Ingénierie des Systèmes d'Information
Vol. 30, No. 4, April, 2025, pp. 845-853
Journal homepage: http://iieta.org/journals/isi

# Efficient Lightweight Cryptographic Framework for Securing Medical Images in IoT Systems

Fadhil Hanoon Abbood[1*], Leila Ben Ayed[2]

[1] Department of Computer Science, College of Education, Mustansiriyah University, Baghdad 61002, Iraq
[2] National School of Computer Science, University of La Manouba, Manouba 2010, Tunisia

Corresponding Author Email: fadhil_alsaadi@uomustansiriyah.edu.iq



https://doi.org/10.18280/isi.300402

**Received:** 26 September 2024
**Revised:** 25 March 2025
**Accepted:** 8 April 2025
**Available online:** 30 April 2025

***Keywords:***
*linear feedback shift register, logistic map, Internet of things, parallel processing*

**ABSTRACT**

In the modern era of cloud computing and the internet of things (IoT), the safe transfer of medical images is crucial. In healthcare systems, medical images play a crucial role in diagnoses. Images such as X-rays, ultrasounds, CT scans, MRIs, and brain scans of patients include private and sensitive information. Unfortunately, unauthorized people could view these photos illegally, using them for non-diagnostic purposes due to weak communication channel security and vulnerabilities in healthcare facilities' storage systems. One standard method for protecting sensitive medical image from attackers is image encryption, which also helps keep data transmission and storage systems secure. A hybrid stream cipher and pixel rearrangement for rows and columns form using parallel processing is the basis of our proposed lightweight cryptosystem. An integral part of medical image encryption is the key generation process, which uses a logistic map and a set of linear feedback shift register (LFSRs) to generate a stream of bytes at random. The suggested method is efficient based on metrics like peak-to-signal noise ratio, encryption time, information entropy, number of pixels changing rate, histogram analysis, and mean square error (MSE). Experiments have proven that the suggested cryptosystem is an effective means of encrypting sensitive patient data stored in images while remaining lightweight.

## 1. INTRODUCTION

Rapid growth of the internet of things (IoT) and cloud computing changes the controls, stores, and transfers medical data, particularly high-resolution medical imaging, in healthcare systems. Access to these technologies has bright sides in reducing time schedules and making services efficient on the one hand, but on the other hand, numerous threats related to security and privacy are implicated [1]. Most medical images need protection against unauthorized access, changes, and disclosure; therefore, the most important due to the increasing rate of cyber-attacks is the setup considered. This paper discusses the issue pertaining to safe transmission and storage of medical images within IoT and cloud-based environments. The major objective is to design a lightweight encryption algorithm suitable for constrained devices while maintaining high security. This work introduces a novel hybrid encryption scheme that combines the cryptographic strength of linear feedback shift register (LFSRs) with the randomness of a one-dimensional chaotic logistic map. This technology is big because it can give great safety with low computing cost, making it right for real-time use in IoT-based healthcare systems. The way improves the field by giving a good and flexible solution made for modern data safety needs. The hybrid encryption system enhances the security of medical image data by generating dynamic stream random encryption keys based on logistics map outputs and linear feedback offset registers in cryptographic systems. One notable property of low-prevention support representations is the remarkable efficiency with which they generate pseudorandom sequences. On the other hand, the high sensitivity of the logistics map to the starting conditions makes it completely unpredictable. This article presents an encryption technique that effectively protects medical images from unauthorized access by integrating the benefits of these two methods and use parallel processing to make the proposed encryption faster and more efficient. Our technique ensures the protection of sensitive information and that the data remains unaltered and reliable throughout its entire duration. This article offers an in-intensity rationalization of the problematic technical additives of our hybrid encryption technique. Furthermore, it examines the practical effects and challenges of integrating this technique into the IoT and cloud networks. As we delve into the aggregate of cryptography and healthcare generation, we are on the brink of accomplishing stable and immediate sharing and garage of clinical photos. Our approach has the capability to revolutionize the virtual panorama of the healthcare industry, resulting in more suitable acceptance as true with, performance, and safety. This article affords an in-depth manual on enhancing protection in linked healthcare.

## 2. RELATED WORK

Encrypting images is essential to uphold healthcare data's security, integrity, and validity, leading researchers to investigate several encryption methods. A novel stenographic technique tailored for medical images is introduced, blending quantum walks, chaotic systems, and the particle swarm optimization algorithm [2]. This technique leverages a 3-D chaotic system, and quantum walks to operate the particle swarm optimization algorithm.

Suggesting a method to encrypt medical images, the approach [3] utilizes an LFSR to generate pseudo-random numbers and rearrange pixel positions, ensuring secure image scrambling for transmission via an online platform and subsequent decryption at the receiver's end node.

The study [4] lays out a 3-stage version: first, the plain picture is processed using the Message Digest five set of rules to generate a seed key for the Lorenz chaotic map. Then, a chaotic key collection is generated with the use of iterated Lorenz mapping. Finally, encryption is ensured using making use of twin confusion strategies and diffusion operations.

A new method was provided [5] for image encryption that makes use of hash functions and dual chaos structures. By hashing plain image with SHA-256 and private keys with SHA-512, we can defend records domestically inside every picture zone and increase encryption resistance towards differential assaults. The proposed encryption method includes two wonderful steps. The preliminary phase employs a chaotic device that relies upon zoning and rotation to purpose confusion, alongside twin hash functions. Part 2 disseminates facts about the use of logistic map processes. Two chaotic systems and two hash capabilities are utilized in a new way to encrypt statistics [6].

In order to boost resistance towards differential attacks and enable local encryption inside each image sector, the obvious image and private keys are processed with the usage of the hashing methods SHA-256 and SHA-512. First, via partitioning and rotating encrypted blocks, the cautioned encryption technique carries a chaotic system and dual hash characteristic; 2nd, through using logistic map processes, it contains diffusion. This essay proposed a novel cryptosystem for secure healthcare [7].

It has two strong modules: one that uses content-aware permutation and diffusion and another that randomly encodes DNA. A novel idea that builds on the LFSR technique was presented [8]. In this two-stage encryption procedure, first, we use the XOR method to shuffle pixels, and then we generate random numbers to rearrange them in rows and columns. Reverse encryption, which involves XOR execution and column and row decryption, is subsequently used to decrypt the final encrypted image. Additionally, the use of discrete Fourier transform watermarking in combination with LFSR was recommended [9] as a method for secure picture authentication.

A chaotic encryption strategy combined with nonlinear filtering based on LFSR was proposed and validated through performance metrics evaluation [10]. The use of LFSR in conjunction with multi-ant cellular automation for image encryption was emphasized [11], while cellular automata was suggested [12] with LFSR for encryption, implemented in Cyclone (FPGA) and tested on various image types, Moreover, an algorithm utilizing LFSR-generated pseudo-random sequences and chaotic functions for image encryption, resistant to statistical attacks [13]. A chaotic-based LFSR strategy for image encryption, incorporating key generation by RC4 key generator was present [14], in which image encryption employed LFSR, with key generation through a stream generator, and intermediate cipher image pixels subjected to XOR operation for final cipher image generation. Recent advances in chaotic encryption have demonstrated promising results for securing medical data.

A crypto compression scheme combining the AES algorithm with a hybrid chaotic model (Arnold and Henon maps) has been proposed [15], while a 4D chaotic circuit was deployed for image encryption [16]. Other approaches include rapid image encryption using lifting wavelet transforms with chaotic functions [17], improved chaotic systems for medical image encryption [18], and IoT-focused healthcare encryption leveraging chaotic functions [19]. Additionally, novel methods employing sine tangent chaotic functions for medical image encryption [20] and systematic reviews on medical image security in telemedicine [21] have further expanded this field.

## 3. STREAM CIPHER ENCRYPTION

Text encryption includes the complicated use of circulation ciphers, wherein each single little bit of the ciphertext is carefully built to suit every binary digit in a given data stream cipher. This method is typically referred to as bit-through-bit encryption. Using a one-time panel as the encryption secret is crucial to the move cipher crypto scheme. The vital component is this distinct panel is consistently no smaller than the encrypted message, making certain a terrific degree of protection. Given the precise homes of the only-time pad, it's miles extraordinarily hard to compromise the security of this encryption approach. Stream ciphers outperform block ciphers in phrases of execution speeds due to their advanced performance. Their full-size utilization in numerous packages is also ascribed to the faded hardware intricacy wished for his or her execution. Stream ciphers are prominent through their potential to generate ciphertext always while provided with same blocks of plaintext. Every piece of plaintext reviews modifications in its encryption key in the course of this process. The keys' dynamic nature and intrinsic randomization appreciably boost the safety of the system.

### 3.1 Encryption using LFSRs

The linear comments shifter registers deliver dynamic encryption and specific facts moving. The subsequent kingdom is created by way of bit-linearly merging the current state with a unique OR (XOR) operation in LFSRs, which can be shift registers. In cryptography, LFSRs' cyclic and inescapable behavior is like an allure. The number one advantage of LFSRs in encryption is their efficiency in generating pseudorandom sequences. Cryptographical robustness is predicated on LFSRs' potential to generate prolonged sequences and their robust mathematical characteristics. Using pseudo-randomness makes encryption more unpredictable. The fundamental generators in stream ciphers can also be LFSRs. Bit-by using-bit or byte-by using-byte encryption may be executed fast with keystreams generated with the aid of LFSR. Cryptographic structures are nicely-proper for actual-time encryption or applications with low computational overhead due to their performance and the simplicity and velocity of LFSR operations. In the end, LFSRs

are a powerful encryption technology that effectively combines ease of use, efficiency, and strong cryptography. They are mathematically perfect for use in circulation cipher designs that encrypt touchy records due to their pseudorandom sequences, as shown in Figure 1 [8].

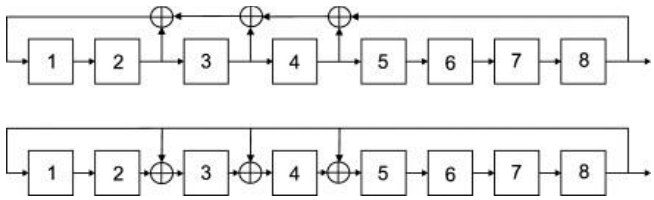



**Figure 1.** Two equivalent methods for generating pseudorandom bits from an 8-bit

### 3.2 One-dimensional logistic map

It is usual practice to simulate population dynamics using a one-dimensional logistic map, which is a mathematical function. Educationally, this is a degree 2 polynomial mapping:

$$xn + 1 = rxn\,(1 - xn) \qquad (1)$$

The populace at time n is represented by way of $(xn)$, and the parameter $r$ impacts how the map behaves. Complex, chaotic conduct can originate from fundamental systems, as established through this easy nonlinear dynamical equation. A fundamental version inside the take a look at of dynamical structures and chaos idea, the logistic map demonstrates special acts, including periodic orbits, chaotic behavior, and stuck-factor attractor. The logistic map is regularly depicted in segment diagrams, which display the population values at diverse instances and the conduct of the map, inclusive of fixed-factor attractor and chaotic rule additives as shown in Figure 2. The map's chaotic first-rate is more desirable via its sensitivity to initial situations, which reasons modest changes inside the preliminary populace value to have drastically numerous lengthy-time period outcomes (the butterfly impact). Many disciplines have investigated and used the logistic map, along with cryptography, biology, and physics. Understanding the behaviour of complex systems, producing random sequences, and encrypting facts are all made simpler via its simple yet deep dynamics.

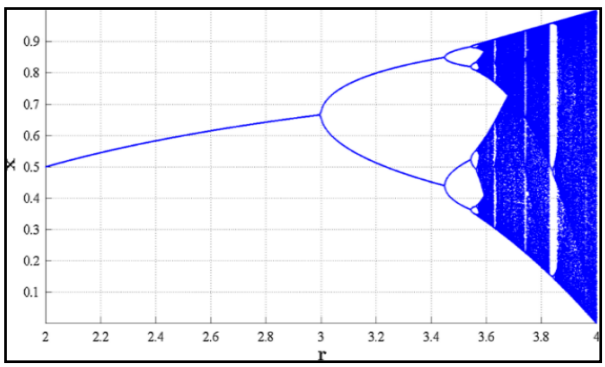



**Figure 2.** The logistic map's bifurcation diagram

## 4. GENERAL DESIGN

Medical image is essential in healthcare, and telemedicine is turning into extra sizeable. Telemedicine is the procedure of sending medical images to distinct locations to diagnose and expect illnesses. Security is important even as moving facts, specifically between cloud networks. The task pursuits to simplify the transmission of scientific facts across the cloud community. The study employs a cryptography approach with a circulation cipher key generator to make sure the secure transmission of clinical pix [3]. Figure 3 indicates the cryptographic machine based at the IoT particularly created for medical photograph purposes. The encryption technique entailed reordering pixel values the usage of random numbers in rows and columns. The encryption model became created the usage of a Raspberry Pi four CPU using the Python programming language. The software program had a graphical person interface for user engagement. The encrypted photograph become sent throughout the cloud community. Decryption changed into performed on the receiving node to reconstruct the encrypted scientific picture and produce the unique photograph.

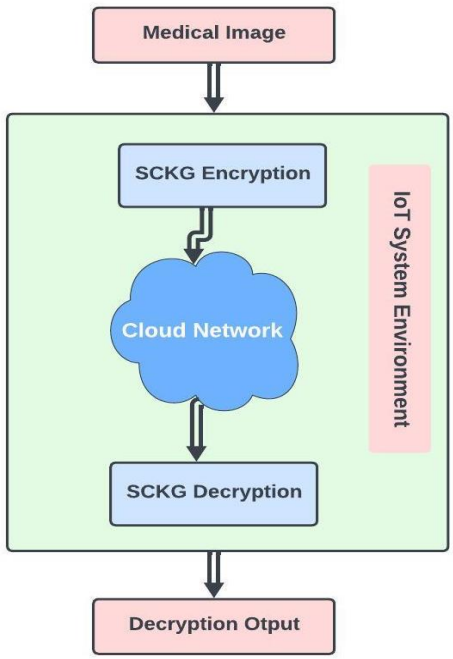



**Figure 3.** General design for proposed system

### 4.1 Key generation using SCKG algorithm

The cryptographic system employs Stream Cipher Key Generation (SCKG) which utilizes four LFSRs with a length of 8 bits each. These registers work together to generate four bytes of data. At first, the LFSRs are initialized with distinct initial values to begin their pseudo-random sequences. LFSRs increment their states the use of a comments mechanism that entails specific OR (XOR) operations on distinctive bit positions, guaranteeing the development of a pseudo-random sequence. At the equal time, a one-dimensional logistic map is used to generate a byte of records, that is then delivered to the important thing generation technique. The logistic map makes use of a chaotic mathematical function to iteratively produce values within a described variety, ensuing in unpredictability and complexity inside the generated byte. Every byte generated by way of the LFSRs is blended with the byte obtained from the logistic map the usage of XOR operation. This introduces unpredictability and improves the

cryptographic strength of the generated bytes. Afterwards, the four resultant bytes from the XOR operation are merged using any other XOR operation, this time with a byte produced by way of a fifth LFSR. The inclusion of this additional LFSR enhances the important thing era method through presenting a further source of pseudo-randomness. The XOR process in the long run produces the four-byte cryptographic keys, which might be critical for protecting sensitive facts and communique. To provide a comprehensive explanation, the system of key era is described as follows:

1. Initialize 4 linear remarks shift registers (LFSRs) with 8 bits each and seed them with particular initial values.
2. Advance the states of the LFSRs the usage of a comments mechanism that consists of XOR operations on specific bit positions.
3. Simultaneously, iterate via a one-dimensional logistic map to generate a facts byte characterized with the aid of chaotic conduct.
4. XOR every byte produced by way of the LFSRs with the byte acquired from the logistic map.
5. Combine the ensuing 4 bytes through XOR operations to reap an intermediate key.
6. Initialize a fifth LFSR with 8 bits and seed it with a unique preliminary price.
7. Advance the nation of the fifth LFSR using a feedback mechanism similar to the other LFSRs.
8. XOR the intermediate key obtained in step 5 with the byte generated with the aid of the fifth LFSR.

The result of this XOR operation yields the four-byte cryptographic keys, which can be used for securing facts and communications, as proven in Figure 4.

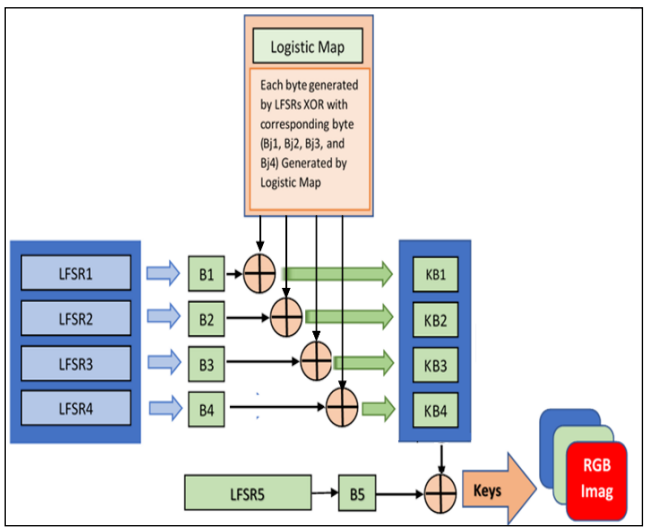



**Figure 4.** Key generation diagram using SCKG algorithm

## 5. ENCRYPTION METHOD

In the encryption part, the input medical image undergoes a meticulous and methodical alteration technique to bolster its safety and confidentiality. The initialization of critical parameters, consisting of the image row and column is step one in the Stream Cipher Key Generation (SCKG) manner. The SCKG functions as the fundamental basis for cryptographic activities, supplying a nicely-organized framework for the method of encryption. Afterwards, a chain of random numbers is created, with each wide variety corresponding to a certain row of the photo. The random numbers determine the rearrangement of pixel coordinates in each row, adding randomness and confusion to the spatial format of image elements. After encrypting the rows, a corresponding method is finished for the columns, in which a glowing set of random numbers is generated for every column. The random numbers determine how the pixels inside the columns are rearranged, improving the encryption procedure and strengthening the photograph's safety. Ultimately, the encryption technique is concluded by way of making use of a distinct OR (XOR) function to all pixels. This technique enhances the obfuscation of the image statistics and strengthens its protection towards unlawful get right of entry to and manipulation. This encryption era makes use of the competencies of SCKG and employs precise random variety era techniques to offer sturdy safety for touchy picture records, substantially lowering functionality safety risks and weaknesses. Figure 5 depicts a schematic representation of the encryption method. The manner of encrypting medical image using Stream Cipher Key Generation (SCKG) may be succinctly defined as follows:

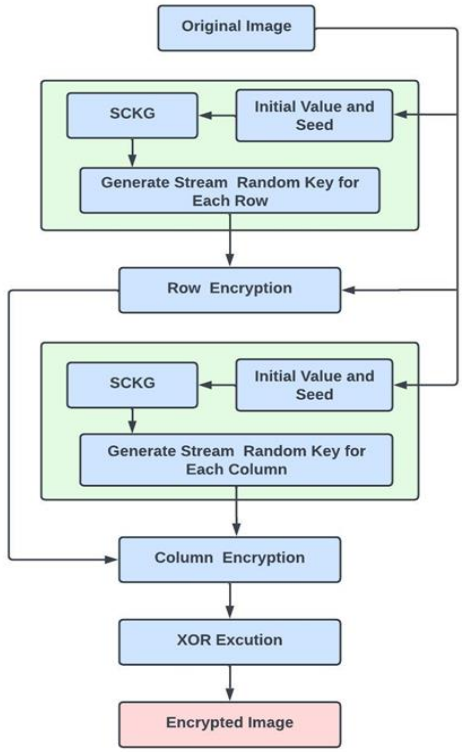



**Figure 5.** Block diagram of the encryption method

**Algorithm 1. Parallelized image encryption**

**Input:** Medical image
**Output:** Encrypted medical image
**Step 1:** Set the appropriate seed values for LFSR and one-dimensional logistic map.
**Step 2:** Generate a random number using SCKG for each row of the medical image.
**Step 3:** Encrypt each row in the medical image using the generated random numbers.
**Step 4:** Generate a random number using SCKG for each column of the medical image.
**Step 5:** Encrypt each column using the generated random numbers.
**Step 6:** Execute an XOR operation on the encrypted rows and columns of the medical image.
**Step 7:** The final result (encrypted medical image).

## 6. DECRYPTION METHOD

The decryption technique is a carefully coordinated collection of strategies to repair the encrypted image to its true, unencrypted image. The decryption method is commenced by using way of utilizing the XOR feature for all encrypted image pixels. This preliminary step is essential for the subsequent decryption techniques because it establishes the muse for methodically getting better the original image facts. After the initial XOR operation, the decryption method sets up crucial parameters, which include row, column, and duration information, in LFSRs and one-dimensional logistic maps. The initialization process is crucial reason to supply dynamic random numbers through Stream Cipher Key Generation. This section is important for processing rows and columns in the sequence of decryption process. After initializing the LFSRs and one-dimensional logistic maps with the specified seed values and parameters, the ensuing random numbers are methodically used to modify the columns and rows of the encrypted image. This software program approach is important in coordinating the alternative conversion of the encryption activities, thus permitting the healing of the authentic image. By utilizing the capabilities of LFSRs, one-dimensional logistic maps, and SCKG the decryption method efficaciously decrypts the encrypted image, thinking about the successful retrieval of the right image statistics. The decryption technique ensures the integrity and accessibility of the original image information, and the work of the important dreams of regular image transmission and garage through cautious plans and execution, Figure 6 illustrates the encryption method.

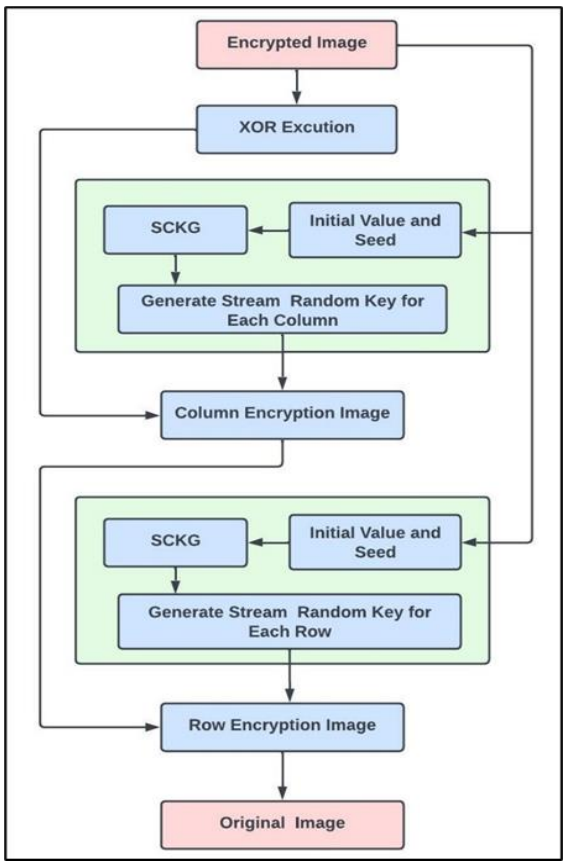



**Figure 6.** The decryption method diagram

The following steps represent the decryption phase for getting the original medical image:

**Algorithm 2. Parallelized image decryption**

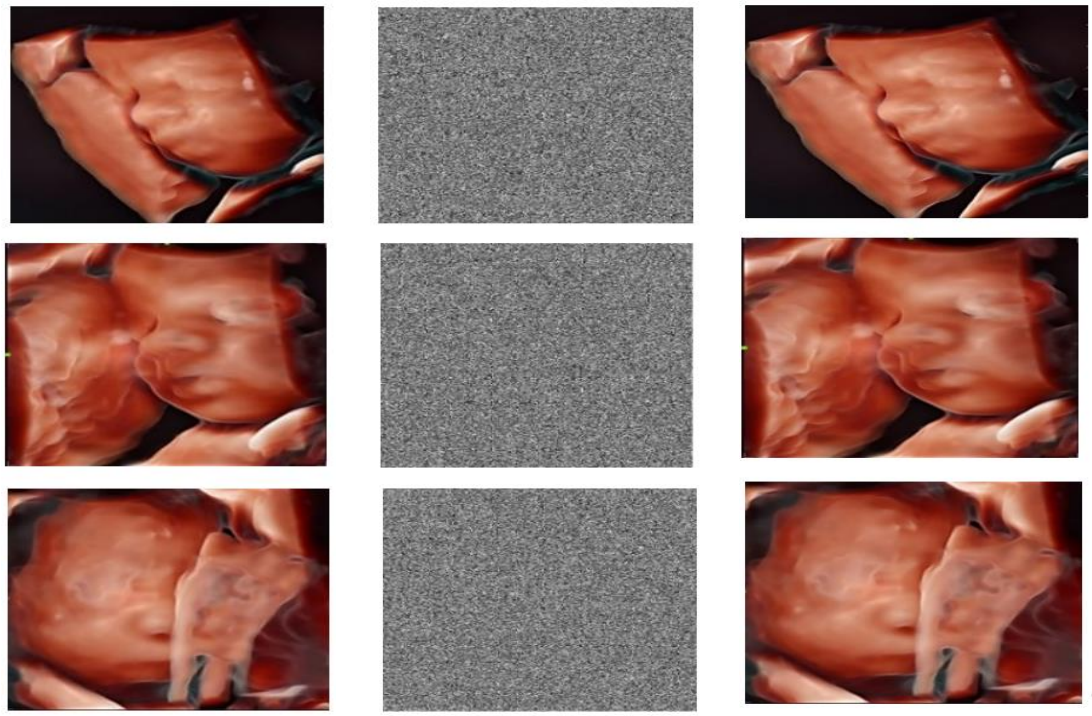
**Input:** Encrypted medical image
**Output:** Plain medical image
**Step 1:** Perform and execute the XOR process.
**Step 2:** Initialize seed values for LFSR and one-dimensional logistic map.
**Step 3:** Generate a random number for each column of the encrypted image using SCKG.
**Step 4:** For each pixel in the column execute the XOR process with the generated random numbers of the encrypted medical image.
**Step 5:** Using SCKG generate a random number for each row of the encrypted image.
**Step 6:** XOR process of the encrypted medical image for each row with generated random numbers.
**Step 7:** End process (decrypted image).

## 7. RESULTS AND EFFICIENCY CRITERIA

The suggested encryption scheme was implemented on a Raspberry Pi 4 Model B (ARM Cortex-A72, 1.5 GHz, 4–8 GB RAM) for encryption and a conventional PC (Intel Core i5/i7, 8 GB RAM) as a server for decryption. This configuration assesses parallel processing inside a practical IoT-to-cloud ecosystem. An analysis of the consequences placed up-encryption of medical image with the proposed technique and Stream Cipher Key Generation (SCKG) on this take a look at has shown huge findings. Using the encryption technique and SCKG has progressed safety talents for encrypted scientific pics via facilitating the introduction of robust and unpredictable cryptographic keys. Consequently, this complements the safety of touchy clinical facts in opposition to unauthorized get rights of entry and capacity breaches. Additionally, assessing the encrypted photos showcases the successful incorporation of the encryption technique and the use of SCKG into the encryption framework, sure the confidentiality and integrity of the medical information contained inner. Besides, an intensive evaluation of the encryption results emphasizes the protection of image and diagnostic integrity, with minimal distortion or degradation decided within the direction of the encryption system. In summary, the consequences of encrypting medical images using SCKG based parallel processing illustrate its efficacy as a reliable encryption method for defensive sensitive medical records while upholding the integrity of diagnostic image. Figure 7 shows the plain, encrypted, and decrypted image.

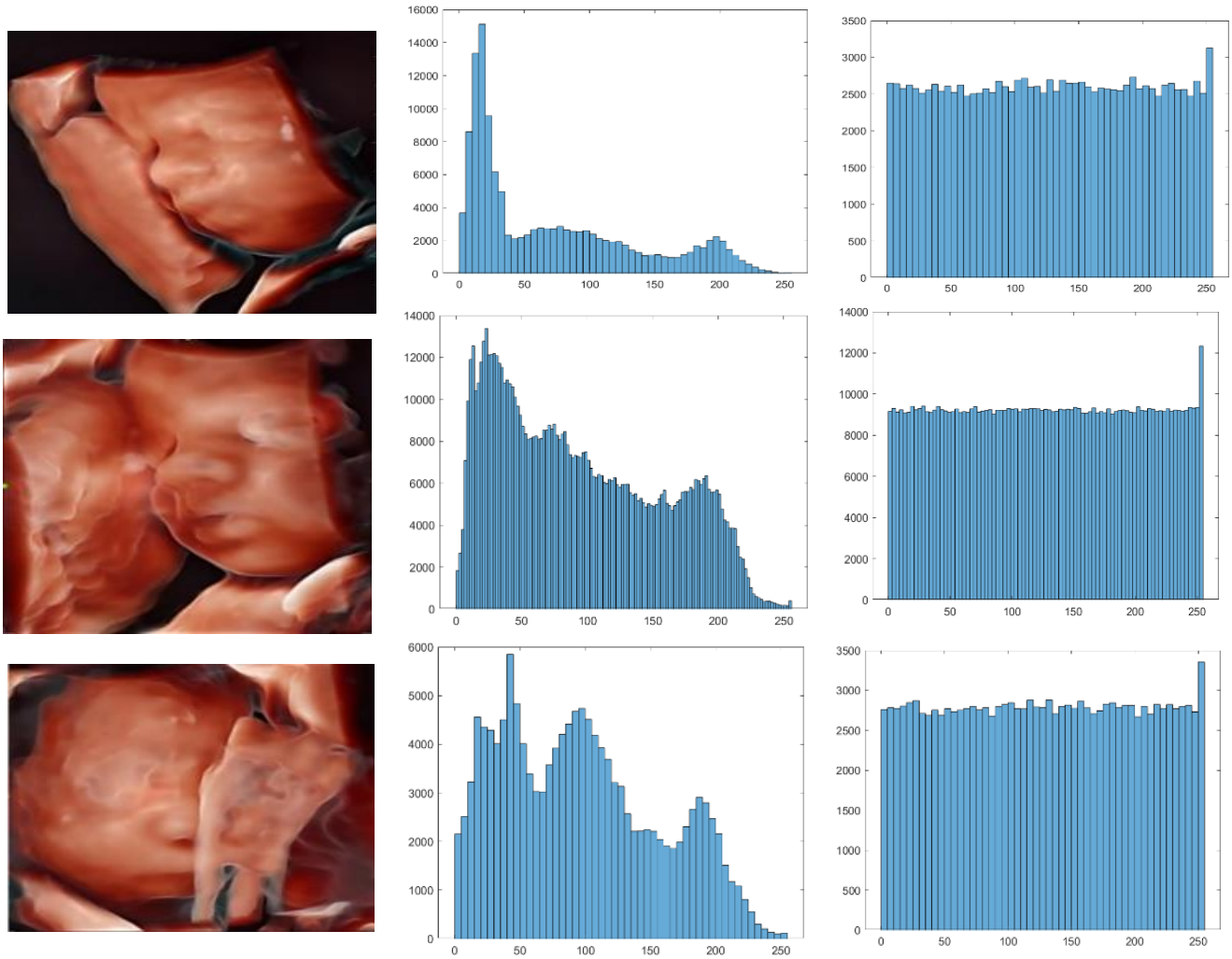
### 7.1 Pixel intensity distribution

Histogram calculation offers valuable insights into the distribution of pixel intensities in a single encrypted medical image. A balanced histogram displays the best image with exceptional diagnostic readability [22]. After encryption with Stream Cipher Key Generation (SCKG), the histogram of the encrypted image may additionally display a more uniform distribution and reduced pixel value range due to the encryption system. However, it's essential to ensure that critical image traits are retained, consisting of distinguishable peaks representing anatomical capabilities [23]. Analyzing both histograms helps assess the impact of encryption on image characteristics and ensures that diagnostic information remains intact while maintaining patient privacy. Histogram of original and encrypted image is presented in Figure 8.



(a) (b) (c)

**Figure 7.** (a) Plain image, (b) Encrypted image, and (c) Decrypted image



(a) (b) (c)

**Figure 8.** (a) Original image, (b) Histogram of the original image, and (c) Histogram of the encrypted image

### 7.2 MSE and PSNR

Mean square error (MSE) and Peak signal to noise ratio (PSNR) are essential metrics for assessing the fine and integrity of encrypted clinical pics while using the recommended method and SCKG encryption. PSNR evaluates photo fidelity by evaluating the picture's electricity to the noise's power, in which better values represent advanced nice [24]. Elevated PSNR values suggest minimum facts loss and sustained photo exceptional in medical image encryption the usage of the proposed approach and SCKG. On the other hand, MSE gauges the disparity between the authentic and encrypted pixel values, with decreased values denoting better alignment and encryption efficacy. In the situation in which the image dimensions are represented by M and N, the preliminary image is denoted as I1, and the encrypted image is marked as E.

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [I_1(i,j) - E(i,j)]^2 \quad (2)$$

$$SNR = 10\_\log 10 \left[\frac{M \times N \times 255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P(i,j) - C(i,j))^2}\right] \quad (3)$$

Table 1 illustrates that all medical images get low MSE values and a consistent PSNR of approximately 6.02 dB, signifying efficient encryption with low distortion in the decrypted images.

Table 2 presents results of this study of encryption and decryption times, derived from parallel processing, indicate that the proposed lightweight approach exhibits efficient performance across various 4D Ultra images. The encryption durations span from 0.7450 to 0.8981 seconds, and decryption durations fluctuate between 0.5035 and 0.6773 seconds. The results validate that the strategy sustains little computational time in both phases. The consistent execution speed underscores the appropriateness of the method for time-critical applications, such as secure image transfer in IoT settings, especially when employing parallel processing to mitigate latency.

**Table 1.** MES and PSNR values for medical image

| Image | MSE | PSNR |
|---|---|---|
| 4D Ultra 1 | 0.0323 | 6.02079 |
| 4D Ultra 2 | 0.0017 | 6.02149 |
| 4D Ultra 3 | 0.0301 | 6.02086 |

**Table 2.** Encryption and decryption time

| Image | Encryption Time (sec.) | Decryption Time (sec.) |
|---|---|---|
| 4D Ultra 1 | 0.7450 | 0.6071 |
| 4D Ultra 2 | 0.8981 | 0.6773 |
| 4D Ultra 3 | 0.7661 | 0.5035 |

### 7.3 Entropy analysis

Determine the degree of randomness in an image. The encrypted image should have a greater amount of entropy compared to the original image [25]. When the entropy of the encrypted image is near the maximum value of 8, it signifies that the encryption based on entropy is highly successful [26]. The entropy can be calculated using Eq. (4), and its results are presented in Table 2.

$$Hi = -\sum_{0}^{2^8-1} p_i \log_2 (p_i) \quad (4)$$

The symbol *Hi* denotes entropy, $p_i$ and $\log_2 p_i$ refer to the probability of occurrence of the symbol $i$ and based 2 logarithms, respectively. According to the findings outlined in Table 1, it is evident that there has been a notable rise in the entropy outcomes. The entropy value is in close proximity to 8, indicating the effectiveness of the security provided by the image encryption based on entropy.

### 7.4 Plain sensitivity analysis

NPCR and UACI are key metrics for assessing the effectiveness of cryptographic algorithms in photograph encryption. NPCR measures the share of pixel trade between encrypted image because of a single bit change inside the plaintext image, with a better cost indicating expanded safety [27]. On the opposite hand, UACI evaluates the average intensity alternate across all pixels in the encrypted image from an unmarried-bit alteration within the plaintext image, with a lower value indicating higher diffusion and superior safety. Analysing these values allows researchers to examine cryptographic energy and image encryption security, making sure the confidentiality and integrity of touchy image statistics in one-of-a-kind applications [28]. The equation for NPCR and UACI can be proven under:

$$NPCR = \frac{\sum_{i,j} I(i,j)}{M \times H} \times 100\% \quad (5)$$

$$UACI = \frac{1}{M \times H}\left[\frac{\sum_{i,j} C(i,j) - C'(i,j)}{255}\right] \times 100\% \quad (6)$$

In the case where $C(i, j)$ equals $C'(i, j)$, the value of $I(i, j)$ is set to 1. Conversely, when $C(i, j)$ does not equal $C'(i, j)$, the value of $I(i, j)$ is set to 0. This condition applies to an image with width $M$ and height $H$ [29].

Table 3 demonstrates the robust security efficacy of the proposed encryption technique. All 4D Ultra images exhibit NPCR values exceeding 99.60%, signifying exceptional resilience against differential attacks.

The UACI value of around 35.84% indicates substantial alterations in pixel intensity post-encryption. The entropy levels approaching 8 indicate a significant degree of randomness in the encrypted images. These measures jointly validate the strength and unpredictability of the encryption method.

Table 4 demonstrates that the suggested method achieves higher UACI (35.844) and entropy (7.9994) relative to previous methods, signifying enhanced pixel alteration and improved randomness, while sustaining a competitive NPCR (99.6045), so affirming its resilience against differential attacks.

**Table 3.** NPCR, UACA, and entropy values for medical image

| Image | NPCR | UACI | Entropy |
|---|---|---|---|
| 4D Ultra 1 | 99.6040 | 35.846 | 7.9994 |
| 4D Ultra 2 | 99.6045 | 35.846 | 7.9994 |
| 4D Ultra 3 | 99.6043 | 35.844 | 7.9993 |

**Table 4.** Comparison results with existing methods

| Image | NPCR | UACI | Entropy |
|---|---|---|---|
| [30] | 99.990 | 25.33 | 7.991 |
| [31] | 99.690 | 7.9975 | 7.7445 |
| [32] | 99.5971 | 33.4136 | 7.9972 |
| Ours | 99.6045 | 35.844 | 7.9994 |

## 8. CONCLUSIONS

This study presents a secure encryption method for medical images in IoT settings utilizing Stream Cipher Key Generation (SCKG) to improve confidentiality. The method dynamically initializes keys according to image dimensions (rows, columns, and size) for structured encryption, while incorporating unpredictability via unique random number generation for rows and columns, hence enhancing confusion. Implementing XOR operations on every pixel provides an extra security layer that guarantees strong protection against illegal access. The integration of SCKG and stringent randomization significantly reduces vulnerabilities in medical image transmission, rendering it exceptionally appropriates for IoT-based healthcare systems. This method enhances data security, protecting patient confidentiality and diagnostic accuracy in sensitive medical contexts.

The technique may demonstrate degraded performance with very large images, which can be a drawback on effectiveness in high-resolution medical imaging. The future work will concentrate on the optimization of the algorithm so as to enhance the processing speed and diminish resource usage for larger image sizes in an IoT environment that is constrained.

## ACKNOWLEDGMENT

We would like to sincerely thank Mustansiriyah University and the University of Sfax for their invaluable support and assistance throughout our research project.

## REFERENCES

[1] Belazi, A., Talha, M., Kharbech, S., Xiang, W. (2019). Novel medical image encryption scheme based on chaos and DNA encoding. IEEE Access, 7: 36667-36681. https://doi.org/10.1109/ACCESS.2019.2906292

[2] Abd-El-Atty, B. (2023). A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. Neural Computing and Applications, 35(1): 773-785. https://doi.org/10.1007/s00521-022-07830-0

[3] 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

[4] Rajendran, S., Doraipandian, M. (2021). Chaos based secure medical image transmission model for IoT-powered healthcare systems. IOP Conference Series: Materials Science and Engineering, 1022(1): 012106 https://doi.org/10.1088/1757-899x/1022/1/012106.

[5] Budiman, F., Andono, P.N., Setiadi, M. (2022). Image encryption using double layer chaos with dynamic iteration and rotation pattern. International Journal of Intelligent Engineering & Systems, 15(2): 57-67. https://doi.org/10.22266/ijies2022.0430.06

[6] Kaur, M., AlZubi, A.A., Singh, D., Kumar, V., Lee, H.N. (2023). Lightweight biomedical image encryption approach. IEEE Access, 11: 74048-74057. https://doi.org/10.1109/ACCESS.2023.3294570

[7] Wu, Y., Zhang, L., Berretti, S., Wan, S. (2022). Medical image encryption by content-aware DNA computing for secure healthcare. IEEE Transactions on Industrial Informatics, 19(2): 2089-2098. https://doi.org/10.1109/TII.2022.3194590

[8] Krishnapriya, P.V., Suresh, S. (2023). Image security using linear feedback shift register. International Journal of Innovative Science and Research Technology, 2(6): 282-285.

[9] Din, M., Pal, S.K., Muttoo, S.K., Jain, A. (2016). Applying Cuckoo Search for analysis of LFSR based cryptosystem. Perspectives in Science, 8: 435-439. https://doi.org/10.1016/j.pisc.2016.04.098

[10] Al-Ageelee, A.A., Salim, N.J., Kadhum, R. (2017). Cryptanalysis of nonlinear stream cipher cryptosystem based on improved particle swarm optimization. International Journal of Applied Information Systems, 19(1): 78-84. https://doi.org/10.5120/ijais2017451658

[11] Sadkhan, S.B., Yaseen, B.S. (2018). A DNA-sticker algorithm for cryptanalysis LFSRs and NLFSRs based stream cipher. In 2018 International Conference on Advanced Science and Engineering (ICOASE), pp. 301-305. https://doi.org/10.1109/ICOASE.2018.8548888

[12] Din, M., Pal, S.K., Muttoo, S.K. (2019). Analysis of RC4 crypts using PSO based swarm technique. In Harmony Search and Nature Inspired Optimization Algorithms: Theory and Applications, ICHSA 2018, pp. 1049-1056. https://doi.org/10.1007/978-981-13-0761-4_98

[13] Din, M., Pal, S.K., Muttoo, S.K. (2019). Applying PSO based technique for analysis of Geffe generator cryptosystem. In Harmony Search and Nature Inspired Optimization Algorithms: Theory and Applications, ICHSA 2018, pp. 741-749. https://doi.org/10.1007/978-981-13-0761-4_71

[14] Boryczka, I.P.M. (2019). Tabu cryptanalysis of VMPC stream cipher. Tatra Mountains Mathematical Publications, 73(1): 145-162. https://doi.org/10.2478/tmmp-2019-0011

[15] Jawad, R., Ali, F. (2020). Using evolving algorithms to cryptanalysis nonlinear cryptosystems. Baghdad Science Journal, 17(2): 682-688. https://doi.org/10.21123/bsj.2020.17.2(SI).0682

[16] Mishra, G., Gupta, I., Krishna Murthy, S.V.S.S.N.V.G., Pal, S.K. (2021). Deep learning-based cryptanalysis of stream ciphers. Defence Science Journal, 71(4): 499-506. https://doi.org/10.14429/dsj.71.16209

[17] Jawad, R.N. (2022). Proposed hybrid technique in cryptanalysis of cryptosystem based on PSO and SA. Iraqi Journal of Science, 4547-4558. 63(10): https://doi.org/10.24996/ijs.2022.63.10.37

[18] Jain, M., Saihjpal, V., Singh, N., Singh, S.B. (2022). An overview of variants and advancements of PSO algorithm. Applied Sciences, 12(17): 8392. https://doi.org/10.3390/app12178392

[19] Lee, S.H., Cheng, C.H., Lin, C.C., Huang, Y.F. (2023). PSO-based target localization and tracking in wireless sensor networks. Electronics, 12(4): 905. https://doi.org/10.3390/electronics12040905

[20] Minh, H.L., Khatir, S., Rao, R.V., Abdel Wahab, M., Cuong-Le, T. (2023). A variable velocity strategy particle swarm optimization algorithm (VVS-PSO) for damage assessment in structures. Engineering with Computers, 39(2): 1055-1084. https://doi.org/10.1007/s00366-021-01451-2

[21] Chen, Z., Li, X., Zhu, Z., Zhao, Z., Wang, L., Jiang, S., Rong, Y. (2020). The optimization of accuracy and efficiency for multistage precision grinding process with an improved particle swarm optimization algorithm. International Journal of Advanced Robotic Systems, 17(1). https://doi.org/10.1177/1729881419893508

[22] Dai, H.P., Chen, D.D., Zheng, Z.S. (2018). Effects of random values for particle swarm optimization algorithm. Algorithms, 11(2): 23. https://doi.org/10.3390/a11020023

[23] Shibeeb, A.K., Ahmed, M.H., Mohammed, A.H. (2021). A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation. Karbala International Journal of Modern Science, 7(3): 2. https://doi.org/10.33640/2405-609X.3117

[24] Jabbar, K.K., Ghozzi, F., Fakhfakh, A. (2023). Robust color image encryption scheme based on RSA via DCT by using an advanced logic design approach. Baghdad Science Journal, 20(6 (Suppl.)): 2593-2593.

[25] Gad, M., Hagras, E.A., Soliman, H., Hikal, N.A. (2021). A new parallel fuzzy multi modular chaotic logistic map for image encryption. The International Arab Journal of Information Technology, 18(2): 227-236. https://doi.org/10.34028/iajit/18/2/12

[26] Chen, Y., Xie, S., Zhang, J. (2022). A hybrid domain image encryption algorithm based on improved henon map. Entropy, 24(2): 287. https://doi.org/10.3390/e24020287

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

[28] Alsaadi, E.M.T.A., Fayadh, S.M., Alabaichi, A. (2020). A review on security challenges and approaches in the cloud computing. AIP Conference Proceedings, 2290(1): 040022. https://doi.org/10.1063/5.0027460

[29] Ahmed, M.H., Shibeeb, A.K., Abbood, F.H. (2020). An efficient confusion-diffusion structure for image encryption using plain image related Henon map. International Journal of Computing, 19(3): 464-473. https://doi.org/10.47839/ijc.19.3.1895

[30] Mohammed, A.H., Shibeeb, A.K., Ahmed, M.H. (2022). Image cryptosystem for IoT devices using 2-D Zaslavsky Chaotic Map. International Journal of Intelligent Engineering & Systems, 15(2): 543-553. https://doi.org/10.22266/ijies2022.0430.48

[31] Al-Bahrani, E.A., Kadhum, R.N. (2019). A new cipher based on Feistel structure and chaotic maps. Baghdad Science Journal, 16(1): 270-280. https://doi.org/10.21123/bsj.2019.16.1(Suppl.).0270

[32] Maryoosh, A.A., Dhaif, Z.S., Mustafa, R.A. (2021). Image confusion and diffusion based on multi-chaotic system and mix-column. Bulletin of Electrical Engineering and Informatics, 10(4): 2100-2109. https://doi.org/10.11591/eei.v10i4.2942