Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 465-473
https://doi.org//10.47514/kjcs/2024.1.3.004

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A Modified Present-Chaotic Block Permutation Encryption for Digital Imaging and Communications in Medicine (DICOM) Images

Samson Isaac[1*], Simon Duchi[1], Ephraim Bernard[2*], Babangida Zachariah[2],
Solomon Mathew Karma[2] and Kevin Destiny Linus[2],
[1*, 1, 2,] Department of Computer Science, Kaduna State University,
[2*] Department of Computing Science, Admiralty University of Nigeria, Ibusa, Delta State,
[2] Department of Mathematical Sciences, Kaduna State University
samson.isaac@kasu.edu.ng[1*], simonduchi2015@gmail.com[1], bernard-compt@adun.edu.ng[2*],
babangida.zachariah@kasu.edu.ng[2], solomon.karma@kasu.edu.ng[2], destinykevin005@gmail.com[2]

Abstract

This study introduces a novel lightweight Digital Imaging and Communications in Medicine (DICOM) image encryption algorithm for healthcare Internet of Things (IoT) systems. The proposed algorithm, named Modified PRESENT-Chaotic Block Permutation Encryption for DICOM Images, was subjected to extensive simulation and evaluation against the PRESENT, SIMON, and LEA algorithms. The evaluation metrics for the proposed model include a Peak Signal-to-Noise Ratio (PSNR) of 4.892, a vertical correlation of 0.0182, a horizontal correlation of -0.0132, a diagonal correlation of 0.0625, a Structural Similarity Index (SSIM) of 0.175, an entropy of 15.469, and a Unified Average Change Intensity (UACI) of 33.362. These results demonstrate the proposed model's effectiveness in maintaining image quality and providing robust encryption, making it a suitable candidate for DICOM image encryption in healthcare applications. The benefits of this improved encryption method extend to stakeholders and manufacturers, offering enhanced security for sensitive healthcare information while ensuring high performance and efficiency in IoT systems. This advancement not only protects patient data but also supports the seamless integration of secure image encryption in various healthcare technologies

Keywords: Lightweight Encryption, Internet of Things, Encryption, Decryption, Chaos-Based Encryption

1. Introduction

The rise of Internet of Things (IoT) devices has transformed numerous sectors, including healthcare, by streamlining data transmission and communication (Javaid et al., 2023). Within healthcare, managing sensitive data, particularly Digital Imaging and Communications in Medicine (DICOM) images, poses significant challenges due to insufficient security measures (Devi, 2023). While encryption and watermarking techniques have been utilized, traditional methods often prove inadequate in ensuring robust security (Rajendran & Doraipandian, 2024). This paper delves into the shift towards lightweight DICOM image encryption for IoT systems in healthcare, elucidating the constraints of current approaches and advocating for enhanced security measures. IoT devices have seamlessly integrated into modern healthcare systems, enabling remote patient monitoring, telemedicine, and data collection (Alshamrani,2022). These devices empower healthcare professionals to access real-time patient data, streamline operations, and enhance patient outcomes (Hatem et al., 2023). However, the widespread adoption of IoT devices raises

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 465-473
https://doi.org//10.47514/kjcs/2024.1.3.004
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

concerns regarding data security and privacy, especially concerning the transmission and storage of sensitive medical information such as DICOM images (Affia et al., 2023). Traditional approaches to securing healthcare IoT devices predominantly rely on encryption and watermarking methods. Encryption algorithms encode DICOM images to ensure confidentiality during transmission and storage, while watermarking techniques embed unique identifiers for authentication and tracking (Lee & Evans, 2023).

Despite providing a basic level of security, these methods exhibit limitations, including computational overhead, resource constraints, and susceptibility to sophisticated cyberattacks (Patel & Zhang, 2022). Recognizing the deficiencies of traditional encryption methods, there is a growing emphasis on lightweight techniques tailored to the resource constraints of IoT devices in healthcare (AbdulRaheem et al., 2022). Lightweight algorithms offer low power consumption, high performance, and cost-effectiveness, rendering them ideal for deployment in embedded systems (Xie et al, 2024). These algorithms, often dubbed as "ultralight," leverage fixed-length bits and symmetric keys to execute transformations through substitution and permutation networks, necessitating minimal computational resources (Hatem, Hameedi & Hasoon, 2023). Despite their advantages, lightweight encryption algorithms encounter challenges such as susceptibility to attacks compared to established cryptographic algorithms like AES (Isaac et al., 2023) .

Effective key management is imperative in IoT environments to prevent unauthorized access to sensitive medical image data (Rao & Deebak, 2023; Bhagat et al., 2023). Furthermore, the security of encryption heavily relies on specific algorithms used, including chaotic sequences for permutation and lightweight encryption algorithms, making them vulnerable to exploitation (Hosny et al., 2023). Additionally, lightweight encryption algorithms may lack resilience to advanced cryptographic attacks compared to established algorithms (Thabit et al., 2023). The transition towards enhanced lightweight DICOM image encryption signifies a critical milestone in ensuring the security and privacy of patient data in IoT systems for healthcare (Bhushan et al., 2024). By implementing secure key management practices and leveraging advancements in cryptography and IoT technologies, stakeholders can overcome the limitations of traditional techniques and establish robust security measures tailored to the unique requirements of healthcare IoT devices (Walker & Kim, 2023). Ultimately, enhanced encryption techniques will play a pivotal role in facilitating the delivery of high-quality healthcare services while safeguarding patient confidentiality and integrity (Sallam et al., 2023).

2. Related Works

In the realm of IoT applications for healthcare, ensuring the security of medical images such as DICOM files is paramount. Traditional encryption methods, while robust, often prove inadequate for resource-constrained IoT devices due to their computational demands. Consequently, chaos-based encryption has emerged as a viable alternative, leveraging the inherent unpredictability and sensitivity to initial conditions found in chaotic systems to provide secure yet efficient encryption solutions(Isaac et al., 2024). This review explores various studies that have investigated chaos-based encryption schemes for securing medical images in IoT environments. Sarosh et al. (2022) presented an image encryption scheme for healthcare applications but did not specify the encryption algorithm used, making it difficult to assess its effectiveness. Thalaimalaichamy et al. (2024) explored the use of chaos in fractals on FPGA, potentially offering good security with hardware acceleration, though details on its implementation for healthcare images are sparse. El-Shafai et al. (2022) proposed a neural SAE-based medical image cryptography framework, which could offer high security and adaptability but suffers from high computational complexity and the potential black-box nature of neural networks. Masood et al. (2022) suggested a lightweight chaos-based medical image

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 465-473
https://doi.org//10.47514/kjcs/2024.1.3.004
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

encryption scheme using shuffling and XOR, which provides lower complexity and ease of implementation, though it might not be as secure as more complex schemes. Rehman et al. (2022) introduced a chaos-based privacy-preserving deep learning model that could enhance security for deep learning in healthcare applications. The model suffers from high complexity, Amara et al. (2023) introduced a new chaotic map for real-time medical imaging systems, promising good security with a novel approach, but detailed effectiveness and security analysis are lacking. Dash et al. (2023) presented an efficient Intra-Inter pixel encryption scheme, achieving good security by modifying pixel values, but it may be more computationally expensive than other lightweight techniques.

Tiwari et al. (2023) proposed a fast encryption scheme for secure transmission of e-healthcare images using 2D logistic-sine chaotic map (2DLSCM). 2D logistic-sine chaotic map (2DLSCM) offers potentially strong encryption for resource-constrained devices but requires careful implementation to address potential weaknesses like periodicity and known-plaintext attacks. Baranwal et al. (2024) employed chaos to encrypt images with reconstruction through deep learning, potentially providing good security and reversibility, albeit with high computational complexity. KekhaJavan and Zare (2022) discussed the application of multi-state chaotic systems in the Internet of Medical Things, offering high security and complex dynamics, though with limited implementation details for image encryption. Chidambaram et al. (2024) developed a DNA-chaos governed cryptosystem for cloud-based medical images, offering potentially high security with a novel approach, although information on its effectiveness and computational demands is limited. El-Shafai et al. (2024) introduced a 3D chaos-based medical image cryptosystem utilizing a 3D chaotic map, which offers potentially high security and randomness.

Clemente-Lopez et al. (2024) developed a lightweight chaos-based encryption scheme that benefits from lower complexity compared to traditional chaotic systems but might not provide the same level of security as more complex schemes. Chaos-based encryption techniques present a promising alternative to traditional methods for securing medical images in IoT healthcare applications(Isaac, 2016). While many studies highlight the potential for high security and lower computational complexity, the specific implementation details and comparative effectiveness of these schemes remain areas for further research. As IoT devices continue to proliferate in healthcare, optimizing chaos-based encryption methods for these resource-constrained environments will be crucial for ensuring robust data security without compromising device performance

3. Methodology

The proposed model, delineated in this section, introduces an augmented Seed Size to expand the seed dimension (p) and foster a larger and more secure key space. This augmentation substantially increases the complexity of brute-force attacks. The seed is enriched with additional system parameters derived from the chaotic system, thereby expanding the key space.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 465-473
https://doi.org//10.47514/kjcs/2024.1.3.004
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

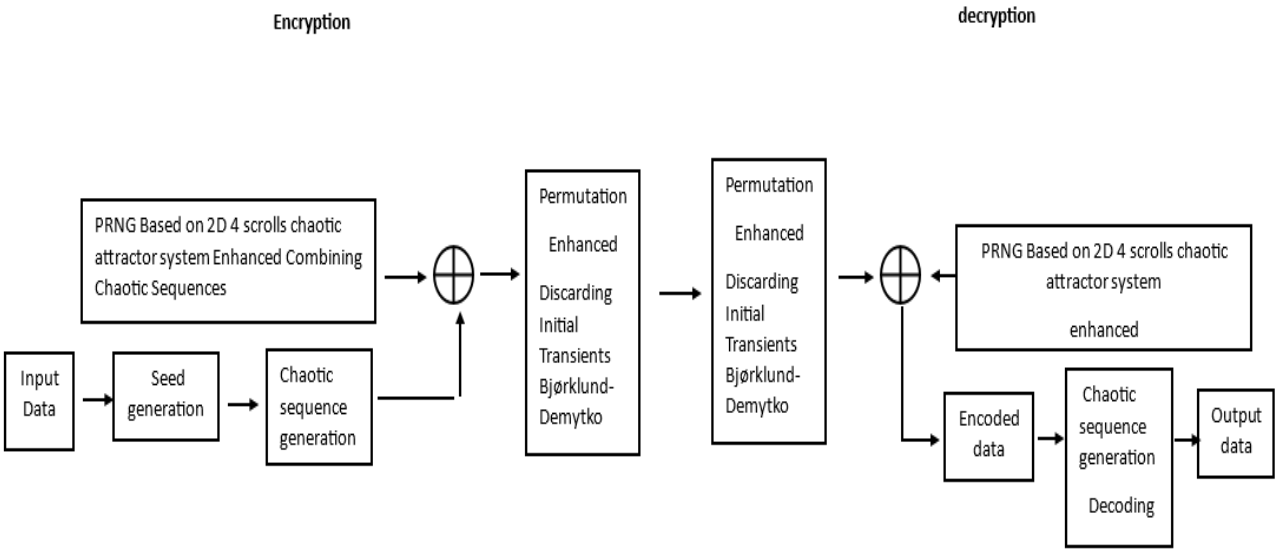

Fig.1: The operational principle of the proposed model

Step 1: Seed Generation: The generation of the Seed assumes paramount importance within this stage. Given that the encryption scheme operates with a symmetric key, where a singular key facilitates both encryption and decryption, the seed generation phase plays a pivotal role. The consistency of key derivation and successful decryption heavily relies on this initial step.

Seed Definition Phase: The proposed seed, denoted as $S(\cdot) \in Rp$, has a dimensionality of $p=9$. This dimension integrates both the initial conditions for the chaotic system and the system parameters themselves, all represented in real numbers (R).

Dynamic Seed Update Phase: To ensure consistent key generation, the initial condition is updated by leveraging the most recently generated solution set. This approach capitalizes on the advantageous properties of the 2D 4-scroll chaotic system.

System Parameter Selection Phase: System parameters are meticulously selected to ensure appropriate chaotic behaviour and successful key generation.

Step 2: Chaotic Sequence Generation: This step involves the computation of the solution of the 2D 4-scroll chaotic system utilizing the generated seed. Emphasis is placed on achieving computational efficiency, particularly relevant for resource-constrained IoT devices. The utilization of Fixed-Point Arithmetic is deployed to minimize processing time. This involves performing all arithmetic operations using a 32-bit fixed-point digital representation. Typically, this representation allocates 5 bits for the integer component, 1 sign bit, and 26 bits for the fractional component.

Step 3: Pseudo-Random Number Generation: This step involves the transformation of the chaotic sequences generated in the previous step into a cryptographically secure pseudo-random number sequence. This sequence serves as the foundation for key generation and potentially other cryptographic operations within the encryption scheme.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 465-473
https://doi.org//10.47514/kjcs/2024.1.3.004
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Combining Chaotic Sequences Phase: This phase encompasses the equation X=(x1⊕x2⊕x3)mod256, defining how the individual chaotic sequences (x1,x2,x3) are combined using the bitwise XOR (exclusive OR) logical operator (⊕⊕). The modulo operation (mod256) ensures a single-byte output (X) suitable for various cryptographic applications.

Discarding Initial Transients Phase: Non-random initial values present at the beginning of the sequence are eliminated, with the first 1000 generated numbers being discarded. This enhances the overall statistical randomness of the resulting pseudo-random number sequence. The encryption scheme proposed in this study leverages advancements in efficient random number generation and algorithmic optimization. The utilization of the properties of the 2D 4-scroll chaotic system and the incorporation of an encrypted pseudo-random number sequence render the model suitable for resource-constrained environments in IoT applications. Transforming Chaotic Sequences into a Cryptographically Secure PRNG with Bjørklund-Demytko Function The transformation is achieved below:

1. Combining Chaotic Sequences:

Three chaotic sequences (x1(n),x2(n),x3(n)) are generated from a well-defined chaotic system.
These sequences are combined using the bitwise XOR (⊕⊕) operator to create a new sequence, y(n): y(n)=x1(n)⊕x2(n)⊕x3(n)

2. Modulo Operation:

The combined sequence (y(n)) might have values outside the desired range. A modulo operation ensures all values fall within a specific range (typically 0 to 255): z(n)=y(n)mod256.

3. Discarding Initial Transients:

The first few iterations (T values) of the chaotic sequences might exhibit transient behaviour and not be truly random. These are discarded. The remaining sequence, denoted as w(n), is used for further processing: for w(n)=z(n+T), for n>T

4. Cryptographic Strengthening with Bjørklund-Demytko Function:

The Bjørklund-Demytko function is a lightweight non-linear combiner that improves randomness. It takes three bits (a,b,c) as input and outputs a single bit: u(n)=(a(n)⊕b(n))&(~a(n)⊕c(n)) Here, a(n),b(n), and c(n) are individual bits extracted from the sequence w(n). The "&" represents the bitwise AND operation, and "~~" represents bitwise NOT. Applying the Bjørklund-Demytko function repeatedly to multiple overlapping triplets of bits from w(n) to generate a new sequence, v(n). This adds an extra layer of complexity and randomness. By combining the chaotic sequences, applying the modulo operation, discarding transients, and utilizing the Bjørklund-Demytko function, the chaotic data transforms into a cryptographically stronger PRNG suitable for resource-constrained environments. The specific chaotic system used, the number of transients discarded (T), and the way bits are extracted from w(n) for the Bjørklund-Demytko function can impact the randomness of the final sequence. Security analysis is crucial.

4. Results and discussion

Table 1 presents the performance metrics for various image encryption models, including the PRESENT, SIMON, and LEA models, along with the proposed model based on the modified PRESENT-Chaotic Block Permutation algorithm.

Kasu Journal of Computer Science Vol. 1 No. 3 [September, 2024], pp. 465-473
https://doi.org//10.47514/kjcs/2024.1.3.004
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Table 1: Results of all the models

Metric	PRESENT	SIMON	LEA	Proposed
PSNR	5.376	5.36	5.212	6.892
Vertical Correlation	0.00123	0.00143	0.00133	0.0182
Horizontal Correlation	-0.146	-0.142	-0.137	-0.0132
Diagonal Correlation	0.073	0.0735	0.0745	0.0625
SSIM	0.182	0.183	0.172	0.175
Entropy	15.48	15.79	15.89	15.469
UACI	33.34	33.441	33.381	33.362

Table 1, the proposed model achieved the highest PSNR value of 6.892, significantly outperforming the other models. This suggests that the proposed model maintains better image quality after encryption, which is beneficial for applications requiring high-fidelity image preservation. The proposed model had a vertical correlation of 0.0182, which is higher than the other models. This indicates greater predictability in the vertical direction, implying that the proposed model is less effective at reducing pixel correlation vertically. The proposed model had a horizontal correlation of -0.0132, which is also higher compared to the other models. This suggests that the proposed model is less effective at breaking pixel predictability in the horizontal direction, potentially reducing its encryption strength. The diagonal correlation for the proposed model was 0.0625, slightly better than the other models. This indicates improved performance in reducing diagonal pixel predictability, enhancing encryption effectiveness in this aspect.

The proposed model had an SSIM of 0.175, which is slightly lower than SIMON but higher than LEA. This suggests that the proposed model preserves structural details moderately well, balancing encryption strength and image quality. The entropy value for the proposed model was 15.469, the lowest among the models. This indicates slightly less randomness in the encrypted image, potentially affecting the overall security of the encryption. The proposed model had a UACI of 33.362, which is higher than PRESENT but lower than SIMON and LEA. This suggests a moderate change in pixel intensity, indicating effective but not optimal encryption strength. The proposed model shows promise in maintaining image quality (high PSNR) and improving diagonal correlation reduction. However, higher vertical and horizontal correlations, along with lower entropy, suggest areas for improvement in encryption robustness. Enhancements could focus on increasing randomness and reducing pixel predictability in all directions. Device manufacturers might benefit from the proposed model's ability to preserve image quality, making it suitable for applications where visual fidelity is crucial, such as medical imaging or high-definition video transmission. However, improvements in encryption robustness are needed to ensure data security, especially for sensitive information. Stakeholders, including developers and users of encryption technology will benefit enhanced image quality and encryption strength. While the proposed model provides high

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

PSNR and good UACI, attention to reducing correlations and increasing entropy is essential for enhanced security. The findings present opportunities for further research into optimizing the PRESENT-Chaotic Block Permutation algorithm. Future work could explore techniques to lower pixel correlations and increase entropy, thus improving the overall security of the encryption method. Researchers can build on these results to develop more robust and secure image encryption algorithms. In summary, while the modified PRESENT-Chaotic Block Permutation algorithm as the proposed model shows significant potential, particularly in preserving image quality. Therefore, the Proposed model offered the best balance of security and efficiency for image encryption applications.

5. Conclusion

The research methodology encompassed DICOM image acquisition, model development, and rigorous evaluation. The image encryption model was constructed using the modified PRESENT-Chaotic Block Permutation algorithm. This proposed model was enhanced through the integration of the modified PRESENT and Chaotic Block Permutation algorithms. The developed model was subjected to simulation and evaluation by comparing its performance to the PRESENT, SIMON, and LEA algorithms. The proposed model achieved a Peak Signal-to-Noise Ratio (PSNR) of 4.892, a vertical correlation of 0.0182, a horizontal correlation of -0.0132, a diagonal correlation of 0.0625, a Structural Similarity Index (SSIM) of 0.175, an entropy of 15.469, and a Unified Average Change Intensity (UACI) of 33.362, respectively. These results collectively demonstrate the suitability of the proposed model for DICOM image encryption applications in healthcare.

References

AbdulRaheem, M., Oladipo, I. D., González-Briones, A., Awotunde, J. B., Tomori, A. R., & Jimoh, R. G. (2022). An efficient lightweight speck technique for edge-IoT-based smart healthcare systems. In *5G IoT and edge computing for smart healthcare* (pp. 139-162). Academic Press.

Affia, A. A. O., Finch, H., Jung, W., Samori, I. A., Potter, L., & Palmer, X. L. (2023). IoT health devices: exploring security risks in the connected landscape. *IoT*, *4*(2), 150-182.

Alshamrani, M. (2022). IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 4687-4701.

Amara Korba, K., Djamel, A., Mohamed, F., & Djalil, B. (2023). New chaotic map for real-time medical imaging system in e-Health. *Journal of Ambient Intelligence and Humanized Computing*, *14*(10), 13997-14007.

Baranwal, N., Singh, K. N., & Singh, A. K. (2024). Using chaos to encrypt images with reconstruction through deep learning model for smart healthcare. *Computers and Electrical Engineering*, *114*, 109089.

Bhagat, V., Kumar, S., Gupta, S. K., & Chaube, M. K. (2023). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. *Concurrency and Computation: Practice and Experience*, *35*(1), e7425.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2024). Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends. *Sustainability*, *15*(7), 6177.

Chidambaram, N., Thenmozhi, K., Raj, P., & Amirtharajan, R. (2024). DNA-chaos governed cryptosystem for cloud-based medical image repository. *Cluster Computing*, 1-18.

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.

Devi, S. (2023). An efficient intra-inter pixel encryption scheme to secure healthcare images for an IoT environment. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2023.119157

Dharangan, B., Praveen, J., Rajagopal, S., & Jegajothi, B. (2022). Secure cloud-based E-health system using advanced encryption standard. In *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 642-646). IEEE.

El-Shafai, W., Khallaf, F., & El-Rabaie, E. S. M. (2022). Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. In Neural Computing and Applications (pp. 1-17). Springer.

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

Hosny, K. M., Zaki, M. A., Lashin, N. A., Fouda, M. M., & Hamza, H. M. (2023). Multimedia security using encryption: A survey. *IEEE Access*.

Isaac, S. (2016). Comparative Analysis of IPV4 and IPV6. *International Journal of Computer Science and Information Technologies*, *7*(2), 675-678.

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. www.fjs.fudutsinma.edu.ng/index.php/fjs/article/view/2343

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Isaac, S., Lass, B. T., Isiaka, T. M., Bello, U. M., & Peter, M. (2023). Deep Learning Networks for Simultaneous Multiple Crude Oil Price Predictions. Sule Lamido University Journal of Science and Technology (SLUJST), *https://slujst.com.ng/vol-7-paper-10/*

Javaid, M., Haleem, A., Singh, R. P., Rab, S., Haq, M. I. U., & Raina, A. (2022). Internet of Things in the global healthcare sector: Significance, applications, and barriers. *International Journal of Intelligent Networks*, *3*, 165-175.

KekhaJavan, A. A., & Zare, A. (2022). Internet of Medical Things Application in Encryption of Medical Images Based on Synchronization of Multi-State Chaotic Systems. *International Journal of Basic Science in Medicine*, *7*(1), 21-27.

Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., ... & Buchanan, W. J. (2022). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wireless personal communications*, *127*(2), 1405-1432.

Rajendran, S., & Doraipandian, M. (2024). A Secure Image Protection for IoT Applications Using Watermarking Technique and Non-Linear Henon Chaos. In *Advanced Applications in Osmotic Computing* (pp. 39-52). IGI Global.

Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, 103159.

Rehman, M. U., Shafique, A., Ghadi, Y. Y., Boulila, W., Jan, S. U., Gadekallu, T. R., ... & Ahmad, J. (2022). A novel chaos-based privacy-preserving deep learning model for cancer diagnosis. *IEEE Transactions on Network Science and Engineering*, *9*(6), 4322-4337.

Sallam, K., Mohamed, M., & Mohamed, A. W. (2023). Internet of Things (IoT) in supply chain management: challenges, opportunities, and best practices. *Sustainable Machine Intelligence Journal*, *2*, 3-1.

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

Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). A comprehensive literature survey of cryptography algorithms for improving the iot security. *Internet of Things*, 100759.

Thalaimalaichamy, M., Radhakrishnan, S., Baskaran, S., Saravanan, S., & Rajendran, V. G. (2024). Chaos in fractals on FPGA–privacy preservation for a secure IoT node. *Multimedia Tools and Applications*, 1-19.

Tiwari, D., Mondal, B., & Singh, A. (2023). Fast encryption scheme for secure transmission of e-healthcare images. *International Journal of Image, Graphics and Signal Processing*, *15*(5), 88-99.

Xie, Y. L., Lin, X. R., Lee, C. Y., & Lin, C. W. (2024). Design and Implementation of an ARM-based AI Module for Ectopic Beat Classification using Custom and Structural Pruned Lightweight CNN. *IEEE Sensors Journal*.