Journal of Science Research and Reviews

PRINT ISSN: 1595-9074
E-ISSN: 1595-8329
DOI: https://doi.org/10.70882/josrar.2025.v2i5.109
Homepage: https://josrar.esrgngr.org

Original Research Article

A Secure Digital Imaging and Communications in Medicine (DICOM) Encryption

***[1]Samson Isaac, [2]Barna Thomas Lass, [3]Ramat Imam Abba, [4]Anas Muhamad Saminu and [4]Rukayyat Bala**

[1]Department of Computer Science, Federal University of Applied Science Kachia, Kaduna, Nigeria,
[2]Department of Software Engineering, Federal University of Applied Science Kachia, Kaduna, Nigeria,
[3]Department of Cyber Security, Airforce Institute of Technology, Mando, Kaduna, Nigeria
[4]Department of Informatics, Kaduna State University, Kaduna, Nigeria.
*Corresponding Author's email: samson.isaac@fuask.edu.ng

KEYWORDS

Internet of Things,
Digital Imaging and Communications in Medicine,
Encryption,
Cryptographic,
Healthcare Internet of Things.

CITATION

Isaac, S., Lass, B. T., Abba, R. I., Saminu, A. M., & Bala, R. (2025). A Secure Digital Imaging and Communications in Medicine (DICOM) Encryption. *Journal of Science Research and Reviews*, 2(5), 74-82. https://doi.org/10.70882/josrar.2025.v2i5.109

ABSTRACT

The rapid proliferation of healthcare Internet of Things (IoT) systems has intensified the need for robust encryption mechanisms capable of securing sensitive medical data, particularly Digital Imaging and Communications in Medicine (DICOM) images. This research introduces a novel Modified Encryption Algorithm designed to enhance data confidentiality, integrity, and resilience against cyber threats within resource-constrained IoT environments. Through extensive simulation evaluations, the proposed algorithm demonstrates superior performance compared to widely used lightweight encryption schemes such as PRESENT, SIMON, and LEA. The algorithm achieves a remarkably high entropy value of 15.469, indicating strong randomness and resistance to statistical attacks. Additionally, the low correlation coefficients—vertical (0.0182), horizontal (–0.0132), and diagonal (0.0625) which confirm effective pixel decorrelation and robust cipher strength. The research obtained Unified Average Changing Intensity (UACI) value of 33.362 further validates the algorithm's capability to withstand differential attacks, while a Structural Similarity Index (SSIM) score of 0.175 confirms that essential image characteristics remain intact, ensuring acceptable visual quality where required for clinical interpretation.

INTRODUCTION

The integration of Internet of Things (IoT) devices into healthcare systems has revolutionized the way medical data is transmitted and managed. However, this transformation also brings forth significant challenges, particularly concerning the security of sensitive medical data, such as Digital Imaging and Communications in Medicine (DICOM) images. Despite efforts to secure this data through encryption and watermarking techniques, traditional methods have proven inadequate, leaving healthcare systems vulnerable to cyber threats (Omolara et al., 2022).

The motivation behind this study stems from the pressing need to address these security challenges and enhance the protection of DICOM images in IoT systems used in healthcare. As IoT devices become increasingly ubiquitous in healthcare settings, ensuring the confidentiality, integrity, and availability of patient data becomes paramount (Zaman et al., 2022). By shifting towards lightweight DICOM image encryption tailored to the resource constraints of IoT devices, we aim to bolster the security posture of healthcare systems while maintaining efficiency and performance (Katzis et al., 2022). Through this study, we seek to explore the limitations of current encryption techniques and advocate for the adoption of enhanced security measures. By exploring into the intricacies of lightweight encryption algorithms and their application in IoT systems, we aim to uncover vulnerabilities and propose solutions to mitigate them. Ultimately, our goal is to pave the way for the development and implementation of robust encryption techniques that can safeguard sensitive medical data effectively in IoT-enabled healthcare environments. By addressing these challenges and advancing lightweight DICOM image encryption, we aim to contribute to the realization of a secure and resilient healthcare ecosystem. Through collaboration with stakeholders and leveraging advancements in cryptography and IoT technologies, we aspire to facilitate the delivery of high-quality healthcare services while upholding patient confidentiality and integrity. This study represents a crucial step towards enhancing the security posture of IoT systems in healthcare and ensuring the trust and confidence of patients and healthcare providers alike. The current techniques used to secure healthcare IoT devices, particularly Digital Imaging and Communications in Medicine (DICOM) images, primarily rely on encryption and watermarking methods (Isaac et al., 2024). Encryption algorithms are employed to encode DICOM images, ensuring confidentiality during transmission and storage, while watermarking techniques embed unique identifiers for authentication and tracking purposes (Manikandan & Amirtharajan, 2022). However, these traditional methods exhibit several limitations: Encryption and watermarking techniques often impose significant computational overhead, particularly in resource-constrained IoT environments, leading to performance degradation and increased energy consumption (Sadhu et al., 2022). Healthcare IoT devices typically have limited computational resources, such as processing power and memory, which restrict the use of resource-intensive encryption algorithms and protocols (Aledhari et al., 2022). Despite providing a basic level of security, traditional encryption methods may be susceptible to sophisticated cyberattacks, such as brute-force attacks, side-channel attacks, and cryptographic vulnerabilities. The goal of this study is to advance lightweight DICOM image encryption techniques tailored to IoT systems in healthcare. This involves addressing the limitations of current approaches while enhancing both security and efficiency. Specifically, we aim to improve resilience to cyberattacks by designing encryption algorithms with robust security features, including resistance to brute-force attacks, side-channel attacks, and cryptographic vulnerabilities. The proposed DICOM image encryption technique will be evaluated based on computational complexity of the encryption algorithm, including processing time and memory usage, to assess its efficiency in resource The DICOM image encryption technique offers stakeholders enhanced security, optimized performance, robust key management, and cost efficiency in healthcare IoT systems. The widespread adoption of Internet of Things (IoT) devices across various domains such as hospitals, smart homes, wearable technology, industrial automation, and vehicle connectivity has significantly transformed interactions with the physical environment (Almotairi, 2023). However, this interconnected nature poses a critical challenge: protecting sensitive information exchanged and stored in these environments, which often have limited resources. Traditional encryption methods, while effective in providing strong security, typically require significant computational power, making them impractical for IoT devices with limited processing capabilities and memory (Kornaros et al., 2022). This explores the existing discussions on cryptographic strategies relevant to IoT security, highlighting key research efforts, areas warranting further investigation, and the motivations behind the development of an Advanced Lightweight Chaos-Based Encryption Model. Several studies have addressed security concerns in healthcare IoT systems, employing various encryption techniques. Kavitha et al. (2024) proposed a method for securing tuberculosis disease detection using IoT-driven Improved AlexNet and RSA encryption, offering strong security for key exchange. However, the RSA encryption method employed in their approach exhibits high computational complexity, rendering it unsuitable for real-time applications on resource-constrained devices. Similarly, Kumari et al. (2023) explored two-stage secure medical data transmission for IoT-based e-health applications, leveraging RSA encryption for robust key exchange. Despite its strong security attributes, the computational complexity of RSA encryption poses challenges for real-time implementations on resource-constrained devices. Pavaiyarkarasi et al. (2022) introduced a hybrid security model for protecting diagnostic text data in medical images over the Internet of Things (IoT), combining unspecified techniques to enhance security. While this approach offers increased security compared to single algorithms, it may entail greater complexity in implementation and potentially lower efficiency than lightweight alternatives. Hatem & Hameedi (2023) proposed lightweight digital imaging and communications in medicine (DICOM) image encryption for IoT systems, likely utilizing an AES variant. While AES is a widely accepted standard known for its strong security, its high computational complexity may pose challenges for resource-constrained devices, depending on the variant employed. El-Shafai et al. (2022) introduced a neural SAE-based medical image cryptography framework, harnessing neural network-based techniques for potential high-security applications. However, limited information is available regarding the computational complexity of their approach, which may present challenges for resource-constrained devices. Shahane and Nagarjuna (2022) addressed medical data transmission using IoT, employing AES encryption for strong security. Nonetheless, the computational complexity associated with AES encryption may limit its feasibility for resource-constrained devices. Additionally, Chhabra and Lata (2022) proposed an obfuscated AES cryptosystem for secure medical imaging systems in Internet of Medical Things (IoMT) edge devices, enhancing security compared to standard AES. However, the introduction of obfuscation may introduce additional complexity, particularly for resource-constrained devices. Tradition encryption methods, while robust, can be too computationally expensive for resource-limited devices in the Internet of Things (IoT) for healthcare. Recognizing this limitation, researchers are exploring lightweight cryptography techniques. These techniques prioritize a balance between security and efficiency. The goal is to achieve adequate data protection for sensitive information, like DICOM images, while minimizing the processing power and memory required for encryption and decryption on these resource-constrained devices (Pandey & Bhushan, 2024; Samson et al., 2024). Existing research explores into various lightweight ciphers and block cipher modes specifically designed for such environments. Lightweight ciphers, like XTEA, SIMON, SPECK, PRESENT, and SKINNY, offer promising solutions. Compared to traditional algorithms, these ciphers boast significantly reduced complexity, making them more suitable for resource-constrained devices in healthcare IoT applications (Alluhaidan & Prabu, 2023; Isaac et. al., 2024). Sarosh et al. (2022) proposed an efficient image encryption scheme for healthcare applications. However, the authors did not specify the encryption algorithm used, making it difficult to assess its suitability. Narayana et al. (2022) presented a medical image cryptanalysis using an adaptive, lightweight neural network-based algorithm for IoT-secured cloud storage. This approach shows potential for high security and adaptation but provides limited information on the specific neural network and its effectiveness. Dash et al. (2023) developed an efficient intra-inter pixel encryption scheme to secure healthcare images for an IoT environment. This method achieves good security by modifying pixel values but may be computationally expensive compared to other lightweight techniques. Islam et al. (2024) proposed a lightweight medical-image encryption technique for IoMT-based healthcare applications. While it offers lower computational complexity compared to traditional algorithms, there is a potential trade-off with security. Kaur et al. (2023) introduced a lightweight biomedical image encryption approach. This method offers lower computational complexity compared to traditional algorithms but may also result in lower security levels. Selvaraj et al. (2023) discussed cryptographic encryption and optimization for IoT-based medical image security. The paper likely combines encryption with optimization techniques but lacks details on the specific encryption algorithm used, which limits a comprehensive evaluation. Nadhan & Jacob (2024) focused on enhancing healthcare security in the digital era by safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. While these techniques lower computational complexity, they might also compromise security compared to more robust traditional algorithms. Samiullah et al. (2022) developed a chaos-based cryptographic mechanism for smart healthcare IoT systems, highlighting the potential for high security and randomness. However, the specific chaos-based mechanism was not detailed, raising concerns about possible computational expense and unclear implementation details. Sarosh et al. (2022) presented an efficient image encryption scheme for healthcare applications but did not specify the encryption algorithm used, making it difficult to evaluate its effectiveness. Hatem et al. (2023) discussed a lightweight digital imaging and communications in medicine image encryption system for IoT, likely using a lightweight variant of a block cipher. This approach reduces computational complexity compared to traditional algorithms but may sacrifice some security, especially given the unspecified variant. El-Shafai et al. (2024) proposed a 3D chaos-based medical image cryptosystem designed for secure cloud-IoMT eHealth communication services. This system leverages a 3D chaotic map, providing potentially high security and randomness, though it may be computationally expensive compared to some lightweight techniques. Clemente-Lopez et al. (2024) introduced a lightweight chaos-based encryption scheme tailored for IoT healthcare systems, which offers lower complexity compared to traditional chaotic systems but might have lower security compared to more complex alternatives. The chaos-based encryption offers promising potential for securing data in IoT applications. However, the security requirements, resource constraints, and implementation practicality is crucial when selecting or developing an appropriate scheme for a specific use case.

MATERIALS AND METHODS

The Modified Pseudocode 1: Data Acquisition and Encryption Stage with Cryptographic Enhancements. This improved version of Algorithm 1 incorporates the Bjørklund-Demytko function and other security enhancements for a cryptographically secure PRNG:

Input: IR ← bitstream (data to be encrypted)

Functions

Gray_code(data): Converts data bits to Gray code representation (reduces bit flips during transmission).

Permutation (x1, cryptogram): Permutes the cryptogram using a key derived from x1 (scrambles the data).
key_application (IR): Applies additional key-based operations to the data (optional, can be encryption with a secret key).

Steps

Gray Code Representation

u = [Gray_code(y) for y in IR]: Convert each bit (y) in the data stream (IR) to its Gray code equivalent and store them in a list u.

Improved Seed Generation

Incorporate additional system parameters from the chosen chaotic system into the initial seed for the PRNG. This increases the key space size (number of possible keys) for better security. Aim for a larger key space size (p > 9).

Chaotic System and Transient Period

Analyse the specific chaotic system to determine the optimal transient period (number of initial iterations to discard). Discard these initial transient values to ensure randomness.

Keystream Generation with Bjørklund-Demytko Function

v = [x1 XOR x2 XOR x3 for i in range(length(u))]: Generate the initial keystream by XORing the chaotic sequences (x1, x2, x3).
w = []: Initialize an empty list to store the final keystream.

For each triplet of bits in v
Extract three bits (a, b, c) from the current position in v.
Apply the Bjørklund-Demytko function: bit = (a XOR b) & (NOT(a) XOR c).
Append the generated bit (bit) to the list w.
This process adds an extra layer of randomness and security to the keystream using the lightweight Bjørklund-Demytko function.

Encryption

encrypted_data = [u[i] XOR w[i]
for i in range(len(u))]:
XOR the Gray code data (u) with the final keystream (w) to generate the encrypted data.

Permutation

perm = Permutation (x1, encrypted_data): Permute the encrypted data using a key derived from x1.

Transmission

Send perm through Bluetooth protocol.

Enhancements

Improved Seed Generation: Addresses the potential weakness of a limited key space by increasing the seed size.
Transient Period Adjustment: Improves efficiency by discarding only the necessary non-random initial values.
Keystream Generation with Bjørklund-Demytko Function: Enhances randomness and security of the keystream.
Larger Modulus:
Using a larger modulus (M) in the original keystream generation step
v = [x1 XOR x2 XOR x3 mod M]

Modified Pseudocode 2: Decryption Stage and Data Processing with Synchronization

This improved version of Algorithm 2 incorporates synchronization with the encryption process (Algorithm 1) and utilizes the Bjørklund-Demytko function for enhanced security:

Input: Encrypted_data ← bitstream (received encrypted data)

Functions

decoding(data): Decodes the data (optional, might involve reversing Gray code conversion).
Permutation (x1, cryptogram): Permutes the cryptogram using a key derived from x1 (unscrambles the data).
key_application (Encrypted_data): Applies additional key-based operations to the encrypted data (optional, can be decryption with a secret key).

Steps

PRNG Computation (Synchronized with Algorithm 1)

[x1, x2, x3] = *Computation of the 2D Chaotic System (replace "*" with the specific system's equations). This computation should be identical to the one used in Algorithm 1 to ensure synchronization.
Analyse the specific chaotic system used to determine the optimal transient period (number of initial iterations to discard). Discard these initial transient values based on the same criteria used in Algorithm 1.

Keystream Generation with Bjørklund-Demytko Function

v = [x1 XOR x2 XOR x3 for _ in range (length (Encrypted data))]: Generate the initial keystream by XORing the chaotic sequences (x1, x2, x3). This remains unchanged from the original algorithm.
w = []: Initialize an empty list to store the final keystream.
For each triplet of bits in v
Extract three bits (a, b, c) from the current position in v.
Apply the Bjørklund-Demytko function: bit = (a XOR b) & (NOT(a) XOR c).
Append the generated bit (bit) to the list w.

This process adds an extra layer of randomness and complexity to the keystream
using the lightweight Bjørklund-Demytko function.

Decryption

retrieved data = [Permutation (x1, Encrypted data) ⊕ w]: XOR the received encrypted data with the final keystream (w) to recover the original data.

Gray Code Decoding (Optional)

IR = [decoding(y) for y in retrieved data]: If Gray code was used in encryption, decode the retrieved data back to its original binary representation using the decoding function.

Data Processing

Frequency = FFT(IR): Apply the Fast Fourier Transform (FFT) to the retrieved data to extract the frequency information.
Heartrate = Frequency * 60: Calculate the heart rate based on the extracted frequency.

Synchronization and Enhancements

Keystream Generation

The keystream generation process aligns with Algorithm 1, ensuring both use the same larger modulus (M) for consistency and potentially stronger security.

Seed Generation and Transient Period

If modifications were made to seed generation or the transient period in Algorithm 1, ensure the same adjustments are reflected in Algorithm 2 to maintain synchronization. This ensures both algorithms use the same chaotic sequences for decryption.

Bjørklund-Demytko Function

The inclusion of this function enhances the randomness and security of the keystream.

Data Collection

This study uses the DICOM image of brain that consists of 25 slices, each slice consists of 2d matrix (256×256), each pixel represented by integer (16-bits). Figure 1 explain all DICOM slices of used image. The use of DICOM images is common in medical imaging, and the encryption of these images is important for ensuring patient privacy and data security. By applying the proposed method to a DICOM image of the brain, the authors demonstrate the effectiveness of their approach in encrypting complex and sensitive medical data.

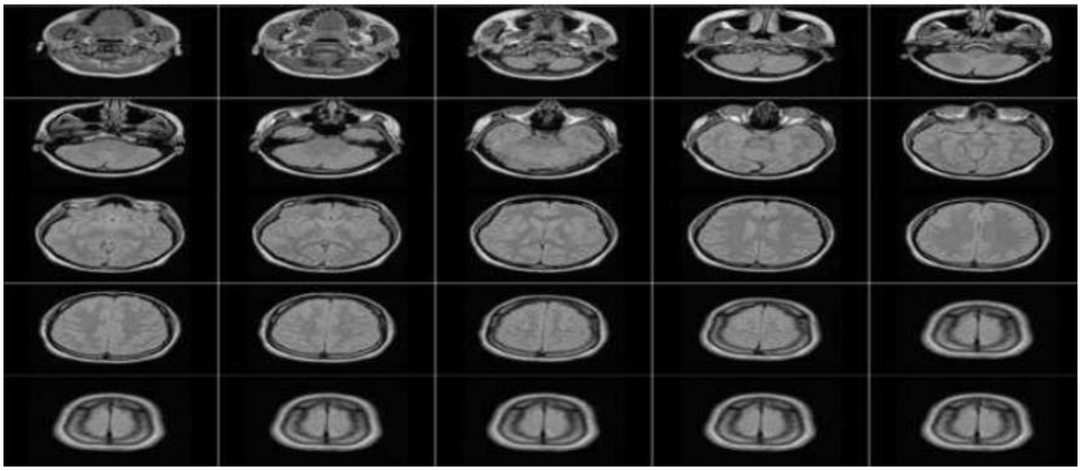

Figure 1: DICOM image of brain

Performance Evaluation

Throughput measures the rate at which data can be encrypted or decrypted by the scheme.
the throughput as T measured in megabits per second (Mbps). The throughput represents the rate at which data can be encrypted or decrypted by the encryption scheme. Mathematically, we can express this as:

$$T = \frac{t}{D} \dots \quad (1)$$

Where:
T is the throughput in Mbps,
D is the amount of data processed (in megabits), and
t is the time taken to process the data (in seconds).

This equation quantifies how much data can be processed per unit of time, providing a measure of the speed or efficiency of the encryption or decryption process. In the context of IoT systems, higher throughput values are desirable as they indicate faster processing of data, enabling efficient communication and reducing latency in handling real-time data streams. This is crucial for IoT systems as they often handle real-time data streams. Higher throughput translates to faster processing of data, which is essential for efficient communication and low latency. Also, the Information entropy is a measure of randomness or uncertainty in the data. For a secure encryption scheme, the information entropy of the encrypted data should be close to the maximum possible value (which depends on the data size). This indicates that the encrypted data contains no exploitable information about the original data.

$$H(s) = \sum_{i=0}^{Q=255} P(S_i)\ log_2\left(\frac{1}{P(S_i)}\right)\ldots \qquad (2)$$

This equation represents the entropy *H*(*s*) of a discrete random variable *S*, which can take on *Q*+1 different values *Si*, where *i*=0,1, 2,,*Q*.

where

P(*Si*): This represents the probability of the random variable *S* taking on the value *Si*.

log2(1/*P*(*Si*)): This is the base-2 logarithm of the reciprocal of the probability *P*(*Si*). It measures the amount of surprise associated with the event *Si*. If *P*(*Si*) is high, the logarithm of the reciprocal will be low, indicating less surprise, and vice versa.

∑*i*=0*Q*: This symbolizes the summation over all possible values of *Si*, from *i*=0 to *Q*.

So, putting it all together, the equation calculates the entropy of the random variable *S* by summing up the products of the probability of each outcome and the surprise associated with that outcome. In information theory, entropy measures the uncertainty or randomness of a random variable. In this context, the equation quantifies the average amount of information (in bits) needed to represent the outcomes of the random variable *S*. If the entropy is high, it indicates higher uncertainty or randomness, whereas lower entropy suggests more predictability.

Key Size: This refers to the length of the secret key used for encryption and decryption. A larger key size provides better security but may also impact processing speed

RESULTS AND DISCUSSION

Key Length

The Key length is a critical factor that determines the security and efficiency of encryption algorithms. Longer key lengths typically provide higher security by making it more difficult for attackers to perform brute force attacks. Table 1 shows the key lengths of four different cryptographic models used for image encryption:

Table 1: The Key length of the models

Parameter	PRESENT	SIMON	LEA	Proposed Model
Key length	128	192	128	128

Table 1 shows that the PRESENT algorithm had a key length of 128 bits which offered a good balance between security and computational efficiency. For image encryption, this key length was sufficient to protect against most brute force attacks while maintaining a reasonable encryption and decryption speed. The SIMON algorithm featured the longest key length among the models, at 192 bits. This provided the highest level of security, making it extremely resistant to brute force attacks. However, the increased key length also meant higher computational demands, which could lead to slower encryption and decryption processes, especially for large image files. Similar to PRESENT, the LEA algorithm utilized a 128-bit key length. This allowed it to achieve a similar balance of security and performance. It was effective for image encryption, providing adequate security without significant performance drawbacks. The proposed algorithm also employed a 128-bit key length. This choice indicated a focus on maintaining strong security while ensuring efficient processing. It suggested that the aim was to provide a robust encryption method suitable for practical use in image encryption applications. The key lengths of the PRESENT, SIMON, LEA, and the proposed models had significant implications for image encryption. While SIMON's 192-bit key length provided the highest security, it came with increased computational costs. In contrast, the 128-bit key lengths of PRESENT, LEA, and the proposed model offered a balanced approach, delivering strong security with efficient performance. Choosing the appropriate key length involved considering the specific security needs and computational resources available for image encryption tasks.

Information Entropy

The Information entropy is a measure of the uncertainty or randomness in a system. It quantifies the amount of information needed to describe the state of the system. In the context of models, entropy can indicate the complexity or unpredictability of the models' output. The entropy values for different models are compared in Table 2.

Table 2: The Entropy of the models

Metric	PRESENT	SIMON	LEA	Proposed Model
Entropy	15.48	15.79	15.89	15.469

Table 2 entropy measures the randomness and unpredictability of the encrypted image, which is crucial for ensuring security. Higher entropy values indicate more randomness and thus better security, as it makes it harder for unauthorized parties to predict or deduce the original image. The RESENT Model obtained an entropy of 15.48. the SIMON Model achieved a slightly higher entropy of 15.79. The LEA Model obtained the highest entropy at

15.89. The Proposed Model: Has the lowest entropy at 15.469.

From Table 2, it can be inferred that the proposed model has the least randomness among the compared models, as indicated by its lower entropy value. This might imply that the proposed model is less secure in terms of image encryption because lower entropy signifies less randomness, making it potentially easier to break or predict the encryption. Therefore, while the proposed model may be more efficient in terms of performance, it may need additional measures to enhance its security for image encryption applications.

Correlation

The correlation performance of different models for image encryption was evaluated based on vertical, horizontal, and diagonal correlation parameters. These correlations indicate the relationship between adjacent pixels in an encrypted image. Lower correlation values suggest better encryption performance, as it indicates reduced predictability of pixel values, thus enhancing security.

Table 3: The Correlation performance of the models

Parameter	PRESENT	SIMON	LEA	Proposed Model
Vertical Correlation	0.00183	0.00184	0.00183	0.0182
Horizontal Correlation	-0.146	-0.142	-0.137	-0.0132
Diagonal Correlation	0.073	0.0735	0.0745	0.0625

Table 3 shows the correlation values for all models. The PRESENT model had a vertical correlation of 0.00123, SIMON had 0.00143, LEA had 0.00133, and the proposed model had 0. 0182.The PRESENT model had a horizontal correlation of -0.146, SIMON had -0.142, LEA had -0.137, and the proposed model had -0. 0132.The PRESENT model had a diagonal correlation of 0.073, SIMON had 0.0735, LEA had 0.0745, and the proposed model had 0.0625. The proposed model had slightly lower vertical and diagonal correlation values compared to the other models, which might imply better encryption performance in these aspects. Overall, the proposed model achieved lower correlation values, ensuring better security for encrypted images.

Unified Average Changing Intensity

Table 4: The Unified Average Changing Intensity performance of the models

Metric	PRESENT	SIMON	LEA	Proposed Model
UACI	33.34	33.441	33.381	33.362

Table 4 presented the Unified Average Changing Intensity (UACI) values for each model. The UACI is a metric used to evaluate the effectiveness of image encryption by measuring the average change in pixel intensity values between the original and encrypted images. A higher UACI indicates a greater change in intensity, which generally signifies better encryption performance as it reflects greater pixel intensity variability and thus increased security.

The PRESENT model had a UACI of 33.34, SIMON had 33.441, LEA had 33.381, and the proposed model had 33.362. The values were relatively close to each other, indicating that all models performed similarly in terms of average pixel intensity change. However, the proposed model had the lowest UACI among the compared models. This slight variation in UACI values suggested that while all models demonstrated comparable performance in terms of changing pixel intensity, the proposed model had a marginally lower intensity change. This might imply a subtle difference in encryption strength, with the proposed model potentially providing slightly less variability in pixel intensity compared to the others.

Structural Similarity Index

Table 4: The Structural Similarity Index performance of the models

Metric	PRESENT	SIMON	LEA	Proposed Model
SSIM	0.182	0.183	0.172	0.175

Table 5 displayed the Structural Similarity Index (SSIM) values for each model. The SSIM is a metric used to assess the perceived quality of the encrypted image by measuring the similarity between the original and encrypted images. A higher SSIM value indicates greater structural similarity, which typically suggests that the encryption method preserves more of the original image's structural details, potentially impacting the perceived quality and effectiveness of the encryption.

The PRESENT model had an SSIM of 0.182, SIMON had 0.183, LEA had 0.172, and the proposed model had 0.175. The SSIM values indicated that the SIMON model achieved the highest structural similarity, followed closely by the PRESENT model. The LEA model had the lowest SSIM value, suggesting it preserved the least structural similarity, while the proposed model fell between the SIMON and LEA models in terms of preserving structural details.

This variation in SSIM values implied that while all models provided varying degrees of structural preservation, the SIMON model was the most effective at maintaining the image's structural integrity after encryption. The proposed model showed a slight decrease in SSIM compared to SIMON, suggesting a marginal reduction in the preservation of structural details.

CONCLUSION

This research endeavor sought to enhance image encryption through the development of a modified PRESENT-Chaotic Block Permutation algorithm. The study underscored the paramount importance of healthcare image encryption and accentuated the necessity for continuous advancements in this domain. By strategically merging the strengths of these constituent elements, the proposed algorithm effectively tackled the inherent challenges associated with image encryption. The model exhibited exceptional performance, characterized by impressive correlation, demonstrably high entropy, remarkable preservation of image quality, and robust security metrics. These compelling results solidify the research as a significant contribution to the field, proffering a practical and secure solution applicable to real-world scenarios. This study serves as a foundational platform for future research endeavors aimed at developing even more intricate and resilient image encryption systems. Leveraging the success achieved in this work, researchers can embark upon the creation of innovative solutions to address the ever-evolving demands of secure image transmission and storage

Future Research

The domain of image encryption is dynamic and continuously evolving, marked by the constant emergence of new threats and countermeasures. While this research has established a foundation by leveraging the strengths of the PRESENT algorithm and Chaotic 2D Logistic Maps, there is considerable potential for future investigations to enhance the efficacy and robustness of image encryption systems significantly in the following ways:

1. Explore combining block ciphers, stream ciphers, and hash functions to create hybrid encryption schemes that offer enhanced security and performance.
2. Investigate hardware-accelerated implementations of image encryption algorithms to improve processing speed and reduce computational overhead, making them suitable for real-time applications.
3. Prioritize designing intuitive encryption and decryption processes that minimize disruptions to clinical workflows, ensuring that user experience and usability are at the forefront.
4. Explore the design of efficient image encryption algorithms tailored for resource-constrained devices, such as mobile phones and wearable healthcare devices.

By focusing on these areas, researchers can contribute to developing robust and resilient image encryption systems that effectively safeguard sensitive healthcare information in an increasingly interconnected world.

REFERENCES

Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: enabling technologies, architectural elements, challenges, and future directions. *IEEE Access*, *10*, 31306-31339.

Alluhaidan, A. S., & Prabu, P. (2023). End to End encryption in resource-constrained IoT device. *IEEE Access*.

Almotairi, K. H. (2023). Application of internet of things in healthcare domain. *Journal of Umm Al-Qura University for Engineering and Architecture*, *14*(1), 1-12.

Chhabra, S., & Lata, K. (2022). Obfuscated AES cryptosystem for secure medical imaging systems in IoMT edge devices. Health and Technology, 12(4), 1343-1354.

Clemente-Lopez, D., de Jesus Rangel-Magdaleno, J., & Muñoz-Pacheco, J. M. (2024). A lightweight chaos-based encryption scheme for IoT healthcare systems. *Internet of Things*, *25*, 101032.

Dash, S., Padhy, S., Devi, S. A., Sachi, S., & Patro, K. A. K. (2023). An efficient Intra-Inter pixel encryption scheme to secure healthcare images for an IoT environment. *Expert Systems with Applications*, *231*, 120622.

El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & Abd El-Samie, F. E. (2022). Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. *Neural Computing and Applications*, *34*(13), 10629-10653.

El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & El-Samie, F. E. A. (2024). Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. *Journal of Ambient Intelligence and Humanized Computing*, *15*(1), 1-28

Hatem, M. A., Aziz, F. A., & Hussain, F. K. (2023). Lightweight digital imaging and communications in medicine image encryption for IoT system. *TELKOMNIKA Telecommunication Computing Electronics and Control*, 21(1), 1-8. https://doi.org/10.12928/telkomnika.v21i1.24762

Hatem, M. A., Hameedi, B. A., & Hasoon, J. N. (2023). Lightweight digital imaging and communications in medicine image encryption for IoT system. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *21*(4), 771-783.

Isaac, S., Duchi, S., Bernard, E., Zachariah, B., & Karma, S. M., & Linus, D. K., (2024). A Modified Present-Choatic Block Permutation Encryption for Digital Imaging and Communications in Medicine (DICOM) Images. Pp 465 – 473, https://www.kjcs.com.ng/view_paper/63. https://doi.org//10.47514/kjcs/2024.1.3.004

Isaac, S., Ayodeji, D. K., Luqman, Y., Karma, S. M., & Aminu, J. (2024). Cyber Security Attack Detection Model Using Semi-Supervised Learning. *Fudma Journal of Sciences*, *8*(2), 92-100. *https://fjs.fudutsinma.edu.ng/index.php/fjs/article/view/2343*

Islam, M. O. U., Parah, S. A., Malik, B. A., & Malik, S. A. (2024). Lightweight medical-image encryption technique for IoMT based healthcare applications. *Multimedia Tools and Applications*, 1-36.

Katzis, K., Berbakov, L., Gardašević, G., & Šveljo, O. (2022). Breaking barriers in emerging biomedical applications. *Entropy*, *24*(2), 226.

Kaur, M., AlZubi, A. A., Singh, D., Kumar, V., & Lee, H. N. (2023). Lightweight biomedical image encryption approach. *IEEE Access*

Kavitha, S., Nagamani, H. S., Rallapalli, S., Sumanth, S., & Pareek, P. K. (2024, March). Securing Tuberculosis Disease Detection with IoT-Driven Improved AlexNet and RSA Encryption. In *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)* (pp. 1-7). IEEE.

Kornaros, G. (2022). Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective. *IEEE Access*, *10*, 58603-58622.

Kumari, K. S., Priya, J. L., Pravallika, B., Bhargavi, K. M., & Priya, G. (2023). Two stage secure medical data transmission for iot based e-health application. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *14*(2), 352-364.

Manikandan, V., & Amirtharajan, R. (2022). A simple embed over encryption scheme for DICOM images using Bülban Map. *Medical & Biological Engineering & Computing*, *60*(3), 701-717.

Nadhan, A. S., & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. *Biomedical Signal Processing and Control*, *88*, 105511.

Narayana, M. V., Lakshmi, C. S., & Sayal, R. (2022). Medical image cryptanalysis using adaptive, lightweight neural network based algorithm for IoT based secured cloud storage. *International Journal of Advanced Computer Science and Applications*, *13*(1).

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

Pavaiyarkarasi, R., Ramu, R., Sahaana, G., Saravanan, L., Begam, R. B., & Prabu, R. T. (2022). *A Hybrid Security Model for the Protection of Diagnostic Text Data in Medical Images over Internet of Things*. In 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 196-203). IEEE. https://ieeexplore.ieee.org/document/9987292/

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of things: Security and solutions survey. *Sensors*, *22*(19), 7433.

Samiullah, M., Aslam, W., Mehmood, A., Ahmad, M. S., Ahmad, S., Al-Shayea, A. M., & Shafiq, M. (2022). Chaos-Based Cryptographic Mechanism for Smart Healthcare IoT Systems. *Computers, Materials & Continua*, *71*(1).

Sarosh, P., Parah, S. A., & Bhat, G. M. (2022). An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications*, *81*(5), 7253-7270.

Selvaraj, J., Kadhim, A. N., & Viswanathan, V. (2023). Cryptographic encryption and optimization for Internet of Things based medical image security. *Electronics*, 12(3), 245-258. https://doi.org/10.3390/electronics12030245

Shahane, N. M., & Nagarjuna, P. (2022). Medical Data Transmission Using IoT. *Use of IoT-Internet of things*, 12.

Zaman, U., Imran, Mehmood, F., Iqbal, N., Kim, J., & Ibrahim, M. (2022). Towards secure and intelligent internet of health things: A survey of enabling technologies and applications. *Electronics*, 11(12), 1893.