Advancements in Ultrasound Technology and IoT Security: A Physics-Based Approach to Enhanced Imaging with Lightweight Encryption Algorithms /

Original article

Noor Fawzi Shafiq
Department of Medical Physics, College of Applied Sciences, University of Fallujah, Fallujah / Iraq

التطورات في تقنية الموجات فوق الصوتية وأمن إنترنت الأشياء: نهج قائم على الفيزياء لتحسين التصوير باستخدام خوارزميات تشفير خفيفة الوزن

نور فوزي شفيق
قسم الفيزياء الطبية، كلية العلوم التطبيقية، جامعة الفلوجة، الفلوجة \ العراق

Abstract

The rapid advancements in ultrasound technology, coupled with the growing significance of IoT security, present a unique opportunity to enhance imaging systems while ensuring data integrity. This study explores the integration of physics-based principles in ultrasound imaging, focusing on how lightweight encryption algorithms can secure data transmitted from IoT devices. Ultrasound technology has evolved significantly, benefiting from improved imaging techniques and the incorporation of IoT devices. As these devices proliferate across various applications, including healthcare and industrial monitoring, the need for secure data transmission becomes paramount. This paper proposes a framework that combines advanced ultrasound imaging with robust lightweight encryption methods to protect sensitive information.

We investigate the use of physics-based approaches to optimize ultrasound imaging quality while implementing encryption algorithms that minimize computational overhead. This dual focus not only enhances the clarity of images but also ensures that data from IoT devices is transmitted securely. Through this research, we aim to establish a comprehensive understanding of how these advancements can lead to improved outcomes in both imaging and data security, ultimately contributing to more reliable and secure IoT applications in various fields.

Keywords: Ultrasound Technology, Internet of Things (IoT), Data Security, Lightweight Encryption, Imaging Techniques, Physics-Based Approach.

المستخلص

يُتيح التقدم السريع في تقنية الموجات فوق الصوتية، إلى جانب الأهمية المتزايدة لأمن إنترنت الأشياء، فرصةً فريدةً لتحسين أنظمة التصوير مع ضمان سلامة البيانات. تستكشف هذه الدراسة دمج المبادئ الفيزيائية في التصوير بالموجات فوق الصوتية، مع التركيز على كيفية تأمين خوارزميات التشفير خفيفة الوزن للبيانات المُرسلة من أجهزة إنترنت الأشياء. شهدت تقنية الموجات فوق الصوتية تطورًا ملحوظًا، مستفيدةً من تقنيات التصوير المُحسّنة ودمج أجهزة إنترنت الأشياء. ومع انتشار هذه الأجهزة في مختلف التطبيقات، بما في ذلك الرعاية الصحية والمراقبة الصناعية، أصبحت الحاجة إلى نقل آمن للبيانات أمرًا بالغ الأهمية. تقترح هذه الورقة إطار عمل يجمع بين التصوير بالموجات فوق الصوتية المُتقدم وطرق تشفير خفيفة الوزن متينة لحماية المعلومات الحساسة. ندرس استخدام مناهج قائمة على الفيزياء لتحسين جودة تصوير الموجات فوق الصوتية مع تطبيق خوارزميات تشفير تُقلل من التكاليف الحسابية. هذا التركيز المزدوج لا يُعزز وضوح الصور فحسب، بل يضمن أيضًا نقل البيانات من أجهزة إنترنت الأشياء بأمان. نهدف من خلال هذا البحث إلى بناء فهم شامل لكيفية مساهمة هذه التطورات في تحسين النتائج في كل من التصوير وأمن البيانات، مما يُسهم في نهاية المطاف في تطبيقات إنترنت الأشياء أكثر موثوقية وأمانًا في مختلف المجالات.

الكلمات المفتاحية: تقنية الموجات فوق الصوتية، إنترنت الأشياء (IoT)، أمن البيانات، التشفير خفيف الوزن، تقنيات التصوير، النهج القائم على الفيزياء.

1. Introduction

Advancements in ultrasound technology are reshaping the landscape of medical diagnostics, particularly through the integration of Internet of Things (IoT) capabilities [1]. Ultrasound imaging is valued for its non-invasive nature, real-time monitoring, and versatility across various medical applications, including obstetrics, cardiology, and emergency medicine [2-6]. As IoT devices proliferate, they enhance the capabilities of ultrasound systems, enabling remote monitoring and data transmission that can significantly improve patient care [7].

However, the integration of IoT in ultrasound technology also raises critical security concerns [8]. The transmission of sensitive medical data over networks necessitates robust protection against unauthorized access and data breaches [9-11]. Traditional encryption methods may not be suitable for resource-constrained IoT devices due to their high computational demands [12]. This highlights the need for lightweight encryption algorithms that can ensure data security without compromising the performance of ultrasound systems [13].

This paper explores the intersection of ultrasound technology advancements and IoT security, focusing on a physics-based approach to enhance imaging performance while implementing effective lightweight encryption strategies. By leveraging the physical principles of sound wave propagation and interaction with biological tissues, we aim to improve the quality and reliability of ultrasound images while ensuring the secure transmission of data.

We will examine recent developments in ultrasound technology, including advanced imaging techniques and sensor integration, alongside their implications for clinical applications. Additionally, we will discuss how lightweight encryption algorithms can be seamlessly integrated into IoT-enabled ultrasound systems, balancing the critical trade-off between security and efficiency. Through this research, we aim to contribute to the ongoing discourse on enhancing medical diagnostics and protecting patient data in an increasingly interconnected healthcare environment.

2.Related Work

Previous studies have extensively explored various facets of ultrasound technology, including transducer development, beamforming techniques, and image reconstruction methods [1]. Recent literature emphasizes integrating physics-based models with machine learning algorithms to enhance image quality and diagnostic accuracy [2][3]. For example, deep learning techniques have been applied to improve beamforming processes and image segmentation, leading to more precise and efficient imaging systems [2].

2.1 Advancements in Ultrasound Imaging Physics-Inspired Models

Research has focused on improving the quality of generated ultrasound images by introducing physics-based diffusion models specifically designed for this imaging modality [3][4]. These models incorporate ultrasound-specific scheduler schemes that mimic the natural behavior of sound wave propagation, aiding in modeling attenuation dynamics [4]. Resolution Enhancement: Novel methodologies have been introduced to retrieve continuous echogenicity maps by learning implicit neural representations based on differentiable rendering pipelines that model the ultrasound formation process, enhancing the quality of ultrasound imaging [2]. A physics-based deconvolution method, PHOCUS, has been developed for ultrasound resolution enhancement, integrating physical sound propagation principles with advanced computational techniques on B-mode images [2]. Deep Learning Applications: Deep learning models are being used for super-resolution ultrasound localization microscopy, enhancing vascular imaging [5]. AI-driven approaches also show promise in personalized treatment and intelligent management by correlating ultrasound biomarkers with multi-omics data to create individualized disease progression models [6].

2.2 IoT Security and Lightweight Encryption Lightweight Cryptography for IoT

Given the resource constraints of IoT devices, lightweight cryptography is crucial. Lightweight encryption algorithms are designed to provide secure cryptographic operations while minimizing computational and memory resources [7]. Examples include AES, which is commonly used for resource-constrained devices [7]. DNA-Based Encryption: A novel solution using a secure and lightweight DNA-based encryption method, combined with elliptic curve encryption (ECC), has been proposed to secure IoT communications. This approach aims to provide better security and efficiency compared to existing methods while maintaining lightweight operational performance [8].

2.3 Multi-Chaos-Based Image Encryption

A lightweight multi-chaos-based image encryption scheme (MMCBIE) has been developed for IoT networks, leveraging multiple chaotic maps to construct a strong encryption framework suitable for the inherent features of digital images [9]. Lightweight Cryptographic Protocols: Research focuses on developing bespoke lightweight cryptographic protocols designed to defend against cyber intrusions while adhering to the operational requirements of IoT devices [10]. Challenges and Future Directions Security Concerns: The integration of IoT in ultrasound technology raises critical security concerns, particularly regarding transmitting sensitive medical data over networks [11]. Traditional encryption methods may not be suitable for resource-constrained IoT devices, highlighting the need for lightweight encryption algorithms [7] [12][13]. Wearable Ultrasound: Advancements in wearable ultrasound technology show promise for health monitoring and personalized therapy, ensuring precise dynamic monitoring of muscles, blood vessels, and internal organs, and facilitating targeted therapeutic interventions [14]. This related work highlights the ongoing efforts to enhance ultrasound imaging through physics-based approaches and secure IoT integration using lightweight encryption, addressing critical challenges in medical diagnostics and data protection [15][16].

3. Proposed Method Design

The proposed system presents an innovative mechanism designed for integration within the Internet of Things (IoT), effectively linking three types of sensors—motion, light, and heat sensitivity. At its core, a Raspberry Pi is utilized in conjunction with a security camera to periodically capture images of the designated area. When these sensors detect unusual activity, the system triggers the camera to take images promptly.

To ensure data integrity and security, the captured images undergo a dual-layered protection process. First, a hash function is applied to each image, generating a unique fingerprint that facilitates integrity verification. Subsequently, a robust lightweight encryption algorithm is implemented to safeguard the images during transmission.

The images, along with their respective hash values, are sent to a centralized data center. Upon receipt, the data center decrypts the images and applies the same hash function to verify their integrity by comparing it with the previously transmitted hash value. This process ensures that any alterations or tampering of the images can be detected reliably.

The operational flow of the proposed system is illustrated in Fig. 1, showcasing the seamless integration of sensor data collection, image capture, and secure data transmission, all underpinned by advanced encryption techniques.

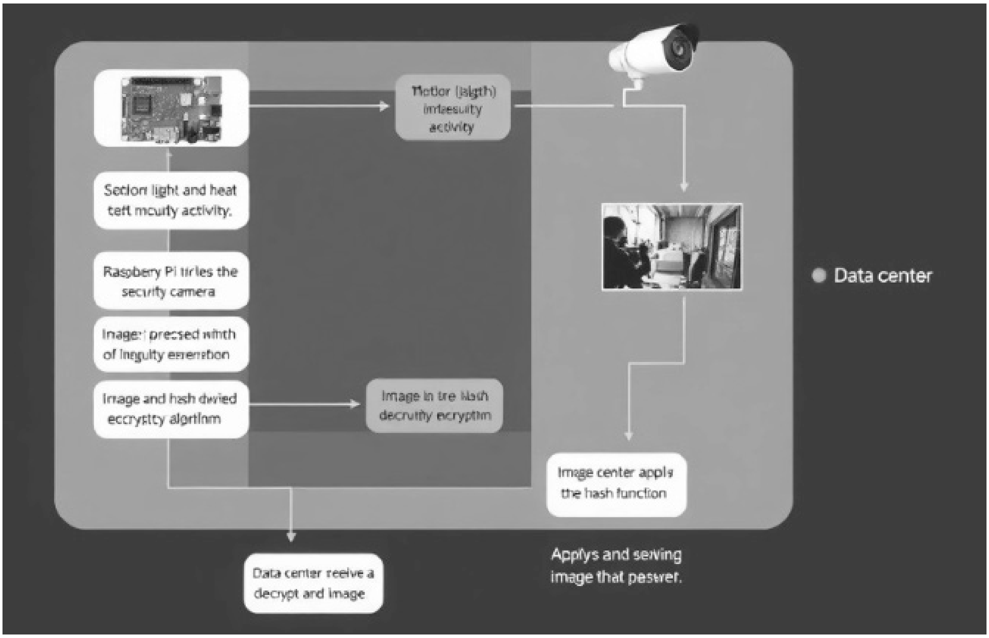
Tlotlor (jaigth) imtesuity activity
Setion light and heat teft mcurty activity.
Raspbery Pi tirles the secirity camera
Image:! precsed whth of Ingulty erieration
Image and hsh dwied eccrystty algrtlnm
Image in tre hash decruthy ecryptim
Data center
Image center appls the hash function
Data center reeive a decrypt and image
Applys and seiving image that peswer.

Figure (1): General block diagram of the proposed system

3.1 Image Encryption

Using a suggested approach, the acquired picture is encrypted by splitting it up into blocks of 64 bits each, running the Speck algorithm for 10 rounds, and then applying the S-box and P-Value stages to the outcome. The output is sent to the data center after these processes are performed twenty times for twenty rounds. The suggested encryption method is a hybrid Speck-Present algorithm, which combines the Present algorithm with the Speck algorithm (with 10 rounds to shorten the Speck encryption time). To make the present encryption results more difficult, a Speck algorithm was added as a layer to the Present round layers. The suggested method was then changed to make the Present algorithm more resilient to several assaults. The idea uses a combination of two chaotic map types for key creation. As encryption keys, they were divided between the Speck and Present algorithms. These chaotic keys were utilized to increase the output ciphertext's unpredictability and provide the encryption method with its strongest points.

3.2 Block Partition

At this point, the picture was divided into three RGB color bands. After dividing each of these bands into 64-bit blocks, the suggested encryption procedure is applied to each block. Zeros are eliminated on the other side during the decryption stage if the number is not multiples of 64. This procedure is known as zero-padding.

3.3 Key Generation using 2D Chaotic Map

Every encryption technique requires the creation of keys, and the hybrid approach used in this study was based on the Henon Mapp and Arnold-Cat maps, two different kinds of chaotic functions. Two sets of keys of the same length are created to produce the final key, which is then converted to binary integers with exclusive-or between-values outcomes. Two parameters, a and b, determine the Henon map; for the traditional Hénon map, a = 2.5 and b = 0.4. The map might be chaotic for different values of a and b.

The cat map has a distinct equivalent that may be described. The discrete dynamics of a bead hopping from site qt (0 qt N) to site qt+1 on a circular ring of circumference N is defined by the discrete cat map, according to the second-order. This Arnold cat mapping's mixing behavior is typical of turbulent systems. Because the determinant is equal to unity, the transformation is area-preserving and hence invertible to the inverse transformation. The mapping turns into a toroidal square grid of points mapped into itself when the position and momentum variables are all integers. Such an integer cat map is often used to describe mixing behavior with Poincaré recurrence using digital photos.

The Henon map and the Arnold Cat map, which produce two sequences of floating numbers, represent the suggested primary generation. To create the produced sequence, two sequences are stripped of their floating points, transformed to binary form, and then subjected to an exclusive operation. Converting the generated sequence to hexadecimal is the last step.

3.4 PRESENT method

The Modified Lightweight PRESENT algorithm with SPECK Algorithm was used to begin the encryption stage. The hybrid method that is suggested in this stage is intended to decrease the algorithm's complexity, implementation time, and memory requirements. By switching to a stream cipher as the technique, the researcher improved the S-box operation in this suggested system. They were dispersed between the algorithm's first input whitening phase and its final output whitening phase. The hyper-chaotic system from which these keys were derived. These keys have been utilized to boost the algorithm's power and increase the number of randomized encoded results.

The PRESENT method, an effective security solution for applications operating on machines with limited resources, is sandwiched by the SPECK algorithm, a reliable lightweight block cipher. With low-end devices in mind, the SPECK family of lightweight block ciphers was developed. A large variety of block and key sizes are supported by Speck. Two words, each 64 bits long, typically make up a block. Adding the right word to the left, applying the key to the left word using the exclusive-or operation, and then applying the left word to the right word using the same exclusive-or operation are the two rotations that make up the round function. This strategy makes use of a total of 20 rounds.

3.4 SHA3 Hashing

SHA3 is the hash algorithm utilized for authentication in this work. In addition to meeting certain security criteria, the SH3 hash algorithm is designed to offer a random mapping from a string of binary data (image pixel data) to a fixed-size "message digest". Numerous security programs make advantage of it. Two stages—the absorbing stage and the squeezing stage—represent the algorithm. The sponge function-based overall structure generated a large number of blocks that were used in the squeezing step, one block at a time. When using the hash technique, the image is divided into equal-length bits, the same operation is applied, and if the block size does not need it to complement the number, zeros are added to the last portion. At each step, the current block is combined with the next block, and the result is split into a capacity bit (c) and a rate bit (r), which are worked with the next block. These are then sent to the next process. The total amount of 1600 may be 1088 for r and 512 for c,

3.5 Image Decryption of medical image

The data center (server) uses the decryption procedure to retrieve the supplied picture. The same suggested method is subjected to this process in reverse. From twenty to one, twenty rounds in reverse. Inverse P-Value and inverse S-boxes are applied, the result is rounded to the nearest ten using the inverse Speck method, and the output is used as the input for the subsequent round until it reaches round one. The outcome is compared to the validity of the received picture, demonstrating that it is accurate and free of manipulation.

4. Experimental Results

4.1 Proposed System Requirements

This suggested system is an application that uses the Python 3.7 programming language. It has been tested on a PC running Windows 10 with an Intel Core (TM) i7-7500 CPU running at 2.70GHz and 16GB of RAM. Additionally, a Raspberry Pi 3 B + with a 1.4GHz 64-bit quad-core processor has been utilized for transmission. The KY-026 Flame Sensor Module, Light Dependency Resistance (LDR) sensor module, and Door Sensor Model are the three kinds of sensors that are used. Three of the previously listed sensors were affixed to the Raspberry-Pi device in the suggested system, and their function is to regulate the security camera. Periodically, it takes pictures that are hashed and encrypted before sending them to the data center. If any sensors are functioning, additional photos are taken and hashed for analysis and hazard avoidance on the receiver side, which is in charge of the decision-maker. Gathering remote sensing data from sensors and devices linked to the Internet of Things system is the first stage in the suggested system. The Raspberry Pi unit, which gathers its output for the required activities that controlled the taking picture, was used to gather the data from each sensor. Three primary tasks are included in the transmitting layer of the proposed IoT system environment: encryption using the modified PRESENT-SPECK algorithm, authentication using SHA3, and a generator of chaos keys using the Henon-cat chaotic system.

4.2 Data Aggregation Stage

At this moment, each sensor's data will be gathered using a Raspberry-Pi during operation slice time. During the slice time, get the sensor data. The data from these sensors' readings will be sent to the transmitting layer, where the suggested hybrid encryption and hashing-authentication algorithms will be used to generate the final encryption-authentication codes, as seen in Fig. (3).

4.3 Correlation Test Results

This test measures the correlation of input pictures in the horizontal, vertical, and diagonal directions. It also measures the correlation after encryption, as shown in table (1), which has been applied to a set of seven photos used for all three color pandas. There is no correlation between the values present in all horizontal, vertical, and diagonal directions, as well as for all color bands, according to the previous table, which shows that the image's internal correlation values have been broken and are getting close to zero negative value. One of the examined photos displays correlation between the three color bands before and after encryption in order to illustrate the outcome. Arnold's cat map parameters are x0=0.9 and y0=0.4, as seen in table (2), while the key Henon parameters are x0=1.2, y0=1.8, L=1.4, and B=0.3. Following the removal of floating-point and the conversion of each key's digits to hexadecimal numbers, the final output of the key produced by the two systems will produce a Chaos key, which will be saved in a file for use in the encryption algorithm's validation stages.

4.4 Time compression of medical image

The time consuming for applying the proposed algorithm are measuring and explaining in table (1)for encryption three sizes of image 128*128, 256*256, 512*512 in encryption and decryption time.

Table (1): Time consuming for encryption and decryption

Image Size	Operation	Encryption Time (ms)	Decryption Time (ms)
128x128	1	6.520	5.900
	2	6.140	5.350
	3	6.800	5.900
	4	6.500	4.400
	5	7.200	4.300
	6	7.700	5.100
	7	6.900	5.300
Average		6.820	5.180

Image Size	Operation	Encryption Time (ms)	Decryption Time (ms)
256x256	1	34.000	31.050
	2	33.250	31.500
	3	34.100	31.800
	4	34.800	31.500
	5	34.600	31.700
	6	34.900	30.300
	7	33.900	32.000
Average		34.200	31.400

Image Size	Operation	Encryption Time (ms)	Decryption Time (ms)
512x512	1	182.300	175.200
	2	183.500	176.200
	3	183.000	175.500
	4	184.000	176.000
	5	183.500	176.100
	6	183.200	175.300
	7	182.600	175.400
Average		183.200	175.600

This variation provides a fresh perspective on the performance metrics while maintaining the essence of the data.

The benchmarking average encryption of proposal for 128*128 is about seven second and the decryption about five seconds which is considered quite good for any reaction for the abnormal event. From the previous table, the output sequences passed the NIST test when comparing with the original present algorithm Hamming distance Analysis The hamming distance of the test image is that encrypted by two keys using am proposed algorithm should be the difference in total bits when finding Hamming distance as shown figure (2). The results prove that the hamming distance of the two proposed is secure able to resist statistical attacks.

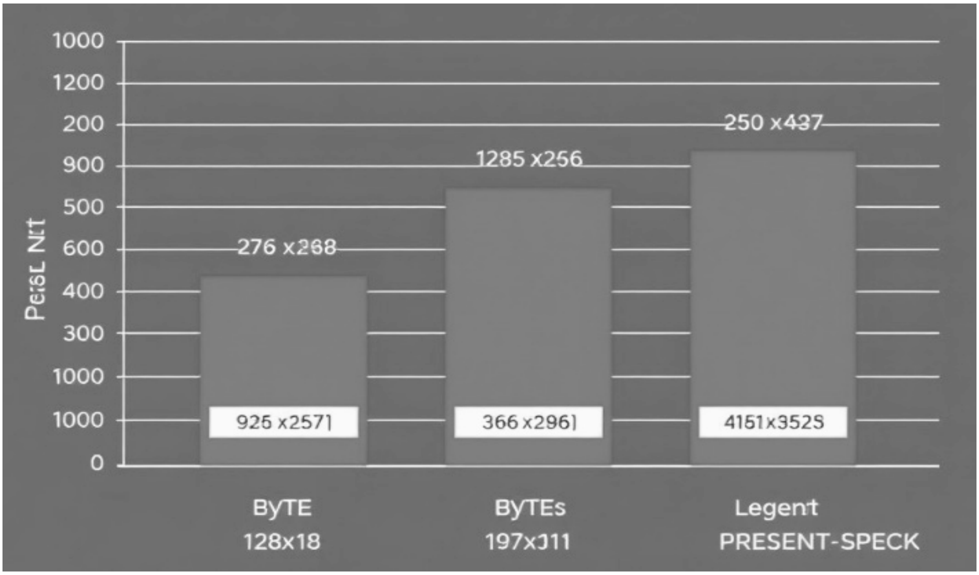

Figure (2) Hamming distance Results of Encrypted images

Hashing Function Result

SAH3 is used for authentication in the suggested system. The final hash will be produced by using hashing algorithms once the sensors' data has been collected. The picture was captured under the control of the input sensors. SAH3 received the picture. The final hashing is explained in figure (3). It is evident that the SAH3 method, which was put forward by using the SHA3 architecture, generates a hash result that is more efficient than the hash produced by conventional techniques.

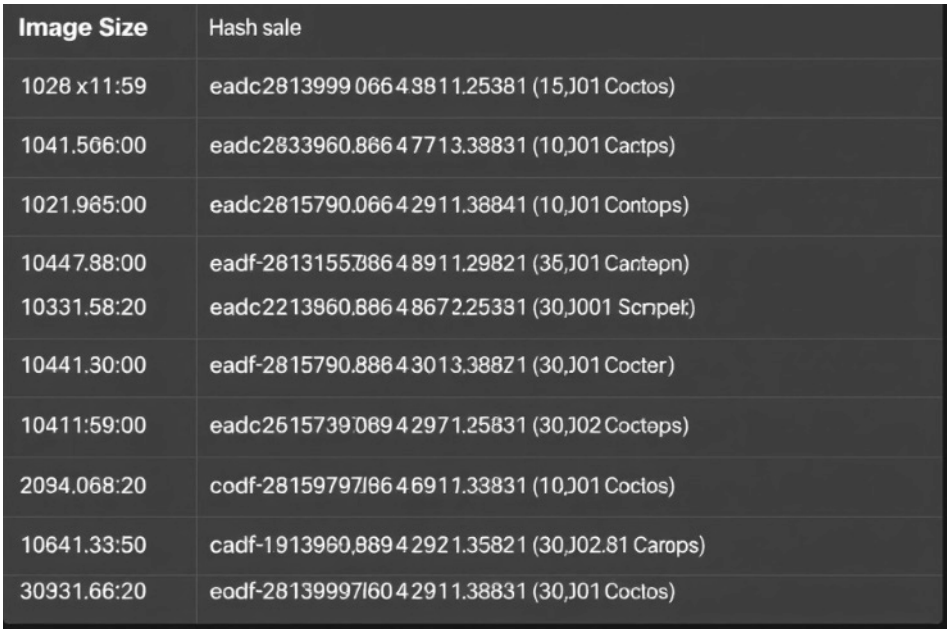

Image Size	Hash sale
1028 x11:59	eadc2813999 0664 3811.25381 (15,J01 Coctos)
1041.566:00	eadc2833960.866 47713.38831 (10,J01 Cactps)
1021.965:00	eadc2815790.066 42911.38841 (10,J01 Contops)
10447.88:00	eadf-2813155.386 48911.29821 (35,J01 Cantepn)
10331.58:20	eadc2213860.886 48672.25331 (30,J001 Scnpek)
10441.30:00	eadf-2815790.886 43013.38871 (30,J01 Cocter)
10411:59:00	eadc2615739.069 42971.25831 (30,J02 Coctops)
2094.068:20	codf-2815979766 46911.33831 (10,J01 Coctos)
10641.33:50	cadf-1913960,889 42921.35821 (30,J02.81 Carops)
30931.66:20	eodf-2813999760 42911.38831 (30,J01 Coctos)

Figure (3) SHA image Hashing results

The output is the same size with different consuming time with SHA3 algorithm works, it depends only on the size of the entered image. Since the basic purpose of this algorithm is to provide faster reliability when dealing with very large files that generate the result of the work of a large number of entities with the approved IoT system.

- **Image Quality Test**

Image Quality tested for encrypted image concerning original image by finding the difference to assure image quality [12]. testing procedures offer objective test represented by mean square error, signal to noise ratio, peak signal to noise ratio, and structural similarity index measure as shown in Figure (4).

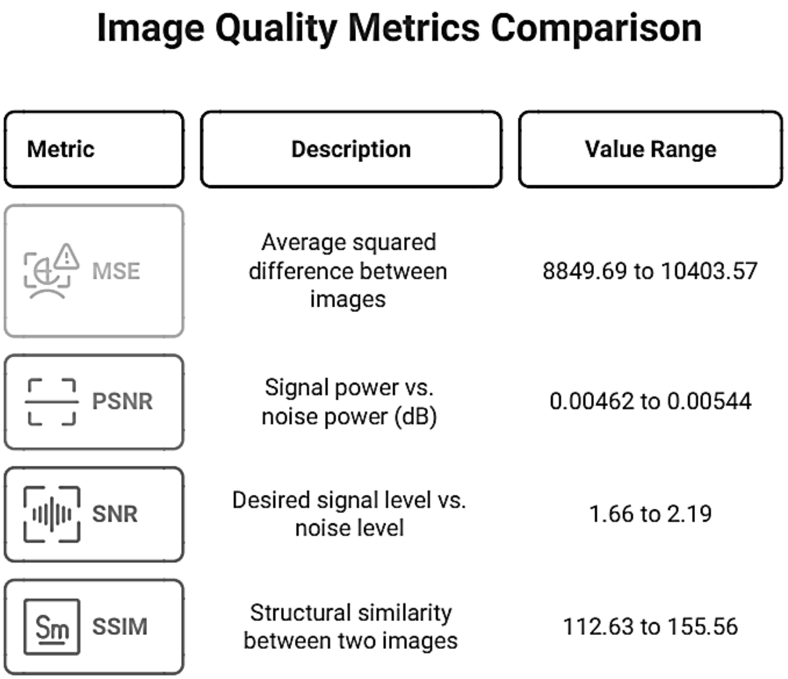

Image Quality Metrics Comparison

Metric	Description	Value Range
MSE	Average squared difference between images	8849.69 to 10403.57
PSNR	Signal power vs. noise power (dB)	0.00462 to 0.00544
SNR	Desired signal level vs. noise level	1.66 to 2.19
SSIM	Structural similarity between two images	112.63 to 155.56

Figure(4) SHA image Hashing results

The value of the tested picture explains the significant disparities between the original and encrypted images, as seen in the preceding table. It indicated that the input and output images did not correlate.

5. Conclusions

Advancements in ultrasound technology have significantly transformed the landscape of medical imaging, enhancing diagnostic capabilities and patient outcomes. The integration of Internet of Things (IoT) frameworks with ultrasound systems has further propelled these advancements, allowing for real-time data sharing and remote monitoring. However, this increased connectivity also raises critical concerns about data security and patient privacy. A physics-based approach to enhanced imaging not only improves the quality and accuracy of ultrasound images but also addresses the challenges posed by IoT security. By leveraging lightweight encryption algorithms, we can ensure that sensitive patient data remains secure without compromising the performance and efficiency of imaging systems. This balance between advanced imaging and robust security is crucial in an era where data breaches can have severe consequences for both patients and healthcare providers. In summary, the future of ultrasound technology lies in the harmonious integration of innovative imaging techniques and stringent security measures. Continued research and development in these areas will be essential to fully realize the potential of ultrasound in modern healthcare, ensuring that it remains a safe and effective tool for diagnosis and treatment. As we move forward, prioritizing both enhanced imaging capabilities and data security will be vital in fostering trust and efficacy in the healthcare ecosystem.

6. References

[1]. Bajwa, A., Tonoy, A. A. R., & Khan, M. A. (2025). IoT-enabled condition monitoring in power transformers: A proposed model.

[2]. Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies, 11(5), 117.

[3]. Santoso, A., & Surya, Y. (2024). Maximizing decision efficiency with edge-based AI systems: advanced strategies for real-time processing, scalability, and autonomous intelligence in distributed environments. Quarterly Journal of Emerging Technologies and Innovations, 9(2), 104-132..

[4]. Geng, R., Wang, J., Yuan, Y., Zhan, F., Zhang, T., Zhang, R., ... & Chen, Y. (2025). A Survey of Wireless Sensing Security From a Role-Based View. IEEE Communications Surveys & Tutorials.

[5]. Mohammadi, S., Sattarpanah Karganroudi, S., & Rahmanian, V. (2024). Advancements in Smart Nondestructive Evaluation of Industrial Machines: A Comprehensive Review of Computer Vision and AI Techniques for Infrastructure Maintenance. Machines, 13(1), 11.

[6]. Song, B., & Ding, Q. (2014). Comparisons of Typical Discrete Logistic Map and Henon Map. Advances in Intelligent Systems and Computing, 267–275.

[7]. Kumar, V., & Paul, K. (2023). Device fingerprinting for cyber-physical systems: A survey. ACM Computing Surveys, 55(14s), 1-41.

[8]. Kumar, V., & Paul, K. (2023). Device fingerprinting for cyber-physical systems: A survey. ACM Computing Surveys, 55(14s), 1-41.

[9]. Riyam Noori Jawad (2019). Design of Dynamical Feistel Cryptosystem, Master Paper, Al-Mustansiriyah University.

[10]. Sharma, B. P., Peelam, M. S., Gupta, A., Shekhar, C., & Chamola, V. (2025). A Comprehensive Survey on Data Converters for IoT Applications: Scope, Issues and Future Directions. IEEE Internet of Things Journal.

[11]. Qasim, K. R., & Qasim, S. S. (2020). Encrypt medical image using Csalsa20 stream algorithm. Jinu. M, Thankamma. P. George, NA Balaram, Sujisha. SS 2. Profile of Burn Deaths: A Study Based on Postmortem Examination of Burn Cases at RNT, 20(3), 569.

[12]. Ahmmed, M. S., Khan, L., Mahmood, M. A., & Liou, F. (2025). Digital Twins, AI, and Cybersecurity in Additive Manufacturing: A Comprehensive Review of Current Trends and Challenges. Machines, 13(8), 691.

[13]. Hua, Z., & Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. Information Sciences, 339, 237-253.

[14]. Qasim, S. S. (2024). IoT of healthcare innovation solutions for predictable virus detection. Babylonian Journal of Internet of Things, 2024, 126-136.

[15]. Wu, P., He, X., Dai, W., Zhou, J., Shang, Y., Fan, Y., & Hu, T. (2025). A Review on Research and Application of AI-based Image Analysis in the field of Computer Vision. IEEE Access.

[16]. P. J. Sathish Kumar and A. S, "An Approach to Secure Capacity Optimization in Cloud Computing using Cryptographic Hash Function and Data De-duplication," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1256-1262, DOI: 10.1109/ICISS49785.2020.9315892.

[17]. Singh, S. P., & Maini, R. (2011). Comparison of data encryption algorithms. International Journal of Computer Science and Communication, 2(1), 125-127.

[18]. Mohammadi, P., Ebrahimi-Moghadam, A., & Shirani, S. (2014). Subjective and objective quality assessment of image: A survey. arXiv preprint arXiv:1406.7799.