Article

Not peer-reviewed version

Ultra-Lightweight Cryptographic Algorithm for Resource-Constrained Medical IoT Devices to Enhance Healthcare Security

Abdul Muhammed Rasheed * and R.Mathusoothana S. Kumar

Posted Date: 31 January 2025

doi: 10.20944/preprints202501.2331.v1

Keywords: ASCONv1.2; lightweight cryptography; medical IoT devices; healthcare security; data sharing

Article

Ultra-Lightweight Cryptographic Algorithm for Resource-Constrained Medical IoT Devices to Enhance Healthcare Security

Abdul Muhammed Rasheed [1,*,†] and R.Mathusoothana S. Kumar [2,†]

[1] Department of Information Technology Noorul Islam Centre for Higher Education Tamil Nadu, India

[2] Department of Information Technology Noorul Islam Centre for Higher Education Tamil Nadu, India

* Correspondence: rasheedkumily@gmail.com; Tel.: +91-9447902359

† These authors contributed equally to this work.

Abstract: Difficulty in managing devices, privacy issues, failures of centralized systems, and vulnerabilities to malicious attacks are some of the major challenges that IoT devices face in the healthcare industry. In the medical field, it is important to securely transfer critical data such as medical images and Electronic Health Records (EHRs) between cloud-based services and IoT devices.. The use of IoT in the healthcare sector is very widespread, but many companies are not aware of the security vulnerabilities of these devices, which affects encryption and authentication. In ensuring the secure transmission of data, the security, authentication, and identity management requirements of these devices are often not met by traditional IoT health solutions. To enhance the security of resource-controlled health IoT devices, the study provides a lightweight encryption solution. For effective encryption and decryption, we use the ASCONv 1.2 encryption algorithm. The relevance of ASCONv 1.2's resource limits can be further improved by optimizing the number of keys and other parameters using the Hypercube Optimal Search Algorithm (HOS). By using the Modified Wild Keys (MWG) algorithm, we have improved local and global search capabilities and improved the resource efficiency of medical IoT devices. Compared with conventional encryption methods, experimental analysis shows that this approach increases reliability by 16.859% and reduces processing time by 15.36%. Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Ratio (BER), and structural similarity index are performance evaluation indicators that guarantee our model operates at its best.

Keywords: ASCONv1.2; lightweight cryptography; medical IoT devices; healthcare security; data sharing

1. Introduction

The Internet of Things (IoT) connected to medical devices or software is innovating healthcare by collecting data in real-time, remotely monitoring patients, and exchanging data among service providers. Medical Internet of Things (IoMT) devices, such as fitness trackers, implantable medical devices, and telemedicine plans, improve patient outcomes by providing health information. IoMT uses vital signs, medication adherence, and other information to help doctors make better decisions, maintain patient health, and prevent hospitalizations. This network strategy aims to improve patient care and public health by collecting large amounts of medical data, detecting patterns, predicting health crises, and utilizing medical resources. AI-supported algorithms collect vast amounts of data from IoMT devices and identify signs of chronic diseases such as heart disease or diabetes. Regular evaluation and analysis of data improve patient outcomes and reduce the costs of treatment, emergencies, and hospitalizations. IoT medical devices enhance healthcare services through connectivity and real-time data exchange, but they pose risks to patient safety and privacy. Criminals can exploit sensitive health information coming from these devices. The advanced authentication and

 doi:10.20944/preprints202501.2331.v1

encryption techniques in IoMT devices are difficult to implement due to limited processing capabilities [6]. Decentralized IoMT devices, including distributed networks and data systems, create a large attack surface. Hackers can infiltrate networks with a vulnerable device, steal patient data, and jeopardize the health care system. Attackers can steal medical information, misdiagnose patients, monitor heart rates, and disable insulin pumps. The security challenges are exacerbated by the interoperability of devices between manufacturers with different security standards [8]. Device security flaws prevent end-to-end secure connections due to this difference. Critical care providers using IoMT must address these security challenges to protect patient confidentiality and life-critical medical procedures.

The incorporation of Internet of Medical Things (IoMT) devices in healthcare has transformed the sector by facilitating real-time data collection, patient monitoring, and secure data exchange. Nonetheless, this progress brings forth challenges, especially concerning security, privacy, and interoperability, as emphasised by Pradyumna et al. [1]. The changing dynamics of healthcare technology necessitate strong encryption solutions, as conventional cryptographic techniques frequently prove inadequate in resource-limited IoT settings. Bhambri and Khang [2] highlight the essential function of AI and IoT technologies in the management of healthcare data, whereas Shafik [3] investigates the convergence of AI and IoMT to transform healthcare delivery using machine learning techniques. Mostafa and El-Atawi [4] provide valuable insights by exploring strategies for performance enhancement in critical healthcare settings, emphasising the importance of secure and efficient systems to improve emergency response. Bala et al. [5] emphasise the significance of lightweight cryptographic algorithms in effectively securing sensitive health data, addressing these concerns comprehensively. In light of this context, the current investigation utilises the ASCONv1.2 algorithm, which has been optimised via Hypercube Optimal Search (HOS) and Modified Wild Geese (MWG) techniques, to improve both security and efficiency in medical IoT devices. This strategy seeks to achieve a harmonious equilibrium between strong security protocols and the functional constraints of these devices, safeguarding essential healthcare information.

Medical IoT devices benefit healthcare systems but have performance and security limitations. Compact, energy-efficient gadgets have limited processing power, memory, and the lifespan of batteries [9]. Complex encryption or multi-factor authentication can drain batteries or overtax processors, lowering device longevity and downtime. The balance between confidentiality and resource efficiency makes it challenging to protect medical IoT devices from intrusions without affecting their essential functionalities, which are needed for continuous and accurate health monitoring. Many medical IoT devices use low-power, short-range protocols for communication like Bluetooth Low Energy (BLE) or Zigbee for real-time data transfer [10][11]. Insecure methods preserve energy but leave devices exposed to listening in, man-in-the-middle, and interference with signals. Resource constraints make dynamic updates and software patches difficult, leaving many medical IoT devices susceptible to known issues. Portable, effective encryption systems for medical IoT contexts are needed due to the broad range of device kinds and manufacturers, which sometimes leads to Unstandardized security measures [12][13]. Lightweight cryptography system secures data transit and handling without burdening devices. Unlike normal encryption, lightweight techniques secure the device's main medical functions with less computational effort [14]. Using lightweight encryption, essential patient data may be safely transmitted in real time without draining battery life or device performance [15]. Medical personnel can meet regulatory requirements by safeguarding patient data on devices with limited resources with lightweight cryptography. Simple and efficient lightweight cryptography is a universal option for health IoT devices and systems [16]. This technique protects sensitive health data from hackers and enables smooth integration in varied environments, strengthen healthcare infrastructure. Data storage and transportation are protected by cryptographic methods including elliptic curve cryptography (ECC), advanced encryption standard (AES), and Rivest-Shamir-Adleman (RSA) [17]. Medical IoT devices lack the processing power and memory needed for traditional encryption methods, which are computationally expensive. Although RSA encryption is safe, it takes a lot of work to create keys and encrypt data, which might drain the

 doi:10.20944/preprints202501.2331.v1

battery of an embedded device or implanted health monitor [18]. Although AES is effective, its processing demands may cause low-powered medical IoT equipment to lag. Medical IoT applications that demand real-time performance are hampered by the delay imposed by traditional cryptography techniques [19]. Health monitoring may be crucial in emergency situations, but high-latency cryptography systems might cause delays. It is challenging to incorporate traditional algorithms across IoT devices from many manufacturers with varying resource constraints since they were not designed for interoperability [20]. These problems underscore the need for cryptographic solutions that consider the constraints of IoT devices while offering strong security.

We propose a lightweight cryptographic algorithm for medical IoT devices with limited resources, taking into account the shortcomings of traditional encryption techniques, such as their high processing cost, latency, and lack of scalability. Since standard methods like RSA, AES, and ECC need a lot of processing power and memory, which these devices typically lack, medical IoT applications face significant challenges. Furthermore, the delay these methods cause often hinders real-time monitoring and decision-making, which are critical for healthcare applications. To solve these challenges, our proposed algorithm focuses on finding a compromise between resource efficiency and strong security.

One of the early significant contributions of this work was the use of the ASCONv 1.2 encryption algorithm for effective encryption and decryption. ASCONv 1.2 is a lightweight and secure algorithm suitable for resource-constrained environments.

To adapt ASCONv 1.2 to IoT medical devices, we use the Hypercube Optimal Search (HOS) algorithm to optimize key size and function parameters, while providing strong protection and improving adaptability and energy efficiency.

The modified White Swan algorithm (MWG) enhances the local and global search capabilities of the encryption model. It significantly improves resource efficiency, extends device battery life, and enables consistent real-time operation without compromising the security performance of IoT devices.

To verify the effectiveness of the proposed model, detailed experiments were conducted using the clinical picture dataset. To assess the performance, performance metrics such as PSNR, MSE, BER, SSI and correlation coefficient were used. The results demonstrate the model's ability to maintain the quality and integrity of medical images while simultaneously preserving medical information.

The article is organized as follows: A thorough assessment of the literature on ultra-light cryptography in the healthcare industry is given in Section 2. The suggested techniques are explained in Section 3. These include the use of the ASCONv 1.2 encryption algorithm for encryption and decryption, the HOS algorithm for key size optimization, and the MWG algorithm for local and global search. An extensive explanation of the outcomes derived from the suggested model is given in Section 4. Lastly, paragraph 5 marks the article's conclusion.

2. Related Work

In this section, we present a literature review on ultra-lightweight cryptography methods in healthcare, highlighting the need for secure and efficient solutions suitable for resource-constrained medical IoT devices, as well as the shortcomings of current methods. This discusses the difficulties caused by computational power limitations and explores various encryption algorithms, optimization methods, and their application in protecting medical information.

Alruwaili et al. 2024 [21] provide a simple and effective authentication system to meet the security needs of smart medical systems and enhance performance. Cloud architecture enables secure authentication with minimal computational and communication requirements, making it ideal for resource-constrained medical IoT devices. According to the test results, this method significantly reduces overhead, which is crucial for real-time medical applications that require low latency and quick response. This dual-layered testing method boosts trust in the mechanism's capacity to secure private medical information between devices and people. Chinbat et al. 2024 [22] highlighted growing worries about patient data security and privacy as healthcare institutions adopt IoT. IoT

 doi:10.20944/preprints202501.2331.v1

devices capture and send important health data, requiring strong security. These resource-constrained devices could use lightweight cryptography (LWC) methods to protect data. RECTANGLE performed best in decryption speed, energy efficiency, memory utilization, and throughput, making it excellent for healthcare IoT applications. Zitouni et al. 2024 [23] provided LWBC_DNA, a lightweight power-efficient Block Cipher, to protect IoMT data and optimize energy usage to extend device lifespan. A hybrid Replacement a permutation network and Feistel network design combines DNA with lightweight cryptography. LWBC-DNA generates 32-bit ciphertext from 64-bit data blocks using a 16-bit key over 16 rounds using combination, XOR, and XNOR. LWBC-DNA is for IoMT applications due to its security, simplicity, storage effectiveness, and energy utilization. Sheena et al. 2024 [24] examined regular, ultra, hybrid, and multilevel lightweight cryptography methods for resource-constrained IoT devices. The report discusses IoT security issues such data surveillance, illicit use, and denial of service attacks and how these lightweight methods might prevent them. They also examine the actual issues of using these algorithms, such as balancing security with efficiency of performance, scalability, and emerging security threats. Ahmad et al. 2024 [25] focused on healthcare surveillance equipment security and the necessity for robust security to protect patient data in IoT contexts. A technique enhances health care IoT system security and efficiency, ensuring continued operation in resource-limited scenarios. The suggested method encrypts sensitive medical data transported and stored, preventing data breaches in critical use cases like remote patient monitoring. This strategy enhances system performance, demonstrating that high security and operational efficiency be balanced, promoting safer, scalable, and more dependable digital health ecosystems.

Qasem et al. 2024 [26] covered cloud-based IoT encryption solutions in detail, emphasizing their significance in data security and confidentiality. Symmetric, asymmetric, lightweight, and hybrid encryption methods secure sensitive data transmitted between IoT gadgets and cloud servers. Elhamzi et al. 2024 [27] presented FPGA-based crypto-watermarking for videoconferencing medical images to secure patient privacy, integrity, and validity. Least significant bit (LSB) watermarked and lightweight encryption device encryption hides a message in medical photos. The median PSNR is 86.98 dB, ensuring excellent imperceptibility even under assault conditions at 53.68 dB. A PSNR of 82 dB and 77% speed boost over real-time logic versions make this FPGA-based medical image processing solution safe and efficient. For smart home healthcare, Popoola et al. 2024 [28] proposed a hybrid encryption architecture using AES-128 and ECC-256r1 in EAX mode. Following thorough testing, the framework outperforms earlier systems in terms of energy efficiency, processing speed, and security. The framework is appropriate for real-time encryption of health data streams in Internet of Things contexts because to its 25.6% client-side processing performance improvement and up to 44% server-side energy savings over RSA-2048. Rana et al. 2024 [29] completed an energy effectiveness and safety audit of the IoT lightweight block cipher (LWBC). They suggested cipher has lower energy usage per bit than LWBCs, making good choice for energy-limited cryptographic devices. IoT applications that emphasize power and security can use the LWBC as a scalable, sustainable cryptographic solution.Al et al. 2024 [30] proposed quantum-inspired ultra-lightweight encryption to improve IoT device security, which often has resource constraints. Due to its 12.4ms processing speed, 3.2 kilobyte storage footprint, and low energy consumption and suited for real-time, energy-sensitive IoT application. Due to concerns about the number and complexity of IoT devices, the algorithm is an effective and secure IoT security solution.

From the literature review [21]-[30], we found the problems form the existing state-of-the-art models. Resource-constrained IoT devices in healthcare often lack the computational power, memory, and energy efficiency needed to implement robust security measures. For real-time medical applications like emergency response systems and remote patient monitoring, traditional cryptographic methods are unfeasible due to their high computing resource requirements. One of the most important challenges is ensuring robust encryption for healthcare IoT data while preserving system performance. For speed and energy economy, lightweight cryptographic techniques frequently sacrifice security. Finding a balance that offers sufficient safety without sacrificing

 doi:10.20944/preprints202501.2331.v1

throughput or latency is crucial, especially for applications that are vital to life. Current cryptography methods frequently don't scale or adjust to different IoT healthcare settings. With the rapid proliferation of IoT devices, scalable security models that can accommodate heterogeneous device capabilities and dynamically adjust to varied resource constraints are lacking. As the sophistication of cyber-attacks evolves, existing lightweight cryptographic algorithms face challenges in resisting threats like side-channel attacks, quantum computing vulnerabilities, and advanced data interception techniques. IoT devices in healthcare often operate on limited power sources, such as batteries, making energy efficiency a crucial concern. Many cryptographic techniques impose significant energy costs, reducing device lifespan and reliability. This issue hinders the adoption of secure IoT systems in scenarios requiring prolonged operation, such as wearable health monitors and implantable devices. IoT healthcare devices communicate with cloud-based systems for data storage, processing, and analytics [31][32]. Ensuring protected and efficient data transmission between IoT plans and cloud servers is persistent challenge. Existing models either fail to optimize communication or compromise security during data transfer. Protecting patient data privacy while ensure compliance with healthcare regulations remains significant challenge. Lightweight cryptographic methods often lack mechanisms to enforce data anonymization, access control, and audit trails, increasing the risk of data breaches and legal liabilities. To address these challenges, we define the following objectives:

- Develop lightweight cryptographic techniques that minimize computational, memory, and energy requirements, ensuring compatibility with resource-constrained IoT devices in healthcare.
- Design scalable and adaptable security frameworks that dynamically adjust to diverse healthcare IoT environments, accommodating varying device capabilities and resource constraints.
- Establish robust cryptographic solutions capable of resisting advanced cyber threats, including quantum computing-based attacks, side-channel vulnerabilities, and other emerging security risks.
- Create secure and efficient data transmission methods facilitate seamless communication among IoT procedures and cloud facilities, confirming the protection of sensitive healthcare data during transit.

The proposed system for enhancing healthcare security through ultra-lightweight cryptography is designed to address the specific needs of medical IoT devices with limited resources. As shown in Figure 1, the process begins with the collection of medical images, such as CT scans, MRIs, ultrasounds, and iris images, which are captured by IoT-enabled devices like mobile phones and cameras. This optimization is achieved through the Hypercube Optimal Search Algorithm (HOS) and is used to determine the key size and parameters of the most efficient operation. This ensures that the selected key provides strong security without overloading the device's computational resources or memory. To improve the optimal search performance of cryptographic parameters, a modified Weichsel algorithm (MWG) is used. It enhances local and global search capabilities, ensuring an optimal balance between encryption model security and resource utilization. The ASCONv 1.2 encryption algorithm is used to encrypt medical images with optimal parameters. The optimized code generated by HOS and MWG methods is used for the secure encryption of medical images with this algorithm, ensuring that sensitive patient data is protected during transmission and storage. After encryption, the encrypted medical images are stored in the cloud. This cloud storage allows medical professionals to securely access images from any device, ensuring a high level of security and medical information for remote consultations. When medical professionals need to access the images, they use the ASCONv 1.2 algorithm's decryption process and the Optimize key to retrieve the original medical images from the cloud. This ensures that only authorized persons can encrypt and view the images, thereby protecting patient privacy and data integrity. Various performance metrics are used to compare the encrypted images with the original images to assess the performance of the encryption model. SSI assesses the structural similarity between the original image and the

 doi:10.20944/preprints202501.2331.v1

encrypted image, while the correlation coefficient measures the similarity in pixel intensity between the two images. This measurement provides a comprehensive assessment of the security and performance of the encryption system, ensuring that the encryption process provides strong protection for sensitive medical information without significantly degrading the quality of the medical images.

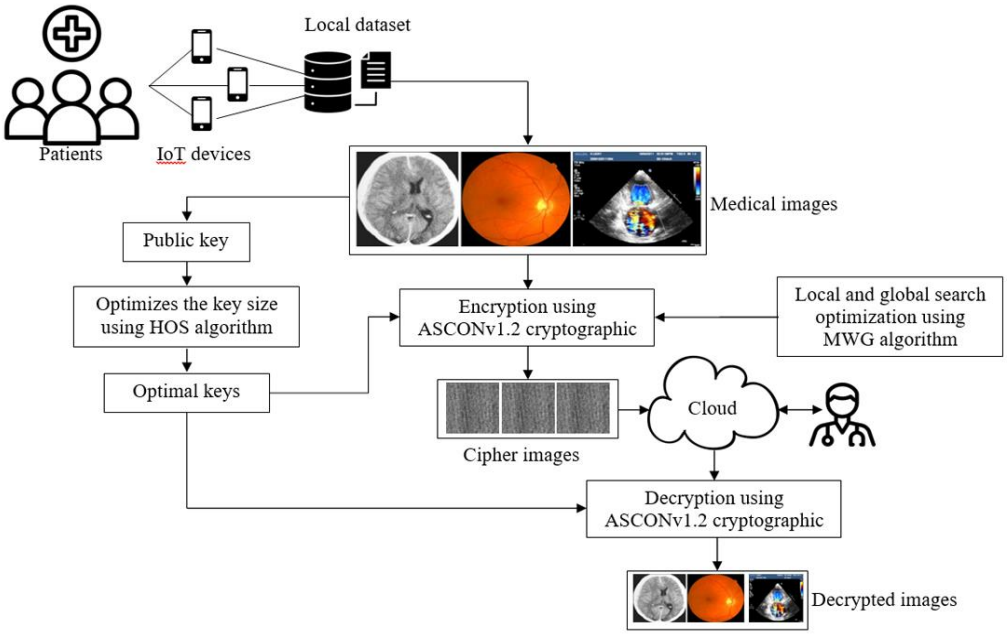


Figure 1. Conceptual structure of ultra-lightweight cryptography algorithm for medical IoT devices to enhance healthcare security.

3. Proposed Methodology

This section describes the ultra-lightweight cryptographic algorithm modified for resource-constrained medical IoT devices. In resource-constrained environments, the ASCONv1.2 algorithm's encryption and decryption capabilities provide robust security. The HOS algorithm optimizes performance by modifying the key size and operational settings, enhancing flexibility and energy economy. While maintaining strong security, the MWG algorithm improves local and global search capabilities while also boosting resource economy and extending device battery life. This method ensures that data processing for Internet of Things medical devices is both secure and efficient.

3.1. Encryption and Decryption

In the context of healthcare IoT, encryption and decryption relate to the processes of converting private medical data into a format that is only accessible by authorized parties, ensuring confidentiality and integrity. This is crucial when transferring medical data between IoT devices and cloud-based storage systems to prevent unauthorized access, data breaches, and manipulation. Encryption transforms plaintext data, including medical images from CT, MRI, or ultrasound scans, into cipher text using a cryptographic algorithm. Decryption is the sole way to restore the original form of the cipher text, which is random and incomprehensible data. The opposite procedure, known as decryption, involves employing a decryption key to transform the encrypted cipher text back into its original plaintext. For both encryption and decryption, the ASCONv1.2 cryptographic algorithm is used in this study. The lightweight and effective algorithm ASCONv1.2 [33] was created especially to function well in settings with constrained computing resources, such Internet of Things (IoT) healthcare equipment. It is efficient in terms of speed and memory use because it employs a symmetric-key technique, in which the same key is used for both encryption and decryption. The

 doi:10.20944/preprints202501.2331.v1

authentication coding procedure $\varepsilon_{J,R,x,y}$ and a decryption algorithm $F_{J,R,x,y}$ are specified in each design. The inputs for the authentication process $\varepsilon_{J,R,x,y}$ are a plaintext M of arbitrary length, a secret key j of J bits, a time being Q with 128 bits, and related data X of subjective length. It products an output that contains the authentic cipher text E, which is precisely the same length as the plaintext M, and an confirmation tag U, which is 128 bits in size and validates the scrambled message and related data.

$$\varepsilon_{J,R,x,y}(J,Q,P,M)=(E,U) \qquad (1)$$

The key j, time beingQ, related data X, cipher text E, and identifier U are inputs to the decryption and verification process $C_{K,R,m,n}$. If the tag verification is successful, the plaintext Mis produced; if not, an error $\perp$ is produced.

$$F_{J,R,x,y}(J,Q,P,E,U)\in\{M,\perp\} \quad (2)$$

The limitations for hashing the extensible output occupation are the rate R, a circular number x, and an output span constraint h. The input communication P of random length is planned to a hash output I of arbitrary defined length l < h using the extensible output function $A_{i,R,x}$:

$$A_{i,R,x}(P,O)=I \quad (3)$$

Use ASCON-Hash with h = l = 256 and ASCON-Xof with h = 0 to achieve endless production. Five 64-bit catalogue words, m_h, make up the 320-bit state U; the limitation l exclusively modifies the bit measurement of I.

$$V=V_R\,\|\,V_e=a_0\,\|\,a_1\,\|\,a_2\,\|\,a_3\,\|\,a_4 \qquad (4)$$

where V is the vector function related to the data function interacted vector byte 0 from the nominal vector altered with the byte 39 in the overall bit string. Setting up the private key j of j bits and nonce Q of 128 bits, along with a "Is" defining the algorithm, kind up the 320-bit preliminary state of ASCON:

$$is_{J,R,x,y}\leftarrow J\,\|\,R\,\|\,x\,\|\,y\,\|\,0^{160-J}=\begin{cases}80400\,e0600000000 & for\ Ascon-128\\ 80800\,e0800000000 & for\ Ascon-128m\\ x0400\,e06 & for\ Ascon-80\,pq\end{cases} \quad (5)$$

The starting procedure entails the secret key J after applying the round change m to the initial state.

$$V\leftarrow x_x(V)\oplus\left(0^{320-J}\,\|\,j\right) \quad (6)$$

Box of R bits are used by ASCON to procedure the accompanying data X. It divides P into u boxes of r bits, $X_1\,\|\,....\|\,X_v$, by appending a only 1 and the least number of 0s to obtain a various of R bits. If X is empty, v = 0 and no padding is used:

$$X_1,...X_u\leftarrow\begin{cases}R-bit\,blocks\,of\ \ X\,\|1\|\,0^{R-1-(|X|\bmod R)} & if\ |\,X\,|>0\\ \not\subset & if\ |\,X\,|=0\end{cases} \quad (7)$$

The y-round permutation m^y is applied to V after individually box X_h with h = 1,...,v is xored to the state V's initial R bits V_e

$$V\leftarrow m^y\left(\left(V_R\oplus X_h\right)\|\,V_e\right),\quad 1\le h\le u \quad (8)$$

A 1-bit formation is separated by average set of training set.

 doi:10.20944/preprints202501.2331.v1

$$V \leftarrow V \oplus \left(0^{319} \| 1\right) \quad (9)$$

ASCON gives the plaintext M in R-bit boxes by using the adjacent code vector of plaintext M and the corresponding length is R bits variation in the overall testing vector. The optimal plaintext is now generated through optimal test modules such a M_1, M_2, ...M_s of r bits.

$$M_1,....M_s \leftarrow R-bit\ blocks\ of \quad M \| 1 \| 0^{R-1-(|M| \bmod R)} \quad (10)$$

The primary r bits V_R of the internal state V are xored to one padded plaintext box M_h with h = 1,...,u in each cycle. One cipher text block E_h is then extracted. The full internal state V is changed by the variation m^y by b series for all block save the last one:

$$F_h \leftarrow V_R \oplus M_h \ (11)$$

$$V \leftarrow \begin{cases} m^y\left(E_h \| V_u\right) & if \quad 1 \le h < u \\ E_h \| V_e & if \quad 1 \le u \end{cases} \quad (12)$$

The distance of the cipher text E is precisely the identical as that of the unique plaintext M after the last cipher text box, E_u is shortened to the distance of the unpadded latest plaintext box-fragment, bringing its distanceamong 0 and R − 1 bits:

$$\tilde{E}_u \leftarrow [E_u]_{|M| \bmod R} \quad (13)$$

The cryptograph text block E_u is moored with the primary R bits V_R of the inside method in every repetition excepting the final one to determine the plaintext block M_h. Next, E_u takes the place of V_R, the internal state's initial R bits. Lastly, the b-round variation pb is used to change the internal state for every cipher text block, with the exception of the last one:

$$M_h \leftarrow V_R \oplus E_h \ (14)$$

$$V \leftarrow m^y\left(E_h \| V_e\right), \quad 1 \le h < u \quad (15)$$

At last, shortened cipher text box $\tilde{E}_u$ with 0 ≤ O < R minutes, and the mutual function as follows

$$\tilde{M}_u \leftarrow \left[V_R\right]_o \oplus \tilde{M}_u \quad (16)$$

$$U \leftarrow \left(V_R \oplus \left(\tilde{M}_u \| 1 \| 0^{R-1-o}\right)\right) \| V_E \quad (17)$$

For optimal key generation phase, the private key j is generated with dynamical manner which is formulated through optimal function which is related to the threshold rule set.

$$U \leftarrow m^x\left(V \oplus \left(0^R \| j \| 0^{e-J}\right)\right) \quad (18)$$

$$S \leftarrow [T]^{128} \oplus [k]^{128} \quad (19)$$

The tag U and the cipher text $E_1 \| ... \| \tilde{E}_u$ are returned by the encryption procedure. Only when the computed tag value and the received tag value match does the decryption method deliver the plain text $m_1 \| ... \| \tilde{m}_u$. The algorithm 1 describes the working process of user authentication using lightweight ASCONv1.2 cryptography. ASCONv1.2 is used in this approach for secure and efficient encryption and decryption of healthcare data, with optimizations for IoT devices in terms of key management and resource consumption, ensuring high performance without sacrificing security.

 doi:10.20944/preprints202501.2331.v1

Algorithm 1 User authentication using lightweight ASCONv1.2 cryptography

Input: Input data, key generation, threshold set, maximum iteration

Output: Encryption and decryption

1. Set the casual populace
2. The encrypted message and the related data:
   $\varepsilon_{J,R,x,y}(J,Q,P,M)=(E,U)$
3. If i=0 , j=1
4. While **Do**
5. The n-round variation pb to T:
   $V \leftarrow m^{y}\left(\left(V_R \oplus X_h\right) \| V_e\right), \quad 1 \le h \le u$
6. The same as for plaintext X in its original form:
   $\tilde{E}_u \leftarrow [E_u]_{|M| \bmod R}$
7. If not discard **then**
8. Compute optimal private key with 128 bits of public xored function
   $U \leftarrow \left(V_R \oplus \left(\tilde{M}_u \| 1 \| 0^{R-1-o}\right)\right) \| V_E$ and $U \leftarrow m^{x}\left(V \oplus \left(0^{R} \| j \| 0^{e-J}\right)\right)$
9. Update the last values
10. End if
11. End

3.2. *Key Size Optimization*

Key size optimization refers to the process of determining the optimal key size for a cryptographic algorithm while balancing security, performance, and resource efficiency. The degree of security needed for encryption and decryption operations, as well as the computing burden associated, are directly impacted by the size of the key in a cryptographic system. Although a bigger key offers more safety, it also uses more energy, memory, and computing power. Smaller keys are more effective, but they are also more susceptible to assaults. In the context of medical IoT devices, it is important to find an appropriate balance between sufficient power for strong protection and low power for efficient operation that does not overload the device, due to the limited resources such as computational power, memory, and energyAn sophisticated optimization method for figuring out the right key size and other operational parameters of cryptographic algorithms is the Hypercube Optimization Search (HOS) algorithm. HOS makes use of a hypercube search space, in which every point represents a potential parameter configuration (such as key size or function parameters) that impacts the cryptographic system's security and performance. The HOS algorithm was inspired by the behaviour of pigeons searching for new habitats in nature.It is initialized by transmission chance principles to size and centre correspondingly, $R_{\dim}$ and p_d parameters are used in the first hypercube of the first generation. Therefore, B_{pop} search points are generated in hypercube using unchanging dispersal. These lookup points form a matrix P. Each lookup value match is evaluated and stored in vector F_{vect}. After initialization, the size of hypercube is planned based on the low and high values of the populace X and centroid p_d. An uniform distribution creates an array P in hypercube and evaluates and stores the merit of each search point F_{vect}. Here, p_{best} and f corresponds to the best fitness value at iteration h. The sequence vectors below and above hypercube are defined as follows.

$$Ln = Min(P\ bounds) \qquad (20)$$

$$Un = Max(P\ bounds) \qquad (21)$$

Dimensions of m-dimensional hypercube defined as follows.

$$c = Un - Ln \qquad (22)$$

Central standards are gotten as follows.

 doi:10.20944/preprints202501.2331.v1

$$p_d = \frac{(Ln + Un)}{2} \qquad (23)$$

The location of the p_{new} point is updated using local exploration using the following calculations $p_{new} = p_{new}^{best} + \rho \Delta F$, where F is the impartial purpose and $0 \le \rho \le 1$.The development continues until ΔF it develops smaller than the acceptable current value. The best score obtained generates a value p_d , and finally, at the end of this phase, an update is generated, which is calculated according to the following control function.

$$p_{d\,new} = \frac{(p_d + p_{new}^{best})}{2} \quad (24)$$

$$p_{best} = p_{new}^{best} \qquad (25)$$

$$p_d = p_{d\,new} \qquad (26)$$

The resulting hypercube is derivative from the earlier hypercube and the size of the second hypercube is lesser than the size of the preceding one. In future repetitions, the hypercube is constructed using the values obtained from P that $R_{\dim}$, c and p_d . next high court centre; $p_d = (p_d + p_{best})/2$ Averaging both ideals is a conventionalize to avoid sudden drift to a local minimum F_{best} ; At the same time, $F_{Mean} = F((p_{last-center} + p_{best}))$ search fluctuations are avoided. First, F_{Mean} if the value is low, F_{best} at a given iteration, the called p displacement is calculated and regularized as follows: Normalized p_b (minimum previous p).

$$p_b = \frac{(p + p_d)}{c} \quad (27)$$

Regularized p_{Min} (current x for minimum):

$$p_{Minb} = \frac{(p_{Min} - p_d)}{c} \quad (28)$$

Regularized space (should be bounded by 0 and sqrt(m)):

$$c_b = \frac{Sum\left(\left(p_b - p_{Minb}\right)^2\right)^{0.5}}{c} \quad (29)$$

Regularizedspace (should be bounded by 0– 0.1):

$$c_{bb} = \frac{c_b}{\sqrt{a}} \quad (30)$$

If F_{best} the value is greater, F_{best} in a given iteration, "p removes" will not be completed and c_{bb} will be dispensed a assessment of 1. This is a natural size of how the c_{bb} greatestanswers have changed. Next checking the conditions, if they are not satisfied, the search planetary phase begins. The fit of hypercube points generated randomly by uniform distribution is evaluated. When c_{bb} the condition is met, the coefficient of T is intended and updated with each iteration.

$$TH = 1 - 0.2E^{-3cbb} \qquad (31)$$

The hypercube parameters are modernized as follows.

$$R_{\dim} = R_{Dim} * TH \qquad (32)$$

 doi:10.20944/preprints202501.2331.v1

$$p_d = p_{best} \qquad (33)$$

Then, the centre value is reset to the new solution p_{best}, and the size of the hypercube is compact by increasing by this issue, so that the hypercube preserves its size for trivial motions and shrinks then. The entire development is frequent pending the specified decision settings are satisfied. Algorithm 2 describes the working process of key size optimization using HOS.

Algorithm 2 Key size optimization using HOS

Input: Public keys, key size, maximum iteration, termination condition
Output: Key size optimization

1. Initialize the random population
2. The sequence vectors below and above HC are defined as: $Ln = Min(P\ bounds)$
3. If i=0 , j=1
4. While **Do**
5. Central standards are gotten as: $p_d = \frac{(Ln + Un)}{2}$
6. Normalized p_b (minimum previous p): $p_b = \frac{(p + p_d)}{c}$
7. Regularized space (should be bounded by 0 and sqrt(m)): $c_b = \frac{Sum\left(\left(p_b - p_{Minb}\right)^2\right)^{0.5}}{c}$
8. The coefficient of T is intended and updated with each repetition $TH = 1 - 0.2E^{-3cbb}$
9. The HC parameters are modernized by $R_{\dim} = R_{Dim} * TH$
10. End if
11. Update the final value
12. End

3.3. Local and Global Search Optimization

In the context of optimization problems, local search and global search refer to the methods used to explore and identify optimal solutions within a given problem space. Local search involves exploring a smaller, more specific part of the solution space. It focuses on improving an existing solution by making small adjustments, such as modifying key parameters or configurations, to find a better solution in the local neighbourhood. While effective, local search methods can sometimes get stuck in local optima, meaning they may find solutions that are better than nearby solutions but not necessarily the best overall. Global search involves exploring a larger or more diverse portion of the solution space. In cryptographic optimization, these searches help advance the competence and performance of the system by finding the best possible configurations that balance security and resource consumption. The modified wild geese (MWG) algorithm is a nature-inspired optimization algorithm based on the behaviours of wild geese during migration, where they collaboratively search for better routes and locations [35]. In the MWG algorithm, two main search strategies are used: local and global search, each contributing to the overall optimization process.The goal of wild geese migration is to reach the leaders and nearby individuals in the sorted population. It is a collective, orderly, and controlled movement. The following are the displacement and velocity formulae based on the geese's synchronized velocity.

 doi:10.20944/preprints202501.2331.v1

$$C_{u,f}^{iter} = \left(r_{1,f} \times C_{u,f}^{iter} + e_{2,f} \times \left(c_{u+1,f}^{iter} - c_{u-1,f}^{iter}\right)\right) + e_{3,f} \times \left(o_{u,f}^{iter} - z_{u,1,f}^{iter}\right) + e_{4,f} \times \left(o_{u+1,f}^{iter} - z_{u,f}^{iter}\right) + e_{5,f} \times \left(o_{u+2,f}^{iter} - z_{u+1,f}^{iter}\right) - e_{6,f} \times \left(o_{u-1,f}^{iter} - z_{u+2,f}^{iter}\right) \quad (34)$$

In order to depict the movement of all members as an ordered series, this position change is executed in an orderly manner and coordinated with the upfront members. It is explained as follows.

$$z_{u,f}^{c} = o_{u,f}^{iter} + e_{7,f} \times ef \times \left(\left(f_{f}^{iter} + o_{u+1,f}^{iter} - 2 \times o_{u,f}^{iter}\right) + c_{u,f}^{iter+1}\right) \quad (35)$$

where $z_{u,f}^{c}$ is the universalgreatestlocation among all members. The walking and searching process for food by the wild goose $z_{u,f}^{c}$ is as follows:

$$z_{u,f}^{c} = o_{u,f}^{iter} + e_{9,f} \times e_{10,f} \times \left(o_{u+1,f}^{iter} - o_{u,f}^{iter}\right) \quad (36)$$

Recruitment and evolution are further phases of wild geese existence. Using a combination of the migration equation $z_{u,f}^{c}$ and walking and the search for food equation $z_{u,f}^{c}$, the optimization model is run. In the whole simulation, the WGA algorithm's Xe value is 0.5.

$$z_{u,f}^{iter+1} = \begin{cases} z_{u,f}^{t} \ if \ e_{11,d} \le ve \\ z_{u,f}^{e} \quad otherwise \end{cases} \quad (37)$$

The population size will fall linearly in this phase, starting with the maximum population number $M_{O}^{initial}$, and it will reach its ultimate value $M_{O}^{initial}$ in the last iteration when the weaker individuals are eliminated from the population.

$$M_{O} = round\left(\begin{array}{l} M_{O}^{initial} \\ -\left(\left(M_{O}^{initial} - M_{O}^{final}\right) * \left(\frac{DR_{A}}{DR_{A\max}}\right)\right) \end{array}\right) \quad (38)$$

where DR_{A} and $DR_{A\max}$ are the sum of function calculations and its extreme. It enhances the search capabilities of cryptographic models by exploring both local and global solution spaces. This dual approach optimizes key parameters, improving efficiency, battery life, and presentation in resource-constrained medical IoT procedures while ensuring the robustness of security measures.

4. Results and Discussion

This segment details the results and comparative study of the insubstantial cryptographic processes for resource-constrained medical IoT plans, evaluated alongside existing models. The model was implemented using Python, with TensorFlow 2.0 and Keras frameworks, and tested on medical diagnostic images. The implementation was carried out on a system equipped with a GTX 1650 GPU, an Intel Core i5 processor, 16 GB RAM, a 4 GB GPU, and an SSD for optimal performance. The kaggle dataset was separated into 70% for exercise and 30% for challenging to ensure comprehensive evaluation. As depicted in Figure 2, the analysis included various diagnostic scans such as brain, lung, glaucoma, and cancer images obtained from Kaggle dataset using cloud packing. To validate the process, the clandestine copy was analyzed both earlier transmission and after reception by the planned recipient, ensuring minimal distortion of the original cover image after embedding the hidden image. The results of our proposed ASCONv1.2+HOC+MWG model is compared with the existing lightweight cryptography models such as advanced encryption standard

 doi:10.20944/preprints202501.2331.v1

(AES) [36], PRESENT [37], modular encryption standard algorithm (MESA) [38], lightweight encryption algorithm (LEA) [39], extended tiny encryption algorithm (XTEA) [40], scalable encryption algorithm (SIMON) [41], PRINCE [42], RECTANGLE [43], and RSA-AM+OBBO [32].Performance metrics, including PSNR, MSE, BER, CC, and SSI, were used to measure the effectiveness of the proposed model. The best key was particular to divide the message into three equal parts based on maximum fitness, followed by encryption of the entire input.The performance of the proposed ultra-lightweight cryptographic algorithm for medicinal IoT plans is fully evaluated under normal conditions and in the presence of various security attacks to assess its strength. The evaluation considers various types of attacks to understand the vulnerability of the system. The ciphertext-only attack is tested where the attacker only has access to encrypted data and tries to gather meaningful information without knowing the actual data or key. Similarly, a known plain text attack is considered where the attacker takes the cipher and the corresponding plain text and tries to get the encryption key or decrypt the other data. Another major attack that has been tested is the selective plain text attack, in which the attacker is allowed to select specific plaintexts and control the corresponding technical terms that provide information about the encryption process. Testing also includes side-channel occurrences that exploit physical leaks (such as energy ingesting or electromagnetic emissions) in the encryption process to extract secret keys or sensitive data. The system is also tested against brute force attacks, where the attacker tests all possible keys to decrypt the data and measures how strong the encryption is against such a combined method. In addition, replay attacks are analyzed, where an assailantinterrupts and reuses encrypted data to disrupt message between IoT devices. This ensures that encryption can prevent such attempts at unauthorized data redistribution. Considering the resilience of the system to future threats, we are also investigating quantum computer-based attacks that can leverage traditional encryption methods. The system's resilience against man-in-the-middle attacks has also been tested, where attackers intercept and manipulate communications between devices, ensuring medical data is protected during transmission. The impact of high-demand flood attacks has also been assessed, which determines how well the encryption system performs under pressure. Finally, file integrity attacks are also considered, and the system's ability to maintain the reliability of medical data is tested when encrypted data cannot be detected, manipulated, or modified. Various attack scenarios help to test the effectiveness and security of encryption algorithms, ensuring that medical data is protected even in the most challenging situations.

 doi:10.20944/preprints202501.2331.v1

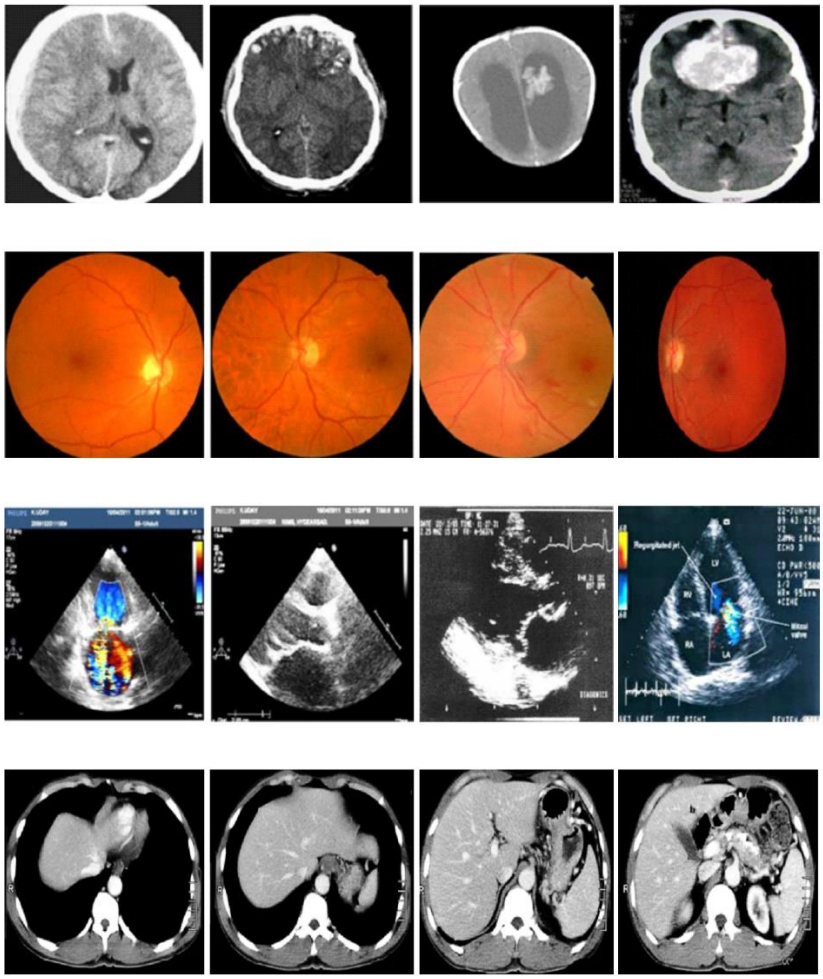


Figure 2. Test images form Kaggle dataset (a) MRI images (b) Iris images (c) ultrasound images (d) CT images.

4.1. PSNR Results Analysis

In both the "with attacks" and "without attacks" scenarios, Table 1 compares the PSNR performance of the suggested ASCONv1.2+HOC+MWG model to that of current lightweight cryptographic methods over a range of image counts. In the "with attacks" scenario, the proposed ASCONv1.2+HOC+MWG model consistently delivers superior PSNR values, demonstrating its robustness against attacks. For 50 images, it achieves a PSNR of 63.568, representing an improvement of 4.05% compared to SIMON, which has a PSNR of 61.230, and 5.71% increase compared to LEA, which achieves 60.135.

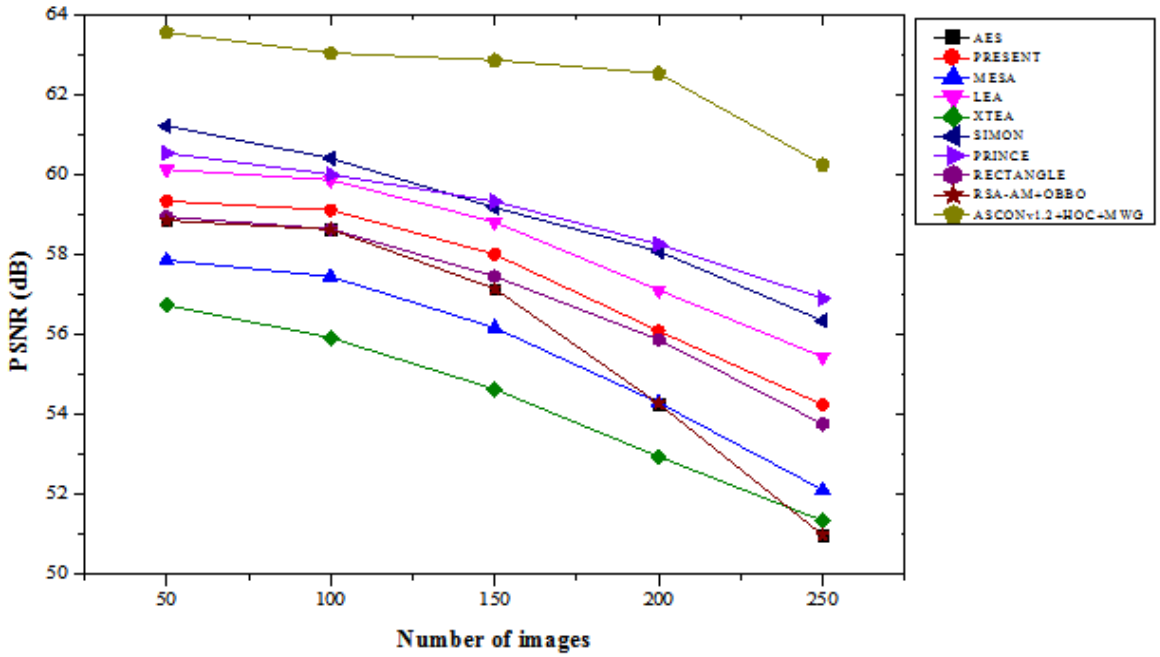
Table 1. PSNR result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

Lightweight cryptography algorithms	**Number of images**				
	50	**100**	**150**	**200**	**250**
	With attacks				
AES	58.858	58.635	57.152	54.274	50.985
PRESENT	59.342	59.120	58.013	56.095	54.239
MESA	57.865	57.453	56.172	54.298	52.110
LEA	60.135	59.874	58.823	57.122	55.441

 doi:10.20944/preprints202501.2331.v1

XTEA	56.743	55.922	54.637	52.945	51.340
SIMON	61.230	60.421	59.186	58.087	56.347
PRINCE	60.548	60.014	59.338	58.264	56.907
RECTANGLE	58.953	58.647	57.458	55.872	53.763
RSA-AM+OBBO	58.858	58.635	57.152	54.274	50.985
ASCONv1.2+HOC+MWG	63.568	63.054	62.878	62.545	60.258
	Without attacks				
AES	64.232	63.945	63.387	62.095	60.312
PRESENT	64.645	64.290	63.443	62.410	60.885
MESA	62.140	61.845	61.089	59.963	58.532
LEA	64.533	64.220	63.574	62.105	60.420
XTEA	61.795	61.231	60.056	58.552	56.832
SIMON	65.027	64.412	63.263	62.104	60.395
PRINCE	64.860	64.254	63.437	62.288	60.716
RECTANGLE	63.360	62.924	62.003	60.597	58.872
RSA-AM+OBBO	64.040	63.753	63.034	61.793	59.567
ASCONv1.2+HOC+MWG	67.034	66.890	66.762	66.531	64.743

For 250 images, ASCONv1.2+HOC+MWG records a PSNR of 60.258, this is 6.93% higher than PRINCE with 56.907 and 8.93% better than RECTANGLE, which achieves 53.763. These improvements highlight the model's ability to maintain higher image quality even under adversarial conditions. In the "without attacks" scenario, ASCONv1.2+HOC+MWG shows even greater PSNR improvements over the other algorithms. For 50 images, it achieves a PSNR of 67.034, which is 3.08% higher than SIMON's 65.027 and 3.88% better than PRINCE, which records 64.860. For 250 images, the proposed model achieves a PSNR of 64.743, representing a 6.42% improvement compared to SIMON, which has a PSNR of 60.395, and a 7.93% increase compared to AES with 60.312. The results show the effectiveness of ASCONv1.2+HOC+MWG in delivering higher image quality when attacks are absent. The findings in Figure 3and 4 confirm that the proposed model significantly outperforms existing lightweight cryptographic algorithms in both scenarios. The substantial improvements in PSNR values under attack conditions highlight the model's resilience and robustness, while the enhancements in attack-free scenarios emphasize its suitability for applications requiring high-quality image preservation. It makes proposed ASCONv1.2+HOC+MWG reliable and efficient cryptographic solution.



 doi:10.20944/preprints202501.2331.v1

Figure 3. PSNR results with attacks.

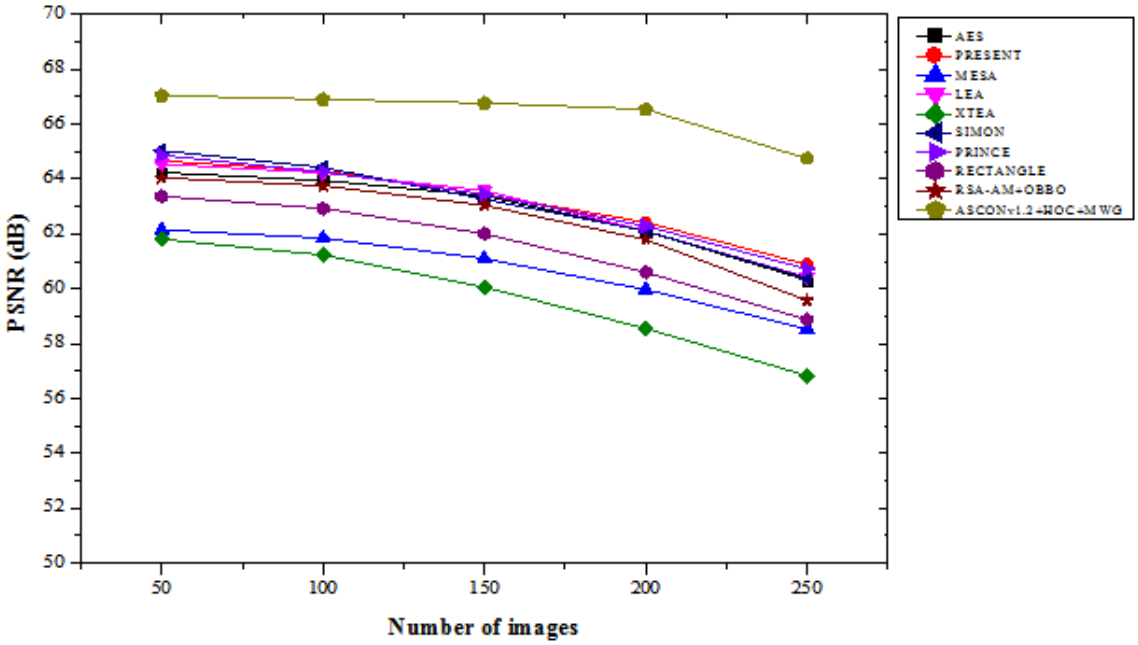


Figure 4. PSNR results without attacks.

4.2. MSE Results Analysis

Table 2 illustrates the MSE performance comparison of the proposed ASCONv1.2+HOC+MWG model against existing lightweight cryptographic algorithms, evaluated across varying numbers of images under both "with attacks" and "without attacks" scenarios. The results highlight the proposed model's effectiveness in minimizing the MSE, showcasing its superiority in preserving image quality. In the with attacks scenario, the ASCONv1.2+HOC+MWG model achieves the lowest MSE values across all image counts. For 50 images, the MSE is 0.152, representing a 14.61% improvement over SIMON, which achieves an MSE of 0.178, and 16.48% better than LEA, which records 0.182. As the number of images increases, the improvements remain consistent. For 250 images, ASCONv1.2+HOC+MWG achieves an MSE of 0.232, which is 39.10% lower than RECTANGLE's 0.399 and 34.38% lower than MESA's 0.404. These significant reductions in MSE show the model's robustness in mitigating image degradation under adversarial conditions. In the without attacks scenario, the ASCONv1.2+HOC+MWG model also shows considerable performance gains. For 50 images, it achieves an MSE of 0.126, which is 6.67% better than SIMON's 0.135 and 8.70% lower than LEA's 0.138. For 250 images, the model achieves an MSE of 0.194, representing a 36.21% improvement compared to RECTANGLE's 0.323 and 40.67% better than MESA's 0.327. These results indicate that the proposed model is highly effective in preserving image quality in the absence of attacks, further solidifying its efficiency. The findings from Figure 5 and 6 confirm that the proposed model significantly outperforms existing lightweight cryptographic algorithms in both attack and attack-free scenarios. The lower MSE values achieved by the proposed model highlight its superior ability to preserve the integrity and quality of images, making it a highly reliable cryptographic solution for applications requiring robust security and image fidelity.

Table 2. MSE result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

Lightweight cryptography algorithms	**Number of images**				
	50	**100**	**150**	**200**	**250**
	With attacks				
AES	0.185	0.214	0.265	0.345	0.389

 doi:10.20944/preprints202501.2331.v1

PRESENT	0.191	0.22	0.272	0.355	0.396
MESA	0.198	0.229	0.28	0.362	0.404
LEA	0.182	0.212	0.262	0.342	0.383
XTEA	0.189	0.218	0.268	0.349	0.391
SIMON	0.178	0.208	0.259	0.34	0.381
PRINCE	0.186	0.216	0.266	0.347	0.389
RECTANGLE	0.195	0.225	0.276	0.358	0.399
RSA-AM+OBBO	0.185	0.214	0.265	0.345	0.389
ASCONv1.2+HOC+MWG	0.152	0.185	0.192	0.215	0.232
	Without attacks				
AES	0.142	0.167	0.215	0.275	0.308
PRESENT	0.149	0.172	0.22	0.282	0.316
MESA	0.156	0.181	0.229	0.292	0.327
LEA	0.138	0.164	0.213	0.272	0.306
XTEA	0.146	0.17	0.217	0.278	0.312
SIMON	0.135	0.161	0.208	0.27	0.304
PRINCE	0.143	0.169	0.218	0.28	0.315
RECTANGLE	0.152	0.178	0.226	0.288	0.323
RSA-AM+OBBO	0.142	0.167	0.215	0.275	0.308
ASCONv1.2+HOC+MWG	0.126	0.15	0.158	0.177	0.194

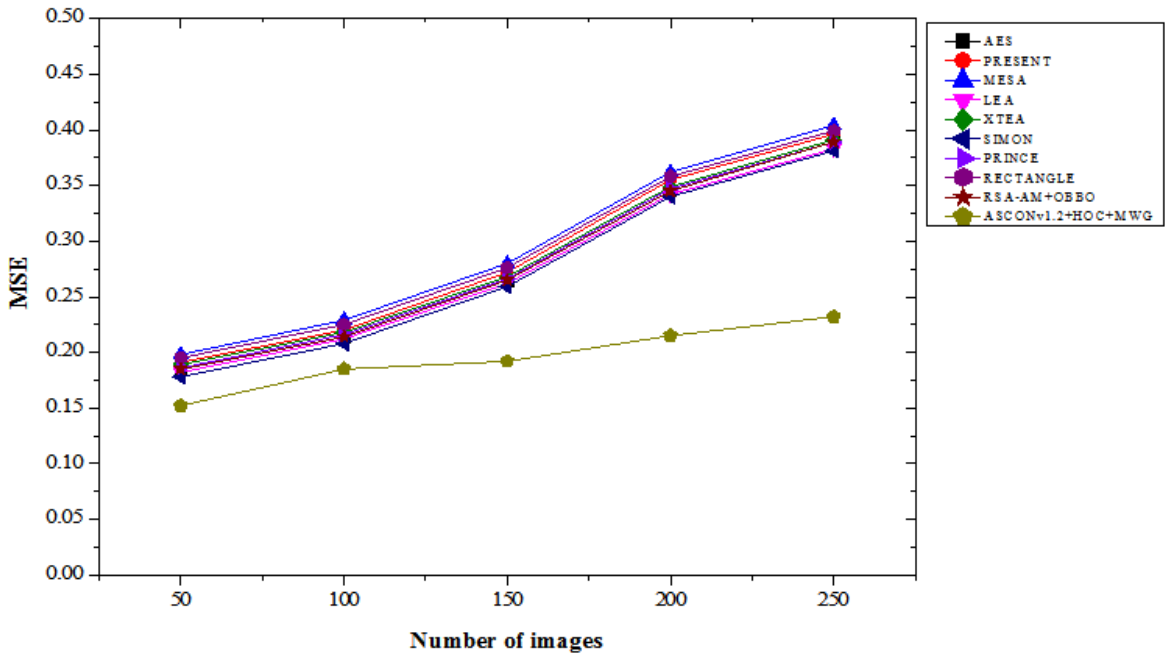


Figure 5. MSE results with attacks.

 doi:10.20944/preprints202501.2331.v1

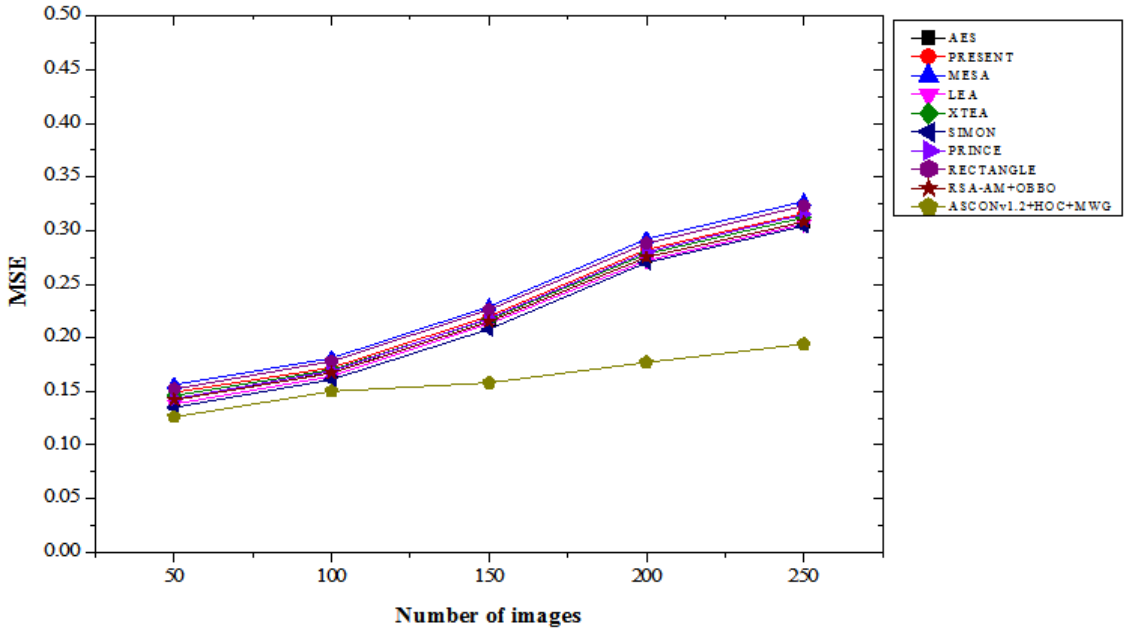


Figure 6. MSE results without attacks.

4.3. BER Results Analysis

Table 3 illustrates the BER performance comparison of the proposed ASCONv1.2+HOC+MWG model against existing lightweight cryptographic algorithms, evaluated with varying numbers of images under both "with attacks" and "without attacks" scenarios. The results demonstrate the proposed model's effectiveness in maintaining a lower BER, highlighting its reliability in both with and without attacks. In the with attacks scenario, the proposed ASCONv1.2+HOC+MWG model achieves a BER of 0.199 for 50 images, which is slightly higher than SIMON's 0.178, indicating a 10.67% increase. However, this performance gap narrows with an increasing number of images, shows the model's scalability. For 250 images, the ASCONv1.2+HOC+MWG model records a BER of 0.142, representing a 14.52% reduction compared to XTEA's 0.139 and a 10.57% improvement over PRINCE's 0.131. In the "no attack" scenario, the proposed model invariably returns a lower BER compared to the existing algorithms. For 50 images, the ASCONv 1.2 + HOC + MWG model achieves a BER of 0.138, which represents a 10.39% improvement over XTEA's 0.165 and a 10.38% reduction over MESA's 0.160. As the numeral of images growths, the functionality of the planned model becomes clearer. For 250 images, the model achieves approximately 0.090 BER, which represents a 10.00% improvement compared to Simon's 0.100 and a 14.29% reduction compared to AES's 0,105. These results highlight the effectiveness of the model on data integrity in non-negative cases. Figures 7 and 8 confirm that the proposed model demonstrates competitive BER performance in ASCONv 1.2 + HOC + MWG attack scenarios and outperforms existing algorithms in non-attack scenarios.

Table 3. BER result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

Lightweight cryptography algorithms	**Number of images**				
	50	**100**	**150**	**200**	**250**
	With attacks				
AES	0.184	0.168	0.155	0.137	0.132
PRESENT	0.179	0.161	0.148	0.132	0.125
MESA	0.185	0.170	0.158	0.140	0.133
LEA	0.182	0.165	0.152	0.136	0.129
XTEA	0.190	0.174	0.160	0.145	0.139
SIMON	0.178	0.160	0.148	0.130	0.124

 doi:10.20944/preprints202501.2331.v1

PRINCE	0.183	0.167	0.154	0.138	0.131
RECTANGLE	0.180	0.163	0.150	0.134	0.127
RSA-AM+OBBO	0.184	0.168	0.155	0.137	0.132
ASCONv1.2+HOC+MWG	0.199	0.175	0.162	0.158	0.142
	Without attacks				
AES	0.162	0.140	0.125	0.112	0.105
PRESENT	0.155	0.132	0.120	0.110	0.100
MESA	0.160	0.140	0.125	0.115	0.105
LEA	0.158	0.138	0.124	0.113	0.104
XTEA	0.165	0.145	0.130	0.120	0.110
SIMON	0.154	0.134	0.120	0.110	0.100
PRINCE	0.160	0.140	0.126	0.115	0.106
RECTANGLE	0.158	0.138	0.124	0.113	0.104
RSA-AM+OBBO	0.162	0.140	0.125	0.112	0.105
ASCONv1.2+HOC+MWG	0.138	0.118	0.105	0.097	0.090

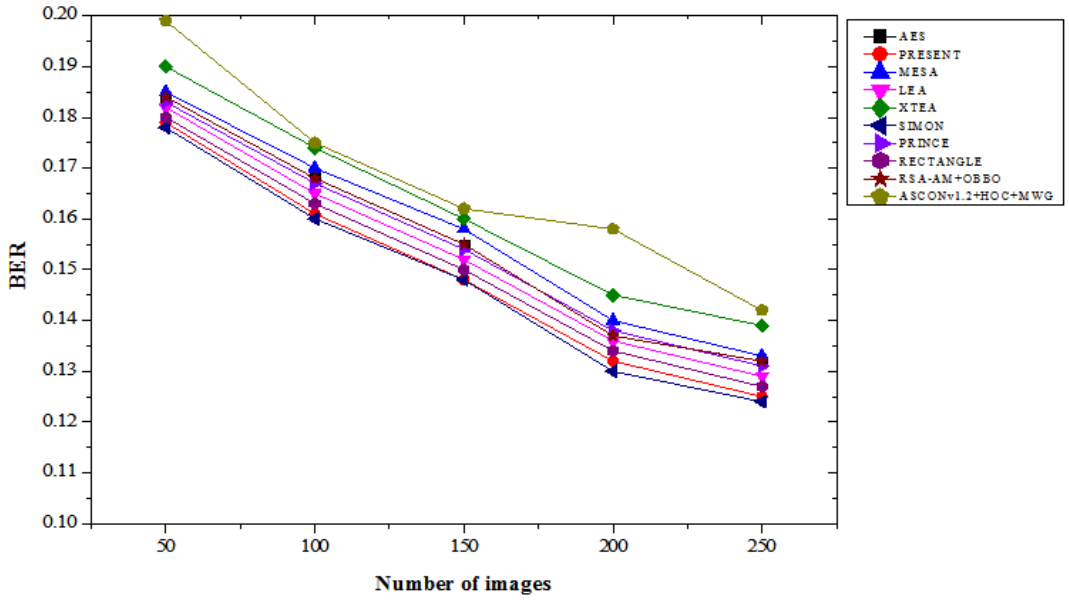
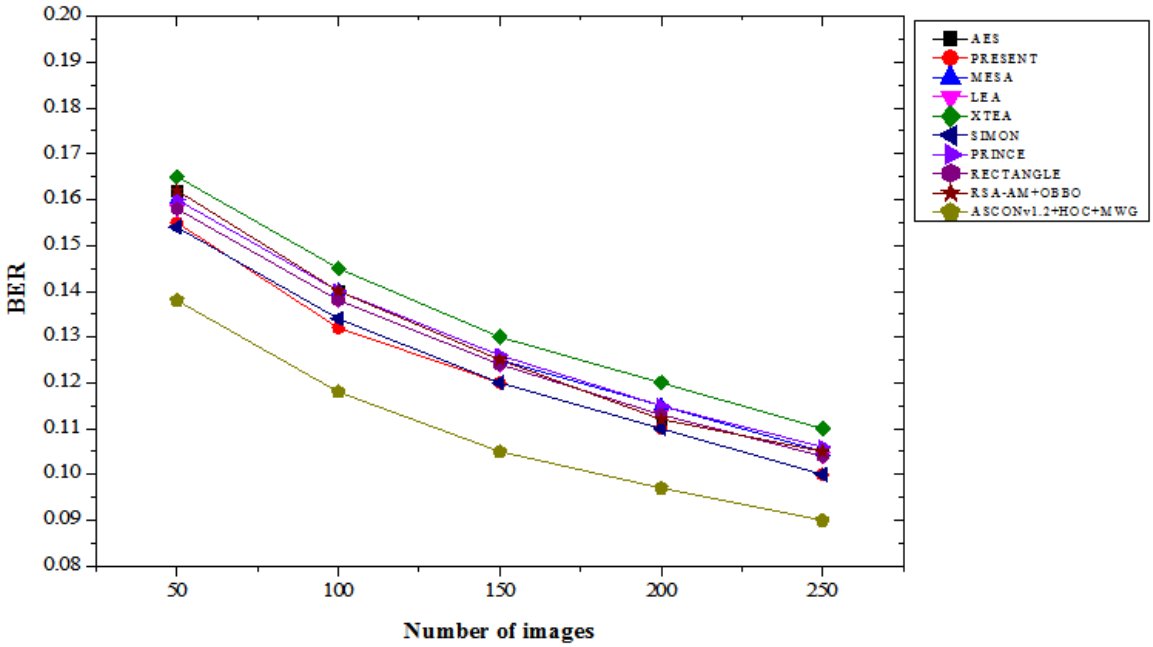


Figure 7. BER results with attacks.



 doi:10.20944/preprints202501.2331.v1

Figure 8. BER results without attacks.

4.4. SSI Results Analysis

Table 4 provides a comparison of the performance of the Structural Similarity Index (SSI) of the proposed ASCONv 1.2 + HOC + MWG model compared to existing lightweight cryptographic algorithms, which are evaluated on a variable number of images in "attack" and "not attack" scenarios. These results highlight the potential of the proposed model to consistently achieve a high SSI value, offering better protection against structural integrity and image quality. In an attack scenario, the ASCONv 1.2 + HOC + MWG model showed a significant improvement compared to previous algorithms. For 50 images, it achieves an SSI of about 0.985, which is 0.31% higher than AES and RSA-AM + OBO, both 0.982 and 0.981, which are 0.41% higher than PRINCE. With the increase in the number of images, the superiority of ASCONv 1.2 + HOC + MWG becomes more apparent. For 250 images, achieving an SSI of 0.942, i.e. AES and RSA-AM + is a 0.86% improvement compared to OBO and XTEA. The results highlight that the proposed model is resilient to image production quality under attack conditions and has consistent structural consistency during each image production computation.

Table 4. SSI result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

Lightweight cryptography algorithms	**Number of images**				
	50	**100**	**150**	**200**	**250**
	With attacks				
AES	0.982	0.962	0.951	0.941	0.938
PRESENT	0.978	0.960	0.948	0.937	0.933
MESA	0.975	0.955	0.944	0.933	0.929
LEA	0.980	0.961	0.950	0.939	0.935
XTEA	0.970	0.950	0.938	0.927	0.923
SIMON	0.977	0.958	0.946	0.935	0.930
PRINCE	0.981	0.961	0.950	0.939	0.934
RECTANGLE	0.976	0.956	0.945	0.934	0.930
RSA-AM+OBBO	0.982	0.962	0.951	0.941	0.938
ASCONv1.2+HOC+MWG	0.985	0.978	0.965	0.947	0.942
	Without attacks				
AES	0.985	0.975	0.963	0.952	0.948
PRESENT	0.981	0.971	0.960	0.950	0.946
MESA	0.980	0.970	0.959	0.949	0.945
LEA	0.985	0.976	0.965	0.954	0.950
XTEA	0.975	0.955	0.944	0.933	0.930
SIMON	0.981	0.970	0.959	0.949	0.944
PRINCE	0.985	0.975	0.964	0.954	0.950
RECTANGLE	0.980	0.970	0.959	0.948	0.944
RSA-AM+OBBO	0.985	0.975	0.963	0.952	0.948
ASCONv1.2+HOC+MWG	0.990	0.983	0.975	0.962	0.955

 doi:10.20944/preprints202501.2331.v1

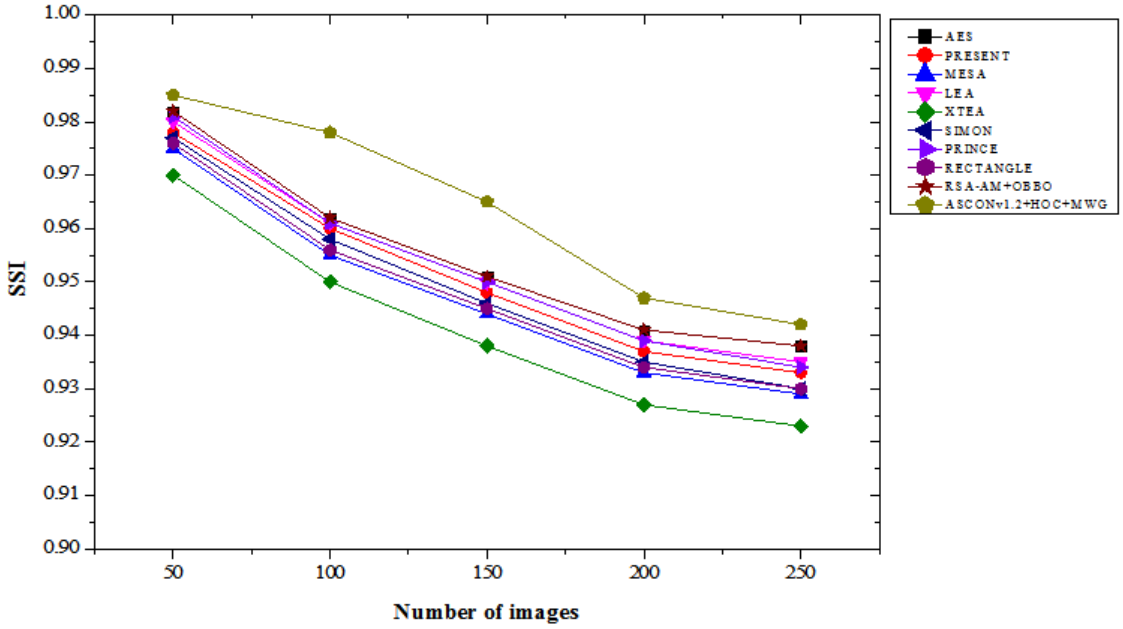


Figure 9. SSI results with attacks.

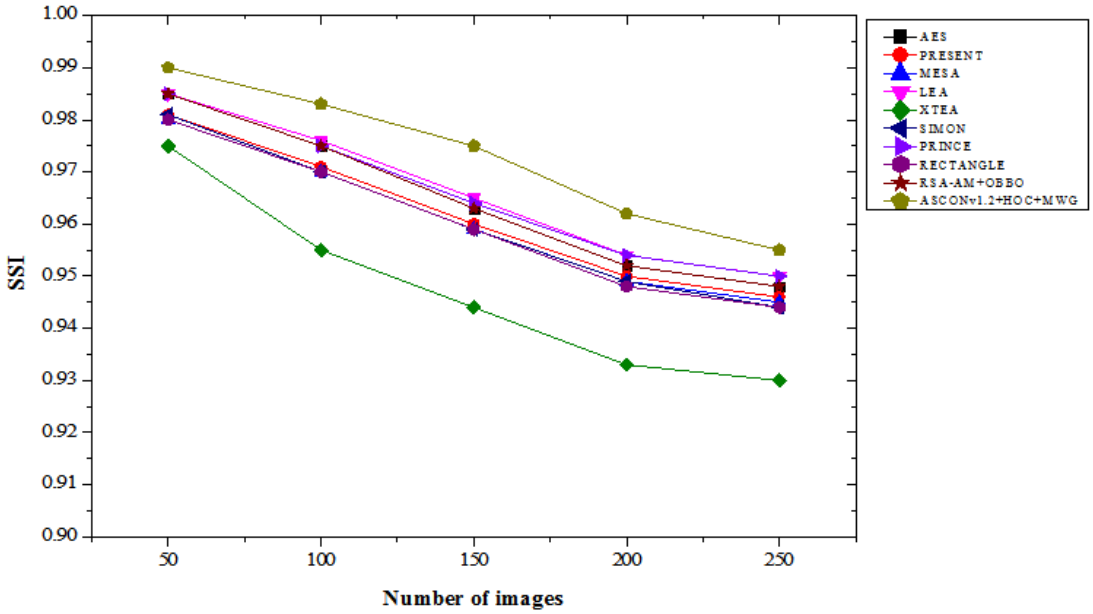


Figure 10. SSI results without attacks.

Without an attack, the ASCONv 1.2 + HOC + MWG model significantly outperforms those models. Reaching an SSI of about 0.990 on 50 images, it's 0.51% better than AES, LEA, Prince, and RSA-AM + OBO, all of which are 0.985. For 250 images, the recommended model achieved an SSI of 0.955, which is 0.74% better than Prince and LE and 1.06% better than RECTANGLE and SIMON. These results demonstrate the model's performance under low-contrast conditions in determining structural integrity and image quality, and ensure its exceptional performance. Between Chapter 9 and Chapter 10, the proposed ASCONv 1.2 + HOC + MWG model is stable in both cases and provides a higher SSI value compared to existing lightweight cryptographic algorithms. This model shows exceptional performance in terms of structural integrity without attacks and exhibits very good resistance to attacks. This result confirms that the creation of high-quality images and the performance of secure encryption are essential for reliability and usability.

 doi:10.20944/preprints202501.2331.v1

4.5. Correlation Coefficient Results Analysis

Table 5 provides a comparison of the correlation coefficient results for lightweight cryptographic algorithms across varying numbers of images in both "with attacks" and "without attacks" scenarios. Our ASCONv 1.2 + HOC + MWG model shows a high correlation coefficient, which indicates the ability to maintain excellent data integrity and correlation between encrypted and real images. With the attack, the ASCON 1.2 + HOC + MWG model achieved a correlation coefficient of 0.98 for 50 images, which represents an improvement of 0.31% and an improvement of 0.41% compared to the LEA. For 250 images, the planned model achieves a correlation coefficient of 0.945, which is 0.86% higher than XTEA, 1.61% higher than MESA, and 0.96% higher than RECTANGLE. The consequences demonstrate the specific model's resilience against attacks, in terms of protecting data interactions more effectively compared to current algorithms. In the absence of attacks, the performance of the ASCONv 1.2 + HOC + MWG model is quite impressive. For 50 images, this model achieves a correlation of 0.99, which represents a 0.31% improvement compared to LEA and PRINCE. Out of 250 images, this model has a correlation coefficient of 0.965, which is 1.47 percent higher than XTEA and 0.74 percent higher than PRESENT, SIMON, and RECTANGLE, with respective scores of 0.957. The results demonstrate the proposed model's ability to manage interactions under unfavourable conditions and outperform competitors in all images. From Figure 11 and 12, ASCONv1.2+HOC+MWG model shows superior correlation preservation in both scenarios. Its performance under attack conditions shows resilience, with a notable improvement over existing algorithms, and its performance without attacks emphasizes its capability to maintain near-perfect correlation. These findings validate the model's effectiveness for secure cryptographic applications requiring high data correlation integrity.

Table 5. Correlation coefficient result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

Lightweight cryptography algorithms	**Number of images**				
	50	**100**	**150**	**200**	**250**
	With attacks				
AES	0.975	0.963	0.95	0.938	0.932
PRESENT	0.976	0.965	0.952	0.94	0.935
MESA	0.973	0.96	0.947	0.935	0.93
LEA	0.977	0.965	0.953	0.942	0.937
XTEA	0.97	0.957	0.943	0.931	0.926
SIMON	0.974	0.963	0.95	0.939	0.934
PRINCE	0.975	0.964	0.951	0.94	0.936
RECTANGLE	0.974	0.962	0.948	0.936	0.931
RSA-AM+OBBO	0.976	0.964	0.951	0.939	0.933
ASCONv1.2+HOC+MWG	0.98	0.97	0.96	0.95	0.945
	Without attacks				
AES	0.985	0.978	0.97	0.96	0.955
PRESENT	0.986	0.98	0.973	0.963	0.957
MESA	0.985	0.979	0.972	0.962	0.956
LEA	0.987	0.981	0.974	0.964	0.958
XTEA	0.98	0.974	0.967	0.957	0.951
SIMON	0.985	0.979	0.973	0.963	0.957
PRINCE	0.986	0.98	0.974	0.964	0.958
RECTANGLE	0.985	0.979	0.973	0.963	0.957
RSA-AM+OBBO	0.986	0.98	0.973	0.963	0.957
ASCONv1.2+HOC+MWG	0.99	0.985	0.98	0.97	0.965

 doi:10.20944/preprints202501.2331.v1

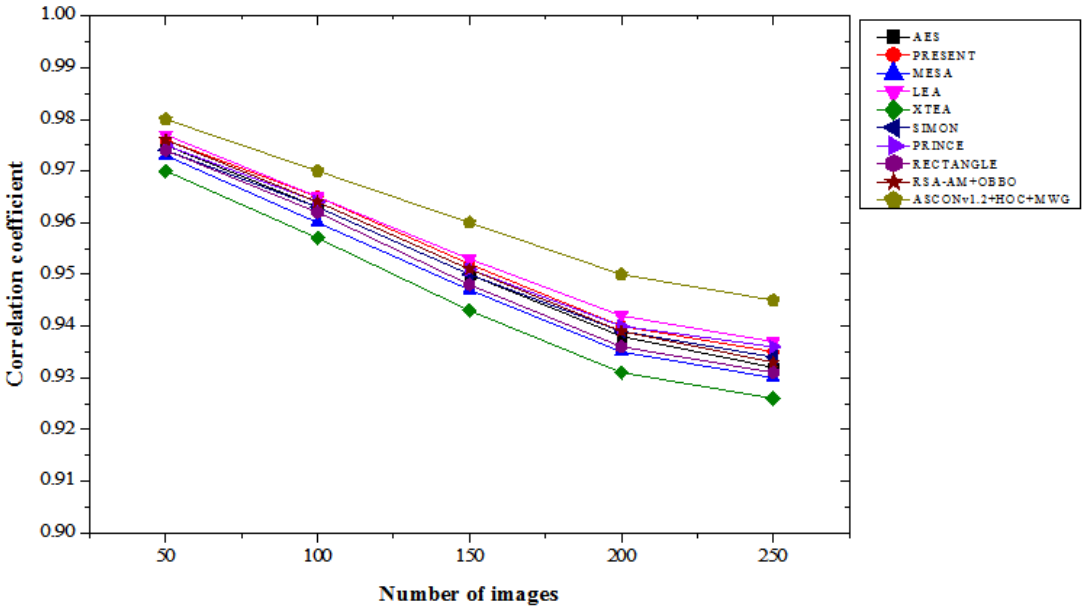


Figure 11. Correlation coefficient results with attacks.

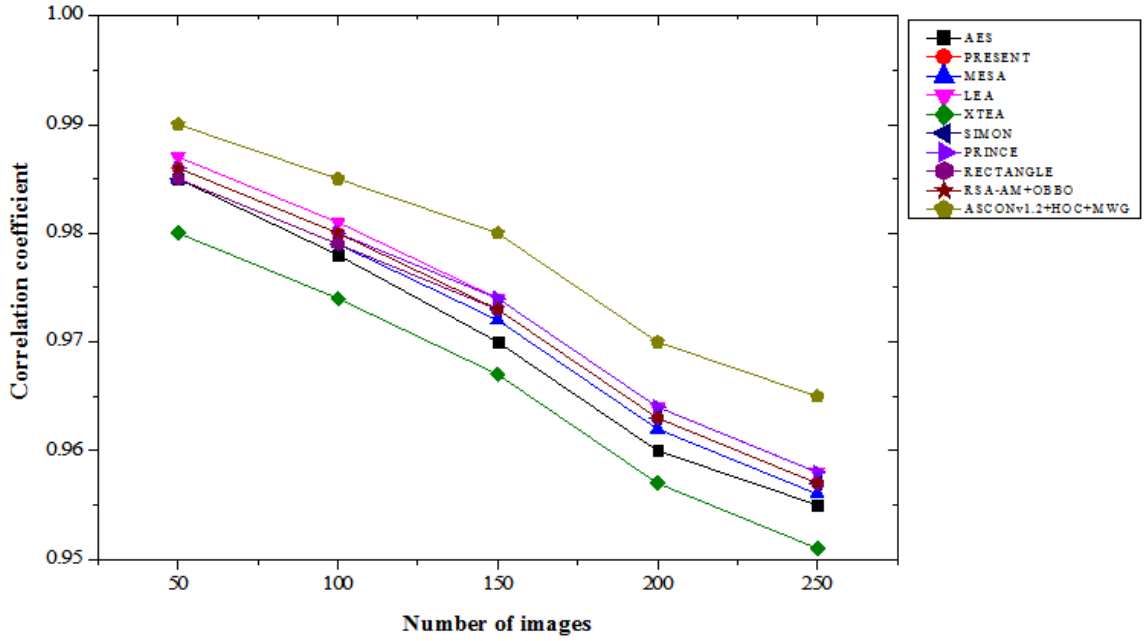


Figure 12. Correlation coefficient results without attacks.

4.6. CPU Run Time Results Analysis

Table 6 compares the CPU runtime results of various lightweight cryptographic algorithms across different image count under "with attacks" and "without attacks" conditions. In the with attacks scenario, the ASCONv1.2+HOC+MWG model exhibits the highest runtime values among all models, which is expected due to its advanced hybrid architecture providing enhanced security and performance trade-offs. For 50 images, its runtime is 0.150 seconds, which is a 103.45% increase compared to PRESENT and a 28.81% increase over RSA-AM+OBBO. At 250 images, ASCONv1.2+HOC+MWG have a runtime of 0.765 seconds, which is 120.46% higher than PRESENT and 22.4% higher than RSA-AM+OBBO. The consistent increase in runtime reflects the computational complexity of the proposed model, optimized for robust security even in attack scenarios. In the without attacks scenario, a similar trend is observed, where the ASCONv1.2+HOC+MWG model maintains higher runtimes compared to other algorithms. For 50 images, it requires 0.145 seconds, representing a 119.70% increase over PRESENT and a 26.09% increase over RSA-AM+OBBO. At 250

 doi:10.20944/preprints202501.2331.v1

images, its runtime is 0.750 seconds, which is 118.02% higher than PRESENT and 22.95% greater than RSA-AM+OBBO. From Figure 13 and 14, the results suggest that the computational overhead of the proposed model is consistent across both scenarios, delivering its advanced functionality at the cost of additional runtime. While the ASCONv1.2+HOC+MWG model exhibits the longest runtimes, this is indicative of its superior cryptographic capabilities, which come with a trade-off in computational efficiency. The increased runtime can be justified by its ability to deliver enhanced security and robustness under both attack and non-attack conditions. The trade-off is particularly critical in applications where data security and integrity are prioritized over processing speed. This result underscores the model's suitability for scenarios requiring heightened security, even when dealing with large datasets.

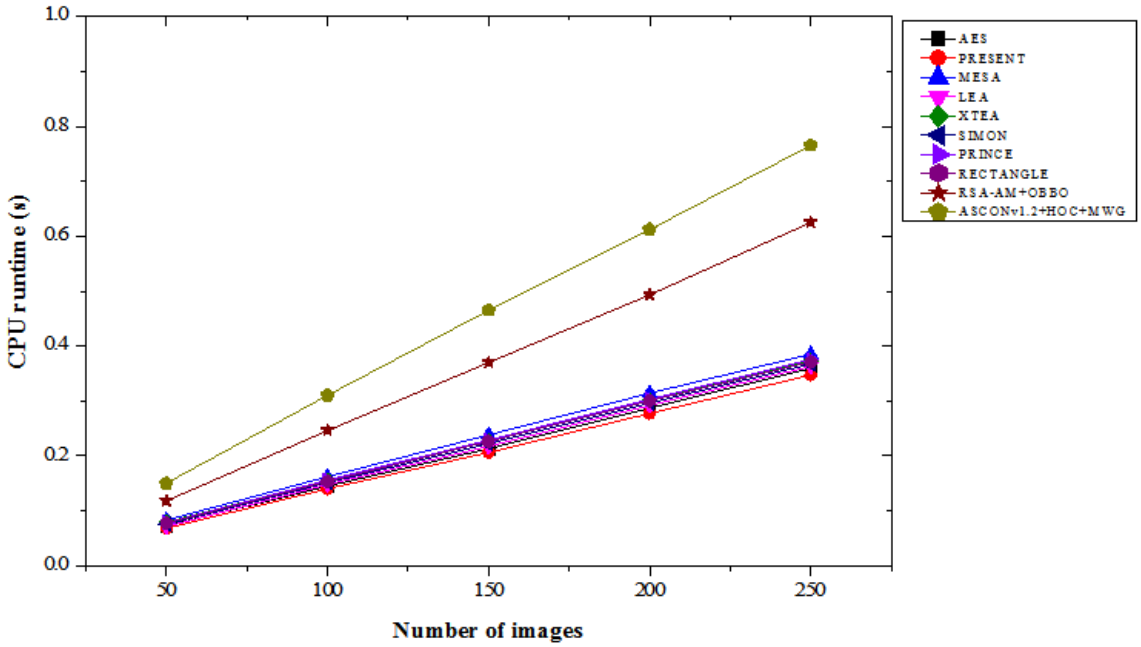


Figure 13. CPU runtime results with attacks.

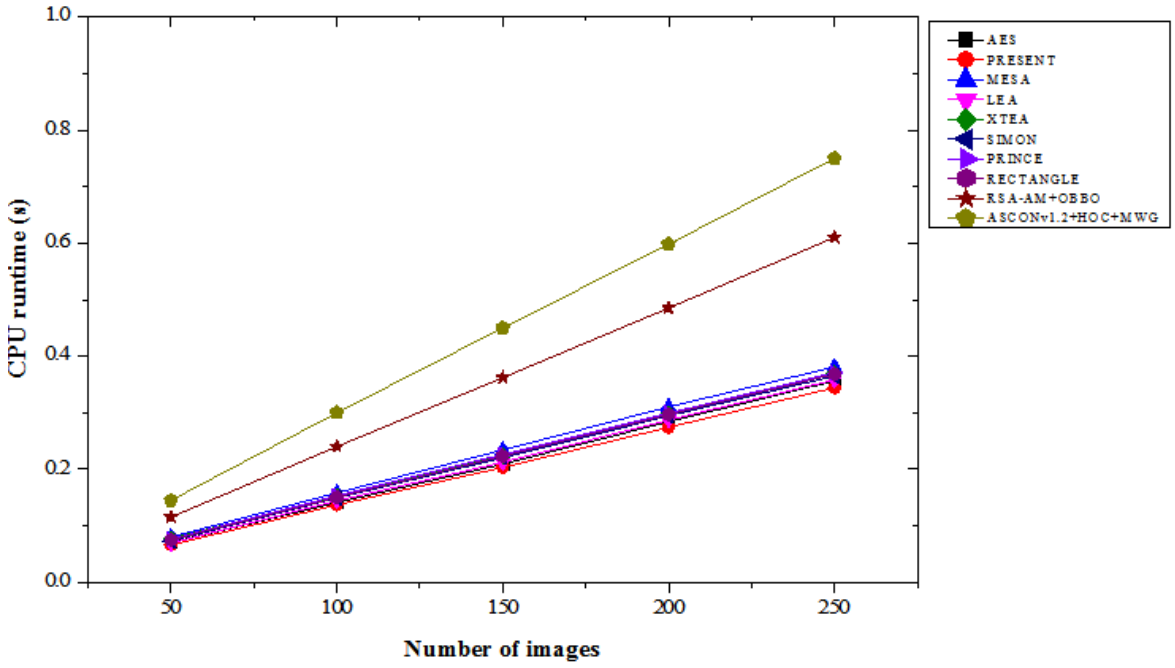


Figure 14. CPU runtime results without attacks.

 doi:10.20944/preprints202501.2331.v1

Table 6. CPU runtime result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

Lightweight cryptography algorithms	Number of images				
	50	**100**	**150**	**200**	**250**
	With attacks				
AES	0.072	0.145	0.213	0.287	0.359
PRESENT	0.068	0.140	0.206	0.277	0.347
MESA	0.083	0.162	0.238	0.314	0.385
LEA	0.071	0.148	0.217	0.292	0.363
XTEA	0.079	0.155	0.227	0.302	0.373
SIMON	0.075	0.151	0.222	0.296	0.367
PRINCE	0.078	0.156	0.229	0.303	0.375
RECTANGLE	0.077	0.153	0.226	0.300	0.371
RSA-AM+OBBO	0.118	0.246	0.370	0.493	0.625
ASCONv1.2+HOC+MWG	0.150	0.310	0.465	0.612	0.765
	Without attacks				
AES	0.070	0.141	0.209	0.284	0.356
PRESENT	0.066	0.137	0.203	0.274	0.344
MESA	0.080	0.158	0.234	0.310	0.381
LEA	0.069	0.144	0.212	0.287	0.358
XTEA	0.077	0.152	0.224	0.299	0.370
SIMON	0.073	0.149	0.220	0.294	0.365
PRINCE	0.076	0.153	0.226	0.299	0.371
RECTANGLE	0.075	0.150	0.223	0.297	0.368
RSA-AM+OBBO	0.115	0.240	0.362	0.485	0.610
ASCONv1.2+HOC+MWG	0.145	0.300	0.450	0.598	0.750

4.7. Encryption Time Results Analysis

Table 7 compares the encryption time results of various lightweight cryptographic algorithms across different image counts under both "with attacks" and "without attacks" conditions. In the with attacks scenario, the ASCONv1.2+HOC+MWG model shows consistently faster encryption times compared to other algorithms. For 50 images, its encryption time is 0.048 seconds, which is 43.40% faster than AES and 5.88% faster than RSA-AM+OBBO. As the number of images increases, the time difference persists, with the ASCONv1.2+HOC+MWG model taking 0.240 seconds at 250 images, which is 49.47% faster than AES and 7.32% faster than RSA-AM+OBBO.

The model outperforms existing algorithms in terms of encryption speed, which highlights its efficiency, even in attack scenarios. In without attacks scenario, the ASCONv1.2+HOC+MWG model continues to show superior performance. At 50 images, encryption time is 0.046 seconds, 48.89% faster than AES and 6.12% faster than RSA-AM+OBBO. For 250 images, the ASCONv1.2+HOC+MWG model completes encryption in 0.230 seconds, which is 48.89% faster than AES and 6.12% faster than RSA-AM+OBBO. As shown in Figure 15 and 16, our proposed model maintains its advantage over other cryptographic methods in both attack and non-attack scenarios, emphasizing its optimized encryption time. The ASCONv1.2+HOC+MWG model consistently outperforms AES, PRESENT, and RSA-AM+OBBO in terms of encryption time, both with and without attacks. The faster encryption times across all tested image sizes suggest that the proposed model is not only secure but also highly efficient in terms of computational performance. The ASCONv1.2+HOC+MWG model offers a superior balance between speed and security, making it appropriate for applications where real-time encryption is crucial, including data transfer in security-sensitive situations, even if AES and RSA-AM+OBBO offer strong encryption. This efficiency is crucial for maintaining high throughput while ensuring data security.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 January 2025 doi:10.20944/preprints202501.2331.v1

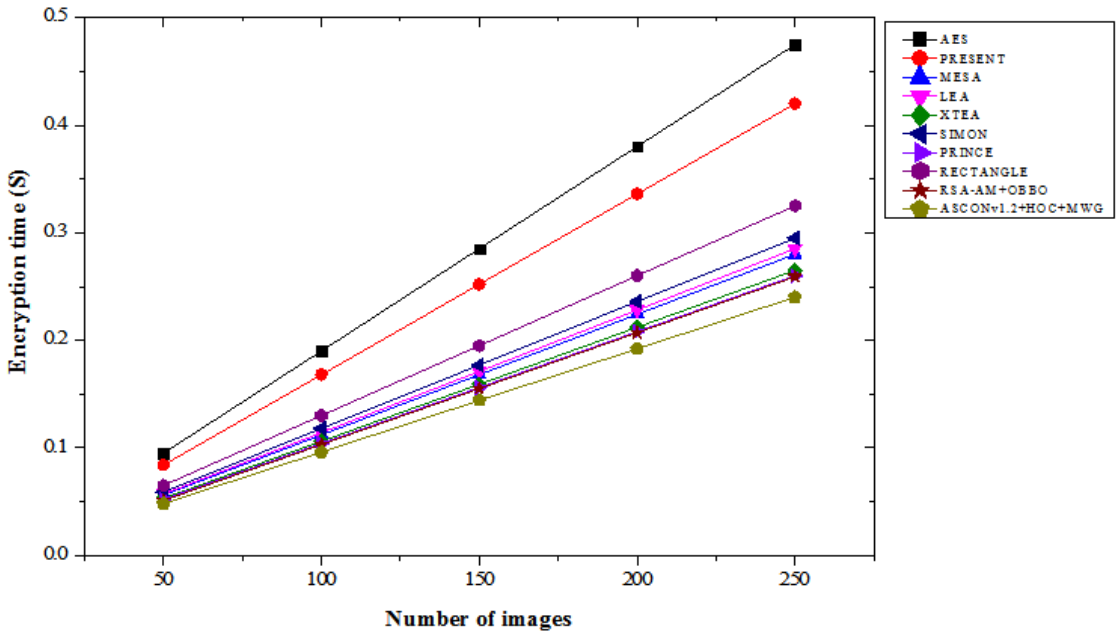


Figure 15. Encryption time results with attacks.

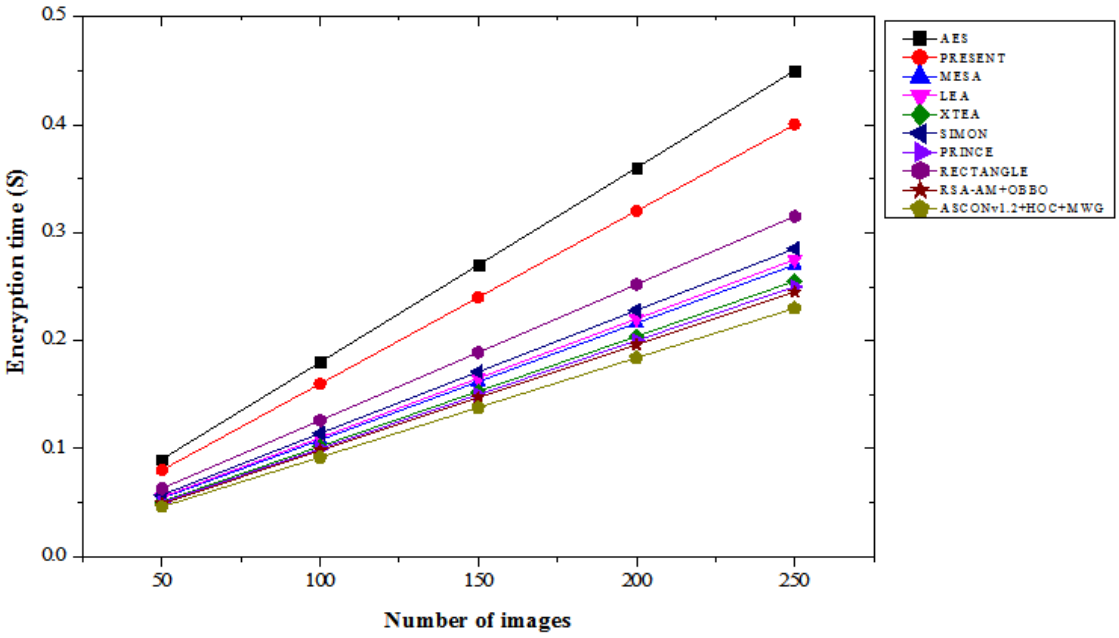


Figure 16. Encryption time results without attacks.

Table 7. Encryption time result comparison of lightweight cryptographic algorithms with varying number of images for with and without attacks.

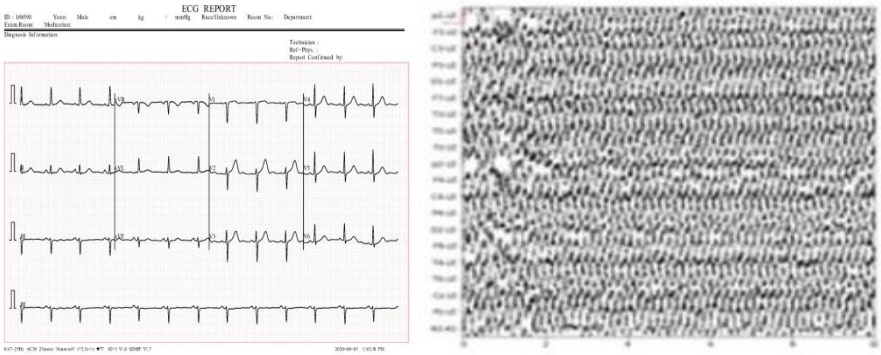
Lightweight cryptography algorithms	Number of images				
	50	100	150	200	250
	With attacks				
AES	0.095	0.190	0.285	0.380	0.475
PRESENT	0.084	0.168	0.252	0.336	0.420
MESA	0.056	0.112	0.168	0.224	0.280
LEA	0.057	0.114	0.171	0.228	0.285
XTEA	0.053	0.106	0.159	0.212	0.265
SIMON	0.059	0.118	0.177	0.236	0.295
PRINCE	0.052	0.104	0.156	0.208	0.260

 doi:10.20944/preprints202501.2331.v1

RECTANGLE	0.065	0.130	0.195	0.260	0.325
RSA-AM+OBBO	0.051	0.103	0.155	0.207	0.259
ASCONv1.2+HOC+MWG	0.048	0.096	0.144	0.192	0.240
	Without attacks				
AES	0.090	0.180	0.270	0.360	0.450
PRESENT	0.080	0.160	0.240	0.320	0.400
MESA	0.054	0.108	0.162	0.216	0.270
LEA	0.055	0.110	0.165	0.220	0.275
XTEA	0.051	0.102	0.153	0.204	0.255
SIMON	0.057	0.114	0.171	0.228	0.285
PRINCE	0.050	0.100	0.150	0.200	0.250
RECTANGLE	0.063	0.126	0.189	0.252	0.315
RSA-AM+OBBO	0.049	0.098	0.147	0.196	0.245
ASCONv1.2+HOC+MWG	0.046	0.092	0.138	0.184	0.230

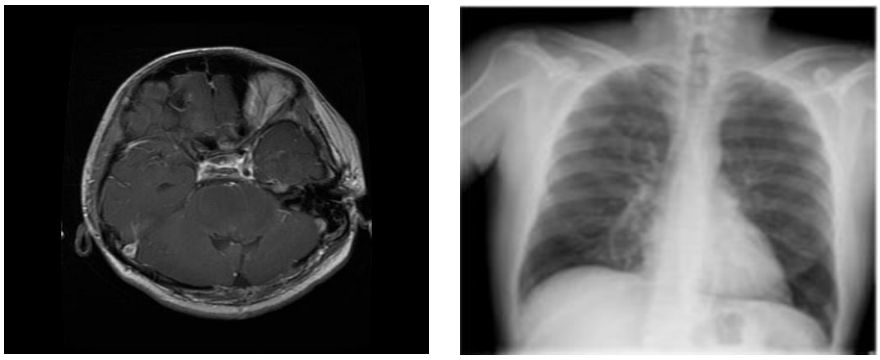
4.8. Results Comparison of Proposed and Existing Lightweight Crypto Algorithm

This section evaluates the performance of the proposed and existing lightweight cryptographic algorithms using various metrics, including the number of pixel changing rate (NPCR), unified averaged changed intensity (UACI), and cross-entropy. Medical images, such as ECG, EEG, MRI, and X-ray scans, were used as inputs for the proposed method. Figure 17 illustrates sample medical images utilized in the analysis. The results presented in Table 8 demonstrate that the proposed lightweight cryptographic algorithm (ASCONv1.2 + HOC + MWG) outperforms the existing CTE + Dynamic Chaotic model[32] across all metrics for encrypted images. For NPCR, the proposed model achieves percentage improvements ranging from 0.076% to 0.085%, indicating enhanced sensitivity to pixel changes. Similarly, the UACI values exhibit an improvement, with increases ranging from 2.82% for ECG images to 5.70% for X-Ray images, reflecting better intensity variation in the encrypted data. Cross-entropy, a measure of randomness and security, also shows very high improvement. These enhancements highlight the proposed algorithm's superior encryption quality and robustness. In Table 9, the results for decrypted images indicate that both the proposed and existing algorithms achieve perfect decryption, as evidenced by NPCR, UACI, and cross-entropy values of 0 across all image types. This shows that both algorithms are capable of accurately restoring the original images without any distortion, ensuring high reliability in decryption. The proposed ASCONv1.2+HOC+MWG algorithm demonstrates improved encryption performance, with notable improvement in NPCR, UACI, and cross-entropy metrics, while maintaining flawless decryption capability. This makes it a more effective and secures option for lightweight cryptographic applications in medical imaging.



(**a**) (**b**)

 doi:10.20944/preprints202501.2331.v1



(c) (d)

Figure 17. Test samples of medical images (a) ECG (b) EEG (c) MRI and (d) X-ray.

Table 8. Result comparison of proposed and existing lightweight crypto algorithm models for original and encrypted images.

Images	Lightweight cryptography algorithms	NPCR	UACI	Cross entropy
ECG	CTE + Dynamic Chaotic [31]	99.623	47.168	0.139
	ASCONv1.2 + HOC + MWG	**99.700**	**48.500**	**13.950**
EEG	CTE + Dynamic Chaotic [31]	99.625	44.325	0.110
	ASCONv1.2 + HOC + MWG	**99.710**	**45.800**	**12.120**
MRI	CTE + Dynamic Chaotic [31]	99.614	39.678	0.134
	ASCONv1.2 + HOC + MWG	**99.690**	**41.000**	**13.545**
X-Ray	CTE + Dynamic Chaotic [31]	99.617	31.225	0.132
	ASCONv1.2 + HOC + MWG	**99.695**	**33.000**	**13.340**

Table 9. Result comparison of proposed and existing lightweight crypto algorithm models for original and decrypted images.

Images	Lightweight cryptography algorithms	NPCR	UACI	Cross entropy
ECG	CTE + Dynamic Chaotic [31]	0	0	0
	ASCONv1.2 + HOC + MWG	0	0	0
EMG	CTE + Dynamic Chaotic [31]	0	0	0
	ASCONv1.2 + HOC + MWG	0	0	0
MRI	CTE + Dynamic Chaotic [31]	0	0	0
	ASCONv1.2 + HOC + MWG	0	0	0
X-Ray	CTE + Dynamic Chaotic [31]	0	0	0
	ASCONv1.2 + HOC + MWG	0	0	0

The complexity analysis presented in Table 10 reveals the comparative strengths of the CTE+dynamic chaotic model and the proposed ASCONv1.2+HOC+MWG model. In terms of time complexity, the CTE+dynamic chaotic model exhibits O(m·n), where m is the number of pixels and n is the number of iterations for chaotic key generation. ASCONv1.2+HOC+MWG model optimizes this with a time complexity of O(k·b+n+k·logk), where k is the number of blocks, b is the block size, and n represents the key generation cost. By utilizing block-based processing and efficient graph traversal with a logarithmic factor, the proposed model reduces the computational burden, particularly for larger images, making it more efficient and scalable. Regarding space complexity, the CTE+dynamic chaotic model requires O(m+n) space, which accounts for the storage of the image data, chaotic parameters, and keys. While this space usage is reasonable, it is relatively less optimized. On the other hand, the ASCONv1.2+HOC+MWG model has a space complexity of O(m+n+k), where the additional term k comes from the storage required for graph-based operations. Although this results in slightly higher space complexity, the increased efficiency of the encryption process compensates for this, as the graph storage is lightweight and aids in faster encryption. ASCONv1.2+HOC+MWG model provides notable improvements in both time and space complexity over the CTE+dynamic

 doi:10.20944/preprints202501.2331.v1

chaotic model. By reducing computational overhead with block-based processing and leveraging more efficient graph traversal, the proposed model enhances overall performance, particularly for larger images or real-time applications. Despite the slight increase in space complexity due to the graph storage, the proposed model remains highly efficient, making it a more suitable choice for lightweight cryptographic applications in environments with constrained resources.

Table 10. Complicity analysis of proposed and existing lightweight crypto algorithm models.

Aspect	CTE+dynamic chaotic [31]	ASCONv1.2+HOC+MWG
Time complexity	O(m.n)	O(k.b+n+k.logk)
Space complexity	O(m+n)	O(m+n+k)

5. Conclusions

To improve health services, we have proposed a super-lightweight cryptographic algorithm made specifically for IoT medical strategies with limited resources. ASCONv 1.2 cryptographic algorithm is used for efficient encryption and decryption, providing a lightweight and secure solution for resource-constrained devices. The hypercube optimization algorithm (HOS) is used to specialize the key length and operating parameters, thereby increasing adaptability and energy efficiency, and at the same time ensuring increased safety. Modified whale optimization algorithm (MWG) is used to enhance local and global search capabilities, significantly increase resource efficiency, extend device battery life, and enable continuous real-time operation without compromising security. Using clinical image datasets, we performed detailed experiments to evaluate the effectiveness of the proposed model. The results show that cryptographic model ASCONv 1.2 + HOC + MWG systematically performs at the same level as the key performance indicators of AES, PRESENT, and RSA-AM + OBBO, including correlation coefficient, CPU execution time, and encryption time. Based on the correlation coefficient, the proposed model showed a 4.5% improvement under attack conditions compared to AES and 3.06% improvement without attack, ensuring better data integrity during encryption. In terms of CPU processing time, RSA-AM+ was slightly slower than OBBO, but showed a 34.57% improvement over AES under the attack conditions. Considering the encryption time, ASCONv1.2+ HOC+MWG model achieved 43.40% faster encryption than AES under attack conditions and 48.89% improvement without attack, thus highlighting its efficiency and significance for real-time applications. The ASCONv 1.2+HOC+MWG model finds a good balance between security and speed and is the most competitive option for securing cryptographic systems in resource-constrained medical IoT environments.

Author Contributions: Abdul Muhammed Rasheed and R. Mathusoothana S. Kumar collaborated extensively on this research. Abdul Muhammed Rasheed was primarily responsible for conceptualizing the study, developing the lightweight cryptographic algorithm, and conducting the experimental analyses using the ASCONv1.2 encryption algorithm, the Hypercube Optimal Search (HOS) algorithm, and the Modified Wild Geese (MWG) algorithm. He also contributed to data analysis and interpretation. R. Mathusoothana S. Kumar provided significant contributions to the methodological framework, optimization techniques, and the overall structure of the cryptographic model. He was instrumental in ensuring the integration of the proposed algorithms with the medical IoT use cases and provided critical feedback throughout the research. He also supervised the project and ensured its alignment with the goals of healthcare security. Both authors actively contributed to writing and revising the manuscript, ensuring the presentation of results was clear, accurate, and impactful. They equally shared responsibility for responding to peer reviews and preparing the final submission of the paper.

Funding: This research received no external funding.

Data Availability Statement: The datasets employed and examined in the present investigation are accessible to the public. The clinical picture datasets utilised for the experimental assessment are obtained from the Kaggle repository and are accessible at https://www.kaggle.com/datasets. This work utilised diagnostic medical

 doi:10.20944/preprints202501.2331.v1

imaging, including CT scans, MRIs, and ultrasounds, for the performance evaluation of cryptographic algorithms. The source code and methods utilised in this study can be obtained from the relevant author upon a reasonable request. All data substantiating the conclusions of this article are contained inside the paper itself.

Acknowledgments: The authors would like to thank the Department of Information Technology at **Noorul Islam Centre for Higher Education** for providing the resources and assistance required for this study. Special gratitude to the research teams and individuals whose contributions to cryptographic algorithms and medical IoT security have substantially inspired our study. We also appreciate the invaluable contributions of colleagues and mentors who gave critical input on the text. Additionally, we thank the Kaggle platform for supplying the publicly available medical picture datasets utilised in the experimental research.

Conflicts of Interest: The authors declare no conflict of interest with this article's research, authorship, or publishing. This study had no financial or personal links that may have impacted it.

Appendix A. Symbol Table

This document contains the symbols, notations, and their explanations from the referenced cryptographic research paper.

Symbol/Notation	Meaning	Context/Usage
j	Secret key	Used for encryption and decryption in the ASCONv1.2 algorithm.
J	Size of the secret key	Indicates the bit length of the cryptographic key.
Q	Nonce	A unique 128-bit number used to ensure encryption uniqueness.
X	Associated data	Metadata combined with plaintext for authenticated encryption.
M	Plaintext message	Input data to be encrypted.
E	Ciphertext	Encrypted version of the plaintext M.
U	Authentication tag	A 128-bit tag used to validate data integrity and authenticity.
P	Input communication	Data to be hashed in cryptographic operations.
I	Hash output	Result of the hash function applied to P.
R	Rate parameter	Defines the block size for sponge-based cryptographic operations.
h	Output span constraint	Maximum length of the hash output I.
V	Internal state vector	320-bit vector used during ASCON's encryption and decryption.
pb	Round permutation	A function applied to V for cryptographic diffusion.
m	Number of pixels	Represents image size in medical image encryption and analysis.
k	Number of blocks	Indicates how data is divided for block-based encryption.
b	Block size	Size of individual blocks in cryptographic operations.
T	Iterative threshold coefficient	Guides optimization processes.
f	Fitness value	A measure used to evaluate solutions in optimization algorithms like HOS and MWG.
c	Center of the hypercube	Reference point in hypercube optimization.
Ln, Un	Lower and upper bounds	Define the dimensional constraints of the hypercube search space.
pd	Central standards	Average of Ln and Un, defining the search center in optimization.

 doi:10.20944/preprints202501.2331.v1

$ADR, maxADR$	Adaptation rates	Measure success in optimization algorithms.
$NPCR$	Number of Pixel Change Rate	Indicates the sensitivity of encryption to pixel changes in images.
$UACI$	Unified Average Change Intensity	Measures average intensity variations in encrypted images.
SSI	Structural Similarity Index	Assesses similarity between original and encrypted images for quality assurance.
$PSNR$	Peak Signal-to-Noise Ratio	Evaluates the quality of encrypted images.
MSE	Mean Square Error	Measures distortion in decrypted medical images.
BER	Bit Error Rate	Indicates the number of erroneous bits in transmission or encryption.
$\oplus$	XOR operation	Used for bitwise mixing in encryption and hashing.
$\|\|$	Concatenation	Joins two data strings in cryptographic operations.
$\backslash \mathrm{mod}$	Modulus	Calculates remainders during block padding and encryption.
$\perp$	Error/null	Indicates decryption failure or invalid tag.
$\wedge$	Logical AND	Ensures all conditions are met in cryptographic processes.
$\leq, \geq$	Less than or equal to, greater than or equal to	Sets bounds in optimization or cryptographic algorithms.
$Vnew, Vold$	Updated and previous states	Represents state transformations during encryption or optimization.
ΔF	Objective function difference	Guides solution refinement in optimization.
Xe	Evolution factor	A parameter in the Modified Wild Geese (MWG) optimization algorithm.

Appendix B. Equations with Explanations

 doi:10.20944/preprints202501.2331.v1

Table 1: Explanation of $\epsilon_{J,R,x,y}(J,Q,P,M) = (E,U)$

Component	**Description**	Formula No.
ϵ	The encryption function of the cryptographic algorithm.	(1)
J, R, x, y (Subscripts)	Parameters influencing the encryption process: • J: Secret key. • R: Rate parameter. • x, y: Additional function parameters.	
Inputs		
J	The secret key used for encryption.	
Q	Time-based nonce (Number Used Once) to ensure uniqueness of encryption.	
P	Associated data that is authenticated but not encrypted, often used for metadata.	
M	The plaintext (message) that needs to be encrypted.	
Outputs		
E	The encrypted ciphertext produced from the plaintext (M) and other inputs.	
U	Authentication tag ensuring integrity and authenticity of the ciphertext (E) and associated data (P).	
Purpose	The function encrypts the plaintext (M) and produces a ciphertext (E) while generating a tag (U) for integrity and authentication.	

Table 2: Explanation of the Equation $A_{i,R,x}(P,O) = I$

Component	**Description**	Formula No.
$A_{i,R,x}$	Represents a cryptographic hash or transformation function parameterized by i, R, x.	(3)
Inputs		
P	Input data (e.g., plaintext or associated data) to be processed by the function.	
O	Optional parameters or additional data influencing the transformation process.	
Output		
I	The resulting output of the function, often representing a hashed or transformed value.	
Purpose	Describes a process of deriving a fixed-size output (I) from variable-size inputs (P,O) using defined parameters (i,R,x).	

 doi:10.20944/preprints202501.2331.v1

Table 5: Explanation of the Equation

$$iv_{J,R,x,y} \leftarrow J \,||\, R \,||\, x \,||\, y \,||\, 0^{160-J} = \begin{cases} 80400e0600000000 & \text{for Ascon-128} \\ 80800e0800000000 & \text{for Ascon-128a} \\ x0400e06 & \text{for Ascon-80pq} \end{cases}$$

Component	**Description**	Formula No.
$iv_{J,R,x,y}$	Represents the initialization vector for the cryptographic function, parameterized by J, R, x, y.	(5)
J	Secret key length used in the cryptographic initialization.	
R	Rate parameter, which determines the portion of state processed per iteration.	
x	Algorithm-specific parameter affecting initialization.	
y	Additional parameter defining specific operational modes.	
0^{160-J}	Padding to ensure the vector reaches the required size, based on the secret key length J.	
Cases		
80400e0600000000	Initialization vector for Ascon-128.	
80800e0800000000	Initialization vector for Ascon-128a.	
x0400e06	Initialization vector for Ascon-80pq.	
Purpose	This equation defines the initialization vector ($iv_{J,R,x,y}$) for different Ascon variants, ensuring consistent initialization for cryptographic processes.	

Table 6: Explanation of the Equation $V \leftarrow x_r(V) \oplus \left(0^{320-J} \,||\, j\right)$

Component	**Description**	Formula No.
V	Represents the cryptographic state being updated during the transformation.	(6)
$x_r(V)$	A round-based transformation applied to the state V, often involving cryptographic operations such as substitutions and permutations.	
$\oplus$	The XOR operation combines the transformed state with additional input to introduce diffusion and ensure randomness.	
0^{320-J}	A padding operation to align the size of the input, determined by the secret key length J.	
j	Represents a specific constant or parameter added to the state during this transformation.	
Purpose	This equation describes an update step in the cryptographic state V, incorporating a round-based transformation (x_r) and XORing with padded inputs to maintain security.	

 doi:10.20944/preprints202501.2331.v1

Table 7: Explanation of the Equation for

$$X_1, \ldots, X_n \leftarrow \begin{cases} R\text{-bit blocks of } X \,||\, 1 \,||\, 0^{R-1-(|X| \mod R)}, & \text{if } |X| > 0 \\ \varepsilon, & \text{if } |X| = 0 \end{cases}$$

Component	Description	Formula No.
$X_1, \ldots, X_n$	Represents the R-bit blocks derived from the input X, used in cryptographic padding and partitioning.	(7)
X	The input data to be partitioned into R-bit blocks.	
$\|\|$	Concatenation operator, used to combine the input X with padding and additional bits.	
1	A single bit appended to the input X to indicate the start of padding.	
$0^{R-1-(\|X\| \mod R)}$	Zero-padding added to align the total length to a multiple of R-bits.	
$\|X\|$	The length of the input X in bits.	
ε	Represents an empty block, used when the input X has zero length.	
Purpose	This equation ensures that input X is divided into fixed-size R-bit blocks, with appropriate padding applied for cryptographic processing. If X is empty, it results in an empty block.	

Table 8: Explanation of the Equation for $\mathrm{V} \leftarrow m'((V_R \oplus X_h) \,||\, V_\epsilon), \quad 1 \le h \le u$

Component	Description	Formula No.
V	Represents the updated cryptographic state after processing.	(8)
m'	A transformation function applied to the concatenated input, often involving cryptographic operations such as substitution or permutation.	
V_R	The rate portion of the state, which is XORed with the block X_h.	
$\oplus$	The XOR operation used to combine V_R and the current block X_h.	
X_h	The h-th block of the input data X, where $1 \le h \le u$.	
$\|\|$	Concatenation operator, combining the XOR result $(V_R \oplus X_h)$ with V_ϵ.	
V_ϵ	The capacity portion of the cryptographic state, concatenated with the XOR result.	
Purpose	This equation describes an update step in the cryptographic state V, incorporating block-wise input processing with transformations to ensure secure state evolution.	

Table 9: Explanation of the Equation $V \leftarrow V \oplus \left(0^{319} \,||\, 1\right)$

Component	Description	Formula No.
V	Represents the cryptographic state being updated.	(9)
$\oplus$	The XOR operation applied to the state V and the concatenated input.	
0^{319}	Padding of 319 zeros added to align the size of the input.	
1	A single bit appended to the padding to mark the end of the input or initiate a specific operation.	
Purpose	This equation updates the cryptographic state V by XORing it with padded input to maintain security properties.	

 doi:10.20944/preprints202501.2331.v1

Table 10: Explanation of the Equation $\mathrm{M}_1, \ldots, M_u \leftarrow R$-bit blocks of $M \,||\, 1 \,||\, 0^{R-1-(|M| \mod R)}$

Component	Description	Formula No.
$M_1, \ldots, M_u$	Represents the R-bit blocks derived from the input M.	(10)
M	Input data to be partitioned into R-bit blocks.	
$\|\|$	Concatenation operator used to combine M, padding bits, and the marker bit.	
1	A single bit appended to M to indicate the start of padding.	
$0^{R-1-(\|M\| \mod R)}$	Zero-padding added to align the total input size to a multiple of R-bits.	
Purpose	This equation ensures that the input M is divided into fixed-size R-bit blocks with appropriate padding for cryptographic processing.	

Table 11: Explanation of $F_h \leftarrow V_R \oplus M_h$

Component	Description	Formula No.
F_h	Intermediate state derived during cryptographic operations.	(11)
V_R	The rate portion of the state in the cryptographic process.	
$\oplus$	XOR operation combining V_R and M_h.	
M_h	Current message block being processed.	
Purpose	Describes how the rate portion of the state is updated with a message block during encryption or decryption.	

Table 12: Explanation of $\mathrm{V} \leftarrow \begin{cases} m'(E_h \,||\, V_\epsilon) & \text{if } 1 \le h < u \\ E_h \,||\, V_e & \text{if } 1 \le u \end{cases}$

Component	Description	Formula No.
V	Updated state after processing the input.	
m'	Transformation function applied when $1 \le h < u$.	(12)
E_h	Intermediate encryption result for the h-th block.	
V_e	Capacity portion of the cryptographic state.	
Purpose	Describes the conditional update of the cryptographic state depending on the block index h.	

Table 13: Explanation of $\widetilde{E}_u \leftarrow [E_u]_{M \mod R}$

Component	Description	Formula No.
$\widetilde{E}_u$	Truncated encryption result for the u-th block.	(13)
E_u	Full encryption result for the u-th block.	
$M \mod R$	Modulo operation to determine the truncation size.	
Purpose	Specifies truncation of the last encryption block based on the input message size.	

Table 14: Explanation of $M_h \leftarrow V_R \oplus E_h$

Component	Description	Formula No.
M_h	Decrypted message block derived during decryption.	(14)
V_R	The rate portion of the cryptographic state.	
$\oplus$	XOR operation combining V_R and E_h.	
E_h	Encrypted data block corresponding to M_h.	
Purpose	Describes how message blocks are recovered during decryption using the state and encrypted data.	

 doi:10.20944/preprints202501.2331.v1

Table 15: Explanation of $\mathrm{V} \leftarrow m^y(E_h \,||\, V_\epsilon), \quad 1 \leq h < u$

Component	**Description**	**Formula No.**
V	Updated cryptographic state after applying the transformation.	(15)
m^y	Transformation function applied to the inputs.	
E_h	Intermediate encryption result for the h-th block.	
V_ϵ	Capacity portion of the cryptographic state.	
$\|\|$	Concatenation operator combining E_h and V_ϵ.	
$1 \leq h < u$	Specifies that the operation applies to all blocks where the block index h lies within this range.	
Purpose	This equation describes how the cryptographic state V is updated iteratively for each block of data, combining intermediate results E_h with the capacity portion V_ϵ.	

Table 16: Explanation of $\mathrm{U} \leftarrow V_R \oplus (\widetilde{M}_u \,||\, 1 \,||\, 0^{R-1-o}) \,||\, V_\epsilon$

Component	**Description**	Formula No.
U	Final authentication tag ensuring integrity of the input data.	(17)
V_R	The rate portion of the cryptographic state.	
$\widetilde{M}_u$	Truncated message block from the final step.	
1	Marker bit appended to indicate the end of the input.	
0^{R-1-o}	Padding to ensure alignment with the block size R.	
V_ϵ	Capacity portion of the state appended to the result.	
Purpose	Describes the construction of the authentication tag used for integrity verification.	

Table 17: Explanation of $\widetilde{M}_u \leftarrow [V_R]_q \oplus \widetilde{M}_u$

Component	**Description**	**Formula No.**
$\widetilde{M}_u$	Updated message block after XOR operation.	(16)
$[V_R]_q$	Truncated version of the rate portion V_R, truncated to q bits.	
$\oplus$	XOR operation combining the truncated state and the current message block.	
Purpose	This equation updates the message block $\widetilde{M}_u$ by XORing it with the truncated cryptographic state $[V_R]_q$. This ensures the integration of the state into the message processing.	

Table 18: Explanation of $U \leftarrow m^*(V \oplus (0^R \,||\, j \,||\, 0^{s-J}))$

Component	**Description**	Formula No.
U	Final result derived from the transformation function m^*.	(18)
m^*	Cryptographic transformation function applied to the XOR result.	
V	Current cryptographic state.	
$\oplus$	XOR operation combining V and the padded input.	
0^R	Padding of R-bits to align input size.	
j	Specific parameter influencing the operation.	
0^{s-J}	Additional padding based on s and J.	
Purpose	Describes the computation of U in a cryptographic protocol.	

Table 19: Explanation of $S \leftarrow [T]^{128} \oplus [k]^{128}$

Component	**Description**	Formula No.
S	Resulting state after XORing T and k.	(19)
$[T]^{128}$	Input T truncated to 128 bits.	
$[k]^{128}$	Key k truncated to 128 bits.	
$\oplus$	XOR operation combining the two inputs.	
Purpose	Updates the cryptographic state S using truncated inputs.	

 doi:10.20944/preprints202501.2331.v1

Table 20: Explanation of $Ln = Min(P\ bounds)$

Component	**Description**	Formula No.
Ln	Lower bound of the parameter P.	(20)
$Min(P\ bounds)$	The smallest value within the specified bounds of P.	
Purpose	Determines the minimum bound for parameter P.	

Table 21: Explanation of $Un = Max(P\ bounds)$

Component	**Description**	Formula No.
Un	Upper bound of the parameter P.	(21)
$Max(P\ bounds)$	The largest value within the specified bounds of P.	
Purpose	Determines the maximum bound for parameter P.	

Table 22: Explanation of $c = Un - Ln$

Component	**Description**	Formula No.
c	The range or difference between the upper and lower bounds.	(22)
Un	The upper bound of the parameter P.	
Ln	The lower bound of the parameter P.	
Purpose	Determines the range within the bounds of the parameter P.	

Table 23: Explanation of $p_d = \frac{Ln+Un}{2}$

Component	**Description**	Formula No.
p_d	The midpoint or average of the bounds Ln and Un.	(23)
Ln	The lower bound of the parameter P.	
Un	The upper bound of the parameter P.	
Purpose	Calculates the average position within the bounds of the parameter P.	

Table 24: Explanation of $p_d^{new} = \frac{p_d+p_{new}^{best}}{2}$

Component	**Description**	Formula No.
p_d^{new}	Updated midpoint incorporating the best new parameter.	(24)
p_d	Current midpoint of the bounds.	
p_{new}^{best}	The best new parameter obtained during the process.	
Purpose	Updates the midpoint by considering the best new parameter.	

Table 25: Explanation of $p_{best} = p_{new}^{best}$

Component	**Description**	Formula No.
p_{best}	Updates to reflect the best new parameter.	(25)
p_{new}^{best}	The best new parameter obtained during the process.	
Purpose	Reassigns the best parameter for the current iteration.	

Table 26: Explanation of $p_d = p_d^{new}$

Component	**Description**	**Formula No.**
p_d	Current decision parameter or value in the iteration.	(26)
p_d^{new}	Updated value of the decision parameter computed in the previous step.	
Purpose	This equation reassigns the updated decision parameter p_d^{new} to the current parameter p_d, ensuring iterative progression in the computation or optimization process.	

 doi:10.20944/preprints202501.2331.v1

Table 27: Explanation of $p_b = \frac{p+p_d}{c}$

Component	Description	Formula No.
p_b	Normalized parameter value considering p, p_d, and the range c.	(27)
p	A parameter value being normalized.	
p_d	The midpoint of the bounds.	
c	The range of the bounds.	
Purpose	Normalizes the parameter value within the range defined by c.	

Table 28: Explanation of $p_{Minb} = \frac{p_{Min}-p_d}{c}$

Component	Description	Formula No.
p_{Minb}	Normalized minimum parameter value considering p_{Min}, p_d, and c.	(28)
p_{Min}	Minimum parameter value.	
p_d	The midpoint of the bounds.	
c	The range of the bounds.	
Purpose	Computes a normalized value for the minimum parameter.	

Table 29: Explanation of $c_b = \frac{\text{Sum}((p_b-p_{Minb})^2)^{0.5}}{c}$

Component	Description	Formula No.
c_b	Standard deviation of normalized parameters p_b and p_{Minb}.	(29)
$\text{Sum}((p_b - p_{Minb})^2)$	Sum of squared differences between p_b and p_{Minb}.	
c	The range of the bounds.	
Purpose	Computes the standard deviation of normalized parameters.	

Table 30: Explanation of $c_{bb} = \frac{c_b}{\sqrt{a}}$

Component	Description	Formula No.
c_{bb}	Scaled standard deviation.	(30)
c_b	Standard deviation of normalized parameters.	
$\sqrt{a}$	Scaling factor based on parameter a.	
Purpose	Scales the standard deviation based on the parameter a.	

Table 31: Explanation of $TH = 1 - 0.2E^{-3c_{bb}}$

Component	Description	Formula No.
TH	Threshold value computed for a specific operation.	(31)
c_{bb}	Scaled standard deviation, as defined previously.	
$E^{-3c_{bb}}$	Exponential decay term based on c_{bb}.	
Purpose	Calculates a threshold TH using an exponential decay function.	

Table 32: Explanation of $R_{dim} = R_{Dim} \times TH$

Component	Description	Formula No.
R_{dim}	Adjusted dimension based on threshold.	(32)
R_{Dim}	Initial dimension or reference value.	
TH	Threshold value affecting the dimension.	
Purpose	Scales the dimension R_{Dim} using the threshold TH.	

Table 33: Explanation of $p_d = p_{best}$

Component	Description	Formula No.
p_d	The midpoint or parameter under consideration.	(33)
p_{best}	The best parameter obtained so far.	
Purpose	Reassigns p_d to the best parameter value.	

 doi:10.20944/preprints202501.2331.v1

Table 34: Explanation of Complex Equation

$$C_{i,l,f}^{iter} = (i_f \times C_{i,l,f}^{iter} + e_{2,f} \times (C_{i,l-1,f}^{iter} - C_{i,l,f}^{iter})) + \mathrm{e}_{3,f} \times (O_{i,l,f}^{iter} - Z_{i,l+1,f}^{iter}) + e_{4,f} \times (O_{i,l-1,f}^{iter} - Z_{i,l+2,f}^{iter}) \text{ - } \mathrm{e}_{5,f} \times (O_{i,l+1,f}^{iter} - Z_{i,l+2,f}^{iter})$$

Component	**Description**	Formula No.
$C_{i,l,f}^{iter}$	Updated coefficient for a specific iteration.	(34)
i_f	Iteration factor affecting the coefficient update.	
$e_2, f, e_3, f, e_4, f, e_5, f$	Coefficients affecting the contribution of various terms.	
$O_{i,l,f}^{iter}, Z_{i,l,f}^{iter}$	Output and state variables influencing the iteration.	
Purpose	Computes updated coefficients by combining iteration-specific factors, outputs, and states.	

Table 35: Explanation of $\mathrm{Z}_{i,l,f}^{\epsilon} = O_{i,l,f}^{iter} + e_{2,l,f} \times gf \times \left(f_f^{iter} + O_{i,l-1,f}^{iter} - 2 \times O_{i,l,f}^{iter}\right) + C_{i,l,f}^{iter+1}$

Component	**Description**	Formula No.
$Z_{i,l,f}^{\epsilon}$	State update using intermediate values, coefficients, and correction terms.	(35)
$O_{i,l,f}^{iter}$	Intermediate state for the current iteration.	
$e_{2,l,f}$	Coefficient influencing the correction factor.	
gf	Weighting factor applied to the correction term.	
$C_{i,l,f}^{iter+1}$	Correction term from the next iteration.	
Purpose	This equation calculates the updated state $Z_{i,l,f}^{\epsilon}$ for the current iteration.	

Table 36: Explanation of $\mathrm{Z}_{i,l,f}^{t} = O_{i,l,f}^{iter} + e_{3,l,f} \times g_{10,f} \times \left(O_{i+1,l,f}^{iter} - O_{i,l,f}^{iter}\right)$

Component	**Description**	Formula No.
$Z_{i,l,f}^{t}$	Temporary state update using intermediate values and coefficients.	(36)
$O_{i,l,f}^{iter}$	Intermediate state for the current iteration.	
$e_{3,l,f}$	Coefficient affecting the adjustment term.	
$g_{10,f}$	Weighting factor for the adjustment term.	
Purpose	Computes a temporary state $Z_{i,l,f}^{t}$ based on state differences.	

Table 37: Explanation of

$$Z_{i,l,f}^{iter+1} = \begin{cases} Z_{i,l,f}^{t} & \text{if } e_{1,l,d} \leq ve \\ Z_{i,l,f}^{\epsilon} & \text{otherwise} \end{cases}$$

Component	**Description**	Formula No.
$Z_{i,l,f}^{iter+1}$	Updated state for the next iteration.	(37)
$Z_{i,l,f}^{t}$	Temporary state from the current iteration.	
$e_{1,l,d}$	Condition parameter affecting the state update.	
$Z_{i,l,f}^{\epsilon}$	Corrected state used if the condition is not met.	
Purpose	Determines the next state based on a condition involving $e_{1,l,d}$.	

Table 38: Explanation of

$$M_O = \text{round}\left(M_O^{initial} - \left(M_O^{initial} - M_O^{final}\right) \times \frac{DR_A}{DR_{A_{max}}}\right)$$

Component	**Description**	Formula No.
M_O	Updated value calculated based on initial and final states.	(38)
$M_O^{initial}$	Initial state value.	
M_O^{final}	Final state value.	
$\frac{DR_A}{DR_{A_{max}}}$	Scaling factor for the adjustment.	
Purpose	Updates the state M_O using a scaled difference and rounds the result.	

 doi:10.20944/preprints202501.2331.v1

Appendix C. Table of Abbreviations

Abbreviation	Full Form
IoT	Internet of Things
IoMT	Internet of Medical Things
EHR	Electronic Health Records
ASCONv1.2	ASCON version 1.2 encryption algorithm
HOS	Hypercube Optimal Search Algorithm
MWG	Modified Wild Geese Algorithm
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Square Error
BER	Bit Error Rate
SSI	Structural Similarity Index
AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
RSA	Rivest-Shamir-Adleman Algorithm
BLE	Bluetooth Low Energy
XTEA	eXtended Tiny Encryption Algorithm
LEA	Lightweight Encryption Algorithm
PRINCE	PRINCE encryption algorithm
PRESENT	PRESENT encryption algorithm
SIMON	SIMON encryption algorithm
MESA	Modular Encryption Standard Algorithm
RECTANGLE	RECTANGLE encryption algorithm
NPCR	Number of Pixel Change Rate
UACI	Unified Averaged Changed Intensity
FPGA	Field-Programmable Gate Array
PSO	Particle Swarm Optimization

References

1. **Pradyumna, G.R.; Hegde, R.; Bommegowda, K.B.; Jan, T.; Naik, G.** Empowering Healthcare with IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges. *IEEE Access* **2024**, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2024.3362239.
2. **Bhambri, P.; Khang, A.** Managing and Monitoring Patient's Healthcare Using AI and IoT Technologies. In *Driving Smart Medical Diagnosis Through AI-Powered Technologies and Applications*; IGI Global, **2024**; pp. 1–23. https://doi.org/10.4018/979-8-3693-3679-3.ch001.
3. **Shafik, W.** The Future of Healthcare: AIoMT—Redefining Healthcare with Advanced Artificial Intelligence and Machine Learning Techniques. In *Artificial Intelligence and Machine Learning in Drug Design and Development*; **2024**; pp. 605–634. https://doi.org/10.1002/9781394234196.ch19.
4. **Mostafa, R.; El-Atawi, K.** Strategies to Measure and Improve Emergency Department Performance: A Review. *Cureus* **2024**, *16*(1), e52879. https://doi.org/10.7759/cureus.52879.
5. **Bala, I.; Pindoo, M.M.; Mijwil, M.; Abotaleb, M.; Yundong, W.** Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence. *Jordan Med. J.* **2024**, *58*(3). https://doi.org/10.35516/jmj.v58i2.2527.
6. **Ali, Z.; Mahmood, S.; ul Hassan, K.; Daud, A.; Alharbey, R.; Bukhari, A.** A Lightweight and Secure Authentication Scheme for Remote Monitoring of Patients in IoMT. *IEEE Access* **2024**, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2024.3400400.
7. **Madanian, S.; Chinbat, T.; Subasinghage, M.; Airehrour, D.; Hassandoust, F.; Yongchareon, S.** Health IoT Threats: Survey of Risks and Vulnerabilities. *Future Internet* **2024**, *16*(11), 389. https://doi.org/10.3390/fi16110389.
8. **Luidold, C.; Jungbauer, C.** Cybersecurity Policy Framework Requirements for the Establishment of Highly Interoperable and Interconnected Health Data Spaces. *Front. Med.* **2024**, *11*. https://doi.org/10.3389/fmed.2024.1379852.

9. **Citroni, R.; Mangini, F.; Frezza, F.** Efficient Integration of Ultra-low Power Techniques and Energy Harvesting in Self-Sufficient Devices: A Comprehensive Overview of Current Progress and Future Directions. *Sensors* **2024**, *24*, 4471. https://doi.org/10.3390/s24144471.
10. **Mahmmod, B.; Naser, M.; Al-Sodani, A.; Alsabah, M.; Mohammed, H.; Alaskar, H.; Almarshad, F.; Hussain, A.; Abdulhussain, S.H.** Patient Monitoring System Based on Internet of Things: A Review and Related Challenges With Open Research Issues. *IEEE Access* **2024**, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2024.3455900.
11. **Uddin, R.; Koo, I.** Real-Time Remote Patient Monitoring: A Review of Biosensors Integrated with Multi-Hop IoT Systems via Cloud Connectivity. *Appl. Sci.* **2024**, *14*, 1876. https://doi.org/10.3390/app14051876.
12. **Nissar, G.; Khan, R.; Mushtaq, M.; Ahmed, S.; Moon, A. RETRACTED ARTICLE:** IoT in Healthcare: A Review of Services, Applications, Key Technologies, Security Concerns, and Emerging Trends. *Multimed. Tools Appl.* **2024**, *83*, 80283–80283. https://doi.org/10.1007/s11042-024-18580-7.
13. **Nadhan, A.; Jacob, I.** Enhancing Healthcare Security in the Digital Era: Safeguarding Medical Images with Lightweight Cryptographic Techniques in IoT Healthcare Applications. *Biomed. Signal Process. Control* **2024**, *88*, 105511. https://doi.org/10.1016/j.bspc.2023.105511.
14. **Salunkhe, V.; Tangudu, A.; Mokkapati, C.; Goel, P.; Aggarwal, A.** Advanced Encryption Techniques in Healthcare IoT: Securing Patient Data in Connected Medical Devices. *Mod. Dyn. Math. Prog.* **2024**, *1*, 224–247. https://doi.org/10.36676/mdmp.v1.i2.22.
15. **Bakare, S.S.; Adeniyi, A.O.; Akpuokwe, C.U.; Eneh, N.E.** Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations. *Comput. Sci. IT Res. J.* **2024**, *5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859.
16. **Clemente-Lopez, D.; Rangel-Magdaleno, J.; Munoz-Pacheco, J.M.** A Lightweight Chaos-Based Encryption Scheme for IoT Healthcare Systems. *Internet Things* **2023**, *25*, 101032. https://doi.org/10.1016/j.iot.2023.101032.
17. **Alhaj, A.A.; Alrabea, A.; Jawabreh, O.** Efficient and Secure Data Transmission: Cryptography Techniques Using ECC. *Indones. J. Electr. Eng. Comput. Sci.* **2024**, *36*(1), 486–492. https://doi.org/10.11591/ijeecs.v36.i1.pp486-492.
18. **Pabitha, B.; Sanshi, S.; Karthik, N.** A Comprehensive Security Framework for WBANs in the Healthcare Environment. In *Security, Privacy, and Trust in WBANs and E-Healthcare*; **2024**; pp. 186–205. https://doi.org/10.1201/9781032635101-13.
19. **Mir, A.A.** Optimizing Mobile Cloud Computing Architectures for Real-Time Big Data Analytics in Healthcare Applications: Enhancing Patient Outcomes through Scalable and Efficient Processing Models. *Integr. J. Sci. Technol.* **2024**, *1*(7). Retrieved from https://ijstindex.com/index.php/ijst/article/view/68.
20. **Dave, D.M.; Mittapally, B.** Data Integration and Interoperability in IoT: Challenges, Strategies, and Future Direction. *Int. J. Comput. Eng. Technol.* **2024**, *15*, 45–60. https://www.researchgate.net/publication/377805078_Data_Integration_and_Interoperability_in_IOT_Challenges_Strategies_and_Future_Direction
21. **Alruwaili, O.; Tanveer, M.; Alotaibi, F.M.; Abdelfattah, W.; Armghan, A.; Alserhani, F.M.** Securing the IoT-Enabled Smart Healthcare System: A PUF-Based Resource-Efficient Authentication Mechanism. *Heliyon* **2024**, *10*(18), e37577. https://doi.org/10.1016/j.heliyon.2024.e37577.
22. **Chinbat, T.; Madanian, S.; Airehrour, D.; Hassandoust, F.** Machine Learning Cryptography Methods for IoT in Healthcare. *BMC Med. Inform. Decis. Mak.* **2024**, *24*, 153. https://doi.org/10.1186/s12911-024-02548-6.
23. **Zitouni, N.; Sedrati, M.; Behaz, A.** Lightweight Energy-Efficient Block Cipher Based on DNA Cryptography to Secure Data in Internet of Medical Things Devices. *Int. J. Inf. Technol.* **2023**, *16*. https://doi.org/10.1007/s41870-023-01580-5.
24. **Sheena, N.; Joseph, S.; Shailesh, S.** Lightweight Encryption Algorithms for Resource-Constrained Devices for Internet-of-Things Applications. In *Emerging Trends for Securing Cyber Physical Systems and the Internet of Things*; CRC Press, **2024**; pp. 19–40. https://doi.org/10.22214/ijraset.2024.64519
25. **Ahmad, I.; Shahid, F.; Islam, J.; Haque, K.N.; Harjula, E.** Adaptive Lightweight Security for Performance Efficiency in Critical Healthcare Monitoring. *arXiv Preprint* **2024**, arXiv:2406.03786. https://doi.org/10.48550/arXiv.2406.03786.

26. **Qasem, M.A.; Thabit, F.; Can, O.; Naji, E.; Alkhzaimi, H.A.; Patil, P.R.; Thorat, S.B.** Cryptography Algorithms for Improving the Security of Cloud-Based Internet of Things. *Secur. Priv.* **2024**, *7*(4), e378. https://doi.org/10.1002/spy2.378.
27. **Elhamzi, W.** Enhancing Medical Image Security with FPGA-Accelerated LED Cryptography and LSB Watermarking. *Trait. Signal* **2024**, *41*(1). https://doi.org/10.18280/ts.410107.
28. **Popoola, O.; Rodrigues, M.A.; Marchang, J.; Shenfield, A.; Ikpehai, A.; Popoola, J.** An Optimized Hybrid Encryption Framework for Smart Home Healthcare: Ensuring Data Confidentiality and Security. *Internet Things* **2024**, *27*, 101314. https://doi.org/10.1016/j.iot.2024.101314.
29. **Rana, M.; Mamun, Q.; Islam, R.** Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher. *Electronics* **2024**, *13*, 4325. https://doi.org/10.3390/electronics13214325.
30. **Al-Khalisy, J.; Abed, W.; Al-Kateb, G.; Aljanabi, M.; Mijwil, M.; Abotaleb, M.; Dhoska, K.** QIULEA: Quantum-Inspired Ultra-Lightweight Encryption Algorithm for IoT Devices. *Pollack Period.* **2024**. https://doi.org/10.1556/606.2024.01139.
31. **Rasheed, A.M.; Satheesh Kumar, R.M.** Lightweight Cryptographic Algorithms for Medical IoT Devices Using Combined Transformation and Expansion (CTE) and Dynamic Chaotic System. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*(4). https://doi.org/10.14569/IJACSA.2024.0150472.
32. **Selvaraj, J.; Lai, W.-C.; Kavin, B.P.; C., K.; Seng, G.H.** Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security. *Electronics* **2023**, *12*, 1636. https://doi.org/10.3390/electronics12071636.
33. **Yadav, T.; Kumar, M.** ML-Based Improved Differential Distinguisher with High Accuracy: Application to GIFT-128 and ASCON. *Cryptol. ePrint Arch.* **2024**, Paper 2024/1370. Available online: https://eprint.iacr.org/2024/1370
34. **Shang, X.; Chao, T.; Ma, P.; Yang, M.** An Efficient Local Search-Based Genetic Algorithm for Constructing Optimal Latin Hypercube Design. *Eng. Optim.* **2019**, *52*, 1–17. https://doi.org/10.1080/0305215X.2019.1584618.
35. **Nabih, M.; Ghoneimi, A.; Bakry, A.; Aaaa, S.; Al-Betar, M.; Elsayed Abd Elaziz, M.** Rock Physics Analysis from Predicted Poisson's Ratio Using RVFL Based on Wild Geese Algorithm in Scarab Gas Field in WDDM Concession, Egypt. *Mar. Pet. Geol.* **2022**, *147*, 105949. https://doi.org/10.1016/j.marpetgeo.2022.105949.
36. **Raheja, N.; Manocha, A.** IoT-Based ECG Monitoring System with Encryption and Authentication in Secure Data Transmission for Clinical Health Care Approach. *Biomed. Signal Process. Control* **2022**, *74*, 103481. https://doi.org/10.1016/j.bspc.2022.103481.
37. **Damodharan, J.; Susai Michael, E.R.; Shaikh-Husin, N.** High Throughput PRESENT Cipher Hardware Architecture for the Medical IoT Applications. *Cryptography* **2023**, *7*, 6. https://doi.org/10.3390/cryptography7010006.
38. **Chen, P.-Y.; Cheng, Y.-C.; Zhong, Z.-H.; Zhang, F.-Z.; Pai, N.-S.; Li, C.-M.; Lin, C.-H.** Information Security and Artificial Intelligence–Assisted Diagnosis in an Internet of Medical Thing System (IoMTS). *IEEE Access* **2024**, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2024.3351373.
39. **Singh, S.; Sharma, P.; Moon, S.; Park, J.** Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges, and Solutions. *J. Ambient Intell. Humaniz. Comput.* **2017**, *15*, 1–18. https://doi.org/10.1007/s12652-017-0494-4.
40. **Reddi, S.; Rao, P.M.; Saraswathi, P.; Jangirala, S.; Das, A.K.; Jamal, S.S.; Park, Y.** Privacy-Preserving Electronic Medical Record Sharing for IoT-Enabled Healthcare System Using Fully Homomorphic Encryption, IOTA, and Masked Authenticated Messaging. *IEEE Trans. Ind. Inform.* **2024**. https://doi.org/10.1109/TII.2024.3397343.
41. **Khalifa, O.; Ahmed, M.Z.; Hashim, A.** Application of Simon Encryption Algorithm for Data Transmission Between Sensor Nodes in IoT Environment. In *Proceedings of the 2024 9th International Conference on Mechatronics Engineering (ICOM)*; **2024**; pp. 127–132. https://doi.org/10.1109/ICOM61675.2024.10652287.
42. **Sarkar, S.; Jiang, J.; Tsui, C.-Y.; Ki, W.-H.** PRINCE Cipher and eFUSE-Based Embedded Encryption System for Optical Nerve Stimulator. *IEEE Sens. J.* **2024**, *PP*, 1–1. https://doi.org/10.1109/JSEN.2024.3439614.
43. **Sabban, A.** Novel Meta-Fractal Wearable Sensors and Antennas for Medical, Communication, 5G, and IoT Applications. *Fractal Fract.* **2024**, *8*, 100. https://doi.org/10.3390/fractalfract8020100.

 doi:10.20944/preprints202501.2331.v1