compliant distributed framework for personal data sharing in IoT ecosystems," *Blockchain: Research and Applications*, vol. 5, no. 4, p. 100220, 2024, doi: https://doi.org/10.1016/j.bcra.2024.10022-0.

[12] O. S. Faragallah, M. Farouk, and H. S. El-Sayed, "Secret Key Optimization for Secure Speech Communications," *Computers, Materials and Continua*, vol. 72, no. 2, pp. 3025–3037, 2022, doi: https://doi.org/10.32604/cmc.2022.01995.

[13] J. Ahmad, M. Al Qathrady, M. S. Alshehri, Y. Y. Ghadi, M. U. Rehman, and S. A. Shah, "A Novel Parallel Computing Confidentiality Scheme Based on Hindmarsh-Rose Model," *Computers, Materials and Continua*, vol. 76, no. 2, pp. 1325–1341, 2023, doi: https://doi.org/10.32604/cmc.2023.040858.

[14] M. F. Khan *et al.*, "Construction and Optimization of TRNG Based Substitution Boxes for Block Encryption Algorithms," *Computers, Materials and Continua*, vol. 73, no. 2, pp. 2679–2696, 2022, doi: https://doi.org/10.32604/cmc.2022.027655

[15] X. Li and Y. Ling, "Research and application of pseudorandom sequence based on Xor," *Procedia Comput Sci*, vol. 183, pp. 814–819,

2021, doi: https://doi.org/10.1016/j.procs.2021.03.003.
[16] R. Zhang, R. Shu, Y. Wei, H. Zhang, and X. Wu, "A Novel S-Box Generation Methodology Based on the Optimized GAN Model," *Computers, Materials and Continua*, vol. 76, no. 2, pp. 1911–1927, 2023, doi: https://doi.org/10.32604/cmc.2023.041187
[17] M. Alawida, J. Sen Teh, A. Mehmood, A. Shoufan, and W. H. Alshoura, "A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Part A, pp. 8136–8151, 2022, doi: https://doi.org/10.1016/j.jksuci.2022.07.025.
[18] J. Ramkumar, K. S. Jeen Marseline, and D. R. Medhunhashini, "Relentless Firefly Optimization-Based Routing Protocol (RFORP) for Securing Fintech Data in IoT-Based Ad-Hoc Networks," *International Journal of Computer Networks and Applications*, vol. 10, no. 4, pp. 668–687, Aug. 2023, doi: 10.22247/ijcna/2023/223319.
[19] J. Ramkumar, V. Valarmathi, D. R. Medhunhashini, and R. Karthikeyan, "Jaguar-Based Routing Protocol (JRP) For Improved Reliability And Reduced Packet Loss In Drone Ad-Hoc Networks (DANET)," *J Theor Appl Inf Technol*, vol. 31, no. 2, 2025, [Online]. Available: www.jatit.org
[20] R. Karthikeyan and R. Vadivel, "Predator an Innovative Routing Protocol for Efficient Node Exploration and Faulty Link Detection in Wireless Sensor Network Environments," in *Proceedings of International Conference on Intelligent Vision and Computing (ICIVC 2023)*, A. K. Saha, H. Sharma, and M. Prasad, Eds., Cham: Springer Nature Switzerland, 2024, pp. 162–173.
[21] Y. Su, X. Wang, and H. Gao, "Chaotic image encryption algorithm based on bit-level feedback adjustment," *Inf Sci (N Y)*, vol. 679, p. 121088, 2024, doi: https://doi.org/10.1016/j.ins.2024.121088
[22] C. Cai, Y. Cao, H. Jahanshahi, J. Mou, and B. Sun, "2D and 3D compatible chaotic image encryption system based on checkers rules and shift register," *J Franklin Inst*, vol. 361, no. 9, p. 106874, 2024, doi: https://doi.org/10.1016/j.jfranklin.2024.106874 .B. Wang *et al.*, "A multiple-image encryption method based on bimodal biometric keys," *Opt Commun*, vol. 565, p. 130651, 2024, doi: https://doi.org/10.1016/j.optcom.2024.130651.
[23] Panwar, G. Biban, R. Chugh, A. Tassaddiq, and R. Alharbi, "An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images," *Heliyon*, vol. 10, no. 11, p. e31618, 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e31618.
[24] Mansouri *et al.*, "A secure medical image encryption algorithm for IoMT using a Quadratic-Sine chaotic map and pseudo-parallel confusion-diffusion mechanism," *Expert Syst Appl*, vol. 270, p. 126521, 2025,doi:https://doi.org/10.1016/j.eswa.2025.126521.
[25] Y. Su *et al.*, "Multiple-image encryption based on authenticable phase and phase retrieval under structured light illumination," *Opt Commun*, vol. 564, p. 130603, 2024, doi: https://doi.org/10.1016/j.optcom.2024.130603.
[26] X. Jiang *et al.*, "Reservoir computing based encryption-then-compression scheme of image achieving lossless compression," *Expert Syst Appl*, vol. 256, p. 124913, 2024, doi: https://doi.org/10.1016/j.eswa.2024.124913.
[27] Y. Li, C. Li, Y. Li, I. Moroz, and Y. Yang, "A joint image encryption based on a memristive Rulkov neuron with controllable multistability and compressive sensing," *Chaos Solitons Fractals*, vol. 182, p. 114800, 2024, doi: https://doi.org/10.1016/j.chaos.2024.114800.
[28] M. Alawida, "A novel DNA tree-based chaotic image encryption algorithm," *Journal of Information Security and Applications*, vol. 83, p. 103791, 2024, doi: https://doi.org/10.1016/j.jisa.2024.103791.
[29] X. Zhang, G. Liu, and C. Zou, "An image encryption method based on improved Lorenz chaotic system and Galois field," *Appl Math Model*, vol. 131, pp. 535–558, 2024, doi: https://doi.org/10.1016/j.apm.2024.04.023.
[30] A. A. Al-Barakati, F. Mesdoui, S. Bekiros, S. Kaçar, and H. Jahanshahi, "A variable-order fractional memristor neural network: Secure image encryption and synchronization via a smooth and robust control approach," *Chaos Solitons Fractals*, vol. 186, p. 115135, 2024, doi: https://doi.org/10.1016/j.chaos.2024.115135.
[31] M. Zhang, Y. Wan, T. Man, H. Zhou, W. Zhang, and Z. Liu, "Multiple images simultaneous encryption and decryption via deep-learning assisted interferenceless coded aperture correlation holography," *Opt Commun*, vol. 573, p. 131018, 2024, doi: https://doi.org/10.1016/j.optcom.2024.131018.

[32] A. Bencherqui *et al.*, "Optimal algorithm for color medical encryption and compression images based on DNA coding and a hyperchaotic system in the moments," *Engineering Science and Technology, an International Journal*, vol. 50, p. 101612, 2024, doi: https://doi.org/10.1016/j.jestch.2023.101612.

[33] F. Alqahtani, "AI-Powered Image Security: Utilizing Autoencoders for Advanced Medical Image Encryption," *CMES - Computer Modeling in Engineering and Sciences*, vol. 141, no. 2, pp. 1709–1724, 2024, doi: https://doi.org/10.32604/cmes.2024.054976.

[34] B. Suchitra, J. Ramkumar, and R. Karthikeyan, "Frog Leap Inspired Optimization-Based Extreme Learning Machine For Accurate Classification Of Latent Autoimmune Diabetes In Adults (LADA)," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 2, pp. 472–494, 2025, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85217140979&partnerID=40&md5=9540433c16d5ff0f6c2de4b8c43a4812

[35] J. Ramkumar, V. Valarmathi, and R. Karthikeyan, "Optimizing Quality of Service and Energy Efficiency in Hazardous Drone Ad-Hoc Networks (DANET) Using Kingfisher Routing Protocol (KRP)," *Int. J. Eng. Trends Technol.*, vol. 73, no. 1, pp. 410–430, 2025, doi: 10.14445/22315381/IJETT-V73I1P135.

[36] R. Jaganathan, S. Mehta, and R. Krishan, "Preface," *Bio-Inspired Intell. Smart Decis.*, pp. xix–xx, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85195725049&partnerID=40&md5=7a2aa7adc005662eebc12ef82e3bd19f

[37] J. Ramkumar, B. Varun, V. Valarmathi, D. R. Medhunhashini, and R. Karthikeyan, "Jaguar-Based Routing Protocol (Jrp) For Improved Reliability And Reduced Packet Loss In Drone Ad-Hoc Networks (DANET)," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 2, pp. 696–713, 2025, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85217213044&partnerID=40&md5=e38a375e46cf43c95d6702a3585a7073

[38] J. Ramkumar and R. Vadivel, "Multi-Adaptive Routing Protocol for Internet of Things based Ad-hoc Networks," *Wirel. Pers. Commun.*, vol. 120, no. 2, pp. 887–909, Apr. 2021, doi: 10.1007/s11277-021-08495-z.

[39] A. Senthilkumar, J. Ramkumar, M. Lingaraj, D. Jayaraj, and B. Sureshkumar, "Minimizing Energy Consumption in Vehicular Sensor Networks Using Relentless Particle Swarm Optimization Routing," *Int. J. Comput. Networks Appl.*, vol. 10, no. 2, pp. 217–230, 2023, doi: 10.22247/ijcna/2023/220737.

[40] S. P. Priyadharshini and J. Ramkumar, "Mappings Of Plithogenic Cubic Sets," *Neutrosophic Sets Syst.*, vol. 79, pp. 669–685, 2025, doi: 10.5281/zenodo.14607210.

[41] J. Ramkumar and R. Vadivel, "Improved Wolf prey inspired protocol for routing in cognitive radio Ad Hoc networks," *Int. J. Comput. Networks Appl.*, vol. 7, no. 5, pp. 126–136, 2020, doi: 10.22247/ijcna/2020/202977.

[42] R. Jaganathan and R. Vadivel, "Intelligent Fish Swarm Inspired Protocol (IFSIP) for Dynamic Ideal Routing in Cognitive Radio Ad-Hoc Networks," *Int. J. Comput. Digit. Syst.*, vol. 10, no. 1, pp. 1063–1074, 2021, doi: 10.12785/ijcds/100196.

[43] J. Ramkumar and R. Vadivel, "CSIP—cuckoo search inspired protocol for routing in cognitive radio ad hoc networks," in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2017, pp. 145–153. doi: 10.1007/978-981-10-3874-7_14.

[44] S. P. Geetha, N. M. S. Sundari, J. Ramkumar, and R. Karthikeyan, "Energy Efficient Routing In Quantum Flying Ad Hoc Network (Q-Fanet) Using Mamdani Fuzzy Inference Enhanced Dijkstra's Algorithm (MFI-EDA)," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 9, pp. 3708–3724, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85197297302&partnerID=40&md5=72d51668bee6239f09a59d2694df67d6

[45] M. P. Swapna, J. Ramkumar, and R. Karthikeyan, "Energy-Aware Reliable Routing with Blockchain Security for Heterogeneous Wireless Sensor Networks," in *Lecture Notes in Networks and Systems*, V. Goar, M. Kuri, R. Kumar, and T. Senjyu, Eds., Springer Science and Business Media Deutschland GmbH, 2025, pp. 713–723. doi: 10.1007/978-981-97-6106-7_43.

[46] J. Ramkumar, K. S. Jeen Marseline, and D. R. Medhunhashini, "Relentless Firefly Optimization-Based Routing Protocol (RFORP) for Securing Fintech Data in IoT-Based Ad-Hoc Networks," *Int. J. Comput. Networks Appl.*, vol. 10, no. 4, pp. 668–687, 2023, doi: 10.22247/ijcna/2023/223319.

[47] K. S. J. Marseline, J. Ramkumar, and D. R. Medhunhashini, "Sophisticated Kalman Filtering-Based Neural Network for Analyzing Sentiments in Online Courses," in *Smart Innovation, Systems and Technologies*, A. K. Somani, A. Mundra, R. K. Gupta, S. Bhattacharya, and A. P. Mazumdar, Eds., Springer Science and Business Media Deutschland GmbH, 2024, pp. 345–358. doi: 10.1007/978-981-97-3690-4_26.

[48] J. Ramkumar and R. Vadivel, "Whale optimization routing protocol for minimizing energy consumption in cognitive radio wireless sensor network," *Int. J. Comput. Networks Appl.*, vol. 8, no. 4, pp. 455–464, 2021, doi: 10.22247/ijcna/2021/209711.

[49] M. P. Swapna and J. Ramkumar, "Multiple Memory Image Instances Stratagem to Detect Fileless Malware," in *Communications in Computer and Information Science*, S. Rajagopal, K. Popat, D. Meva, and S. Bajeja, Eds., Springer Science and Business Media Deutschland GmbH, 2024, pp. 131–140. doi: 10.1007/978-3-031-59100-6_11.

[50] D. Jayaraj, J. Ramkumar, M. Lingaraj, and B. Sureshkumar, "AFSORP: Adaptive Fish Swarm Optimization-Based Routing Protocol for Mobility Enabled Wireless Sensor Network," *Int. J. Comput. Networks Appl.*, vol. 10, no. 1, pp. 119–129, 2023, doi: 10.22247/ijcna/2023/218516.

[51] M. Lingaraj, T. N. Sugumar, C. S. Felix, and J. Ramkumar, "Query aware routing protocol for mobility enabled wireless sensor network," *Int. J. Comput. Networks Appl.*, vol. 8, no. 3, pp. 258–267, 2021, doi: 10.22247/ijcna/2021/209192.

[52] R. Jaganathan, S. Mehta, and R. Krishan, *Bio-Inspired intelligence for smart decision-making*. IGI Global, 2024. doi: 10.4018/9798369352762.

[53] R. Vadivel and J. Ramkumar, "QoS-enabled improved cuckoo search-inspired protocol (ICSIP) for IoT-based healthcare applications," in *Incorporating the Internet of Things in Healthcare Applications and Wearable Devices*, IGI Global, 2019, pp. 109–121. doi: 10.4018/978-1-7998-1090-2.ch006.

[54] J. Ramkumar, R. Karthikeyan, and M. Lingaraj, "Optimizing IoT-Based Quantum Wireless Sensor Networks Using NM-TEEN Fusion of Energy Efficiency and Systematic Governance," in *Lecture Notes in Electrical Engineering*, V. Shrivastava, J. C. Bansal, and B. K. Panigrahi, Eds., Springer Science and Business Media Deutschland GmbH, 2025, pp. 141–153. doi: 10.1007/978-981-97-6710-6_12.

[55] J. Ramkumar, R. Karthikeyan, and V. Valarmathi, "Alpine Swift Routing Protocol (ASRP) for Strategic Adaptive Connectivity Enhancement and Boosted Quality of Service in Drone Ad Hoc Network (DANET)," *Int. J. Comput. Networks Appl.*, vol. 11, no. 5, pp. 726–748, 2024, doi: 10.22247/ijcna/2024/45.

[56] P. Menakadevi and J. Ramkumar, "Robust Optimization Based Extreme Learning Machine for Sentiment Analysis in Big Data," in *2022 International Conference on Advanced Computing Technologies and Applications, ICACTA 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICACTA54488.2022.9753203.

[57] J. Ramkumar, A. Senthilkumar, M. Lingaraj, R. Karthikeyan, and L. Santhi, "Optimal Approach For Minimizing Delays In Iot-Based Quantum Wireless Sensor Networks Using Nm-Leach Routing Protocol," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 3, pp. 1099–1111, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85185481011&partnerID=40&md5=bf0ff974ceabc0ad58e589b28797c684

[58] J. Ramkumar and R. Vadivel, "Improved frog leap inspired protocol (IFLIP) – for routing in cognitive radio ad hoc networks (CRAHN)," *World J. Eng.*, vol. 15, no. 2, pp. 306–311, 2018, doi: 10.1108/WJE-08-2017-0260.

[59] R. Jaganathan, S. Mehta, and R. Krishan, *Intelligent Decision Making Through Bio-Inspired Optimization*. IGI Global, 2024. doi: 10.4018/979-8-3693-2073-0.

[60] R. Jaganathan and V. Ramasamy, "Performance modeling of bio-inspired routing protocols in Cognitive Radio Ad Hoc Network to reduce end-to-end delay," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 1, pp. 221–231, 2019, doi: 10.22266/IJIES2019.0228.22.

[61] R. Karthikeyan and R. Vadivel, "Boosted Mutated Corona Virus Optimization Routing Protocol (BMCVORP) for Reliable Data Transmission with Efficient Energy Utilization," *Wirel. Pers. Commun.*, vol. 135, no. 4, pp. 2281–2301, 2024, doi: 10.1007/s11277-024-11155-7.

[62] R. Karthikeyan and R. Vadivel, "Proficient Dazzling Crow Optimization Routing Protocol (PDCORP) for Effective Energy Administration in Wireless Sensor Networks," in *IEEE International Conference on Electrical,*

Electronics, Communication and Computers, ELEXCOM 2023, 2023, pp. 1–6. doi: 10.1109/ELEXCOM58812.2023.10370559.

[63] N. K. Ojha, A. Pandita, and J. Ramkumar, "Cyber security challenges and dark side of AI: Review and current status," in *Demystifying the Dark Side of AI in Business*, 2024, pp. 117–137. doi: 10.4018/979-8-3693-0724-3.ch007.

[64] J. Ramkumar, S. S. Dinakaran, M. Lingaraj, S. Boopalan, and B. Narasimhan, "IoT-Based Kalman Filtering and Particle Swarm Optimization for Detecting Skin Lesion," in *Lecture Notes in Electrical Engineering*, K. Murari, N. Prasad Padhy, and S. Kamalasadan, Eds., Singapore: Springer Nature Singapore, 2023, pp. 17–27. doi: 10.1007/978-981-19-8353-5_2.

[65] J. Ramkumar, C. Kumuthini, B. Narasimhan, and S. Boopalan, "Energy Consumption Minimization in Cognitive Radio Mobile Ad-Hoc Networks using Enriched Ad-hoc On-demand Distance Vector Protocol," in *2022 International Conference on Advanced Computing Technologies and Applications, ICACTA 2022*, 2022. doi: 10.1109/ICACTA54488.2022.9752899.

[66] J. Ramkumar, R. Vadivel, and B. Narasimhan, "Constrained Cuckoo Search Optimization Based Protocol for Routing in Cloud Network," *Int. J. Comput. Networks Appl.*, vol. 8, no. 6, pp. 795–803, 2021, doi: 10.22247/ijcna/2021/210727.

[67] L. Mani, S. Arumugam, and R. Jaganathan, "Performance Enhancement of Wireless Sensor Network Using Feisty Particle Swarm Optimization Protocol," *ACM Int. Conf. Proceeding Ser.*, pp. 1–5, Dec. 2022, doi: 10.1145/3590837.3590907.