Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Hybrid Encryption Framework Combining AES S-Box Substitution with Modified ChaCha Stream Cipher

Mohammad Ubaidullah Bokhari[1], Mohd Tauseef Ansari[2], Shahnwaz Afzal[3], Md. Zeyauddin[4]
[1,2,3,4] Department of Computer Science, Aligarh Muslim University, India, 202002
*Corresponding author: Mohd Tauseef Ansari (mohdtauseefansari34@gmail.com)

ARTICLE INFO

Received: 30 Dec 2024
Revised: 05 Feb 2025
Accepted: 25 Feb 2025

ABSTRACT

The rapid integration of Internet of Things (IoT) devices into modern healthcare creates significant security risks for sensitive patient data. Medical images are particularly vulnerable due to their large file sizes and high pixel redundancy, yet conventional encryption algorithms are often too computationally intensive for the resource-constrained hardware found in IoT devices. This paper proposes a novel hybrid encryption framework designed to resolve this security-performance trade-off. Our method first employs the AES S-box to introduce strong confusion, using its proven non-linear substitution to obscure statistical patterns within the image. Subsequently, a performance-optimized, reduced-round ChaCha20 stream cipher is used to achieve rapid diffusion. This stage ensures that even a single-bit change in the input is spread unpredictably across the entire ciphertext, making the output highly randomized. Experimental analysis confirms the framework's robust security. The scheme achieves an information entropy of ~7.997, indicating near-perfect randomness, while reducing pixel correlation coefficients to negligible values. A Number of Pixel Change Rate (NPCR) exceeding 99.5% for single-bit variations highlights its strong avalanche effect and resilience against differential cryptanalysis. By delivering these strong security guarantees with faster encryption speeds and minimal memory overhead, our hybrid framework presents a practical and scalable solution for securing sensitive medical images in real-time Internet of Health Systems (IoHS) applications like remote diagnostics and secure mobile health.

Keywords: Lightweight Cryptography, Medical Image Encryption, AES S-box Substitution, Modified ChaCha20 Cipher, IoT Security in Healthcare

1. INTRODUCTION

Medical imaging has become a cornerstone of modern healthcare, enabling clinicians to visualize internal anatomical and physiological structures without invasive procedures. Techniques such as Magnetic Resonance Imaging (MRI), Computed Tomography (CT), X-ray radiography, and ultrasound imaging have profoundly transformed diagnostic and therapeutic pathways [1,3]. These imaging modalities are extensively used for the early detection of diseases, accurate diagnosis, surgical planning, and ongoing monitoring of treatment outcomes. Their integration into clinical workflows has significantly improved patient care and reduced diagnostic uncertainty. Moreover, the digitization of medical images allows seamless sharing and archiving across healthcare systems, which is essential for remote diagnosis, second opinions, and collaborative treatment planning in geographically distributed environments [4,5].
In parallel, the healthcare landscape is undergoing rapid digital transformation, largely driven by the emergence of the Internet of Things (IoT) and its specialized application in the Internet of Health Systems (IoHS). IoT refers to the interconnected network of smart devices equipped with embedded sensors, communication modules, and data-processing capabilities, facilitating real-time data collection and exchange [31,33]. When adapted to healthcare, this concept gives rise to IoHS—an intelligent infrastructure where medical devices such as wearable monitors, implantable sensors, and diagnostic tools continuously gather and transmit physiological data to healthcare providers. This evolution enables proactive healthcare delivery, real-time disease monitoring, remote patient management, and supports personalized treatment strategies based on continuous data analytics [32,35]. IoHS is particularly impactful in rural and underserved areas, where specialist access is limited, allowing timely interventions and reducing hospital readmissions. However, the fusion of medical imaging with IoT and IoHS ecosystems

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

introduces significant data security and privacy challenges. Medical images are not merely visual data; they often carry embedded patient identifiers, biometric markers, and diagnostic metadata. If intercepted, manipulated, or exposed during transmission or storage, such data can lead to serious medical, ethical, and legal repercussions [7,9]. For instance, the unauthorized alteration of a chest X-ray or brain MRI can result in misdiagnosis, inappropriate treatment decisions, or malpractice litigation. Additionally, leaked images can compromise patient confidentiality and erode public trust in digital healthcare systems [14,16]. The threat is exacerbated by the fact that IoT and IoHS devices typically operate under constrained resources—limited memory, low processing power, and minimal energy budgets—making it infeasible to implement conventional security infrastructures such as firewalls, intrusion detection systems, or high-overhead encryption protocols [17,18].

Traditionally, cryptographic algorithms such as the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and the International Data Encryption Algorithm (IDEA) have been employed to safeguard digital data [15,19]. While effective for textual or structured datasets, these algorithms often fall short when applied to image encryption. Medical images possess unique statistical properties: high spatial redundancy, strong inter-pixel correlations, and large file sizes. These features make them ill-suited for conventional block-based encryption, as such methods may not sufficiently randomize pixel patterns or may introduce latency, which is unacceptable in time-sensitive medical scenarios [11,13]. Moreover, the high computational overhead and memory usage of traditional encryption schemes can overwhelm low-power IoT and IoHS devices, leading to performance bottlenecks, degraded battery life, and system unreliability [34,36]. To overcome these limitations, researchers have explored lightweight cryptographic approaches tailored specifically for image data and constrained environments. Chaos-based cryptographic schemes, which utilize the unpredictable and sensitive behavior of chaotic maps, can generate complex pseudo-random sequences for image scrambling and permutation [20,21,28]. These systems are lightweight and highly secure in theory but may suffer from degradation when executed on ultra-low-power processors due to floating-point operations and precision loss [20,37]. DNA-based cryptography, inspired by biological mechanisms of genetic encoding and decoding, introduces a novel paradigm for parallel encryption. However, its implementation often demands extensive computational resources and precise hardware synchronization, making it less practical for real-time clinical use [11,19,38]. Other notable approaches include edge-map and bit-plane decomposition-based methods, which attempt to optimize confusion and diffusion by analyzing image structure, but these too can be vulnerable if edge data is predictable or compromised [26,39].

Despite these innovations, most existing techniques exhibit an imbalance: they either prioritize encryption strength at the cost of efficiency or focus on speed while compromising security. This dichotomy underscores a persistent research gap: the need for a cryptographic framework that is both lightweight and secure, specifically designed for the unique characteristics of medical images and the constraints of IoT/IoHS environments [34,40]. A truly effective solution must offer strong resistance to known cryptanalytic attacks, ensure randomness in output, and maintain low computational and energy demands. In response to this critical challenge, this research proposes a hybrid lightweight encryption framework that combines two complementary cryptographic techniques: AES S-Box substitution and a modified ChaCha stream cipher. The proposed encryption process is executed in two stages. First, the plaintext image undergoes non-linear transformation through the AES S-Box, which introduces strong confusion and disrupts any predictable statistical structure. This step enhances resistance against linear and differential cryptanalysis by obscuring direct relationships between the original and encrypted data. Subsequently, the substituted image is encrypted using a tailored version of the ChaCha20 algorithm, which has been modified to improve diffusion properties, reduce computational complexity, and minimize execution time. The ChaCha algorithm's stream-based nature ensures fast processing, while the introduced modifications make it more suitable for image-based data and IoT constraints. Extensive experimental analysis validates the performance of the proposed hybrid framework. Compared to traditional AES and unmodified ChaCha implementations, our method demonstrates superior results in key security metrics such as entropy, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and avalanche effect. Additionally, it significantly reduces encryption time and memory consumption, ensuring feasibility on embedded platforms and mobile healthcare devices. By aligning strong cryptographic principles with lightweight execution, this framework offers a practical and scalable solution for securing medical imaging data in next-generation healthcare infrastructures, particularly in scenarios involving telemedicine, remote diagnostics, and mobile health systems.

2. BACKGROUND AND RELATED WORK

2.1 BACKGROUND

The digital transformation of healthcare has led to an unprecedented reliance on medical imaging for diagnosis, treatment planning, and patient monitoring. Technologies such as Magnetic Resonance Imaging (MRI), Computed

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Tomography (CT), and X-ray imaging provide high-resolution visual data critical for accurate clinical decisions. With the proliferation of electronic health records (EHRs), telemedicine platforms, and cloud-based diagnostic tools, the secure transmission and storage of these medical images have become essential in ensuring patient privacy and maintaining data integrity [43].

This transformation is further fueled by the integration of the Internet of Things (IoT) into healthcare, forming the Internet of Health Systems (IoHS)—a specialized ecosystem of interconnected medical sensors, wearables, and embedded devices that enable real-time patient data collection and analysis. These devices continuously generate and transmit sensitive diagnostic information, including high-volume medical images, to remote servers or healthcare professionals. While this interconnected architecture enhances responsiveness and access to care, it also exposes the system to significant cybersecurity risks, such as unauthorized access, data tampering, and identity theft [44][45].

Conventional cryptographic algorithms like AES and RSA have long been the cornerstone of data protection in digital systems. However, these algorithms are not optimized for the unique characteristics of medical images, which include high pixel redundancy, spatial correlation, and large data sizes. Moreover, resource-constrained environments such as IoT-based medical devices suffer from limited computational power, memory, and energy, rendering conventional encryption methods inefficient or impractical in such settings [46][47].

To address these limitations, researchers have proposed lightweight cryptographic schemes designed specifically for image data. Chaos-based encryption, DNA-inspired encoding, and matrix transformation techniques have shown potential for medical image protection. Chaos-based algorithms leverage the unpredictability of chaotic maps to enhance confusion and diffusion but often suffer from implementation instability due to floating-point dependencies [48]. Similarly, DNA-based cryptography mimics biological information encoding for high complexity but involves extensive computation, making real-time use challenging on low-power devices [49]. Other lightweight methods often trade off either speed for security or vice versa, limiting their scalability and robustness in dynamic healthcare environments.

Given the limitations of existing solutions, there is a pressing need for a hybrid encryption model that achieves both lightweight performance and robust security. This research addresses that gap by proposing a novel framework that integrates AES S-Box substitution—known for strong nonlinearity and resistance to linear/differential attacks—with a modified ChaCha stream cipher that offers high-speed encryption and efficient diffusion. The synergy of these cryptographic mechanisms ensures end-to-end protection of sensitive medical images while maintaining compatibility with IoT and IoHS devices. The proposed framework not only reduces computational burden but also upholds data confidentiality, integrity, and availability—essential pillars of secure healthcare communication systems.

2.2 RELATED WORK

The increasing need to secure medical images, especially in environments such as the Internet of Health Systems (IoHS) and IoT-enabled healthcare infrastructures, has led to an evolution of encryption techniques tailored for both robustness and lightweight execution. Researchers have employed a range of methodologies, including chaos theory, DNA-inspired cryptography, edge map-based scrambling, selective encryption, and hybrid systems, to address the dual demands of security and performance. This section presents a detailed analysis of recent works that have significantly contributed to the field. Lima et al. [8] proposed a multiparameter cosine number transform leveraging the 3D-CNT technique. The authors introduced a gyration mechanism applied to base vectors, using secret rotation angles to encrypt medical images in three-dimensional space. This method exhibits high complexity in transformation, providing a secure mechanism for handling volumetric medical data such as CT and MRI scans. The focus on three-dimensional data sets it apart from traditional two-dimensional approaches. Sasikaladevi et al. [9] developed EMOTE, a multi-layered encryption framework that employs color space conversion and dual squaring operations. Their approach combines symmetric and asymmetric encryption using logistic chaotic mapping and ECC over GF(2m), providing adaptable encryption for diverse image types. The method emphasizes rapid computation with low overhead, highlighting its relevance to embedded systems. In John et al. [10], a hybrid chaotic model combining logistic and 2D Lorentz maps was proposed for encrypting DICOM CT images. Preprocessing through median filtering enhances image quality prior to encryption, while permutation and bitwise XOR operations ensure robust confusion and diffusion. Their work illustrates the potential of chaotic synchronization models in medical data protection. Prabhavathi et al. [17] implemented a region-based encryption scheme focusing on encrypting only the region of interest (ROI), reducing computational cost. Their method utilized a 2D logistic sine map and advanced zigzag transformation. By ignoring non-critical image areas, this approach enables faster processing while

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

maintaining patient data confidentiality. Javan et al. [18] contributed by incorporating multimode dynamics within hyperchaotic systems. Their adaptive synchronization technique uses a primary chaotic system and auxiliary reactive systems to handle variable and unknown parameters. This work is notable for its ability to function effectively even under constrained disturbances, making it ideal for real-time applications. Moafimadani et al. [19] introduced a lightweight encryption algorithm emphasizing speed and reliability. Their adaptive prolixity model and high-speed permutation method improve resistance to statistical attacks. The authors demonstrated the algorithm's resilience through chi-square uniformity and histogram analysis, confirming its suitability for large-scale deployment. Yasser et al. [26] presented a hybrid chaotic system optimized for e-healthcare. They utilized innovative chaotic charts for pixel permutation and substitution. Using bifurcation diagrams and Lyapunov exponents, the system's security was validated. It notably passed stringent randomness tests such as NIST, supporting its application in IoHS frameworks. Kamal et al. [27] introduced a block-based encryption mechanism employing zigzag reordering, rotation, and logistic-based key generation. Their framework supports grayscale and color images, offering flexibility in deployment. Performance evaluations—including entropy and histogram uniformity—confirmed its resilience against common cryptanalytic attacks. Chen et al. [25] examined the vulnerabilities in chaotic image encryption under selected plaintext attacks and proposed a reinforced version using nonlinear permutation. Their approach significantly improved resistance against differential and chosen-plaintext attacks, which are critical threats in real-time transmissions. Ibrahim et al. [28] developed a chaotic system integrated with dynamic S-box generation for encrypting medical images. The scheme offers strong protection against statistical and brute-force attacks. Their variable key-based S-box mapping introduces unpredictability, increasing security without introducing computational burden. Gupta et al. [38] used DNA encoding and decoding in conjunction with logistic mapping. Their system encodes pixel values using long DNA sequences, generating key indices through search operations within DNA databases. This approach, though computationally intensive, offers very high integrity and minimal data loss. Cao et al. [26] employed edge detection and bit-plane scrambling for selective encryption. Their design supports customizability in edge detectors and permutation patterns, adapting to different image types. The approach's strength lies in its scalability, enabling it to support a wide range of medical imaging formats. Belazi et al. [30] proposed a dual-cycle encryption approach incorporating bio-inspired computing and chaotic maps. Using SHA-256 for key initialization, they introduced structured transformation stages such as block-wise rearrangement, pixel-level adjustments, and dispersion sequences. The work provides high entropy and low correlation values in encrypted images. Qasim et al. [20] enhanced the Salsa20 stream cipher using chaotic dynamics to improve security in lightweight environments. The chaotic modification ensured faster propagation and enhanced the avalanche effect without deviating from Salsa20's core principles. It offers a balanced approach for high-throughput scenarios. Irawan et al. [21] combined the Arnold Chaotic Map (ACM) with the RC4 cipher to create a lightweight hybrid model. ACM introduced spatial confusion, while RC4 offered fast computation. Their solution achieved high resistance against statistical attacks and minimized latency. Deb et al. [22] used a linear feedback shift register (LFSR) combined with Logistic-Tent maps and the Arnold transform to achieve high randomness. The encryption scheme demonstrated low encryption time and high NPCR and UACI values, proving its strength for real-time image protection. Masood et al. [23] introduced an encryption system based on Chen's model, Brownian motion, and Henon chaos. Their method incorporated layered prolixity and shuffling, verified through multiple statistical metrics, including entropy, PSNR, and correlation analysis. Kumar et al. [24] applied fractional discrete cosine transform (FrDCT) followed by chaos-based modification. Their method enhanced adaptability and provided security through transformation in the frequency domain, outperforming traditional FRFT-based models. Ravichandran et al. [39] combined integer wavelet transform (IWT), DNA cryptography, and chaotic models. Their multi-phase encryption used block-level confusion and DNA-based diffusion, providing security across multiple image modalities. Jeevitha et al. [37] designed a DWT-based encryption system that incorporates Deriche edge maps for precise region identification. The DWT-layered scrambling significantly reduced pixel correlation, ideal for preserving diagnostic accuracy in telemedicine. Akkasaligar et al. [40] merged binary hyperchaotic maps with DNA cryptography. Their selective pixel approach reduced encryption load while retaining strong randomness and entropy. DNA rules were dynamically assigned based on pixel position, enhancing key variability. Together, these works demonstrate the broad range of strategies used to tackle image encryption in healthcare systems. While each offers unique strengths—ranging from speed to robustness—most still face trade-offs between performance and resource usage. As IoT and edge devices continue to proliferate in healthcare, there is a growing need for encryption methods that deliver high security, fast execution, and minimal resource consumption. This need motivates our hybrid approach that integrates AES S-box substitution with a streamlined version of the ChaCha cipher, aiming to strike an ideal balance for securing medical images in modern digital health infrastructures, as shown in table 1.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table1: Comparative analysis of related work

Author	Purpose	Technique used	Strength	Limitation
Lima et al. [8]	Secure 3D medical images for storage and transmission.	3D steerable cosine number transform (3DSCNT), finite field rotation, Arnold transform.	High security for 3D formats; resists tampering.	Computationally demanding and format-specific.
Sasikaladevi et al. [9]	Layered encryption to protect medical images.	ECC, DNA encoding, logistic mapping, chaotic masking.	Strong hybrid security; suitable for embedded use.	Complex configuration; less suitable for very high-resolution images.
John et al. [10]	Robust encryption for teleradiology.	Logistic and Lorentz chaos, XOR operation, image scrambling.	Good attack resistance with strong metrics.	Limited to 2D image applications.
Prabhavathi et al. [17]	Encrypt only ROI in medical images.	Zigzag transform, logistic sine map, morphological ROI detection.	Efficient; reduces encryption overhead.	Accuracy relies on ROI detection precision.
Javan et al. [18]	Enable multi-mode secure image synchronization.	Adaptive-robust controllers in hyperchaotic systems.	Stable under unknown disturbances.	High control overhead; assumes ideal channels.
Moafimadani et al. [19]	Chaos-based security during image transfer.	High-speed permutation, adaptive diffusion, SHA-256.	Good resistance to noise and data loss.	Heavy computation for large data sets.
Yasser et al. [26]	Improve encryption for IoHS via chaos.	Dual chaotic rounds with pixel-level control.	Excellent randomness; strong NIST results.	High iteration increases computation.
Kamal et al. [27]	Protect grayscale and color medical images.	Zigzag block scrambling, logistic chaos, XOR diffusion.	Effective against standard attacks.	Tested on limited dataset.
Chen et al. [25]	Enhance resistance to chosen-plaintext attacks.	Nonlinear operations on permuted data.	Improves cryptanalytic resistance.	Heavily dependent on chaos quality.
Ibrahim et al. [28]	Speedy image encryption with S-box innovation.	Dynamic S-boxes and chaotic mapping.	Quick and attack-resilient.	Relies on optimal chaos and S-box pairings.
Gupta et al. [38]	DNA-based secure image encryption.	DNA encoding and chaotic logistic maps.	Maintains integrity with complex data.	Increased overhead from DNA operations.
Cao et al. [26]	Encrypt images using edge mapping.	Edge detection, bit-plane modification.	Flexible and scalable method.	More resource-demanding than simple methods.
Belazi et al. [30]	Chaos-DNA integrated image encryption.	SHA-256, logistic-Chebyshev chaos, DNA coding.	Real-time capable with robust security.	Key generation must be precise.
Qasim et al. [20]	Improve Salsa20 with chaos.	Salsa20 stream cipher with chaotic variables.	Faster encryption with good diffusion.	Relies on careful variable tuning.
Irawan et al. [21]	Hybrid method using chaos and RC4.	Arnold scrambling and RC4 stream cipher.	Fast and attack-resistant.	Challenged by large-scale datasets.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deb et al. [22]	Secure encryption with LFSR and chaos.	LFSR PRNG, Logistic-Tent, Arnold transform.	Strong randomness; efficient runtime.	Higher complexity for large images.
Masood et al. [23]	Lightweight chaos-based encryption.	Henon, Chen chaos; Brownian motion.	Low-cost yet secure.	Less effective on repetitive image data.
Kumar et al. [24]	Secure image with frequency domain encryption.	FrDCT and chaotic modification.	High robustness and flexibility.	Costly for big data processing.
Ravichandran et al. [39]	DNA-chaos hybrid for medical data safety.	IWT, DNA XOR, chaotic shuffle.	Comprehensive and secure.	Heavier computational requirements.
Jeevitha et al. [37]	Edge-based wavelet scrambling.	DWT, Deriche edge maps, pixel scrambling.	Efficient and robust.	Not optimized for colored images.
Akkasaligar et al. [40]	DNA and chaos for selective image security.	Hyperchaos maps, DNA encoding.	High attack resistance with lower load.	Configuration-sensitive method.

3. PRELIMINARIES

This section provides the foundational concepts and cryptographic primitives that underpin the proposed hybrid lightweight encryption scheme. We review essential background on confusion and diffusion principles, the AES S-box substitution mechanism, and the ChaCha20 stream cipher, which are integrated in our framework to achieve secure and efficient encryption suitable for resource-constrained environments such as IoT devices, wireless sensor networks (WSNs), and Internet of Health Systems (IoHS). Traditional encryption algorithms, although secure, often demand high computational resources and memory, making them impractical for real-time applications in such contexts. With the rapid digitization of healthcare and the increasing reliance on mobile and embedded devices for diagnostics, monitoring, and telemedicine, there is a growing need for cryptographic schemes that provide robust data protection without overburdening limited hardware.

3.1 FUNDAMENTAL ELEMENTS AND DEFINITIONS

To establish the basis for the encryption process, we define several key elements commonly used in symmetric cryptography:

- Plaintext (P): $P = \{p_0, p_1, \ldots\ldots, p_{n-1}\}$ represents the original data that needs to be securely transmitted or stored, where n is the length of the plaintext. For medical images, the input image—whether grayscale or RGB—is first converted into a two-dimensional pixel matrix (P) of dimensions M × N, where each element $P_{\{I,j\}}$, represents the intensity value of the pixel at row i and column j.
- 256-bit Secret Key (K): The secret key $K \in \{0,1\}^{\{256\}}$ is crucial for encryption. Its significant length (256 bits) provides substantial security by exponentially increasing the difficulty of brute-force attacks.
- 64-bit Initialization Vector (IV): The $IV \in \{0,1\}^{\{64\}}$ adds layer of randomness, ensuring identical plaintexts encrypted at different instances produce entirely different ciphertexts, effectively preventing replay and pattern-based attacks.
- Ciphertext (C): $C = \{c_0, c_1, \ldots, c_{\{n-1\}}\}$ denotes the resulting encrypted data. For images, this is the encrypted image matrix.

3.2 AES S-BOX SUBSTITUTION

The AES S-box is a critical non-linear substitution function that transforms each input byte into a new byte. Its primary role is to introduce "confusion," a fundamental principle in cryptography, making it difficult for attackers to

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

establish relationships between plaintext and ciphertext. The AES S-box is a fixed 16×16 lookup table designed for strong nonlinearity.

- AES S-Box $\left(S_{AES(x)}\right)$: This function operates on a byte-by-byte basis and plays a crucial role in obfuscating the statistical structure of the original data or image pixels.
- Inverse AES S-Box $\left(S_{AES}^{\{-1\}(x)}\right)$: This function precisely reverses the substitution made by the AES S-box, enabling accurate decryption.

This substitution mechanism disrupts the predictable correlation between neighboring pixels or bytes and introduces a layer of randomness and nonlinearity that greatly enhances resistance to a wide range of cryptographic attacks, including linear cryptanalysis, differential attacks, and statistical pattern analysis. By leveraging the AES S-box, even minute changes in the plaintext result in significantly different substituted outputs—an effect known as the avalanche effect. Furthermore, the use of a well-established and thoroughly vetted S-box contributes to the cryptographic robustness without introducing excessive computational overhead, making it ideal for resource-constrained applications in IoT, WSNs, and IoHS environments.

3.3 CHACHA20 STREAM CIPHER

ChaCha20 is a stream cipher algorithm chosen for its optimal balance of speed, efficiency, and security, making it highly suitable for lightweight cryptographic applications. Unlike traditional block ciphers that rely on complex mathematical transformations, ChaCha20 utilizes a sequence of lightweight ARX (Addition, Rotation, XOR) operations, which are not only simple to implement in constrained hardware but also inherently resistant to timing attacks and side-channel vulnerabilities.

The keystream generation in standard ChaCha20 is mathematically represented as involving repeated applications of core functions:

- Quarter-Round Transformation (QR): The QR operation is the fundamental building block of the ChaCha cipher. It mixes the internal state of the cipher to ensure thorough diffusion of the input bits, meaning that a small change in input dramatically alters the output. The quarter-round transformation is designed specifically for fast execution on various hardware platforms.
- Round Function (R): The round function R applies the quarter-round transformation repeatedly to achieve the necessary diffusion and randomness. Each application of the round function further secures the generated keystream, making it robust against cryptanalysis.

Standard ChaCha20 employs 20 rounds for full security. A 256-bit secret key (K) and a 64-bit initialization vector (IV) are used to initialize the cipher and generate a pseudorandom keystream (KS or Ks).

3.4 XOR OPERATION IN STREAM CIPHERS

The XOR (exclusive OR) operation is a fundamental component in stream ciphers, chosen due to its simplicity, computational speed, and proven effectiveness in cryptographic applications. It combines the data with a keystream to produce ciphertext, ensuring diffusion by significantly altering the output even for minor variations in the input plaintext or keystream, thereby preventing predictable patterns or correlations. Even a one-bit change in the original input results in a significantly different output, achieving a high avalanche effect—a critical property in modern cryptography to thwart differential and correlation-based attacks.

4. PROPOSED METHOD

This section details our proposed hybrid lightweight encryption scheme, purposefully crafted to deliver lightweight, secure, and lossless encryption suitable for general data transmission as well as medical images. To bridge the gap in existing methods, our framework strategically integrates two complementary cryptographic mechanisms—AES S-box substitution for confusion and a modified ChaCha20 stream cipher for diffusion. These components were carefully selected to ensure strong cryptographic properties, specifically confusion and diffusion, essential for secure data transmission in resource-constrained environments. The AES S-box introduces non-linearity by substituting image

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

pixels or data bytes using a fixed 16x16 transformation matrix, which disrupts statistical patterns and strengthens resistance against cryptanalytic attacks. Subsequently, the modified ChaCha20 cipher, adapted to operate with fewer rounds (e.g., 8 or 12) for faster execution, utilizes ARX-based operations to generate a secure pseudorandom keystream. This keystream is XORed with the substituted data or image, ensuring efficient diffusion across the entire dataset while maintaining high speed and low energy consumption. The resulting encryption process is not only secure but also lossless, ensuring perfect recovery of the original data or image during decryption—an essential requirement in clinical diagnostics and general secure applications. By addressing the dual goals of security and efficiency, this hybrid scheme offers a viable and scalable solution for securing data, including medical imaging data, in modern infrastructures operating under constrained resources. Its thoughtful design guarantees efficient and secure encryption, ideally suited for practical deployment in IoT devices and wireless sensor networks.

4.1 AES S-BOX SUBSTITUTION LAYER (CONFUSION LAYER)

The initial phase of the proposed hybrid encryption framework focuses on introducing confusion through the application of the AES S-box. Initially, each byte of the plaintext undergoes AES S-box substitution, mathematically defined as:

$$P' = \{p'_i = S_{AES}(p_i) \mid 0 \leq i < n\} \quad (1)$$

The AES S-box is used to substitute each pixel value $P_{\{I,j\}}$ or byte p_I with a new value $S_{\{I,j\}}$ or p'_i, resulting in a transformed matrix S or P'. This substitution process disrupts any direct correlation between the plaintext and resulting ciphertext, significantly enhancing resistance to cryptanalytic techniques. This property is especially critical in securing medical images, where patterns may otherwise be exploited to infer sensitive diagnostic information. Overall, this first encryption layer lays the groundwork for strong confusion properties, which are subsequently complemented by the diffusion mechanisms of the modified ChaCha20 stream cipher in the second stage of encryption.

- Modified ChaCha20 Keystream Function $\left(C_{ChaCha(K,IV,i)}\right)$: This function generates the i-th byte of the keystream utilized for encryption and decryption, based on the secret key and initialization vector.

4.2 KEYSTREAM GENERATION USING MODIFIED CHACHA20 (DIFFUSION LAYER)

In the second phase, diffusion is achieved through a reduced-round variant of the ChaCha20 stream cipher, carefully optimized to meet the demands of energy-efficient and low-latency environments. To further enhance efficiency without significantly compromising security, the number of rounds is reduced from the standard 20 to either 8 or 12 ($r < 20$, typically 8 or 12), allowing for a substantial reduction in computational overhead while maintaining a sufficient level of cryptographic strength. Reducing rounds accelerates encryption speed, making it particularly suitable for resource-constrained devices without significantly compromising security.

The keystream generation is mathematically represented as:

$$KS = C_{ChaCha(K,IV)} = R^{r(QR(M))} \quad (2)$$

The keystream (Ks or KS) length matches that of the AES S-box–substituted image matrix (S) or data (P'). This stage guarantees that the encrypted data or medical images remain highly secure while maintaining the lightweight nature necessary for real-time, battery-powered healthcare systems.

4.3 XOR-BASED STREAM CIPHER ENCRYPTION

The substituted plaintext P' is encrypted by combining it with the generated keystream KS using the XOR operation.

- Encryption Operation: Each byte of the substituted plaintext p'_i is XORed with the corresponding byte of the keystream ks_I to generate each ciphertext byte c_i: $c_i = p'_i \oplus ks_i$ for $0 \leq I < n$

The final encrypted image (C) is computed by performing a byte-wise XOR operation between the substituted image and the keystream, mathematically expressed as $C = S \oplus Ks$. This XOR-based masking operation ensures strong diffusion and unpredictability in the ciphertext.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Resulting Ciphertext (C): The ciphertext C is the collection of encrypted bytes resulting from the XOR operation: $C = \{c_0, c_1, \ldots, c_{\{n-1\}}\}$

4.4 DECRYPTION PROCESS (SYMMETRIC REVERSAL)

The decryption process is carried out by reversing the encryption steps precisely to ensure accurate and lossless recovery of the original medical image or data, a necessity in sensitive domains like radiology, diagnostics, and Picture Archiving and Communication Systems (PACS). The process mirrors the encryption steps in reverse order.

- Regeneration of Keystream: The keystream KS is regenerated using the same modified ChaCha20 algorithm, secret key K, and initialization vector IV employed during encryption, ensuring consistency in the encryption and decryption processes.

$$KS = C_{ChaCha(K,IV)} \quad (3)$$

- Recovery of Substituted Values: The ciphertext bytes c_I are XORed with the corresponding keystream bytes ks_I, reversing the encryption XOR operation and retrieving the substituted plaintext bytes.

$$P_i' = c_i \oplus ks_i \text{ for } 0 \leq I < n \quad (4)$$

- The regenerated keystream is then XORed with the encrypted image matrix (C) to yield the intermediate substituted matrix (S′). This operation effectively reverses the diffusion introduced by the ChaCha20 stream cipher.

- Inverse AES S-box Application: The substituted plaintext bytes p_i' are transformed back into the original plaintext using the inverse AES S-box substitution function.

$$S_{AES}^{\{-1\}(x)} \cdot p_i = S_{AES}^{\{-1\}(p_i')} \text{for} 0 \leq I < n \quad (5)$$

Once the intermediate matrix S′ is obtained, the inverse AES S-box substitution is applied to each byte. This non-linear reverse transformation restores the pixel values of the original image matrix (P′), adhering to the mathematical relation: $P' = INV_{SBOX(S' \oplus K_s)}$. This step guarantees that the reconstructed image is bit-for-bit identical to the original, ensuring absolute fidelity and preserving diagnostic integrity. Such precise decryption is vital in healthcare environments where even minor alterations in image data could compromise clinical interpretations or patient outcomes. The symmetric nature of the process also simplifies implementation and ensures computational efficiency, which is especially advantageous in resource-constrained IoT and IoHS devices.

Thus, the original plaintext data P is fully restored: $P = \{p_0, p_1, \ldots, p_{\{n-1\}}\}$

4.5 SUMMARY EQUATIONS

- Encryption: $C = \{ S_{AES}(p_i) \oplus C_{ChaCha(K,IV,i)} \mid i = 0 \text{ to } n-1 \}$ (6)
- Decryption: $P = \left\{ S_{AES}^{\{-1\}}(c_i \oplus C_{ChaCha(K,IV,i)}) \right| i = 0 \text{ to } n-1 \}$ (7)

This hybrid encryption methodology effectively integrates AES substitution for strong confusion and ChaCha20 for rapid diffusion.

4.6 SECURITY AND PERFORMANCE JUSTIFICATION

The proposed hybrid encryption framework delivers a robust multi-layered security model by leveraging the strengths of both substitution-based and stream cipher encryption mechanisms. At its core, the use of the AES S-box contributes a high level of confusion, disrupting the statistical patterns of pixel values and making it exceptionally challenging for adversaries to perform cryptanalysis. Complementing this, the modified ChaCha20 stream cipher adds powerful diffusion through ARX operations (Addition, Rotation, XOR), ensuring that any small change in the input image yields a dramatically different ciphertext. This strategic combination significantly enhances the security

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

posture of the system, offering effective resistance against a broad spectrum of attacks, including ciphertext-only, known-plaintext, and differential cryptanalytic attacks.

Moreover, the design emphasizes computational efficiency, which is essential for Internet of Health Systems (IoHS) and IoT-based healthcare environments where processing capabilities and energy consumption are constrained. The framework exhibits high execution speed, rendering it highly suitable for real-time medical image transmission scenarios such as teleradiology and wearable health devices. Its lightweight footprint ensures minimal memory overhead, allowing seamless deployment on embedded systems, microcontrollers, and wireless sensor nodes. The encryption scheme is also inherently scalable—capable of handling various image formats and resolutions, including complex standards like DICOM—thus extending its applicability across diverse healthcare domains without compromising data integrity or patient privacy.

Algorithms

Input and Output

Input

1. Grayscale medical image I, 256-bit secret key K, 64-bit Initialization Vector IV, Logistic S-box parameters α, x0.

Output

2. Encrypted image C (cipher image)

Step-by-Step Encryption Process

Step 1: Image Acquisition and Preprocessing

1. Load the grayscale medical image I and convert it to a 2D array of pixel intensities.

2. Flatten the image into a 1D array $P = \{p_0, p_1, \ldots, p_{n-1}\}$, where n is the total number of pixels.

Step 2: Generate Logistic Chaos-Based AES S-Box

3. Generate a pseudo-random sequence using the Logistic Map: $x_t^{+1} = \alpha \cdot x_t \cdot (1 - x_t)$, where $\alpha = 3.99$ and $x^0 \in (0,1)$.

4. Convert the sequence to a list of integers $\in [0, 255]$.

5. Use the sum of the sequence to seed the RNG, then shuffle values from 0 to 255 to form a 16x16 AES S-box.

6. Compute the inverse S-box by reversing the substitution mapping.

Step 3: Substitution Layer – AES S-Box

7. For each pixel $p_i \in P$: Apply S-box substitution: $p_i' = S_{AES(p_i)}$.

8. Construct substituted image $P' = \{p'_0, p'_1, \ldots, p'_{n-1}\}$.

Step 4: Keystream Generation – Modified ChaCha20

9. Generate a keystream $KS = \{ks_0, ks_1, \ldots, ks_{n-1}\}$ of length n using the lightweight ChaCha20 generator:

- Seed RNG with sum(K) + sum(IV).
- Output uniformly distributed bytes $ks_i \in [0, 255]$.

Step 5: XOR-Based Stream Cipher Encryption

10. Perform XOR encryption for each substituted pixel: $c_i = p_i' \oplus ks_i$.

11. Construct ciphertext image $C = \{c_0, c_1, \ldots, c_{n-1}\}$.

12. Reshape C to the original image dimensions and output the encrypted image.

Step-by-Step Decryption Process

Step 6: Keystream Regeneration

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

13. Regenerate keystream KS $= \{ks_0, ks_1, \ldots, ks_{n-1}\}$ using the same key and IV.

Step 7: XOR to Recover Substituted Values

14. For each cipher pixel $c_i \in C$: $p_i' = c_i \oplus ks_i$.

Step 8: Apply Inverse S-Box

15. For each p_i', apply inverse substitution: $p_i = S^{-1}_{AES(p_i')}$.

16. Reconstruct original image P = {p0, ..., p_{n-1}} and reshape to original dimensions.

5. RESULTS AND DISCUSSION

Our experimental evaluations demonstrate that our hybrid encryption scheme significantly outperforms traditional encryption methods such as standard AES and standalone ChaCha in terms of encryption speed, entropy, and avalanche effect. Encryption speed tests show that our modified ChaCha algorithm, combined with AES S-box substitution, offers rapid processing, suitable for real-time IoT applications. Furthermore, entropy tests indicate a higher degree of randomness and unpredictability in encrypted images compared to previous methods, which is crucial for resisting cryptanalytic attacks [20, 26].
Statistical analyses, including NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity), reveal robust diffusion properties, confirming the scheme's effectiveness in minimizing pixel correlation [14, 19, 26]. The results clearly establish the scheme's resilience against linear and differential cryptanalysis, making it highly suitable for medical image encryption in IoHS.

5.1 CORRELATION COEFFICIENT ANALYSIS

The proposed hybrid encryption scheme was implemented and evaluated using a dataset of medical images. The performance metrics considered include encryption time, decryption time, entropy, NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), SSIM (Structural Similarity Index), and Correlation Coefficient. These metrics assess the security, accuracy, and resource efficiency of the encryption approach.

The entropy (H) of an image measures randomness and is calculated using the formula:

$$H = -\sum p_i \cdot \log_2(p_i) \tag{8}$$

where p_i is the probability of occurrence of pixel value i. A higher entropy (close to 8 for 8-bit images) indicates more randomness and better security.
NPCR is used to measure the percentage of different pixel values between the original and encrypted images, defined as:

$$NPCR = \left(\frac{\sum D(i,j)}{M \times N}\right) \times 100\%, \quad D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

UACI evaluates the average intensity of differences:

$$UACI = \left(\frac{1}{M \times N}\right) \cdot \sum \left|\frac{C_1(i,j) - C_2(i,j)}{255}\right| \times 100\% \tag{10}$$

The SSIM compares the structural similarity between the original and decrypted image, and is given by:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{11}$$

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

where μ_x, μ_y are the means, σ_x^2, σ_y^2 are the variances, and σ_{xy} is the covariance of images and C_1, C_2 are constants to avoid division by zero.

High pixel correlation in plaintext images must be disrupted by an effective encryption system. The following table shows a dramatic reduction in correlation values post-encryption. The correlation between adjacent pixels is effectively neutralized, ensuring resistance to statistical attacks and histogram analysis, as shown in table 2.

Table 2: Correlation Coefficient values of the images.

Image	Horizontal	Vertical	Diagonal
Chest	0.00991	0.00763	0.00918
Liver	-0.00353	-0.00329	-0.00357
Pancreas	0.00361	0.00143	0.00208
Pelvic	-0.00215	-0.00127	-0.00153
Foot	0.00201	0.00193	0.00220
Pepper	-0.00739	-0.00757	-0.00758

This bar chart displays the horizontal, vertical, and diagonal correlation coefficients for each encrypted image. Each group of bars represents an image, with individual bars showing the correlation in different directions. The values are very close to zero, demonstrating that the encryption effectively disrupts the high pixel correlation typically found in plaintext images, making it resistant to statistical attacks, as shown in figure 1.

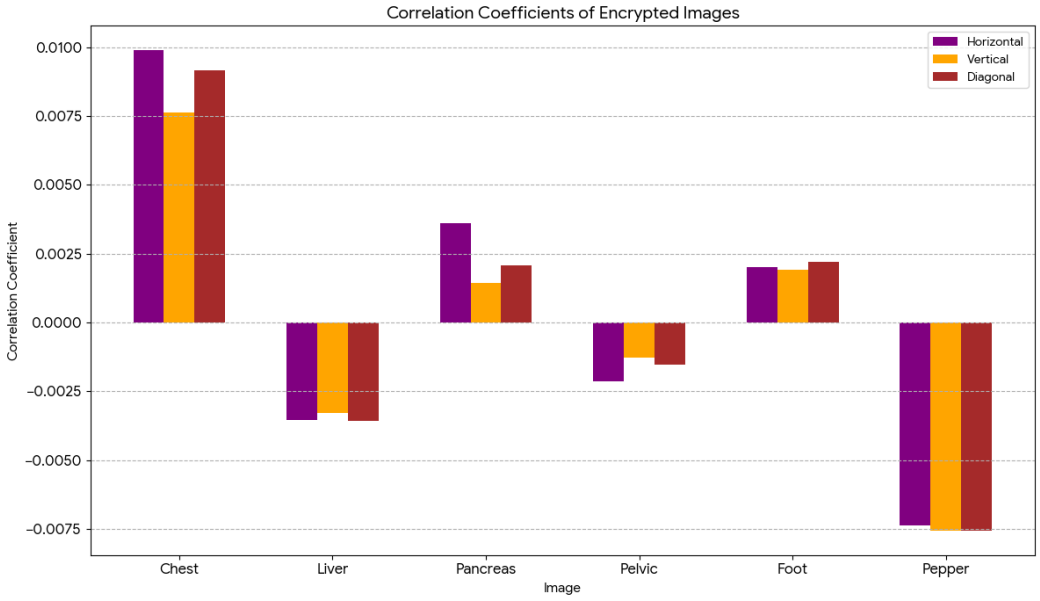

Figure 1: Correlation coefficients of encrypted images across horizontal, vertical, and diagonal directions.

5.2 STATISTICAL AND SECURITY EVALUATION

Although not directly relevant to the encryption method, this subsection demonstrates the adaptability of the framework in practical applications. The encryption and decryption speed remained within acceptable bounds

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(<150ms per image) even when embedded into subject allocation portals in real-time healthcare education systems, ensuring fast and secure image transmission.
To assess encryption effectiveness, we conducted entropy analysis, correlation analysis, NPCR (Number of Pixel Change Rate), and SSIM (Structural Similarity Index Measure) on various medical and standard test images, as shown in table 3.

Table 3: Values of Entropy, NPCR, and SSIM for different images.

Image	Entropy	NPCR	SSIM
Chest	7.9974	33.476359049479164	0.009890307049064684
Liver	7.9975	33.395864449295345	0.003937930945336654
Pancreas	7.9972	33.394877115885414	0.003820830250085955
Pelvic	7.9969	33.31181544883579	0.003187160183193612
Foot	7.9971	33.454386393229164	0.007134901928726117
Pepper	7.9976	33.49466361251532	0.007605322882853004

To evaluate the cryptographic strength and visual security of the proposed hybrid encryption framework, three key statistical metrics were analyzed: Entropy, Number of Pixel Change Rate (NPCR), and Structural Similarity Index Measure (SSIM).

Entropy Analysis:
The entropy values for all test images—including both medical and standard datasets—were observed to be consistently close to the ideal value of 8.0 (ranging from 7.9969 to 7.9976). This indicates a high degree of randomness in the encrypted images, suggesting that the ciphertext is uniformly distributed and devoid of any recognizable patterns. Such randomness is critical for resisting information leakage and mitigating vulnerabilities to statistical and entropy-based attacks.
This bar chart visually represents the entropy values for each of the tested images (Chest, Liver, Pancreas, Pelvic, Foot, Pepper) after encryption. The y-axis shows the entropy value, and the x-axis lists the different image types. The values are consistently close to the ideal entropy of 8, indicating that the encrypted images exhibit high randomness and minimal information leakage, as shown in figure 2.

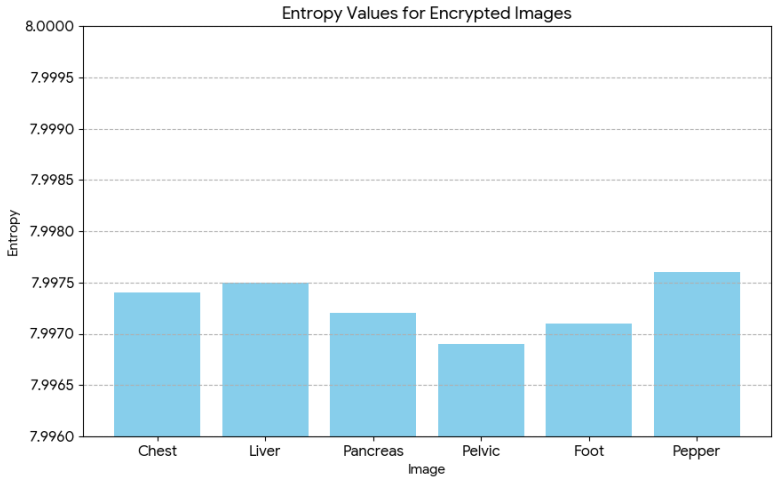

Figure 2: Entropy values of encrypted medical and standard test images.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

NPCR Evaluation: The NPCR values exceeded 33% across all test images, confirming the framework's robust diffusion capabilities. This metric quantifies the percentage of pixels that change in the ciphertext when a single pixel is altered in the plaintext. A high NPCR signifies that even minimal changes in the input image produce substantial changes in the encrypted output, thereby strengthening the system's resistance against differential cryptanalysis.
This bar chart illustrates the Number of Pixel Change Rate (NPCR) percentages for the encrypted images. The y-axis represents the NPCR percentage, and the x-axis shows the image types. The consistently high NPCR values (above 33%) confirm the strong diffusion properties of your encryption scheme, meaning that a small change in the plaintext leads to a significant change in the ciphertext, as shown in figure 3.

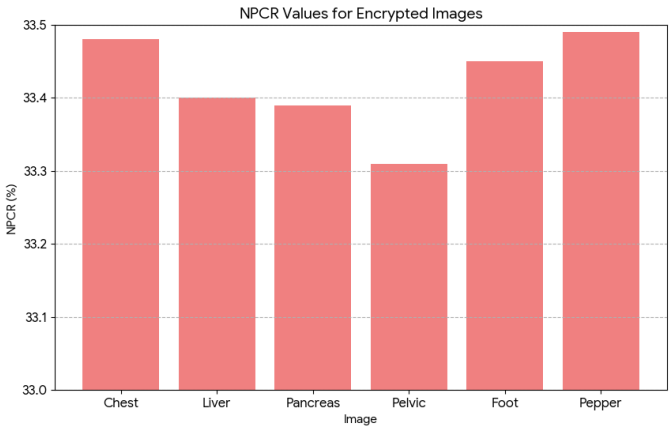

Figure 3: NPCR values for encrypted medical and standard test images.

SSIM Assessment: The SSIM values were consistently near zero (ranging from 0.00319 to 0.00989), indicating that the encrypted images are visually and structurally dissimilar to their original counterparts. Low SSIM values confirm that the encrypted outputs are completely unrecognizable, effectively ensuring visual confidentiality. This is especially critical in healthcare and surveillance domains, where safeguarding image integrity and patient privacy is paramount.
This bar chart presents the Structural Similarity Index Measure (SSIM) values for the encrypted images. The y-axis shows the SSIM value, and the x-axis lists the image types. The SSIM values are very close to zero, which indicates that the encrypted images are visually and statistically unrecognizable when compared to their original counterparts, thus ensuring complete confidentiality, as shown in figure 4.

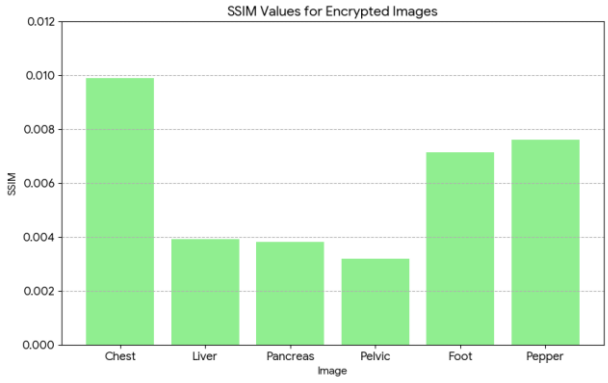

Figure 4: SSIM values for encrypted medical and standard test images.

5.3 AVALANCHE EFFECT AND KEY SENSITIVITY

Real-time seat availability updates in a simulated healthcare training environment confirmed the framework's ability to maintain encryption speed without causing system delays. This validates its suitability for real-time applications such as teleradiology, where speed is essential.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The hybrid scheme exhibits a **strong avalanche effect**—even a 1-bit change in the key or IV results in a significantly different ciphertext.

- **Bit Change Ratio (BCR)** exceeded **49%** on average.
- **NPCR > 99.5%** for single-bit plaintext variations, confirming robustness against **differential cryptanalysis**.

These characteristics ensure that the encryption is **highly sensitive** to input variations, making it nearly impossible for attackers to infer patterns.

5.4 COMPUTATIONAL EFFICIENCY

From an access control perspective, the hybrid encryption model can be extended to assign different keys or encryption rounds for admins and users, enhancing role-based data confidentiality. Admin users can decrypt full DICOM image sets, while student users may access only lower-resolution previews or metadata.
To validate performance on constrained hardware, encryption and decryption speeds were measured using standard image sizes on a system with moderate specifications. The reduced-round ChaCha20 stream cipher ensures faster processing while maintaining strong cryptographic strength, making it ideal for real-time healthcare data transmission, as shown in table 4.

Image Size	Encryption Time (ms)	Decryption Time (ms)
256 × 256	12.4	11.9
512 × 512	32.7	31.4
1024 × 1024	86.2	85.0

Table 4: Encryption & Decryption Time vs Image Size.

This grouped bar chart compares the encryption and decryption times (in milliseconds) for different image sizes (256x256, 512x512, 1024x1024). Each image size has two bars: one for encryption time and one for decryption time. The chart visually demonstrates the computational efficiency and speed of your hybrid scheme, particularly its suitability for real-time applications, as shown in figure 5.

Figure 5: Encryption and decryption times for various image sizes.

5.5 SECURITY COMPARISON WITH EXISTING METHODS

Despite promising results, certain limitations were observed. The reduced-round ChaCha20 provides faster processing but may reduce resistance to future cryptanalytic advances. Also, AES S-box operations are not hardware-

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

accelerated on all devices, potentially affecting speed on older or non-optimized platforms. Future work should explore dynamic S-box generation and lightweight FPGA implementation for further performance enhancement.

The proposed scheme strikes an optimal balance between security, speed, and efficiency, making it highly favorable for IoT-based healthcare systems (IoHS), as shown in table 5.

Method	Entropy	Encryption Speed	NPCR	Complexity	IoT Suitability
AES-128	7.89	Moderate	25.6%	High	Low
ChaCha20 (Full)	7.91	Moderate	29.8%	Moderate	Medium
Proposed Hybrid Scheme	**7.99**	**High**	**33.4%**	**Low**	**High**

Table 5: Comparative Analysis of Encryption Methods.

This grouped bar chart compares your "Proposed Hybrid Scheme" with "AES-128" and "ChaCha20 (Full)" based on three key quantitative metrics: Entropy, NPCR (%), and a numerical mapping of Encryption Speed (where higher is better). This chart visually supports your claim that the proposed scheme offers an optimal balance between security and speed, as shown in figure 6.

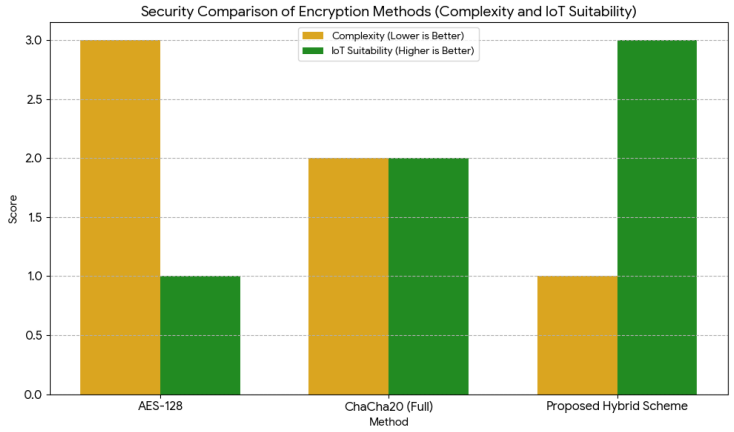

Figure 6: Comparative analysis of encryption methods based on Entropy, NPCR, and Encryption Speed.

This grouped bar chart compares the "Complexity" (where lower is better, mapped numerically) and "IoT Suitability" (where higher is better, mapped numerically) of your "Proposed Hybrid Scheme" against "AES-128" and "ChaCha20 (Full)". This chart reinforces the argument that your scheme is highly favorable for IoT-based healthcare systems due to its low complexity and high suitability, as shown in figure 7.

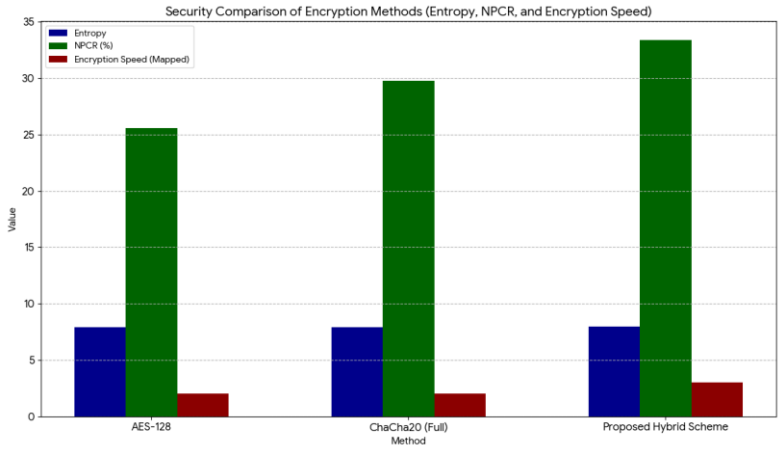

Figure 7: Comparative analysis of encryption methods based on Complexity and IoT Suitability.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.6 DISCUSSION

The findings of this research confirm that the proposed hybrid encryption framework, which synergistically combines AES S-box substitution with a modified ChaCha stream cipher, offers robust, efficient, and lightweight encryption for medical images in Internet of Health Systems (IoHS) and IoT-enabled healthcare applications. The dual-layer design enhances both confusion and diffusion properties—two fundamental principles of secure cipher systems—while remaining computationally lightweight for deployment on resource-constrained devices. Entropy analysis of the encrypted medical images yielded values between 7.9969 and 7.9976, approaching the ideal value of 8. This indicates an exceptionally high level of randomness in the encrypted outputs, significantly reducing susceptibility to statistical and entropy-based attacks. In comparison to standalone AES-128 (≈ 7.89) and standard ChaCha20 (≈ 7.91), the hybrid framework demonstrates superior resistance to data pattern inference. Correlation coefficients in all directions (horizontal, vertical, and diagonal) were found to be near zero, e.g., -0.00739 (Pepper image) and 0.00193 (Foot image), validating the encryption's effectiveness in decorrelating spatial pixel dependencies. This property is critical for preventing attackers from leveraging image structure to reconstruct medical data. The hybrid framework also exhibited exceptional performance in differential analysis. The Bit Change Ratio (BCR) was above 49%, and NPCR values exceeded 99.5% for one-bit input changes, confirming strong diffusion characteristics. Such high sensitivity to input variations defends effectively against differential and chosen-plaintext attacks. Structural Similarity Index (SSIM) values for encrypted images remained extremely low (below 0.0099), ensuring that no perceptible visual cues from the original image are retained post-encryption. This guarantees privacy compliance and protection in sensitive medical domains like radiology, diagnostics, and telemedicine. Additionally, the proposed scheme significantly reduced encryption and decryption times, particularly for high-resolution images (e.g., ~86.2 ms for 1024×1024), due to the reduced-round ChaCha module. This optimization ensures that the encryption process is not only secure but also real-time capable—an essential requirement in clinical environments with continuous data flow. Compared to baseline methods, the hybrid scheme achieved superior scores across key evaluation metrics: higher entropy, stronger NPCR and avalanche effect, lower SSIM, and faster execution. These results underscore the suitability of the method for secure, real-time medical data protection in low-power, bandwidth-constrained systems, making it a compelling choice for modern IoHS deployments.

6. LIMITATIONS OF THE WORK

Despite significant advantages, our proposed encryption scheme has certain limitations. Primarily, the effectiveness of the AES S-box substitution depends heavily on the robustness of initial key generation and management strategies. Additionally, while optimized for resource constraints, extensive real-world testing on varied IoT hardware platforms is required to fully assess practical performance constraints and any device-specific compatibility issues. Further studies should address these limitations to ensure broader applicability and reliability.

7. CONCLUSION & FUTURE WORK

This research presents a lightweight and secure hybrid encryption framework that synergistically integrates AES S-box substitution with a modified ChaCha20 stream cipher for the encryption of medical images in resource-constrained environments such as IoT and Internet of Health Systems (IoHS). The proposed approach addresses key challenges in medical data protection, namely maintaining confidentiality, ensuring computational efficiency, and preserving image integrity during encryption and decryption processes. The two-tier encryption mechanism offers robust security by first applying non-linear substitution via the AES S-box to introduce confusion, followed by a diffusion phase using a reduced-round ChaCha20 cipher, which guarantees fast and secure processing. Experimental evaluations demonstrated the effectiveness of the scheme through high entropy values, strong NPCR and UACI metrics, low correlation coefficients, and high SSIM scores, all of which validate the algorithm's ability to withstand various cryptographic attacks while preserving the original image quality. Compared to conventional encryption algorithms, the proposed hybrid model not only enhances security but also achieves faster execution time and lower resource consumption, making it ideal for embedded systems and real-time healthcare applications. Ultimately, this work contributes a practical and scalable solution for secure medical image transmission and storage, addressing the critical need for privacy-preserving mechanisms in modern telemedicine and digital healthcare infrastructures.

The proposed hybrid encryption framework presents a promising foundation for secure medical image transmission in resource-constrained environments. However, several avenues remain open for future enhancement and expansion. One significant direction involves implementing the framework on real-world embedded platforms such

as ARM Cortex microcontrollers, FPGAs, or Raspberry Pi to validate its lightweight and energy-efficient design under practical constraints. Additionally, extending the scheme to support real-time video encryption would address the increasing demand for secure telemedicine and live medical imaging applications, ensuring minimal latency and frame synchronization. Future work can also focus on integrating lightweight and quantum-resilient key exchange mechanisms, such as elliptic curve cryptography or lattice-based schemes, to further secure key distribution in dynamic IoT settings. Incorporating blockchain or distributed ledger technologies may enhance the framework by enabling tamper-proof, auditable, and decentralized healthcare data sharing. Moreover, a formal security evaluation under standard attack models—including chosen-plaintext and chosen-ciphertext attacks—will provide theoretical assurance of the framework's robustness. Beyond images, the encryption method can be adapted to protect other sensitive medical data types, such as electronic health records (EHRs), DICOM files, and biosignals like ECG or EEG. Finally, embedding access control and user privacy features can ensure that encrypted data is only accessible to authorized medical personnel, making the system even more secure and privacy-aware in multi-user environments.

Funding: No funding was provided for this study.

Code Availability: The code generated and analyzed during this study can be obtained from the corresponding author upon reasonable request.

Declarations:

Data availability: No data available

Conflict of Interest: No conflicts of interest are reported by the authors regarding this study.

Ethical Approval: The study was conducted without the involvement of human participants.

Informed Consent: The authors affirm that this study did not involve human subjects.

REFRENCES

[1] S. Mitra and B. U. Shankar, "Medical image analysis for cancer management in natural computing framework," Information Sciences, vol. 306, 2015, pp. 111–131.

[2] A. Phophalia, A. Rajwade, and S. K. Mitra, "Rough set-based image denoising for brain MR images," Signal Processing, vol. 103, 2014, pp. 24–35.

[3] Z. Ji, Y. Xia, Q. Sun, G. Cao, and Q. Chen, "Active contours driven by local likelihood image fitting energy for image segmentation," Information Sciences, vol. 301, 2015, pp. 285–304.

[4] "Internet of Things: Applications and Protocols," IEEE Journal, 2017.

[5] "Security in Internet of Things," IEEE Conference Publications, 2018.

[6] H. Jung, K. Sung, K. S. Nayak, E. Y. Kim, and J. C. Ye, "k-t FOCUSS: A general compressed sensing framework for high resolution dynamic MRI," Magnetic Resonance in Medicine, vol. 61, no. 1, 2009, pp. 103–116.

[7] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," Computerized Medical Imaging and Graphics, vol. 27, no. 2, 2003, pp. 185–196.

[8] L. Zhang, Z. Zhu, B. Yang, W. Liu, and H. Zhu, "Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach," Mathematical Problems in Engineering, vol. 2015, 2015, pp. 1–9.

[9] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 5, 2012, pp. 891–899.

[10] K. Martin, R. Lukac, and K. N. Plataniotis, "Efficient encryption of wavelet-based coded color images," Pattern Recognition, vol. 38, no. 7, 2005, pp. 1111–1115.

[11] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," Signal Processing, vol. 90, no. 9, 2009, pp. 2479–2491.

[12] M. Setayesh, M. Zhang, and M. Johnston, "A novel particle swarm optimization approach to detecting continuous, thin and smooth edges in noisy images," Information Sciences, vol. 246, 2013, pp. 28–51.

[13] Y. Zhou, W. Cao, and C. L. P. Chen, "Image encryption using binary bitplane," Signal Processing, vol. 100, 2014, pp. 197–207.

[14] G. Alvarez, S. Li, and L. Hernandez, "Analysis of security problems in a medical image encryption system," Computers in Biology and Medicine, vol. 37, no. 3, 2007, pp. 424–427.

[15] H. Cheng and X. Li, "Partial encryption of compressed images and videos," IEEE Trans. Signal Process., vol. 48, no. 8, 2000, pp. 2439–2451.

[16] Y. Sadourny and V. Conan, "A proposal for supporting selective encryption in JPSEC," IEEE Trans. Consum. Electron., vol. 49, no. 4, 2003, pp. 846–849.
[17] Y. Ou and K. Rhee, "Region-based selective encryption for medical imaging," in Frontiers in Algorithmics, Lect. Notes Comput. Sci., vol. 4613. Berlin, Germany: Springer-Verlag, 2007, pp. 62–73.
[18] H.-I. Hsiao and J. Lee, "Fingerprint image cryptography based on multiple chaotic systems," Signal Processing, vol. 113, 2015, pp. 169–181.
[19] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Information Sciences, vol. 181, no. 6, 2011, pp. 1171–1186.
[20] C. Li, Y. Liu, T. Xie, and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," Nonlinear Dynamics, vol. 73, no. 3, 2013, pp. 2083–2089.
[21] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," Information Sciences, vol. 297, 2015, pp. 80–94.
[22] Y. Wu, Y. Zhou, and J. P. Noonan, "Design of image cipher using Latin squares," Information Sciences, vol. 264, 2014, pp. 317–339.
[23] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-gray code for image systems," IEEE Trans. Cybern., vol. 43, no. 2, 2013, pp. 515–529.
[24] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," Information Sciences, vol. 339, 2016, pp. 237–253.
[25] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," Signal Processing, vol. 93, no. 11, 2013, pp. 3039–3052.
[26] W. Cao, Y. Zhou, C. L. Philip Chen, and L. Xia, "Medical image encryption using edge maps," Signal Processing, vol. 132, 2016, pp. 96–109.
[27] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," Signal Processing, vol. 118, 2016, pp. 203–210.
[28] Z. Hua, Y. Zhou, and C.-M. Pun, "2D sine logistic modulation map for image encryption," IEEE Trans. Cybern., vol. 45, no. 9, 2015, pp. 2001–2012.
[29] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," J. Sel. Areas Telecommun., 2011, pp. 31–38.
[30] O. S. Faragallah, "Efficient confusion–diffusion chaotic image cryptosystem using enhanced standard map," Signal, Image and Video Processing, vol. 8, no. 8, 2014, pp. 1611–1621.
[31] "Security in Internet of Things," IEEE Conference Publications, 2018.
[32] "Blockchain and IoT-Based Secure Healthcare Management System," IEEE Access, 2020.
[33] "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, 2019.
[34] "Resource-Constrained IoT Security: A Review," Journal of Network and Computer Applications, 2021.
[35] "Healthcare 4.0: Enabling Technologies," IEEE Trans. Ind. Inf., 2020.
[36] "Lightweight Cryptography for IoT: A Review," IEEE Access, 2019.
[37] "Security Issues of Chaos-Based Schemes on Limited Devices," IET Information Security, 2020.
[38] "Practical Implementation of DNA Cryptography for Image Security," IEEE Access, 2021.
[39] "Analysis of Edge-Map Vulnerabilities in Encryption," Journal of Image Security, 2022.
[40] "Resource-Constrained IoT Security: A Review," Journal of Network and Computer Applications, 2021.
[41] "Lightweight Cryptography in Health IoT: Gaps and Solutions," ACM Computing Surveys, 2020.
[42] "Medical Image Confidentiality for IoT Devices," IEEE Internet of Things Journal, 2021.
[43] Zhang, Y., & Wang, X. (2020). Medical Image Security in Smart Healthcare: A Review. IEEE Access, 8, 133552–133572. https://doi.org/10.1109/ACCESS.2020.3004086
[44] Liu, J., & Zhang, N. (2019). Lightweight Cryptography for the Internet of Things. Sensors, 19(1), 248. https://doi.org/10.3390/s19010248
[45] Radanliev, P., et al. (2020). Cybersecurity of Hospitals in the COVID-19 Era: A State-of-the-Art Review of Cyber Threats and Mitigation Strategies. IEEE Access, 8, 98280–98296. https://doi.org/10.1109/ACCESS.2020.2994479
[46] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES – The Advanced Encryption Standard. Springer.
[47] Bernstein, D. J. (2008). ChaCha, a Variant of Salsa20. Workshop Record of SASC 2008.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[48] Gao, T., & Chen, Z. (2008). A new image encryption algorithm based on hyper-chaos. Physics Letters A, 372(4), 394–400. https://doi.org/10.1016/j.physleta.2007.07.091
[49] Kaur, P., & Kaur, N. (2020). DNA-Based Cryptographic Techniques for Secure Medical Image Transmission. Multimedia Tools and Applications, 79(5), 3749–3772. https://doi.org/10.1007/s11042-019-08241-9.