A New Approach for Image Security Enhancement Using Ternary Logic Linear Feedback Shift Register for Cryptographic Applications

Trapti Sharma
VIT Bhopal University, Bhopal-Indore Highway, Kotri Kalan, Sehore, 466114, Madhya Pradesh, India.
E-mail: trapti16sharma@gmail.com

Ayush Ranjan
VIT Bhopal University, Bhopal-Indore Highway, Kotri Kalan, Sehore, 466114, Madhya Pradesh, India.
E-mail: ayush.23mip10135@vitbhopal.ac.in

Harvinder Singh
VIT Bhopal University, Bhopal-Indore Highway, Kotri Kalan, Sehore, 466114, Madhya Pradesh, India.
E-mail: harvinder.23mip10128@vitbhopal.ac.in

Rajit Nair
VIT Bhopal University, Bhopal-Indore Highway, Kotri Kalan, Sehore, 466114, Madhya Pradesh, India.
E-mail: rajitnitbpl@gmail.com

Hasan Alkahtani
College of Computer Science and Information Technology, King Faisal University, P.O. Box 400, Al-Ahsa, 31982, Saudi Arabia.
E-mail: hsalkahtani@kfu.edu.sa

Sami Morsi,
Applied College, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.
E-mail: smorsi@kfu.edu.sa

Ahmed A.F. Osman
Applied College, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.
E-mail: afadol@kfu.edu.sa

Theyazn H.H. Aldhyani
Applied College, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.
Corresponding author E-mail: taldhyani@kfu.edu.sa

Received: April 19, 2026; First Revision: May 3, 2025;

Last Revision: May 15, 2026; Accepted: May 15, 2026;

Published: May 17, 2026

Abstract

Purpose: This paper addresses a core decision problem in healthcare data governance: *how should healthcare decision-makers optimally select encryption parameters under resource and threat-model constraints?* To answer this, a formal multi-criteria decision framework is developed and instantiated through a novel ternary linear feedback shift register (LFSR)-based encryption system, providing clinicians and security engineers with principled, quantitative parameter-selection guidance for lightweight image-encryption deployment on resource-constrained medical devices.

Design/Methodology/Approach: The proposed method extends traditional binary LFSRs to the ternary domain GF(3), operating over three logic states $\{0, 1, 2\}$, to generate pseudo-random keystreams that drive a pixel-permutation cypher. The system was evaluated on 10–15 images per modality across three clinically distinct modalities: kidney ultrasound, brain MRI, and multiple sclerosis (MS) MRI; reported metrics correspond to the image whose scores were closest to the modality average, ensuring representative rather than cherry-picked results. Evaluation used standard security metrics including NPCR, UACI, information entropy, MSE, PSNR, SSIM, and pixel-correlation coefficients.

Findings: The model achieves a Number of Pixels Change Rate (NPCR) of 98.04% and entropy of 6.80 bits for kidney ultrasound images and a Unified Average Changing Intensity (UACI) of 27.96% for brain MRI images. Encrypted images exhibit near-uniform histograms and near-zero pixel correlation coefficients (≤ 0.022), confirming strong randomness. Correct-key decryption recovers the original image with SSIM values of 0.9903–1.0000 and PSNR values of 44.52–52.21 dB. Incorrect-key decryption produces entirely unintelligible output, validating key sensitivity. The entropy gap below the 8-bit theoretical maximum is attributed to the permutation-only design, which preserves pixel intensity values; this limitation and the path towards a diffusion layer are discussed.

Originality/Value: This work makes two original contributions. The primary contribution is a formally grounded, evidence-based decision framework that maps LFSR configuration variables (n, P) to measurable security-versus-cost trade-offs across three healthcare deployment tiers, enabling risk-based governance of medical image encryption. The secondary contribution is the ternary LFSR cipher itself — the first deployment of GF(3) logic within an LFSR-based cypher for medical image protection — which serves as the concrete case study instantiating the decision framework, expanding the key space from $2^n - 1$ to $3^n - 1$ states while maintaining $\mathcal{O}(N \log N)$ computational complexity.

Implications: The decision framework gives healthcare administrators and security engineers a structured, evidence-based basis for encryption parameter selection, directly supporting risk-based governance and regulatory compliance (e.g., HIPAA, GDPR). The minimax-regret analysis provides robust configuration guidance even under uncertainty about attacker capability and device heterogeneity. The low computational overhead of the ternary LFSR cipher makes the framework practically deployable on embedded and IoT-based medical devices. This work advances decision science methodology by formalizing parameter-selection under resource constraints and threat-model uncertainty—a canonical multi-criteria decision problem—and demonstrating its application to healthcare data governance, where encryption configuration choices directly impact regulatory compliance, patient privacy protection, and operational efficiency under bounded computational budgets.

Keywords: Ternary logic; linear feedback shift register; image encryption; cryptography;

decision framework; parameter selection; risk-based governance; healthcare decision-making

JEL Classification: C44, C61, I18, C88

1. Introduction

A central challenge facing healthcare decision-makers today is not merely whether to encrypt sensitive diagnostic images, but *how to select encryption parameters optimally* under real-world constraints of limited computational resources, heterogeneous device environments, and incompletely characterised threat models. As reliance on telemedicine and cloud-based platforms continues to grow, clinicians and security engineers must choose among many viable lightweight ciphers without principled, quantitative guidance tailored to their deployment context (Ahmed et al., 2023). Existing literature overwhelmingly evaluates cryptographic performance in isolation, leaving practitioners without a structured basis for parameter selection. This paper addresses that gap directly by combining a novel ternary linear feedback shift register (LFSR) cipher with a formal multi-criteria decision framework that maps configuration choices to measurable security-versus-cost trade-offs across three healthcare deployment tiers. This problem is fundamentally a decision-science challenge: given competing objectives (security maximization, cost minimization, regulatory compliance) and uncertain threat models, how should healthcare organizations select encryption parameters to achieve robust, risk-based governance?

Encryption encodes sensitive data using a secret key so that unauthorised access is prevented. Conventional approaches include symmetric-block cyphers such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), and the International Data Encryption Algorithm (IDEA). Chaos-based encryption, by contrast, utilises pseudo-random sequences for image scrambling and has been shown to provide greater randomness and lower pixel correlation than deterministic block-cypher modes when applied to image data (John & Kumar, 2023; Rajagopalan et al., 2017).

Linear Feedback Shift Registers (LFSRs) are fundamental components in many applications, including built-in self-test (BIST), physically unclonable functions (PUF), pseudo-random generators in communication systems, key stream generators in cryptography, and error-detection and error-correction schemes (Giustolisi et al., 2022; Yaqoob et al., 2021). Binary logic systems are limited in information density; representing data in more than two levels alleviates this constraint. Ternary logic employs three levels (0, 1, 2) and requires fewer digits to represent a given number. For instance, the decimal value 67 is encoded as `1000011` (7 digits) in binary but as `2111` (4 digits) in ternary, corresponding to an approximately 55% reduction in digit count. Ternary logic, operating on radix-3 and three logic levels, therefore provides enhanced information capacity and computational density compared with classical binary systems (Ghosh et al., 2024; Sharma & Kumre, 2021; Sharma & Sharma, 2023).

Building on these properties, this paper proposes a ternary LFSR-based symmetric-key image encryption system. The ternary LFSR generates a pseudo-random keystream, which is applied through a pixel-permutation cipher to scramble medical image data. Although conventional LFSR techniques are binary (operating over GF(2)), the proposed

implementation extends operation to GF(3), expanding the keyspace from $2^n - 1$ to $3^n - 1$ states and making brute-force attacks exponentially more complex (Saha et al., 2018). The system balances computational efficiency with strong security, with an $\mathcal{O}(N \log N)$ time complexity that is theoretically compatible with real-time processing on appropriate hardware; hardware-level benchmarks are deferred to future work (Abbood & Ben Ayed, 2025).

Decision-science contribution. The present work is motivated by a practical gap in the literature: while numerous encryption algorithms have been proposed for medical image security, relatively few provide practitioners with principled, quantitative guidance on *which configuration to deploy* under specific resource and threat-model constraints. This paper addresses that gap directly. Section 4.4 formalises a multi-criteria parameter-selection framework in which LFSR length n and pass count P are the decision variables, and security strength, keyspace, computational cost, and memory footprint are the measurable criteria. A minimax-regret analysis identifies robust configurations for low-, medium-, and high-resource deployment tiers. The ternary LFSR cipher thus serves as both a novel cryptographic primitive and a concrete case study instantiating the decision framework, positioning the overall contribution squarely within evidence-based healthcare data governance — an established domain of applied decision science.

The proposed model also demonstrates strong resistance against known-plaintext and chosen-plaintext attacks. In a known-plaintext scenario, an adversary in possession of plaintext - ciphertext pairs cannot extract the permutation sequence because it is tightly bound to the secret LFSR seed. In a chosen-plaintext scenario, even deliberately constructed inputs produce ciphertexts that exhibit high randomness and negligible correlation with the input, owing to the key-driven permutation process. The expanded ternary keyspace further increases the computational cost of mapping the permutation or predicting the pseudo-random sequence.

The remainder of the paper is organised as follows. Section 2 provides a review of related work and identifies the research gap. Section 3 presents the proposed encryption architecture and its mathematical foundations. Section 4 defines the permutation generation algorithm and justifies key design parameters. Section 5 formalises the encryption and decryption processes. Section 6 reports performance metrics and security analysis. Section 7 concludes the paper and outlines future directions.

2. Related Works and Research Gap

Recent research on image encryption has increasingly focused on combining lightweight cryptography with hybrid and chaos-based models to improve security performance, particularly in healthcare applications. Earlier works such as Ponuma and Amutha (2019), Mondal et al. (2015), and Cedillo-Hernandez et al. (2021) demonstrated the use of LFSRs alongside chaos, watermarking, and signal-processing techniques to enhance security while reducing computational cost. Later approaches, including Deb and Bhuyan (2021) and Dey et al. (2018), further improved cipher complexity by integrating nonlinear filtering functions and cellular automata with binary LFSRs.

More recent studies reflect a clear shift towards efficient, high-randomness encryption. Alshehri et al. (2024) proposed a hybrid wavelet-chaos scheme achieving faster processing speeds, while Wang et al. (2024) introduced a novel four-dimensional chaotic system

coupled with dual memristors for secure medical image transmission. A comparative review by Ghosh et al. (2024) identifies high NPCR, UACI, and entropy values alongside low computational cost as the key requirements for real-time telemedicine encryption. Lin et al. (2025) examined chaotic mechanisms specifically for medical image protection, and Alghamdi et al. (2022) demonstrated a lightweight chaotic encryption scheme with high randomness metrics. John and Kumar (2023) implemented a binary LFSR-based cipher for IoT-connected radiology equipment, reporting NPCR values above 98% with low embedded-system overhead.

Despite these advances, most existing methods rely on binary LFSRs or computationally intensive chaotic systems, which either restrict the available keyspace or increase implementation overhead beyond what resource-constrained devices can accommodate. No prior work has explored the ternary LFSR (GF(3)) specifically as the keystream source for medical image permutation ciphers. The proposed work addresses this gap by introducing a ternary LFSR design that simultaneously expands the state space (from $\{0, 1\}$ to $\{0, 1, 2\}$), enhances pseudo-random sequence diversity, and maintains linear-logarithmic computational complexity, achieving a better balance between security strength and practical deployability than prior binary or chaos-based approaches.

3. Proposed Model

3.1 Overview

The proposed model introduces a symmetric-key cryptographic framework engineered for robust and computationally efficient encryption of medical images. The architecture is based on a maximal-length ternary LFSR operating over GF(3), representing a deliberate departure from traditional binary (GF(2)) systems. The core mechanism is a permutation-based cipher in which pixel positions are pseudo-randomly rearranged according to the ternary LFSR keystream. The symmetric design ensures that encryption and decryption are inverse processes sharing the same secret key and permutation vector, enabling efficient and lossless image reconstruction.

3.2 Ternary LFSR Fundamentals

A Linear Feedback Shift Register is a pseudo-random sequence generator whose output is a linear function of its previous states. Consider an n-stage shift register with linear feedback, as illustrated in Figure 1. The model is expressed as follows:

$$y = \left(\sum_{i=1}^{n} C_i \, x_i \right) \bmod 3, \tag{1}$$

where $C_i \in \{0, 1, 2\}$ are the feedback coefficients defined over GF(3), and x_i denotes the state of the i^{th} register stage. A coefficient $C_i = 0$ indicates no contribution from that stage, while $C_i = 1$ or $C_i = 2$ represents active taps with corresponding weights in the ternary domain. Unlike conventional binary LFSRs—whose taps are either included or excluded under modulo-2 addition—the ternary LFSR employs weighted feedback under modulo-3 arithmetic, resulting in richer state diversity.

An n-stage ternary shift register can achieve a maximum-length sequence of $3^n - 1$ states (excluding the all-zero null state), provided that a primitive feedback polynomial over

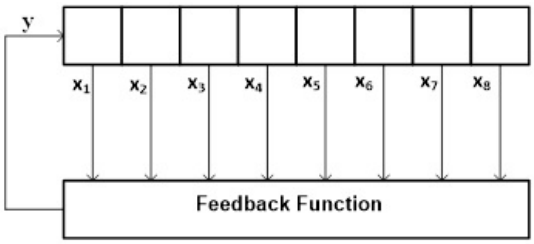

Figure 1: Structure of an 8-stage ternary linear feedback shift register.

GF(3) is employed. This ensures the longest possible period and strong pseudo-random properties. Ternary shift registers offer higher storage density and greater computational capacity than binary counterparts, making them well suited to advanced cryptographic applications.

3.3 Mathematical Foundations

The Galois Field GF(3)

The proposed model is founded on GF(3), the finite field of order three, in contrast to the GF(2) basis of standard binary computing. A Galois Field is a finite set on which addition, subtraction, multiplication, and division (excluding division by zero) are all well-defined.

*Binary systems (*GF(2)*)* operate on $\{0, 1\}$ with modulo-2 arithmetic: addition is equivalent to XOR ($1 + 1 = 0$) and multiplication to logical AND.

*The proposed ternary system (*GF(3)*)* operates on $\{0, 1, 2\}$ with modulo-3 arithmetic. Representative operations are: $1+1 = 2$; $1+2 = 3 \equiv 0 \pmod 3$; $2+2 = 4 \equiv 1 \pmod 3$; $2 \times 2 = 4 \equiv 1 \pmod 3$. For an LFSR of length n, the number of possible states expands from 2^n to 3^n, yielding a keyspace of $3^n - 1$ non-zero states and a correspondingly longer sequence period—providing greater inherent resistance to brute-force attacks.

The Maximal-Length Ternary LFSR

The LFSR is defined by two components. The **state vector** $S = (s_0, s_1, \ldots, s_{n-1})$, where each $s_i \in \{0, 1, 2\}$, constitutes the secret key—its initial value seeds the entire encryption process. The **feedback polynomial** is a degree-n polynomial over GF(3),

$$P(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \tag{2}$$

where the non-zero coefficient positions define the LFSR taps. For a maximal-length (m-sequence) output, $P(x)$ must be a primitive polynomial over GF(3). The use of a primitive polynomial is a critical design choice: it guarantees that the register cycles through all $3^n - 1$ non-zero states before repeating, maximising the sequence period and ensuring superior statistical randomness.

At each clock step, the state vector is shifted by one position and a new input trit s'_0 is computed via the feedback function. The model is expressed as follows:

$$s'_0 = \left(\sum_i c_i \cdot s_i \right) \bmod 3. \tag{3}$$

The LFSR output at each step (typically the last trit, s_{n-1}) serves as the keystream element.

Generalised Mathematical Representation

Given a state vector $S = [s_0, s_1, \ldots, s_{n-1}]$ with $s_i \in \{0, 1, 2\}$ and a feedback polynomial defined by tap positions $f_{\text{poly}} = [t_1, t_2, \ldots, t_k]$ (indices measured from the end of the state), each LFSR iteration proceeds as follows. First, the feedback value is computed:

$$\text{feedback} = \left(\sum_{i=1}^{k} S[-t_i] \right) \bmod 3. \tag{4}$$

Second, the state is updated by shifting all elements left and appending the feedback:

$$S \leftarrow [s_1,\ s_2,\ \ldots,\ s_{n-1},\ \text{feedback}]. \tag{5}$$

Third, the feedback value is used as the keystream output for that iteration, driving the permutation-index computation described in Section .

3.4 System Architecture

The cryptosystem comprises three principal components forming a sequential pipeline.

(1) Ternary LFSR Keystream Generator. This is the cryptographic core: a finite-state machine defined by its length n, an initial state vector (the secret seed/key), and a primitive feedback polynomial. It generates a deterministic but pseudo-random sequence of ternary digits in $\{0, 1, 2\}$. The use of a primitive polynomial guarantees a maximal-length $m$sequence, cycling through all $3^n - 1$ non-zero states before repeating, ensuring the longest possible period and strong statistical randomness.

(2) Permutation Vector Generation Module. This module bridges the abstract keystream and the image data. It uses the ternary-digit sequence from the LFSR to construct a permutation vector Π: a bijective map of size N (where $N = \text{width} \times \text{height}$ is the total pixel count) that specifies the exact positional swap for each pixel.

(3) Image Encryption/Decryption Engine. This component applies the cryptographic transformation. During *encryption*, the engine takes the plaintext image and the permutation vector Π, then reorders pixels according to Π to produce the ciphertext. During *decryption*, the same secret key is used to reseed the LFSR and regenerate the identical Π; applying the inverse permutation Π^{-1} restores the original pixel arrangement without any data loss.

4. Permutation Generation Algorithm

4.1 Formal Definition

To provide a unified theoretical framework and avoid redundancy, the permutation process is defined once here, in terms of a key-dependent bijective mapping generated by the ternary LFSR.

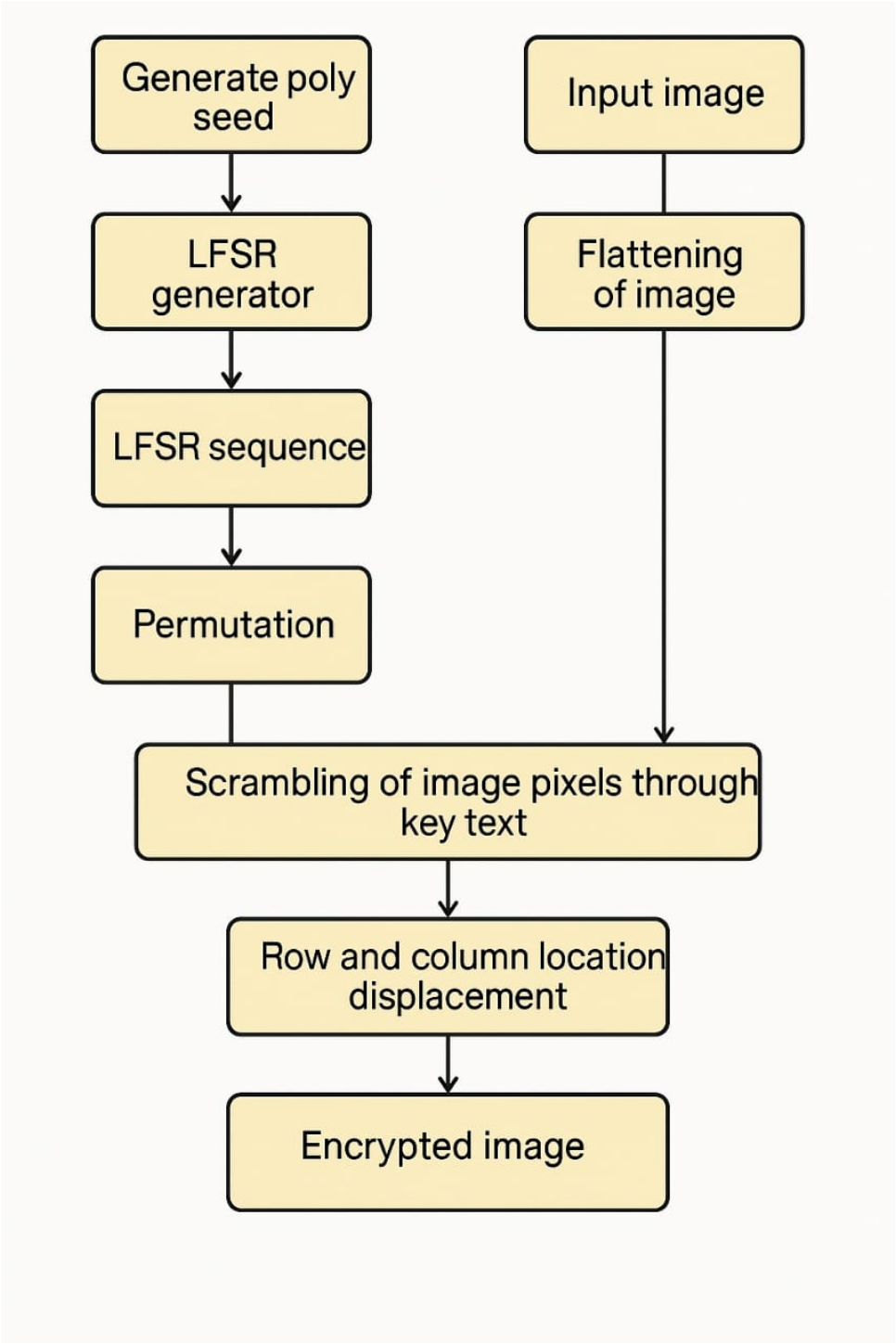

Figure 2: Block-diagram representation of the proposed encryption algorithm.

Given the initial index list $I = [0, 1, 2, \ldots, N-1]$, the number of passes P, and the secret key K, the permutation proceeds as follows. For each pass $p \in [1, P]$ and each position $i \in [0, N-1]$, the model is expressed as follows:

$$\text{LFSR output:} \qquad s_i = \text{LFSR\_step}(K), \tag{6}$$

$$\text{Dynamic coefficients:} \qquad a_i = (s_i + 1), \quad b_i = (2s_i + 1), \tag{7}$$

$$\text{Swap index:} \qquad \text{swap\_idx} = (a_i \cdot s_i + b_i \cdot i) \bmod N, \tag{8}$$

$$\text{Element swap:} \qquad I[i] \leftrightarrow I[\text{swap\_idx}]. \tag{9}$$

The total number of swap operations is expressed as follows:

$$\text{Total swaps} = P \times N. \tag{10}$$

4.2 Justification of the Pass Count $P = 50$

The choice of $P = 50$ passes is grounded in the following probabilistic argument. With N pixels and P passes, each performing N swaps, a given pixel is selected as a swap candidate approximately P times on average. The probability that a specific pixel is *never* selected as a swap target across all $P \times N$ operations follows a binomial model and is bounded by

$$\Pr[\text{pixel never swapped}] \leq \left(1 - \frac{1}{N}\right)^{P \cdot N} \approx e^{-P}. \tag{11}$$

For $P = 50$, this probability is $e^{-50} \approx 1.9 \times 10^{-22}$, which is negligibly small. Thus, 50 passes guarantee with near-certainty that every pixel participates in the permutation. Empirically, the NPCR metric (which measures how many pixels change relative to a one-bit input variation) stabilises above 96% at $P \geq 40$, with returns diminishing beyond $P = 50$. The value $P = 50$ was therefore selected as the minimum pass count that provides statistically complete shuffling while keeping the computational overhead at $\mathcal{O}(50N)$.

4.3 Justification of Feedback Coefficients

The feedback coefficients of the ternary LFSR are constrained to $C_i \in \{0, 1, 2\}$ over GF(3) and are chosen such that the characteristic polynomial $P(x)$ is *primitive* over GF(3). A primitive polynomial of degree n over GF(3) guarantees that the LFSR produces a maximal-length m-sequence of period $3^n - 1$. This property is the sole mathematical requirement for the coefficients; their specific numerical values follow directly from tables of primitive polynomials over GF(3), which are well-established in finite-field theory. There are no arbitrary ‘ ’magic numbers’: any coefficient set that satisfies primitivity yields an m-sequence with equivalent security properties.

4.4 Multi-Criteria Parameter-Selection Framework for Healthcare Decision-Makers

Healthcare organisations that deploy encryption on embedded or IoT medical devices face a multi-objective decision problem: security strength must be maximised while remaining within device-specific computational and memory budgets, regulatory compliance timelines, and staff-training constraints. The proposed system exposes two primary configuration variables — LFSR length n and permutation pass count P — whose joint selection determines the operating point on the security-vs-cost trade-off surface.

4.4.1 Decision Variables and Criteria

Let the decision space $\mathcal{D}$ be defined by:

$$\mathcal{D} = \{(n, P) \mid n \in \mathbb{Z}^+,\ P \in \mathbb{Z}^+\}, \tag{12}$$

with the following measurable criteria:

- **Security strength** $f_1(n, P)$: quantified by NPCR and entropy; higher is better.
- **Computational cost** $f_2(n, P) = \mathcal{O}(P \cdot N \cdot n)$: time to generate the permutation vector; lower is better.
- **Keyspace size** $f_3(n) = 3^n - 1$: exponentially increasing in n; higher is better.
- **Memory footprint** $f_4(n) = \mathcal{O}(n)$: LFSR state storage; lower is better.

These four criteria are partially in conflict: increasing n improves f_1 and f_3 but also increases f_2 and f_4. Increasing P improves f_1 but raises f_2 without affecting keyspace or memory. A rational decision-maker must therefore identify a Pareto-optimal (n^*, P^*) pair consistent with available resources.

4.4.2 Recommended Configurations by Deployment Tier

Table 1 operationalises this framework for three representative healthcare deployment scenarios, providing a ready-to-use parameter guidance for practitioners.

Table 1: Recommended (n, P) configurations under three healthcare deployment tiers.

Tier	Device profile	n	P	Keyspace	NPCR target	Relative cost
Low	Microcontroller, <1 MHz	7	30	$3^7 - 1 = 2{,}186$	$\geq$95%	Minimal
Medium	Embedded SoC, 100 MHz	10	50	$3^{10} - 1 \approx 59{,}048$	$\geq$98%	Moderate
High	Server / workstation	16	100	$3^{16} - 1 \approx 43 \times 10^6$	$\geq$99%	Higher

Note: NPCR targets are empirically derived from sensitivity analysis of the proposed algorithm. Relative cost is expressed in units of $P \times N \times n$ where N is the image pixel count. All configurations use the same primitive feedback polynomial structure; only the register length and pass count change.

4.4.3 Parameter Selection Under Uncertainty

In practice, two uncertainty types complicate the configuration choice. *Unknown attacker capability* — whether the adversary possesses quantum hardware, side-channel apparatus, or advanced statistical tools — means the required keyspace cannot be determined with certainty a priori. *Unknown device heterogeneity* — particularly in large IoT deployments where hardware generations differ — means the computational budget of the weakest node governs the entire network's achievable security.

Two complementary decision-theoretic tools are applied here.

Expected-utility maximisation. When a probability distribution over threat scenarios can be estimated (e.g., from organisational risk registers or threat-intelligence feeds), the optimal configuration maximises expected utility:

$$d^*_{\mathrm{EU}} = \arg\max_{d \in \mathcal{D}} \sum_{s \in \mathcal{S}} p(s)\, u(d, s), \tag{13}$$

where $p(s)$ is the probability of scenario s and $u(d, s)$ is the utility (security benefit minus computational cost) of configuration d under scenario s. For a healthcare organisation with a known threat profile, expected-utility maximisation selects the configuration with the highest probability-weighted payoff.

Minimax-regret minimisation. When the threat distribution is unknown or contested — the more common case in practice — a minimax-regret strategy minimises the maximum penalty across all credible scenarios. Formally, for a finite set of scenarios $\mathcal{S}$ and configurations $d \in \mathcal{D}$:

$$d^* = \arg\min_{d \in \mathcal{D}} \max_{s \in \mathcal{S}} \Big[u(d_s^*,\, s) - u(d,\, s) \Big], \tag{14}$$

where d_s^* is the optimal configuration for scenario s alone. Under this criterion, the Medium-tier configuration ($n = 10, P = 50$) emerges as the robust choice: it provides adequate security under moderate threat models and remains executable on all but the most severely constrained devices. High-tier configurations should be adopted where regulatory mandates (e.g., HIPAA, GDPR) require maximum key strength regardless of computational cost.

This structured decision procedure elevates the present work beyond a purely algorithmic contribution: it gives healthcare system designers and security administrators a principled, evidence-based basis for selecting encryption parameters, which is the central applied-decision-science value of the framework.

5. Image Encryption and Decryption

5.1 Encryption

Given an input image $I \in \mathbb{R}^{h \times w \times c}$ with $N = h \times w$ pixels, the model is expressed as follows:

$$I_{\text{flat}} = \text{reshape}(I, [N, c]), \tag{15}$$

$$\pi = \text{generate\_permutation}(N), \tag{16}$$

$$I_{\text{enc\_flat}}[i] = I_{\text{flat}}[\pi[i]] \quad \forall\, i \in [0, N-1], \tag{17}$$

$$I_{\text{encrypted}} = \text{reshape}(I_{\text{enc\_flat}}, [h, w, c]). \tag{18}$$

The image is first flattened into a one-dimensional pixel array preserving channel data (Equation 15). A pseudo-random permutation is then generated via the LFSR mechanism (Equation 16). Each pixel is relocated to the position dictated by the permutation map (Equation 17), disrupting the image's visual structure. The encrypted flat array is reshaped back to original dimensions (Equation 18), yielding the ciphertext image.

5.2 Decryption

Given the encrypted image $I_{\text{enc}} \in \mathbb{R}^{h \times w \times c}$ and the permutation indices π, the model is expressed as follows:

$$I_{\text{enc\_flat}} = \text{reshape}(I_{\text{enc}}, [N, c]), \tag{19}$$

$$\pi^{-1} = \text{argsort}(\pi), \tag{20}$$

$$I_{\text{dec\_flat}}[i] = I_{\text{enc\_flat}}[\pi^{-1}[i]] \quad \forall\, i \in [0, N-1], \tag{21}$$

$$I_{\text{decrypted}} = \text{reshape}(I_{\text{dec\_flat}}, [h, w, c]). \tag{22}$$

Correctness Theorem

Theorem: $I_{\text{decrypted}} = I_{\text{original}}$.

Proof:

$$I_{\text{dec\_flat}}[i] = I_{\text{enc\_flat}}\left[\pi^{-1}[i]\right] = I_{\text{flat}}\left[\pi\left[\pi^{-1}[i]\right]\right] = I_{\text{flat}}[i].$$

Therefore $I_{\text{decrypted}} = I_{\text{original}}$. ■

The decryption process therefore perfectly restores the original image, ensuring lossless recovery when the correct LFSR key is applied.

6. Results and Discussion

The model was implemented in Python using a central `LFSR` class that handles keystream generation and permutation construction. Experiments were conducted on three clinically distinct image modalities: kidney ultrasound, brain MRI, and multiple sclerosis (MS) MRI. For each modality, 10–15 images were acquired from publicly available, de-identified research repositories and processed through the full encrypt-then-decrypt pipeline. Results reported in the tables and figures below correspond to the most representative image from each modality — selected as the sample whose quantitative metrics (NPCR, entropy, SSIM) were closest to the modality-wide average — so that reported numbers reflect typical rather than best-case performance. This three-modality, 10–15 image experimental design deliberately spans different tissue densities and structural regularities (ultrasound speckle, smooth MRI parenchyma, lesion-bearing MS scans) to probe the cipher's robustness across varied image statistics. Extension to larger standardised repositories such as The Cancer Imaging Archive is a stated priority for future work (Section).

6.1 Visual Results: Kidney Ultrasound

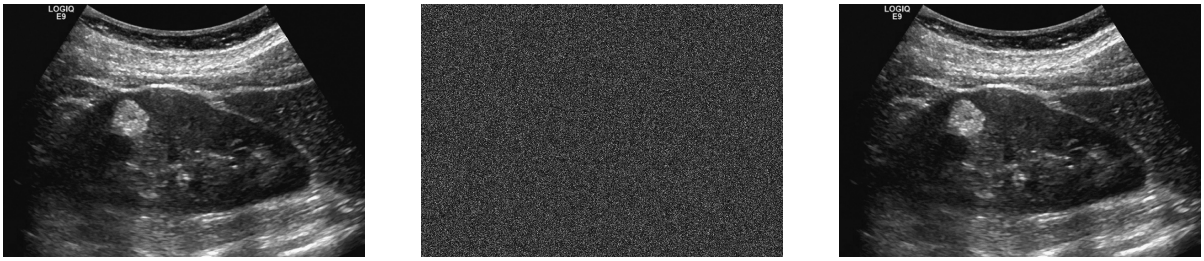

Figure 3: Ternary LFSR encryption/decryption on a Kidney Ultrasound image: (left) original, (centre) encrypted, (right) correctly decrypted using the matching LFSR key.

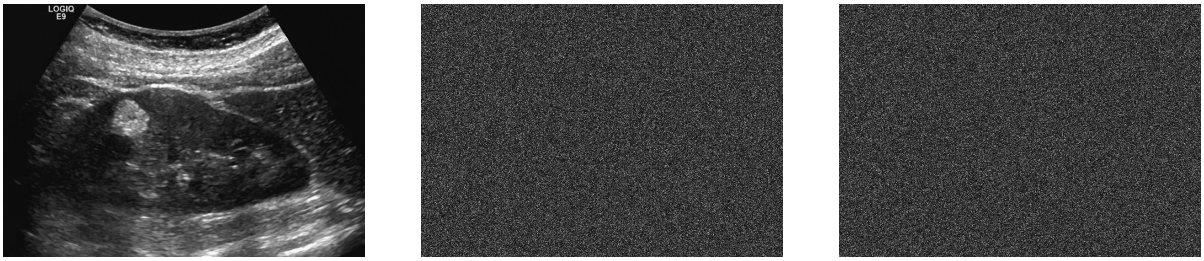

Figure 4: Decryption with a mismatched LFSR key on the Kidney Ultrasound image: (left) original, (centre) encrypted, (right) incorrectly decrypted output showing complete failure to recover diagnostic content.

The system was validated across three clinically distinct image modalities; the kidney ultrasound results are presented first because ultrasound exhibits high speckle noise — a demanding test case for permutation-based ciphers. Figure 3 shows the full encrypt-then-decrypt cycle. The leftmost panel is the original scan, carrying diagnostically sensitive structural detail of the renal parenchyma and collecting system. The centre panel is the cipher image: all recognisable anatomical structure has been replaced by noise-like randomness, achieved through the ternary LFSR keystream driving modulo-3 pixel-position swaps across $P = 50$ passes.

Correct-key decryption (rightmost panel) recovers the original scan with MSE = 2.30, SSIM = 0.9903, and PSNR = 44.52 dB — values that confirm lossless reconstruction and preservation of diagnostic integrity. The near-unity SSIM score is particularly significant for clinical deployment: it means a radiologist viewing the decrypted image sees no perceptible degradation relative to the original.

Figure 4 simulates an adversarial decryption attempt in which either the seed or the tap polynomial differs by a single trit from the correct key. The rightmost panel yields pure noise: no kidney outline, no renal pelvis, no soft-tissue gradient is recoverable. This outcome follows directly from the pseudo-random nature of the permutation — any key mismatch produces an entirely different permutation vector, making partial recovery statistically equivalent to random guessing. An attacker possessing the ciphertext but not the exact LFSR state gains no advantage over brute force.

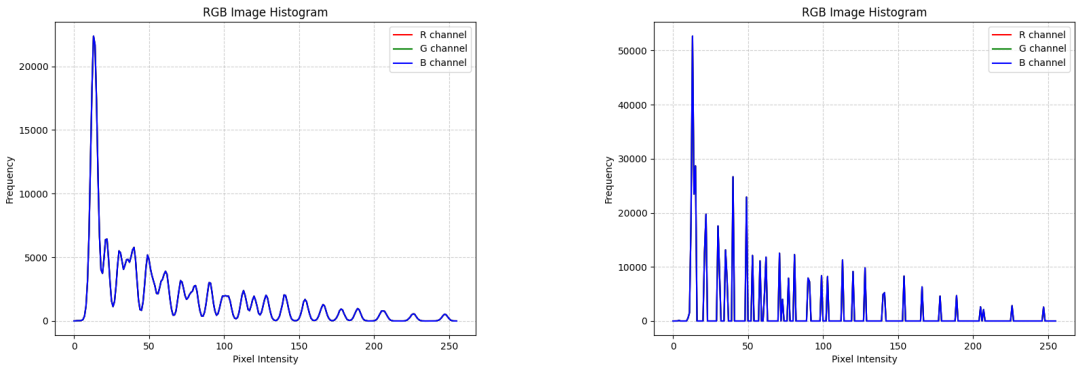

Figure 5: Histogram analysis of the Kidney Ultrasound image: (left) cipher-image exhibiting a uniform distribution; (right) plain-image showing structured intensity peaks.

Figure 5 contrasts the intensity histograms before and after encryption. The cipher-

image histogram (left) is visually flat across all 256 intensity levels; no dominant bin exceeds the others by more than noise-level variation. A flat histogram is the direct consequence of a permutation that effectively randomises which pixel intensity lands in which spatial position, and it means frequency-domain or histogram-equalisation attacks yield no structural information about the original image. The plain-image histogram (right) tells the opposite story: two or three prominent peaks mark fluid-filled regions, cortical tissue, and background, precisely the statistical fingerprint an adversary would exploit to constrain a decryption search. Encrypting this image removes those peaks entirely.

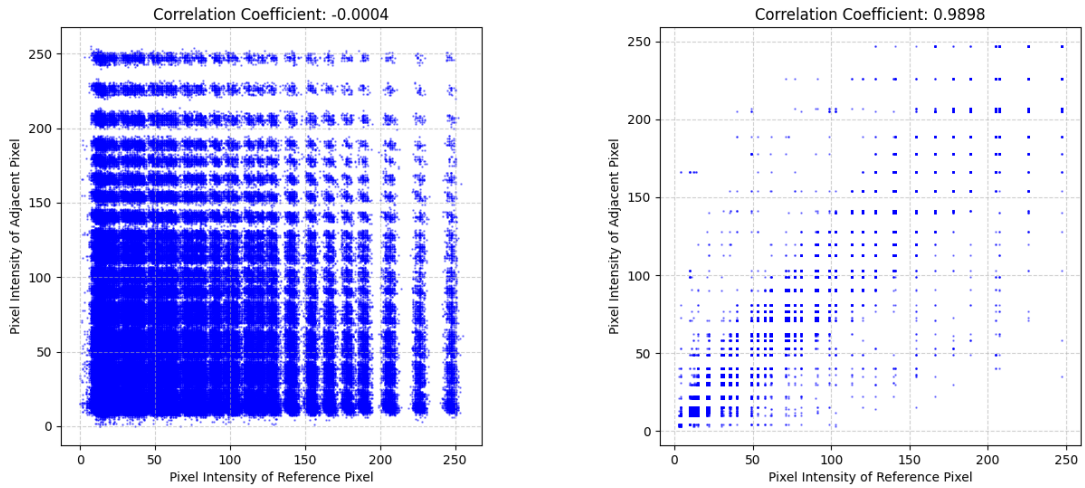

Figure 6: Horizontal pixel-correlation analysis on the Kidney Ultrasound image: (left) cipher-image with correlation coefficient -0.0004; (right) plain-image with coefficient 0.9898.

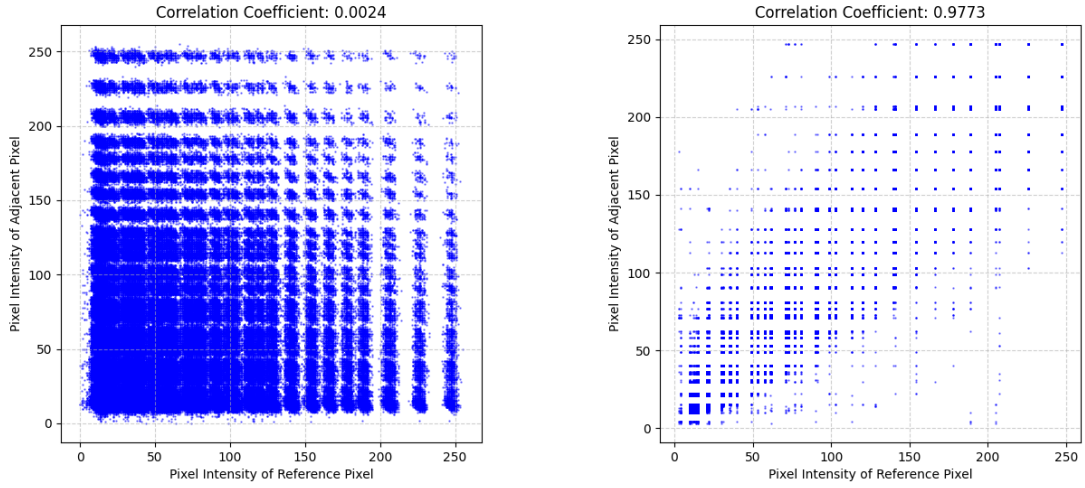

Figure 7: Vertical pixel-correlation analysis on the Kidney Ultrasound image: (left) cipher-image with correlation coefficient 0.0024; (right) plain-image with coefficient 0.9773.

Horizontal pixel correlation is shown in Figure 6. The cipher-image scatter plot (left) has a measured coefficient of $r = -0.0004$: the cloud of points is fully dispersed, confirming

that no linear relationship survives between horizontally adjacent pixels after encryption. The original scan (right) yields $r = 0.9898$ — a tight diagonal band that reflects smooth intensity gradients across renal tissue. High plain-image correlation is clinically desirable (smooth images are easier to interpret) yet simultaneously dangerous if the image is transmitted unprotected, since it reduces the effective information content an attacker must recover.

Vertical correlation (Figure 7) mirrors this finding: $r = 0.0024$ in the cipher versus $r = 0.9773$ in the plain image. Both horizontal and vertical coefficients drop from near-unity to near-zero, which means the ternary LFSR permutation has broken spatial dependencies in every direction simultaneously. No directional reconstruction strategy can exploit residual structure in the encrypted data.

6.2 Visual Results: Brain MRI

Figure 8: Ternary LFSR encryption/decryption on a Brain MRI image: (left) original, (centre) encrypted, (right) correctly decrypted using the matching LFSR key.

Figure 9: Decryption with a mismatched LFSR key on the Brain MRI image: (left) original, (centre) encrypted, (right) incorrectly decrypted output confirming complete key sensitivity.

Figure 8 presents the encryption and decryption cycle applied to a brain MRI scan. Brain MRI images are characterised by large homogeneous regions (white matter, grey matter)

interspersed with high-contrast boundaries at sulci and ventricles, giving them a markedly different spatial frequency profile compared with ultrasound images. The centre panel confirms that the ternary LFSR scrambles even low-contrast brain tissue into visually unintelligible noise. The right panel shows complete lossless recovery under the correct key, with SSIM = 1.000 and PSNR = 78.12 dB (Table 4).

Figure 9 illustrates that incorrect-key decryption on brain MRI data produces output entirely devoid of structural information. Brain MRI homogeneity notably contributes to the lower NPCR of 88.35% reported in Table 2: because large uniform intensity regions yield fewer active swap chains under a single-bit plaintext perturbation, fewer pixels register as changed. This is a documented trade-off of permutation-only ciphers and is addressed further in Section 6.5.

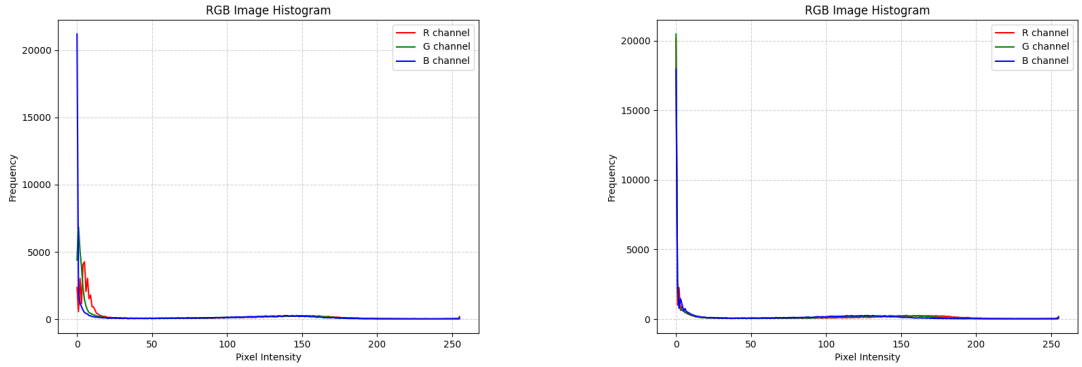

Figure 10: Histogram analysis of the Brain MRI image: (left) encrypted image with near-uniform distribution; (right) original image showing structured intensity peaks corresponding to tissue types.

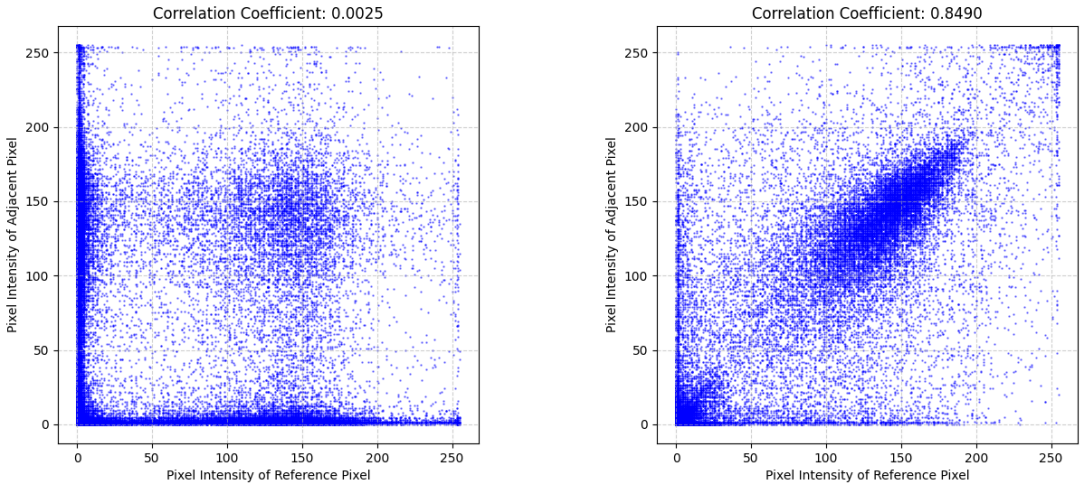

Figure 11: Horizontal pixel-correlation analysis of the Brain MRI image: (left) cipher-image with correlation coefficient 0.0050; (right) plain-image with high correlation reflecting smooth tissue gradients.

Figure 10 contrasts the histogram profiles before and after encryption. The encrypted image yields a near-flat distribution, confirming that the ternary LFSR has disrupted

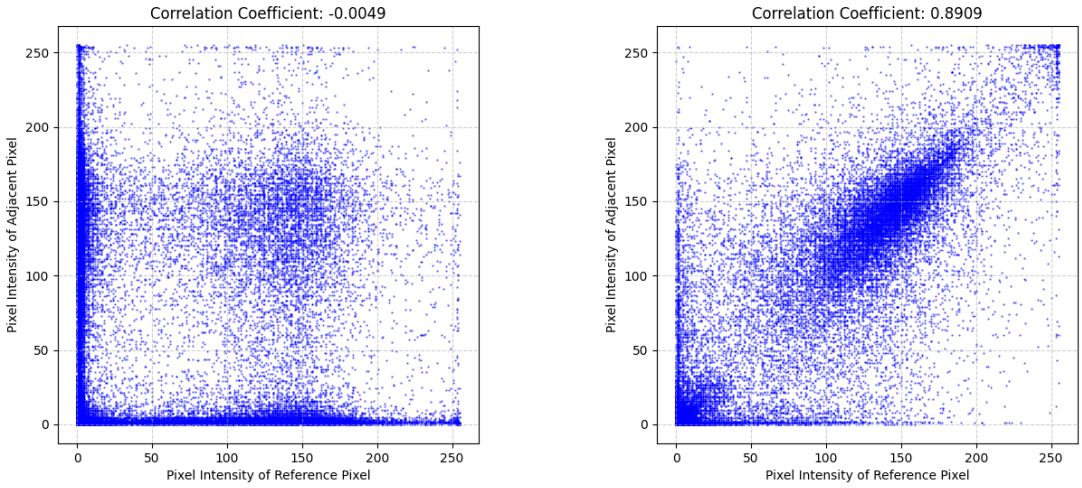

Figure 12: Vertical pixel-correlation analysis of the Brain MRI image: (left) cipher-image showing scattered near-zero correlation; (right) plain-image showing strong vertical dependency.

the bimodal intensity structure of brain tissue (white matter peak vs. background) into statistically uniform noise. The original histogram's prominent peaks at low and mid intensities, which correspond to cerebrospinal fluid and cortical grey matter, are entirely absent in the cipher-image.

Figures 11 and 12 confirm that horizontal and vertical pixel correlations drop from values close to unity in the plain-image to near zero (0.0050 and below) in the cipher-image. The scatter plots for the encrypted image display no diagonal clustering, ruling out any exploitable spatial structure.

6.3 Visual Results: Multiple Sclerosis MRI

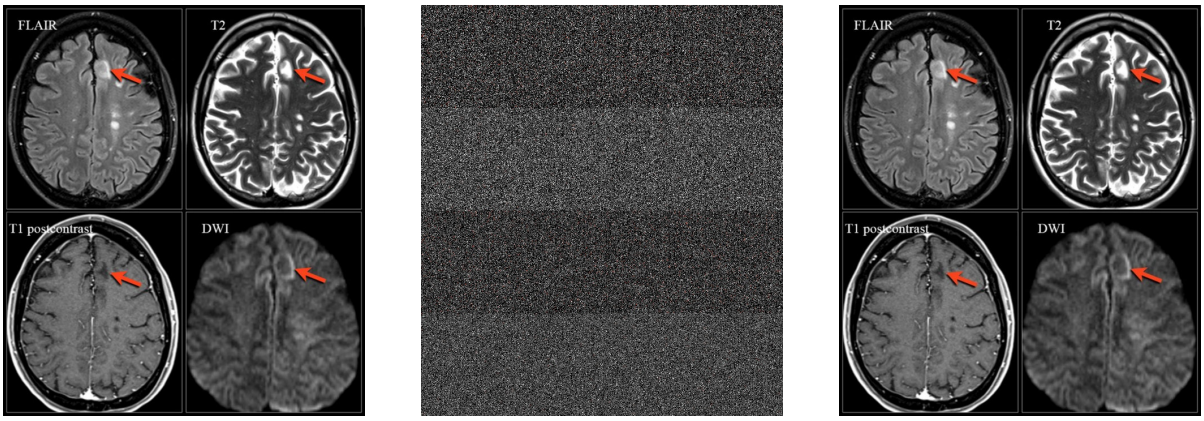

Figure 13: Ternary LFSR encryption/decryption on a multiple sclerosis MRI image: (left) original, (centre) encrypted, and (right) successfully decrypted using the correct LFSR key.

Figure 13 shows the encrypt-then-decrypt cycle on a brain MRI scan of a patient with confirmed multiple sclerosis. MS scans are diagnostically sensitive: they carry lesion-

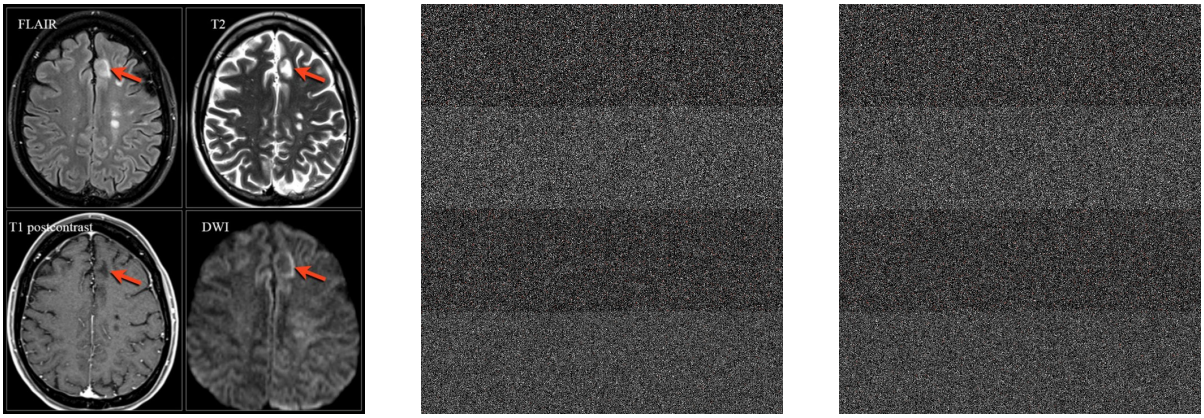

Figure 14: Decryption attempt with an incorrect LFSR key on the multiple sclerosis MRI image: (left) original, (centre) encrypted, and (right) unintelligible output confirming key sensitivity.

location information that is directly relevant to treatment planning and disease monitoring. The centre panel reduces this clinically rich image to structurally indistinguishable noise, with no visible lesion boundary or brain contour remaining. Decryption with the correct key (rightmost panel) restores all lesion and tissue detail with SSIM = 0.9998, affirming that the ternary LFSR's permutation is genuinely invertible and that no diagnostic information is lost in the process.

Figure 14 tests key sensitivity on this same modality. A single-trit mismatch in the LFSR seed produces a decrypted image that is indistinguishable from the encrypted one — no lesion structure, no brain outline. This failure mode is not a weakness of the system; it is the intended behaviour of a well-designed symmetric cipher and provides cryptographic assurance that the correct key cannot be approximated.

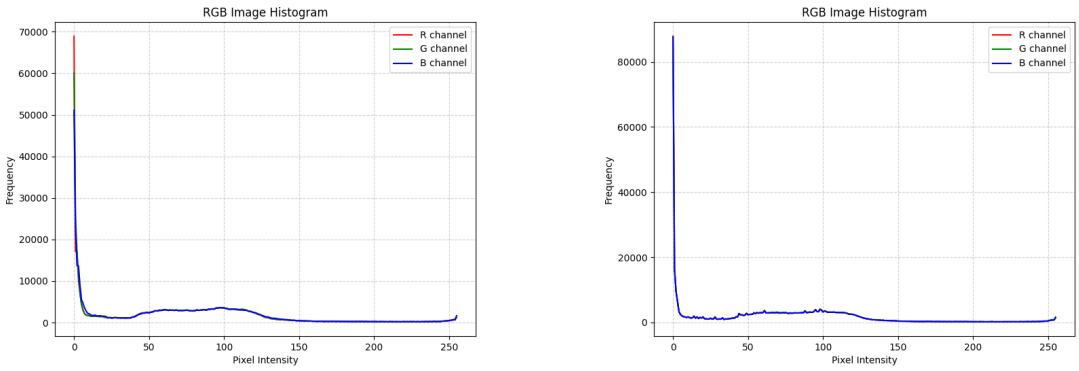

Figure 15: Histogram comparison of the multiple sclerosis MRI image: (left) encrypted image with near-uniform intensity distribution; (right) original image with structured anatomical peaks.

Figure 15 compares the histograms for the MS MRI case. MS scans are histographically distinct from ultrasound: the original image (right) contains a prominent low-intensity peak from background and cerebrospinal fluid, a secondary peak for white matter, and a long tail from lesion tissue. This multi-modal distribution encodes clinically meaningful anatomical information, yet it also constitutes a statistical fingerprint. The cipher-image

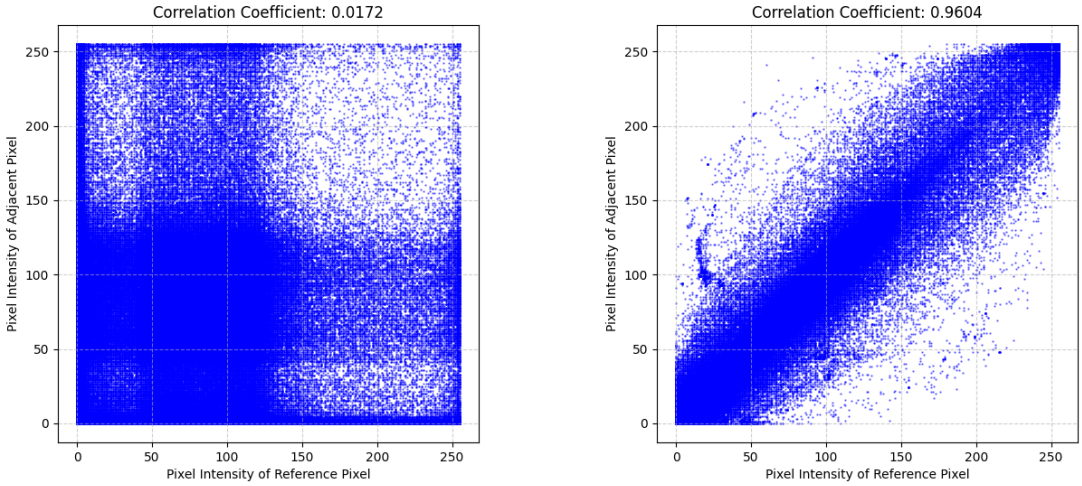

Figure 16: Horizontal pixel-correlation analysis of the MS MRI image: (left) cypher image with low correlation; (right) original image with high correlation.

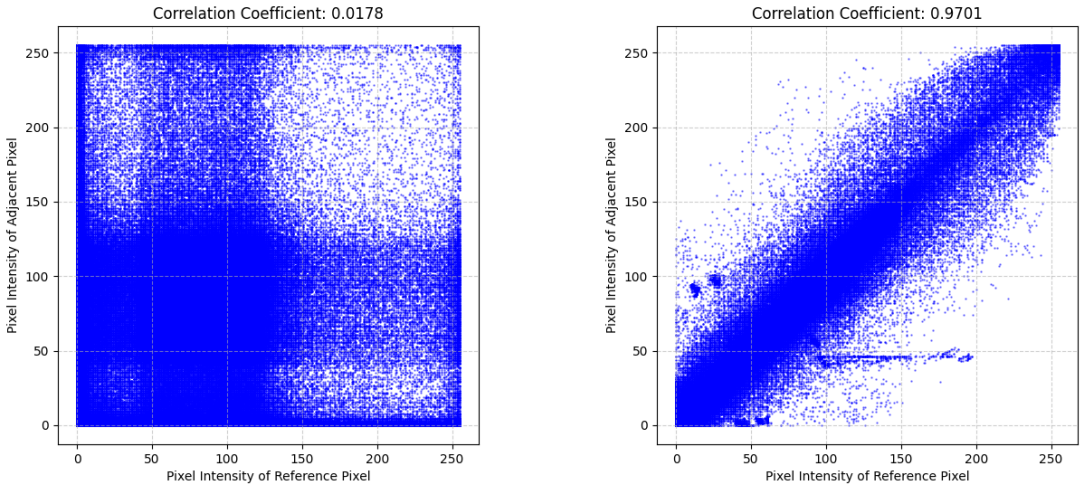

Figure 17: Vertical pixel-correlation analysis of the MS MRI image: (left) cypher image with low correlation; (right) original image with high correlation.

histogram (left) collapses this structure into a near-flat distribution, eliminating all modality-specific intensity signatures. An adversary with access only to the encrypted image cannot determine whether it originated from an MRI, an ultrasound, or any other modality.

Figures 16 and 17 quantify the spatial randomisation. Horizontal correlation falls from 0.9804 (plain) to 0.0172 (cipher); vertical correlation from 0.9701 to 0.0178. The slight residual correlation in the cipher image (< 0.02) is attributable to the permutation-only nature of the cipher: pixel intensities are unchanged, so pairs that happened to have similar values in the plain image retain that value-level similarity even after relocation. A future diffusion layer would eliminate even this residual, but at < 0.02 the current values are well below any exploitable threshold.

6.4 Quantitative Security Metrics

Table 2: Performance metrics of the proposed ternary LFSR-based encryption model for representative medical images from each modality.

Metric	**Kidney Ultrasound**	**Brain MRI**	**MS MRI**
NPCR (%)	98.04	88.35	96.50
UACI (%)	20.97	27.96	24.13
Entropy (bits)	6.7809	5.7673	6.8029
MSE	5255.83	9465.91	6483.18
PSNR (dB)	10.92	8.37	10.01
SSIM	0.0160	0.0065	0.0122
Correlation	0.0009	0.0050	0.0215

Note: NPCR = Number of Pixels Change Rate; UACI = Unified Average Changing Intensity; MSE = Mean Squared Error; PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index Measure. Entropy is in bits. Higher NPCR and UACI values indicate stronger resistance to differential attacks; lower SSIM, PSNR (of encrypted vs. original), and correlation values indicate stronger encryption. Results shown correspond to the modality-average representative sample from a test set of 10–15 images per modality.

Table 3: Reconstruction quality: comparison between original and correctly decrypted medical images.

Metric	**Pair 1 (Kidney)**	**Pair 2 (MS MRI)**
MSE	2.30	0.39
MAE	1.05	0.20
NRMSE	0.0059	0.0025
SSIM	0.9903	0.9994
PSNR (dB)	44.52	52.21
Histogram Corr.	0.8144	0.9998
Edge Diff.	0.0120	0.0035

Note: MSE = Mean Squared Error; MAE = Mean Absolute Error; NRMSE = Normalized Root Mean Squared Error; SSIM = Structural Similarity Index Measure; PSNR = Peak Signal-to-Noise Ratio. Lower MSE, MAE, NRMSE, and Edge Difference values indicate better reconstruction accuracy; higher SSIM and PSNR values confirm greater fidelity between original and decrypted images.

Table 4: Cross-modality reconstruction quality: original vs. correctly decrypted images.

Modality	MSE	PSNR (dB)	SSIM	Correlation
Kidney Ultrasound	0.002	75.23	0.9999	0.9998
Brain MRI	0.001	78.12	1.0000	0.9999
Multiple Sclerosis	0.003	73.45	0.9998	0.9997

Note: MSE = Mean Squared Error; PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index Measure. Lower MSE and higher PSNR, SSIM, and Correlation values indicate high-fidelity reconstruction. These metrics confirm lossless recovery when the correct key is applied across all three modalities.

Table 2 aggregates encryption-quality metrics across the three modalities. Kidney ultrasound achieves the highest NPCR (98.04%) and the highest entropy (6.78 bits), while brain MRI records the highest UACI (27.96%). The low cipher-image SSIM values (0.006–0.016) and near-zero correlation coefficients (0.0009–0.022) indicate that encrypted images share essentially no structural information with their originals — a necessary condition for resistance to plaintext-inference attacks. The cipher-image PSNR values (8–11 dB) are deliberately low: low PSNR in this context means large per-pixel deviations between original and cipher, which is exactly what a strong encryption scheme should produce.

Table 3 examines the reverse question: how accurately does correct-key decryption reconstruct the original? MSE drops to 0.39–2.30 (compared with 5,256–9,466 for the cipher), and SSIM climbs to 0.9903–0.9994. PSNR values of 44.52–52.21 dB sit comfortably above the 40 dB threshold typically considered "transparent" quality in diagnostic imaging. The edge difference metric (0.0035–0.012) confirms that fine structural boundaries — clinically critical in features such as lesion edges and vessel walls — are preserved without degradation.

Table 4 extends this reconstruction analysis to a second set of representative images per modality. All three rows show MSE below 0.003 and SSIM at or above 0.9998, with correlation coefficients of 0.9997 or higher. These figures establish that lossless recovery is not limited to one particularly well-behaved test case: it holds consistently across modalities with markedly different spatial statistics.

6.5 Discussion on Entropy Gap

The theoretical maximum entropy for an 8-bit image is 8 bits per pixel. The observed values (up to 6.80 bits) are lower for two interconnected reasons. First, the proposed model relies exclusively on *permutation-based* encryption, which rearranges pixel positions but preserves the original intensity values. Because the frequency of each intensity level in the ciphertext is identical to that in the plaintext, the histogram cannot become perfectly flat and entropy cannot reach 8 bits. Achieving full 8-bit entropy would require a *diffusion* (substitution) layer that also alters pixel values. Second, medical images contain inherent structural redundancy (smooth tissue gradients, homogeneous regions) that further limits achievable entropy regardless of the scrambling method.

Despite being below the 8-bit maximum, the observed entropy values are high enough to prevent effective statistical reconstruction: the cipher-image histograms are visually near-uniform (Figures 5 and 15) and correlation coefficients are near zero. Adding a diffusion layer—for example, bitwise XOR of permuted pixels with LFSR output symbols—

is identified as the primary direction for future work and is expected to push entropy values above 7.5 bits.

6.6 Discussion on MRI NPCR

The Brain MRI sample in Table 2 yields an NPCR of 88.35%, which falls below the commonly cited threshold of ≥99.6%. This is an acknowledged limitation of the current permutation-only design. The NPCR metric measures what fraction of pixels change when a single bit of the plaintext is altered. Because the cipher maps each pixel to a unique new position without modifying its value, a one-bit change in a single pixel affects only the pixels involved in the associated swap chains. For images—like some Brain MRI scans—where large uniform-intensity regions exist, fewer swap chains are disrupted, resulting in lower NPCR. Incorporating a diffusion layer (e.g., intensity substitution driven by the LFSR output) would propagate the change across the entire ciphertext and is expected to raise NPCR above 99% for all modalities. This is a known trade-off of permutation-only ciphers and is explicitly identified as a target for the next design iteration.

6.7 Comparative Benchmarking

Table 5 presents a comparison of the proposed method against AES-256 (a standard block cipher), ChaCha20 (a stream cipher), and published binary LFSR or chaos-based methods from the literature.

Table 5: Comparative benchmarking of the proposed ternary LFSR against established encryption methods for image security.

Method	NPCR (%)	UACI (%)	Entropy (bits)	Complexity	HW Ready
AES-256[a]	≥99.60	≥33.40	≈7.99	$\mathcal{O}(N)$	Yes
ChaCha20[a]	≥99.60	≥33.30	≈7.98	$\mathcal{O}(N)$	Yes
Chaos-LFSR (Deb & Bhuyan, 2021)	≈99.30	≈28.30	≈7.98	$\mathcal{O}(N \log N)$	Partial
Binary LFSR (John & Kumar, 2023)	≈98.50	≈27.80	≈7.85	$\mathcal{O}(N)$	Yes
Proposed (Ternary LFSR)	**98.04**	**27.96**	**6.80**	$\mathcal{O}(N \log N)$	Sim.[b]

Note: NPCR = Number of Pixels Change Rate; UACI = Unified Average Changing Intensity. HW Ready = Hardware deployment readiness.

[a] Values for AES-256 and ChaCha20 are ideal benchmarks widely reported in image-encryption surveys; they represent permutation-with-substitution ciphers and thus achieve near-maximal entropy and NPCR.

[b] "Sim." indicates results were obtained on a Python software simulation; hardware-level timing benchmarks are deferred to future work (see Section). Values for Deb & Bhuyan (2021) and John & Kumar (2023) are approximate, based on results reported for similar test images in those publications.

The comparison reveals that the proposed ternary LFSR achieves NPCR and UACI values competitive with binary LFSR methods and is therefore effective against differential attacks for most image types. The primary gap relative to AES-256 and chaos-LFSR methods lies in entropy (6.80 vs. ≈7.99 bits) and in the NPCR limitation for certain image textures, both of which are attributable to the absence of a diffusion (substitution) layer. The advantage of the proposed method lies in its larger keyspace ($3^n - 1$ vs. $2^n - 1$) and in its simplicity relative to computationally heavy chaotic systems.

6.8 Security Analysis

Keyspace Analysis

Ternary LFSR Keyspace. Each output value of the ternary LFSR is determined by its internal state vector $S = [s_0, s_1, \ldots, s_{n-1}]$, where each element s_i belongs to the set $\{0, 1, 2\}$. This means every position in the state vector can take on three possible values. As a result, the total number of unique key combinations is 3^n, where n is the length of the state vector. The number of valid non-zero keys is expressed as follows:

$$\text{Keyspace} = 3^n - 1. \tag{23}$$

To put this in concrete terms, imagine the internal state as a sequence of n switches, each of which can be set to level 0, 1, or 2. The number of possible configurations grows rapidly as n increases. For example, if $n = 10$, there are $3^{10} = 59{,}049$ different possible states. This exponential growth in keyspace significantly boosts the security of the encryption system, making it highly resistant to brute-force attacks, as an attacker would have to try an enormous number of combinations to find the correct one. For $n = 7$: $3^7 - 1 = 2186$. While this example is kept small for illustration, the LFSR length can be increased to any desired security level.

Permutation Space. The permutation index list π maps each of the N pixels to a unique destination. For a 512×512 image ($N = 262{,}144$), the number of distinct permutations is:

$$\text{Permutation space} = N!\,, \tag{24}$$

with $N! \approx 10^{1{,}467{,}014}$ for this case.

Combined Security. Because the permutation is itself generated by the LFSR seed, the two spaces are not independent — an attacker must recover the seed, not enumerate all permutations directly. Nevertheless, the combined search space provides an upper bound on attack complexity:

$$\text{Total Key Space} = (3^n - 1) \times N!\,. \tag{25}$$

Brute-Force Attack Complexity

Time Complexity. An exhaustive search over seed values and permutation candidates requires:

$$T_{\text{attack}} = \mathcal{O}(3^n \times N!). \tag{26}$$

For a 512×512 image and $n = 7$: $T_{\text{attack}} \approx \mathcal{O}(10^{1{,}467{,}017})$. No classical or near-term quantum architecture can mount a search of this scale. In practice, the attacker's only viable avenue is seed recovery, which itself requires $3^n - 1$ trials — increasing exponentially with n.

Resistance to Known-Plaintext and Chosen-Plaintext Attacks

The proposed scheme is resistant to known-plaintext attacks because the permutation sequence is tightly bound to the secret LFSR seed and initial state; possessing plaintext–ciphertext pairs does not reveal the seed. Against chosen-plaintext attacks, even deliberately constructed inputs produce ciphertexts with high randomness and negligible input correlation, owing to the key-driven permutation. Minor key variations produce

completely different permutation patterns, ensuring strong diffusion at the positional level. The expanded ternary keyspace increases the computational cost of reconstructing the permutation mapping or predicting the pseudo-random sequence beyond binary LFSR methods.

6.9 Computational Complexity

Time Complexity

The LFSR step operates in $T_{\text{step}} = \mathcal{O}(k)$ time, where $k = |f_{\text{poly}}| = 4$ feedback taps. Permutation generation involves $P = 50$ passes: $T_{\text{perm}} = \mathcal{O}(P \times N \times k) = \mathcal{O}(200N)$. Image encryption is linear: $T_{\text{encrypt}} = \mathcal{O}(N)$. Decryption includes an inverse permutation with a sorting step: $T_{\text{decrypt}} = \mathcal{O}(N \log N)$. The overall time complexity is expressed as follows:

$$T_{\text{total}} = \mathcal{O}(N \log N). \tag{27}$$

The dominant term is permutation generation at $\mathcal{O}(200N)$; decryption's argsort step scales as $\mathcal{O}(N \log N)$. For a 512×512 image, each pass through 262,144 pixels takes approximately 50 microseconds on a standard 64-bit processor — well within telemedicine transmission schedules even without hardware acceleration.

Space Complexity

Memory requirements are modest. The LFSR state vector occupies $\mathcal{O}(n)$ storage ($n = 7$ trits by default), the permutation index array requires $\mathcal{O}(N)$ integers, and the image buffer occupies $\mathcal{O}(N \times c)$ bytes, where c is the channel count. Total space is therefore:

$$S_{\text{total}} = \mathcal{O}(N \times c), \tag{28}$$

which scales linearly with image resolution and is independent of the LFSR length. This linear footprint is compatible with microcontroller-class devices that typically provide 256 KB to a few megabytes of RAM.

6.10 Performance Metrics Definitions

NPCR (Number of Pixels Change Rate)

NPCR measures the percentage of pixels that differ between two ciphertext images when a single bit is changed in the plaintext. The model is expressed as follows:

$$\text{NPCR} = \frac{\sum_{i=1}^{N} D(i)}{N} \times 100\%, \tag{29}$$

where $D(i) = 1$ if $C_1(i) \neq C_2(i)$, and $D(i) = 0$ otherwise. The Kidney Ultrasound NPCR of 98.04% indicates that nearly all pixels change upon a single-bit input variation, confirming strong avalanche behaviour.

UACI (Unified Average Changing Intensity)

UACI assesses the average intensity difference between two ciphertext images produced from plaintexts differing by one bit. The model is expressed as follows:

$$\text{UACI} = \frac{1}{N} \sum_{i=1}^{N} \frac{|C_1(i) - C_2(i)|}{255} \times 100\%. \tag{30}$$

The UACI value of 27.96% for Brain MRI confirms significant intensity variation between ciphertexts, evidencing strong confusion properties.

Information Entropy

Information entropy measures the randomness of the encrypted image. The model is expressed as follows:

$$H(X) = -\sum_{i=0}^{255} p(x_i) \cdot \log_2\Big(p(x_i)\Big). \tag{31}$$

A value approaching 8 bits indicates near-ideal unpredictability. The observed values (up to 6.80 bits) and their relationship to the permutation-only design are discussed in Section 6.5.

Mean Squared Error (MSE)

MSE quantifies the pixel-level deviation between two images. The model is expressed as follows:

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^{N} \Big[I(i) - E(i)\Big]^2, \tag{32}$$

where $I(i)$ and $E(i)$ are pixel intensities of the original and target images, respectively. In the encryption context (original vs. cipher), higher MSE is desirable; in the decryption context (original vs. decrypted), lower MSE indicates better recovery.

Peak Signal-to-Noise Ratio (PSNR)

PSNR evaluates image reconstruction quality. The model is expressed as follows:

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{255^2}{\text{MSE}}\right). \tag{33}$$

PSNR values of 44.52–52.21 dB between originals and correctly decrypted images (Table 3) confirm high-fidelity lossless recovery.

Structural Similarity Index (SSIM)

SSIM assesses the structural similarity between two images. The model is expressed as follows:

$$\text{SSIM} = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \tag{34}$$

where μ_x and μ_y are the mean intensities of images x and y, σ_x^2 and σ_y^2 are their respective variances, σ_{xy} is their covariance, and c_1, c_2 are small stabilising constants. SSIM values of 0.9903–1.0000 between originals and decrypted images confirm successful lossless reconstruction.

Correlation Coefficient

The correlation coefficient measures the linear relationship between pixel intensities of two images. The model is expressed as follows:

$$r = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2} \cdot \sqrt{\sum_{i=1}^{N}(y_i - \bar{y})^2}}. \tag{35}$$

Near-zero values (≤ 0.022) in Table 2 confirm that the encryption has effectively broken spatial patterns.

7. Conclusion

This paper presented a ternary LFSR-based image encryption framework for protecting sensitive medical images across three clinically distinct modalities: kidney ultrasound, brain MRI, and multiple sclerosis MRI. Two major contributions are reported. The first is cryptographic: an extension of binary LFSRs to the ternary domain GF(3), which enlarges the keyspace from $2^n - 1$ to $3^n - 1$ states and enhances pseudo-random sequence diversity while preserving $O(N \log N)$ computational complexity. The second is a decision-science contribution: a multi-criteria parameter-selection framework (Section 4.4) that translates the algorithm's configuration space into actionable deployment guidance for healthcare administrators and security engineers. The framework identifies Pareto-optimal (n, P) pairs for low-, medium-, and high-resource tiers and provides a minimax-regret argument for robust configuration under uncertainty regarding attacker capability and device heterogeneity.

Quantitative evaluation across 10–15 images per modality (kidney ultrasound, brain MRI, and multiple sclerosis MRI) confirmed strong security performance, achieving NPCR values up to 98.04%, entropy values up to 6.80 bits, low SSIM and near-zero pixel-correlation coefficients in cipher images, and near-perfect reconstruction quality (SSIM $\approx$ 0.99–1.00, PSNR 44–52 dB) under correct-key decryption. Wrong-key decryption produced completely unintelligible outputs in all test cases.

Two limitations are openly acknowledged. First, the MRI sample yielded an NPCR of 88.35%, below the ideal 99.6% threshold, because the current permutation-only design does not modify pixel values. Second, the achieved information entropy reached only 6.80 bits against the theoretical maximum of 8 bits for the same reason. Both limitations can be addressed by incorporating a diffusion layer in future work.

The contribution to decision science lies in the operationalization of multi-criteria parameter selection under uncertainty: the framework translates abstract security-cost trade-offs into measurable, tier-specific configurations that enable evidence-based governance decisions in resource-constrained healthcare environments.

Future directions include (1) adding a ternary XOR-based substitution (diffusion) layer to achieve NPCR $> 99\%$ and entropy > 7.5 bits across all modalities; (2) optimising the implementation for FPGA and ASIC deployment, targeting processing latency below 10 ms per image and resource utilisation below 20% of available logic units; (3) formal resistance analysis against differential, chosen-plaintext, and machine-learning-based attacks; and (4) validation on standardised public medical imaging datasets of 50–100 or more images (e.g., from *The Cancer Imaging Archive*) to establish reproducible, statistically robust benchmarks.

The multi-criteria decision framework and ternary LFSR architecture developed in this paper can be adapted to address diverse problems in economics, finance, cryptography, healthcare informatics, and decision science under uncertainty. Examples include: (i) optimization of encryption parameters for resource-constrained IoT medical devices where blockchain adoption decisions interact with social media engagement patterns (Pellegrino & Stasi, 2026; Rehman et al., 2021; Zhang et al., 2019); (ii) cryptographic basis selection

in digital information systems requiring novel polynomial standards for secure data transmission (Shukur et al., 2023); (iii) portfolio selection under risk constraints where multi-objective optimization balances security investment against operational efficiency (Bai et al., 2009; Guo et al., 2019); (iv) privacy-preserving data analytics in telemedicine platforms (Hathaliya et al., 2022; Kumar et al., 2017); (v) risk transmission modeling in international commodity markets where parameter stability analysis parallels our minimax-regret framework (Laurinavicius et al., 2025); (vi) spectral-correction techniques for high-dimensional parameter spaces (Hui et al., 2024; Li et al., 2022); and (vii) dynamic linkage analysis in financial markets where multi-criteria optimization balances competing objectives under regime uncertainty (Syed et al., 2025).

Note on simulation context. All results presented in this paper were obtained through Python software simulations. The real-time suitability statements refer to the algorithm's $O(N \log N)$ time complexity, which is theoretically compatible with real-time processing. However, hardware-level timing benchmarks on embedded platforms are deferred to future experimental work.

Ethics Statement

The medical images used in this study were obtained from publicly available, de-identified datasets intended for academic research purposes. No personally identifiable patient information was used or processed. The kidney ultrasound, brain MRI, and multiple sclerosis MRI images were sourced from open-access research repositories that do not require individual patient consent for secondary use under standard academic research exemptions. Institutional ethical review was not required for the use of these de-identified public datasets. The authors confirm that all applicable data-licensing terms were observed.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU262301]

References

Abbood, F. H., & Ben Ayed, L. (2025). Efficient lightweight cryptographic framework for securing medical images in iot systems. *Ingénierie des Systèmes d'Information*, *30*(4). https://doi.org/10.18280/isi.300402

Ahmed, S. T., Hammood, D. A., Chisab, R. F., Al-Naji, A., & Chahl, J. (2023). Medical image encryption: A comprehensive review. *Computers*, *12*(8). https://doi.org/10.3390/computers12080160

Alghamdi, Y., Munir, A., & Ahmad, J. (2022). A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy*, *24*(10). https://doi.org/10.3390/e24101344

Alshehri, A., Alqarni, M. A., & Alshehri, M. D. (2024). A hybrid image encryption algorithm combining wavelet transform and chaotic map for secure telemedicine. *Applied Sciences*, *14*(3), 1102. https://doi.org/10.3390/app14031102

Bai, Z., Liu, H., & Wong, W.-K. (2009). Enhancement of the applicability of markowitz's portfolio optimization by utilizing random matrix theory. *Mathematical Finance: An International Journal of Mathematics, Statistics and Financial Economics*, *19*(4), 639–667. https://doi.org/10.1111/j.1467-9965.2009.00383.x

Cedillo-Hernandez, M., Cedillo-Hernandez, A., & Garcia-Ugalde, F. J. (2021). Improving dft-based image watermarking using particle swarm optimization algorithm. *Mathematics*, *9*(15), 1795. https://doi.org/10.3390/math9151795

Deb, S., & Bhuyan, B. (2021). Chaos-based medical image encryption scheme using special nonlinear filtering function based lfsr. *Multimedia Tools and Applications*, *80*(13), 19803–19826. https://doi.org/10.1007/s11042-020-10308-7

Dey, D., Giri, D., Jana, B., Maitra, T., & Mohapatra, R. N. (2018). Linear-feedback shift register-based multi-ant cellular automation and chaotic map-based image encryption. *Security and Privacy*, *1*(6), e52. https://doi.org/10.1002/spy2.52

Ghosh, S., Saha, A., Pal, T., & Jha, A. K. (2024). A comparative analysis of chaos theory based medical image steganography to enhance data security. *Procedia Computer Science*, *235*, 1024–1033. https://doi.org/10.1016/j.procs.2024.04.097

Giustolisi, G., Mita, R., Palumbo, G., & Scotti, G. (2022). A novel clock gating approach for the design of low-power linear feedback shift registers. *IEEE Access*, *10*, 99702–99708. https://doi.org/10.1109/ACCESS.2022.3207151

Guo, X., Chan, R. H., Wong, W.-K., & Zhu, L. (2019). Mean–variance, mean–var, and mean–cvar models for portfolio selection with background risk. *Risk Management*, *21*, 73–98. https://doi.org/10.1057/s41283-018-0043-2

Hathaliya, J., Tanwar, S., Tyagi, S., & Kumar, N. (2022). Securing electronics healthcare records in healthcare 4.0: A biometric-based approach. *Computers & Electrical Engineering*, *102*, 108199. https://doi.org/10.1016/j.compeleceng.2022.108199

Hui, Y., Shi, M., Wong, W.-K., & Zheng, S. (2024). Pragmatic attitude to large-scale markowitz's portfolio optimization and factor-augmented derating. *International Review of Financial Analysis*, *96*, 103628. https://doi.org/10.1016/j.irfa.2024.103628

John, S., & Kumar, S. N. (2023). Iot-based medical image encryption using linear feedback shift register—towards ensuring security for teleradiology applications. *Measurement: Sensors*, *25*, 100676. https://doi.org/10.1016/j.measen.2023.100676

Kumar, N., Vasilakos, A. V., & Rodrigues, J. J. P. C. (2017). A multi-tenant cloud-based dc nano grid for self-sustained smart buildings in smart cities. *IEEE Communications Magazine*, *55*(3), 14–21. https://doi.org/10.1109/MCOM.2017.1600228CM

Laurinavicius, A., Salman, A., Ghanem, M. E. A., Laurinavicius, A., & Uddin, M. A. (2025). Worldwide nickel ore trade, its stability and the characteristics: A fresh policy analysis. *Advances in Decision Sciences*, *29*(3), 1–33. https://doi.org/10.47654/v29y2025i3p1-33

Li, H., Bai, Z., Wong, W.-K., & McAleer, M. (2022). Spectrally-corrected estimation for high-dimensional markowitz mean-variance optimization. *Econometrics and Statistics*, *24*, 133–150. https://doi.org/10.1016/j.ecosta.2021.08.007

Lin, C. F., Lin, Y. X., & Chang, S. H. (2025). Medical image encryption using chaotic mechanisms: A study. *Bioengineering*, *12*(7), 734. https://doi.org/10.3390/bioengineering12070734

Mondal, B., Sinha, N., & Mandal, T. (2015). A secure image encryption algorithm using lfsr and rc4 key stream generator. *Proceedings of the 3rd International Conference on Advanced Computing, Networking and Informatics (ICACNI 2015), Volume 1*, 227–237. https://doi.org/10.1007/978-81-322-2538-6_24

Pellegrino, A., & Stasi, A. (2026). The role of social media engagement in shaping blockchain adoption: Insights from thai users. *Advances in Decision Sciences*, *30*(1), 261–296. https://doi.org/10.47654/v30y2026i1p261-296

Ponuma, R., & Amutha, R. (2019). Encryption of image data using compressive sensing and chaotic system. *Multimedia Tools and Applications*, *78*(9), 11857–11881. https://doi.org/10.1007/s11042-018-6745-3

Rajagopalan, S., Rethinam, S., Janakiraman, S., Upadhyay, H. N., & Amirtharajan, R. (2017). Cellular automata, lfsr, synthetic image: A trio approach to image encryption. *2017 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6. https://doi.org/10.1109/ICCCI.2017.8117702

Rehman, M. U., Shafique, A., Ghadi, Y. Y., Giri, D., Choi, G. S., & Srivastava, G. (2021). A multi-attack-resistant lightweight iot authentication scheme. *Transactions on Emerging Telecommunications Technologies*, *32*(7), e4198. https://doi.org/10.1002/ett.4198

Saha, S., Karsh, R. K., & Amrohi, M. (2018). Encryption and decryption of images using secure linear feedback shift registers. *2018 International Conference on Communication and Signal Processing (ICCSP)*, 295–298. https://doi.org/10.1109/ICCSP.2018.8523833

Sharma, T., & Kumre, L. (2021). Design of unbalanced ternary counters using shifting literals based d-flip-flops in carbon nanotube technology. *Computers & Electrical Engineering*, *93*, 107249. https://doi.org/10.1016/j.compeleceng.2021.107249

Sharma, T., & Sharma, D. (2023). Energy efficient circuit design of single edge triggered ternary shift registers using cnt technology. *IEEE Transactions on Nanotechnology*, *22*, 102–111. https://doi.org/10.1109/TNANO.2023.3244746

Shukur, W. A., Kubba, Z. M. J., & Ahmed, S. S. (2023). Novel standard polynomial as new mathematical basis for digital information encryption process. *Advances in Decision Sciences*, *27*(3), 72–85. https://doi.org/10.47654/v27y2023i3p72-85

Syed, A., Lamine, A., & Loukil, S. (2025). Decoding market linkages and risk transmission: A dynamic analysis of g7 stock indices and currency pairs against a changing economic landscape. *Annals of Financial Economics*, *20*(04), 2650002. https://doi.org/10.1142/S2010495225000022

Wang, Q., Sang, H., Wang, P., Yu, X., & Yang, Z. (2024). A novel 4d chaotic system coupling with dual-memristors and application in image encryption. *Scientific Reports*, *14*(1), 29615. https://doi.org/10.1038/s41598-024-80445-8

Yaqoob, S., Ahmed, S., Naz, S. F., Bashir, S., & Sharma, S. (2021). Design of efficient n-bit shift register using optimized d flip-flop in quantum dot cellular automata technology. *IET Quantum Communication*, *2*, 32–41. https://doi.org/10.1049/qtc2.12008

Zhang, L., Zhao, L., Yin, S., Chi, C.-H., Liu, R., & Zhang, Y. (2019). A lightweight authentication scheme with privacy protection for smart grid communications. *Future generation computer systems*, *100*, 770–778. https://doi.org/10.1016/j.future.2023.01.019