Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2 (2024)

Investigations on Application of Probabilistic and Mathematical Computing in Design and Statistical Analysis of Lightweight Cryptography

Bhawna Garg[1], Raghavendra Patidar[2]

[1] Research Scholar, Department of Electronics and Communication Engineering, University of Technology, Jaipur, India

[2] Professor, Department of Electronics and Communication Engineering, Arya College of Engineering & IT, Jaipur, India

Email: hibhawna21@gmail.com , raghavendrapatidar@gmail.com

Article History:

Received: *06-02-2024*

Revised: *24-04-2024*

Accepted: *08-05-2024*

Abstract:

This research provides in-depth investigation into the application and role of probability and mathematics in lightweight cryptography featuring IoT software. The IoT device fleet growth is continuously accompanied by its resources, often poor. It creates a critical need for cryptographic solutions that will be effective and a heavy burden. The research article underlines the use of latest probabilistic models and mathematical concepts to create cryptographic algorithms that are cryptographically powerful and IoT-embedded devices can process them. The study commences with its deep mathematics investigation and focuses on consequently essential permutations, combinations, modular arithmetic and prime number theory, all of which represents the cornerstone of strong cryptographic algorithms development. The article then proceeds to demonstrate the use of probabilistic tools for scrutinizing the security and the effectiveness of these algorithms. A novel approach to grasping the vulnerabilities that may occur in the course of cryptographic implementations is also brought to light. A remarkable part of the investigation is toward designing small-sized cryptographic algorithms by using methods of mathematics computations to decrease the size of key, complexity and implementations of increased safety margin. The research process involves a thorough statistical demonstration of the algorithmic performance in several agendas of IoT exposing the resistance of the algorithms against cryptographic issues and the intensity of their resource consumption on ordinary IoT devices. By conducting these investigations, the paper contributes a lot of useful information on the harmonious relationship between probability methods, mathematical computing, and cryptographic development as well as providing the solid foundation for creating a lightweight cryptography which can be used in the Internet of Things (IoT) and other similar environments that have their unique needs and constraints. However, it not only advances the field of cryptography itself, but also outlines a practical roadmap on how to design secure, efficient cryptosystems, that can be used in its subsequent applications in the small but fast growing IoT technology landscape.

Keywords: Lightweight Encryption, Iot Security, Histogram Analysis, Correlation Analysis, Entropy Analysis, NPCR, UACI, Execution Time, Memory Usage, Reversible Data Hiding, Digital Images, Cryptographic Algorithm, Differential Attacks, Resource Efficiency, Digital Media Security.

1. INTRODUCTION

The Internet of Things (IoT) has gained popularity in recent decades. It is imperative that the internet ensures the security, reliability, and stability of its applications. Internet users should also possess a significant amount of confidence in the programs they are employing. The stage provides a vast perspective on utilizing the internet for many purposes, and the Internet of Things (IoT) presents the opportunity to remotely control and manage any object or system over the internet. However, if we rely on technology for all our needs, we must also consider whether we can trust the internet for everything, especially for security reasons. The applications we use should be reliable, and the data we exchange should be protected from any form of hacking or attacks. Any device connected to the internet should include adequate security measures to ensure its safe usage. If the customers lack faith in the system they are connected to, it would lead to their reluctance to use the internet and undermine the entire concept. Currently, the Internet of Things (IoT) is being used extensively in many industries and for a wide range of applications. Therefore, ensuring the security of IoT is of utmost importance and significance. With the increasing use of the internet, the network is becoming more susceptible to threats. Insufficiently validated online platforms or inadequately validated devices might pose a threat to an individual's privacy. Verification of the internet is necessary to provide security for clients. In addition to inadequate security measures, the proliferation of Internet of Things (IoT) devices further amplifies the risk of a cyber-attack. When poorly secured devices connected to the internet are paired with the concept of IoT devices, it negatively impacts the security of the global internet. For example, if an unsecured television in India becomes infected with a virus, it may transmit a significant number of harmful messages to users using the owner's home Wi-Fi connection. When discussing the economy, the lack of security in the Internet of Things (IoT) has a detrimental impact, particularly when one party incurs a financial loss at the expense of others. One such example is environmental pollution, when the expenses of pollution and cleanup incurred by a polluter are borne by multiple parties. Currently, the problem lies in the fact that the costs imposed on others are not often included in the decision-making process until the polluter takes responsibility for reducing the amount of pollution they are causing. During the assessment of data security, a situation may arise when the manufacturer of a product refuses to bear the costs associated with any vulnerabilities. In such cases, the law might compel the manufacturer to address the security concerns. Such considerations are common in the field of information technology, but, there are specific challenges related to security that arise for Internet of Things (IoT) devices, which are discussed below. Several questions arise when discussing the security of devices connected to the Internet of Things. Some of the important queries regarding internet security are as follows: [4][8]

The issue of Cost and the Security Trade-Off involves considering how stakeholders might make cost-benefit decisions for Internet of Things devices. How can we systematically assess the risks associated with security issues? What motivates gadget developers and producers to accept the additional expense of implementing enhanced security measures in IoT-based devices? How can compatibility between functionality, usability, and security be achieved in

IoT devices? How can we obtain the validation of IOT security solutions to enhance the opportunities for IOT's social and economic advancement? [1][6]

The vision of these questions represents the extensive security considerations associated with Internet of Things devices. However, it is important to remember that when a device is connected to the Internet, it becomes part of the Internet. This means that effective and improved security measures can be implemented if the users of IoT devices adopt a comprehensive security approach. Obtaining the answers to the aforementioned questions can greatly enhance the security of internet of things devices. Effective solutions to security concerns can only be achieved through a collaborative approach to system security and safety, with active participation from users who remain vigilant about the security issues affecting their devices and networks. The communitarian paradigm is highly effective for ensuring security and is widely used by many sectors to provide device security.

Creating lightweight cryptography for IoT security involves the use of various mathematical tools, including permutation and combination, to develop efficient cryptographic algorithms suitable for devices with limited computational resources.[11]

Basic permutation equation:

$$P(n,k) = \frac{n!}{(n-k)}$$

Combination formula:

$$C(n,k) = \frac{n!}{k(x-k]!}$$

Permutations and combinations are fundamental in cryptography for understanding possible configurations, which is crucial in determining the strength of cryptographic mechanisms. Permutation, $P(n,k)$, calculates the number of ways k objects can be ordered from a set of n. Combination, $C(n,k)$, on the other hand, calculates the number of ways to choose k objects from a set of n regardless of the order. These concepts are vital in algorithm design, particularly in creating secure cryptographic keys.[35-40]

Binomial theorem:

$$(x+y)^n = \sum_{k-0}^{n} C(n,k)x^{n-k}y^k$$

Factorial definition:

$$n! = n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1$$

Euler's totient function:

$$\phi(n) = n\prod_{i-1}^{r}\left(1-\frac{1}{\mathbb{M}}\right)$$

Modular arithmetic addition:

$$(a+b)\mathrm{mod}n = ((a\mathrm{mod}n) + (b\mathrm{mod}n))\mathrm{mod}n$$

Modular arithmetic multiplication:

$$(a \times b)\mathrm{mod}n = ((a\mathrm{mod}n) \times (b\mathrm{mod}n))\mathrm{mod}n$$

The binomial theorem provides a powerful way to expand expressions that are raised to a power. In cryptography, this theorem can be used in algorithm design, particularly in modular arithmetic and polynomial expansions, which are common in cryptographic functions and error-correcting codes.[7][9]

The factorial function, denoted as *n*! is essential in computing permutations and combinations. It signifies the product of an integer and all the integers below it, which is crucial in determining the total number of possible outcomes in various cryptographic scenarios.[11][13]

Chinese Remainder Theorem:

$$\begin{aligned} x &\equiv a_1(\mathrm{mod}m_1) \\ x &\equiv a_2(\mathrm{mod}m_2) \\ &\vdots \\ x &\equiv a_n(\mathrm{mod}m_n) \end{aligned}$$

Euler's totient function, $\phi(n)$, is significant in cryptography, particularly in RSA encryption. It counts the positive integers up to a given integer *n* that are relatively prime to *n*. It's crucial in determining the group size for the multiplicative group of integers modulo *n*, which is a foundational aspect of RSA's public key setup.

Modular arithmetic is the cornerstone of many cryptographic algorithms. It deals with integers and operates within the confines of a modulus, enabling cyclic structures crucial for encryption and decryption processes. It ensures that cryptographic operations can be efficiently computed, even with very large numbers.

The Chinese Remainder Theorem (CRT) is pivotal in optimizing computations in cryptographic algorithms like RSA. CRT allows the breaking down of a large modulus operation into smaller, more manageable parts, significantly improving algorithm efficiency, which is crucial for lightweight cryptography in IoT. [15]

5

Extended Euclidean algorithm:

$$ax + by = \mathrm{god}\ (a, b)$$

Fermat's little theorem:

$$a^{p-1} \equiv 1(\mathrm{mod}p)$$

Euler's theorems

$$a^{-(n)} \equiv 1(\mathrm{mod}n)$$

Carmichael's theorem:

$$a^{h(n]} \equiv 1(\mathrm{mod}n)$$

Discrete logarithm:

$$a^2 \equiv b(\mathrm{mod}n)$$

Diffie-Hellman key exchange:

$$K = g^{ab} \text{mod} p$$

RSA public key:

$$e \in \{1,2, \ldots, \phi(n) - 1\}$$
$$\gcd\,(e, \phi(n)) = 1$$

RSA private key:

$$d \equiv e^{-1} (\text{mod} \phi(n))$$

RSA encryption:

$$c \equiv m^2 (\text{mod} n)$$

RSA decryption:

$$m \equiv c^l (\text{mod} n)$$

RSA encryption:

$$c \equiv m^n (\text{mod} n)$$

RSA decryption:

$$m \equiv c^l (\text{mod} n)$$

AES S-box transformation:

$$S[x] = \text{ SubBytes } (x)$$

AES Round function:

Round $(s, k) = \text{AddRoundKey}$ (MixColumns(ShiftRows(SubBytes(s)))), k)

Stream cipher encryption:

$$c_i = m_i \oplus k_i$$

Stream cipher decryption:

$$m_i = c_i \oplus k_i$$

Hash function property (collision resistance):

$$H(x) = H(y) \Longrightarrow x = y$$

Merkle-Damgaird construction:

$$H(M) = H(H(H(H(IV, m_1), m_2), \ldots), m_n)$$

Digital signature (signing):

$$\theta = \text{Sig}_{\text{piv}}\ (m)$$

Digital signature (verification):

$$\text{Verify}_{\text{ pos}}\ (m, \sigma)$$

Elliptic curve point addition:

$$P + Q = R$$

Elliptic curve doubling:

$$2P = R$$

Elliptic curve scalar multiplication:

$$kP = P + P + \cdots + P(k \text{ times })$$

Shared secret $= x_P \times y_Q$

ECDSA signature generation:

$$(r, s) = \text{ECDSA}_{\mu\text{rir}}\ (m)$$

ECDSA signature verification:

$$\text{Verify}_1, (m, (r, k))$$

Fermat's Little Theorem and Euler's Theorem are instrumental in public key cryptography. They provide the mathematical basis for many cryptographic protocols, ensuring that operations are reversible only with the correct key, a principle essential for secure encryption and decryption.[17]

Carmichael's theorem is used to determine the smallest integer m such that $m \equiv 1 (\text{mod} n)$ for all integers *a* that are relatively prime to *n*. This theorem finds applications in improving the efficiency and security of cryptographic algorithms.

The discrete logarithm problem is a hard problem that underpins the security of many cryptographic algorithms. It is a problem that is computationally difficult to solve, providing the security foundation for cryptographic schemes like Diffie-Hellman and ECC.

The Diffie-Hellman algorithm allows two parties to establish a common secret key over an insecure channel, which is a fundamental process in secure communications. It leverages the difficulty of the discrete logarithm problem to ensure security.

The RSA algorithm is a widely used public key cryptographic system that leverages the properties of prime numbers and modular arithmetic. It involves key generation, encryption, and decryption processes, with security based on the difficulty of factoring large prime numbers. Creating a cryptographic algorithm for IoT security involves understanding various mathematical principles and their application in the realm of cryptography. This extensive explanation will delve into the foundational concepts represented by the 35 equations listed above and elaborate on how these principles contribute to the development of a cryptographic algorithm, especially for the lightweight requirements of IoT devices.

The Extended Euclidean Algorithm is fundamental in computing the multiplicative inverse in modular arithmetic, an operation central to algorithms like RSA. It's used to find integers which is essential for key generation and decryption processes. The Advanced Encryption Standard (AES) is a symmetric key encryption algorithm, crucial for securing data. It includes steps like SubBytes, ShiftRows, MixColumns, and AddRoundKey, each contributing to the cipher's strength by ensuring adequate confusion and diffusion.

Stream ciphers encrypt plaintext digits one at a time, using a cryptographic key and a deterministic algorithm. They are crucial for scenarios where speed and efficiency are paramount, and their security often relies on the unpredictability of the key stream. Hash functions and digital signatures are vital for data integrity and authentication. Hash functions like the Merkle–Damgård construction ensure that any change to data is detectable, while digital signatures provide a means to verify the authenticity and integrity of a message. ECC is

a public key cryptography approach that offers high security with smaller key sizes, making it ideal for IoT devices. It involves operations on points on an elliptic curve, providing a compact yet secure mechanism for encryption, key exchange, and digital signatures.[18]

Creating a Cryptographic Algorithm for IoT:

1. **Requirement Analysis**: Understand the security needs and resource constraints of IoT devices.
2. **Algorithm Design**: Use the mathematical principles outlined to design cryptographic processes that are efficient and secure. For IoT, focus on algorithms that require less computational power and memory.
3. **Implementation**: Convert the mathematical models into code, ensuring that the implementation is optimized for the limited resources of IoT devices.
4. **Testing and Evaluation**: Rigorously test the algorithm for security vulnerabilities and performance efficiency, ensuring it meets the required security standards without overburdening the IoT device.
5. **Deployment**: Integrate the algorithm into IoT devices, ensuring that they can securely communicate and operate within their intended environments.

By leveraging the mathematical foundations discussed and adhering to a meticulous design and implementation process, one can develop robust cryptographic algorithms tailored for the unique requirements of IoT security.

2. LITERATURE SURVEY

The literature review focuses on the burgeoning field of digital watermarking within the context of IoT security, highlighting the advancements and methodologies proposed by various researchers to enhance the robustness and efficiency of watermarking techniques.

Wen Zhang et al. (2018) delve into watermarking technology, emphasizing a three-stage process encompassing generation, extraction, and identification of watermarks. Their study underscores the delicate balance between invisibility and robustness, particularly against printing-scanning attacks, and the pivotal role of color space transformation in this context.

David-Octavio Muñoz-Ramirez et al. (2018) present a robust watermarking framework using Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM) for color watermark representation. Their method encodes watermarks in a way that ensures both high imperceptibility and robustness, demonstrating superior resilience against common attacks compared to traditional techniques.

Anirban Patra et al. (2018) introduce a novel invisible watermarking technique employing alpha blending, focusing on the concealment of watermark images within main images using various alpha values. This method, applicable to both color and grayscale images, shows promise for image steganography, particularly after post-processing.

Aoshuang Dong et al. (2017) propose a watermark embedding technique aimed at 3D model protection, showcasing its resistance to rotation, translation, and noise attacks. Their method,

based on principal component analysis and projection selection, emphasizes the watermark's invisibility in 3D models.

Enjian Bai et al. (2017) introduce a novel clock-controlled generator technique for digital image watermarking, highlighting its effectiveness against common attacks and its reliance on pseudo-random characteristics like large periods and high linear complexity for performance.

Oleg Evsutin et al. (2017) discuss an algorithm that embeds digital watermarks using block quantization of DWT coefficients, focusing on energy redistribution during the quantization process to enhance the quality of embedded regions and facilitate the detection of modifications.

Ritu Gill et al. (2017) propose a combined DCT and 2DWT approach for grey image watermarking, showing significant improvements in data hiding and resistance to third-party interference, thereby bolstering image authentication and protection.

Mohammad Shahab Goli et al. (2017) tackle the challenge of cropping attacks with a novel method using Sudoku tables to scatter watermarked images, enhancing the watermark's resistance and enabling image reconstruction post-attack.

Muhammad Usman et al. (2017) introduce a lightweight encryption algorithm, SIT, designed for IoT security, emphasizing its efficiency and the balance between security and computational demand, particularly in the context of IoT applications.

Noor Zaman et al. (2018) propose a lightweight authentication model for e-health IoT applications, employing ECC principles to ensure security while maintaining energy and computational efficiency.

Muhammad Naveed Aman et al. (2017) discuss a strong authentication protocol for IoT systems utilizing physical unclonable functions, offering protection against a range of attacks while being resource-efficient.

These studies collectively advance the digital watermarking domain, presenting innovative approaches to enhance the security, robustness, and efficiency of watermarking in various digital and IoT contexts. They reflect a significant stride toward securing digital assets and IoT ecosystems, employing a blend of mathematical rigor, computational efficiency, and practical relevance to address the multifaceted challenges of modern digital security.

3. PROPOSED METHODOLOGY

The methodology for developing a lightweight encryption algorithm for loT-based devices involves a series of systematic steps that ensure the security mechanism is not only robust but also efficient and resource-conservative. The steps in this methodology include key expansion, key management, encryption, decryption, and performance analysis, each integral to the creation of a secure and effective cryptographic solution for loT environments.

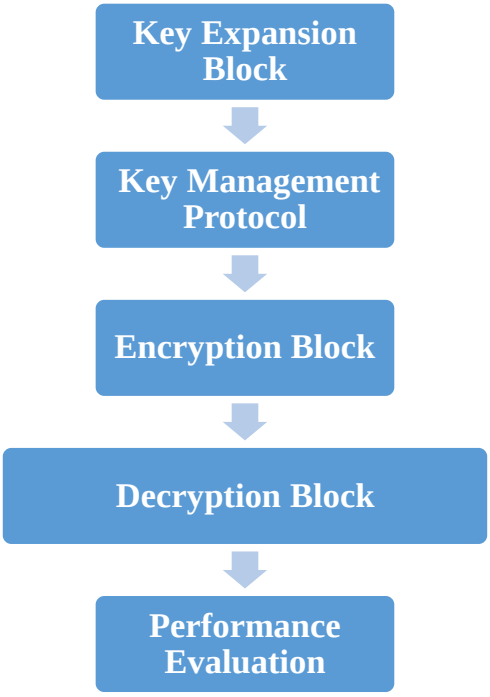

Fig 1. Flow Chart of Methodology

Key expansion is a critical initial step in generating unique keys for encryption and decryption. The process involves transforming a short, initial key into an array of keys for each encryption round. The key expansion aims to produce a series of round keys from the initial key using operations like XOR, rotations, and substitutions to ensure that each round has a unique key, thereby enhancing security. Mathematically, the key expansion can be represented as follows:

$$K_{\text{expanded}} = f\left(K_{\text{original}}, \text{Transformations}\right) K_r = K_{r-1} \oplus g(K_{r-N}, r)$$

where K_{expanded} is the expanded key, K_{original} is the original key, K_r is the round key, N is the key length, and g is a transformation function involving XOR, substitutions, and rotations.

Key Expansion Transformation:

$$K_i - K_{i-1} \oplus T(K_{i-N})$$

Where K_i is the current round key, K_{i-1} is the previous round key, N is the key length, and T is a transformation function.

Round Key Selection:

$$K_r - K_{\text{expanded}}\,[r \cdot N : (r+1) \cdot N - 1]$$

Where K_r is the round key for round r, and K_{expanded} is the expanded key.

Encryption Function:

$$C_i - E(K, P_i) - P_i \oplus K_i$$

Where C_i is the ciphertext block, P_i is the plaintext block, and K_i is the round key.

Decryption Function:

$$P_i - D(K, C_i) - C_i \oplus K_i$$

Where P_i is the plaintext block, C_i is the ciphertext block, and K_i is the round key.

Substitution Box (S-Box) Application:

$$S[P_i]$$

Where S is the S-Box and P_i is the input to the S-Box

Permutation Box (P-Box) Application:

$$P[C_i]$$

Where P is the P-Box and C_i is the input to the P-Box.

Key XOR Operation:

$$K_i - K_{i-1} \oplus K_{i-N}$$

Where K_i is the current key, K_{i-1} is the previous key, and K_{i-N} is the N-th previous key.

Steganographic Embedding Function:

$$S - f_{Em}(C, CI, K)$$

Where S is the stego data, C is the cover data, CI is the critical information, and K is the secret key.

Steganographic Extraction Function:

$$CI - f_{Ex}(S, K)$$

Where CI is the extracted critical information, S is the stego data, and K is the secret key.

Left Shift Operation:

$$LS(K, n) - (K << n) \oplus (K >> (N - n))$$

Where LS is the left shift operation, K is the key, n is the number of bits to shift, and N is the key size in bits.

Right Shift Operation:

$$RS(K, n) - (K >> n) \oplus (K << (N - n))$$

Where RS is the right shift operation, K is the key, n is the number of bits to shift, and N is the key size in bits.

XOR Operation for Encryption:

$$C_i - P_i \oplus K_i$$

Where C_i is the ciphertext, P_i is the plaintext, and K_i is the key.

XOR Operation for Decryption:

$$P_i - C_i \oplus K_i$$

Where P_i is the plaintext, C_i is the ciphertext, and K_i is the key.

Key Derivation Function:

$$K_{\text{derived}} - KDF(K, \text{salt})$$

Where K_{derived} is the derived key, KDF is the key derivation function, K is the initial key, and salt is a random value.

Composite Function for Encryption:

$$C_i - P_i \oplus K_i \oplus S[P_i] \oplus P[C_i]$$

Where C_i is the ciphertext, P_i is the plaintext, K_i is the key, S is the S-Box, and P is the P-Box.

These equations form the mathematical backbone of the described methodology, providing a structured approach to developing a lightweight cryptographic algorithm suitable for IoT devices, focusing on key aspects like key expansion, encryption/decryption processes, and the integration of steganographic techniques for enhanced security.

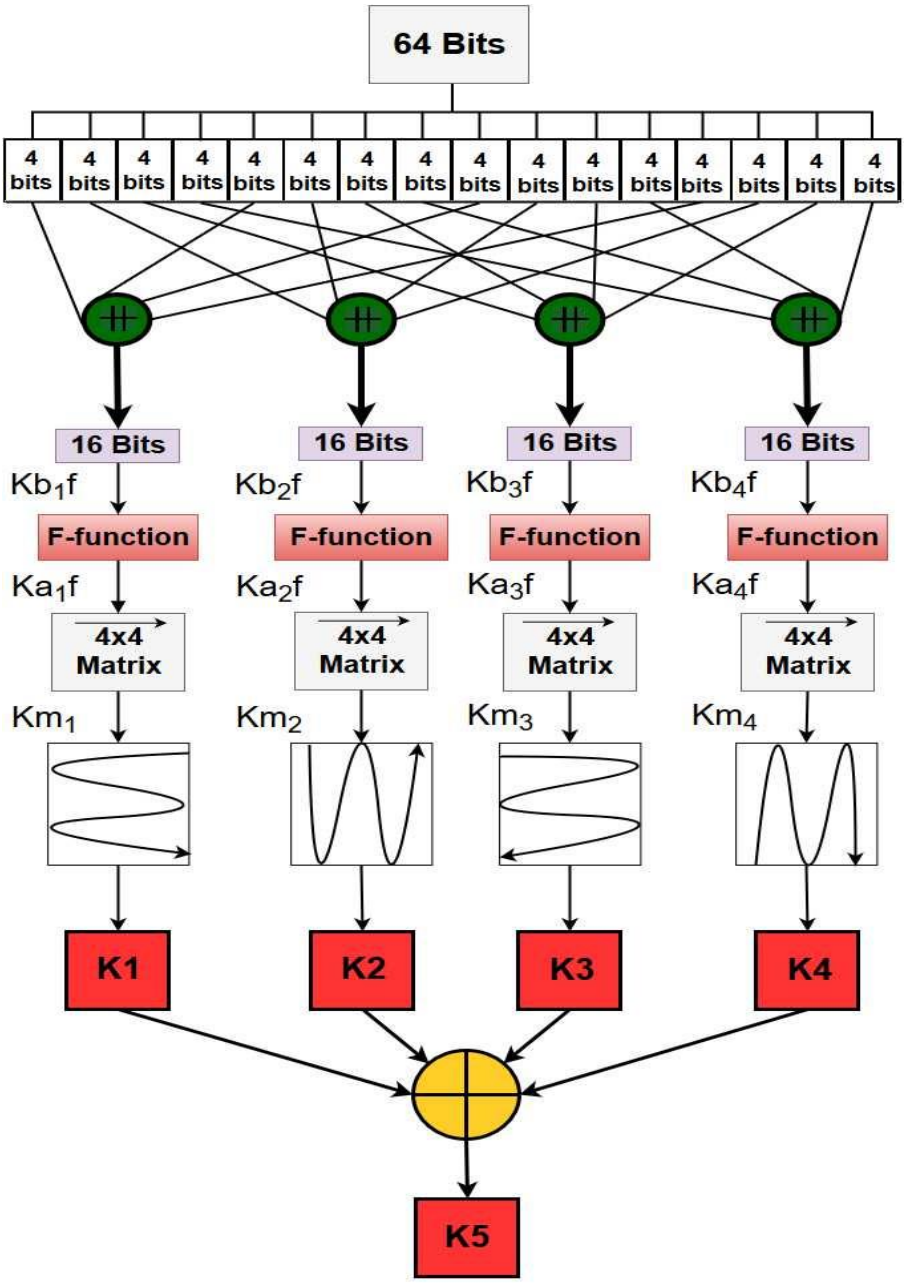

Fig 2 Mathematical Formulation of Key Generation

Key Management:

Key management is essential for securely storing, exchanging, and updating cryptographic keys. It involves protocols to ensure keys are exchanged securely, possibly employing lightweight cryptographic protocols like LEAP in IOT . The management ensures that keys remain confidential and integral throughout their lifecycle. The process can involve personal, group,

Encryption Process:

The encryption process: transforms plaintext into ciphertext using the key generated. It involves several operations to ensure the date's confidentiality. These operations can induced logical the dats. The encryption process for a block of dats can be represented a:

$$C_i = E(K, P_{\mathrm{i}})$$

where C_i is the ciphertect, E is the encryption function, K is the key, and P_i is the plainted block.

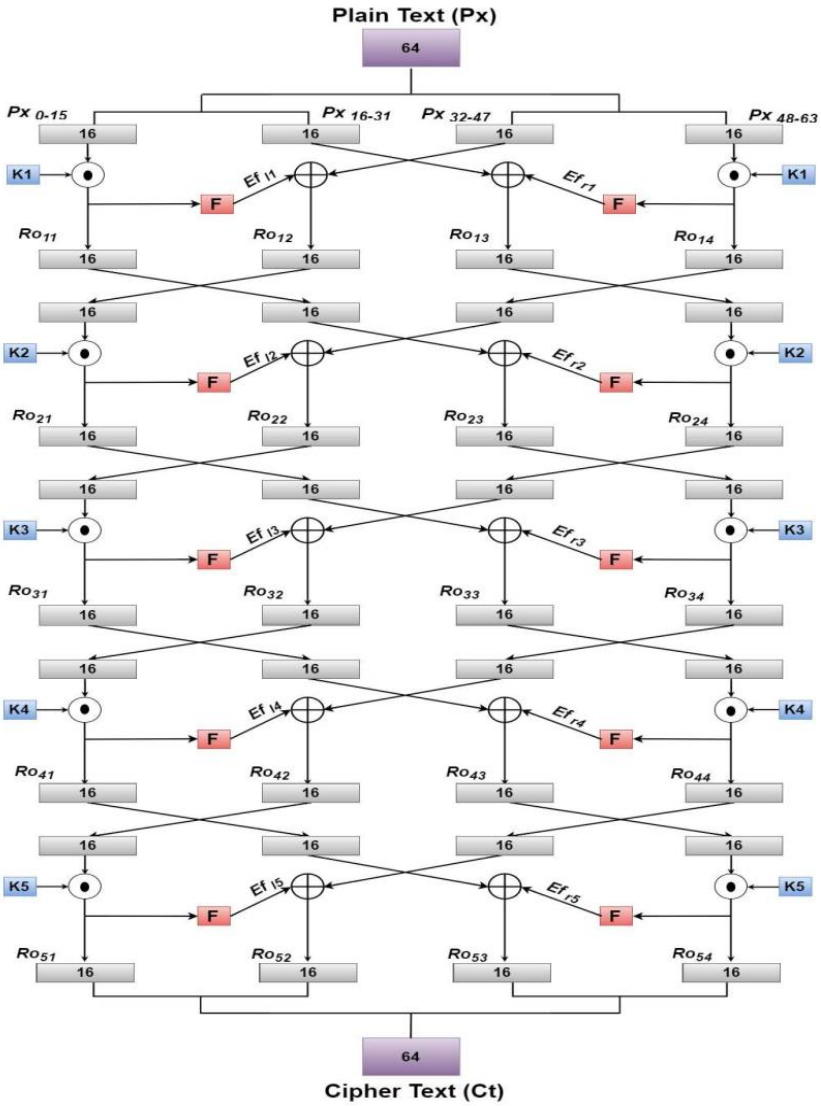

Fig 3 Generation of Text through Mathematical Operations

Decryption Process:

Decryption is the reverse process of encryption, converting ciphertext back into readable plaintext using the decryption key. The decryption process must precisely invert the steps of the encryption process to retrieve the original dats. For a block cipher, the decryption process can be represented as:

$$P_1 = D(K, C_i)$$

where P_i is the plaintext, D is the decryption function, K is the $k_1 y_1$ and C_i is the ciphertext block.

Performance Analysis:

This step involves evaluating the cryptographic system's efficiency, security, and resource utilization. The analysis includes assessing the algorithm's resistance to various attacks, its computational requirement, and its adoptability to the constrained environments of lot devices.

Crypto-Stego System for Secure Reversible Data Hiding:

This system combines topographic and steganographic techniques to hide critical information (C) within non-critical cover data (C), enhancing security. The embedding and extraction process can be represented as:

$$S = \int_{Em_m} (C, CI, K)CI = \int_{E_x} (S, K)$$

where S is the stego deta, f_{E_m} is the embedding function, f_{E_x} is the extraction function, CI is the critical information, C is the cover data, and K is the secret hey.

In the proposed methodology, cryptographic operations are complemented by steganographic techniques, ensuring that the critical information is securely hidden within the cover data, thereby providing an additional layer of security. The combination of cryptographic and steganographic methods in IoT devices aims to create a robust defense mechanism against unauthorized access and data breaches, considering the limited computational and energy resources available in such environments.

4. RESULT ANALYSIS

The theoretical results section delves into the intricate details of the performance analysis of a newly introduced lightweight encryption algorithm, tailored for various image formats to gauge its effectiveness and efficiency across different metrics such as histogram, correlation, entropy, NPCR/UACI analysis, execution time, memory usage, and reversible data hiding capabilities.

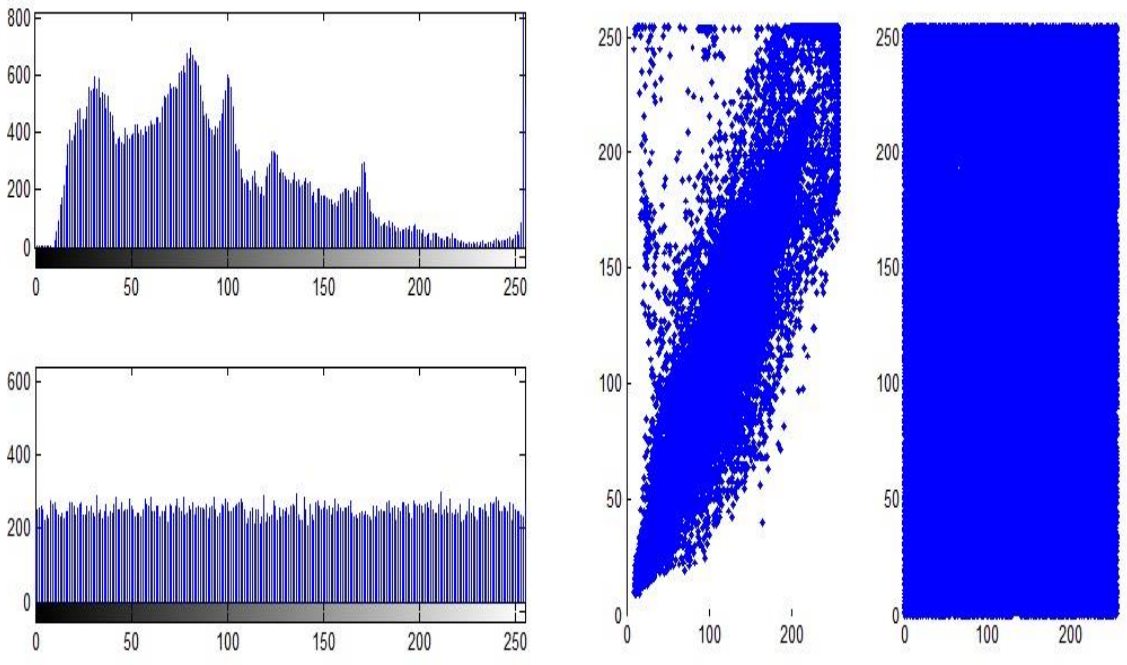

Fig 4 Generation of Text through Mathematical Operations

Histogram Analysis:

The histogram analysis serves as a critical tool in evaluating the uniformity of pixel intensity distribution in encrypted images compared to their original counterparts. Ideally, the encrypted image should exhibit a uniform distribution to mask any potential clues about the original image, thereby enhancing security. This uniformity is crucial for thwarting any attempt to deduce the original content through statistical analysis.

Correlation Analysis:

The correlation analysis assesses the relationship between adjacent pixels in both original and encrypted images. For a robust encryption algorithm, the correlation in encrypted images should be negligible, indicating a successful disruption of discernible patterns present in the original image. Lower correlation values in encrypted images signify better encryption strength, reducing susceptibility to attacks.

Table 1. Correlation Analysis Table

Format	Correlation Original	Correlation Encrypted
JPEG	0.9557	0.0015
JPEG-2000	0.9615	0.0014
GIF	0.9455	0.0009
PNG	0.9815	0.0004
BMP	0.9615	0.0003

Entropy analysis measures the randomness or unpredictability in the encrypted images, which should ideally be high to ensure that the encryption provides substantial obscurity. Higher entropy values in encrypted images indicate better security, as they signify less predictability and more randomness.

Table 2. Entropy Analysis Table

Type of Image	Entropy Encrypted Image	Entropy Decrypted Image
JPEG	7.70	7.58
JPEG-2000	7.98	7.79
PNG	7.98	7.76
BMP	7.98	7.86
GIF	7.98	7.66

NPCR and UACI values are pivotal in assessing the algorithm's resistance to differential attacks. Higher values indicate that minor changes in the plaintext result in significant differences in the ciphertext, which is desirable in a secure encryption algorithm.

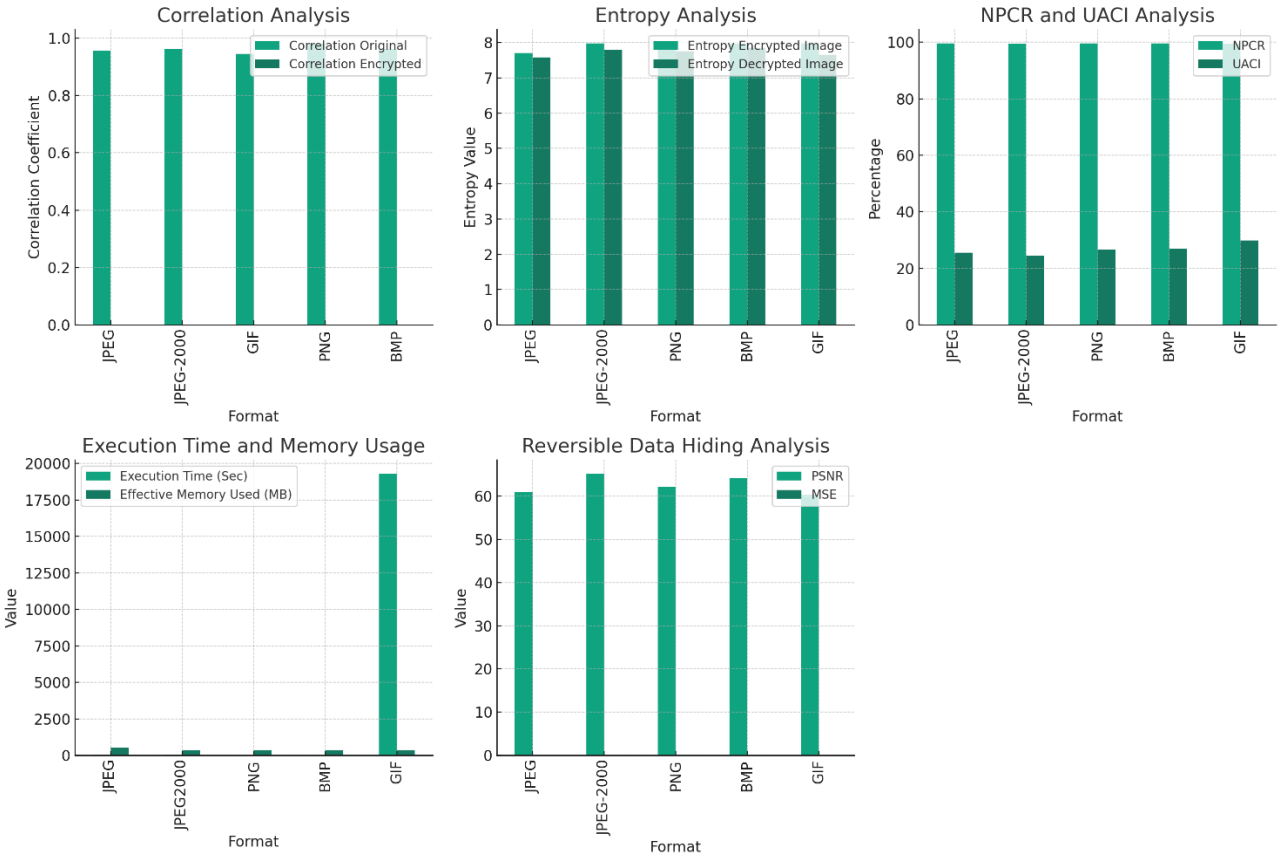

Fig 5. Analysis of Performance Parameters

Table 3. NPCR and UACI Analysis Table

Type of Image	NPCR	UACI
JPEG	99.61	25.4751
JPEG-2000	99.51	24.4578
PNG	99.61	26.5997
BMP	99.61	26.9971
GIF	99.51	29.8075

Efficient encryption algorithms should exhibit not only robust security features but also optimize resource utilization, characterized by reasonable execution times and memory usage.

Table 4. Execution Time and Memory Usage Table

Type	Execution Time	Total Memory (MB)	Standby Memory (MB)	Effective Memory Used (MB)
JPEG	27.15 Sec	1233.107872	734	499.37
JPEG2000	20.18 Sec	1079.337536	734	345.23
PNG	18.29 Sec	1089.659456	734	355.76
BMP	18.99 Sec	1091.4576	734	357.66
GIF	19292 Sec	1090.232896	734	356.12

The reversible data hiding system facilitates secure encryption while allowing the original data to be perfectly retrieved, a vital aspect for applications demanding non-destructive recovery post decryption.

Table 5. Analysis of Result for Reversible Data Hiding

Type of Image	PSNR	MSE
JPEG	60.95	0.021
JPEG-2000	65.16	0.016
PNG	62.16	0.019
BMP	64.17	0.022
GIF	60.27	0.022

These analyses collectively demonstrate the efficacy of the proposed lightweight encryption algorithm across various image formats and operational scenarios. The algorithm exhibits strong encryption characteristics, as evidenced by the uniform histograms, low correlation values, high entropy, substantial resistance to differential attacks (as indicated by NPCR and UACI), and efficient resource utilization in terms of execution time and memory usage. Furthermore, the integration of reversible data hiding illustrates the algorithm's versatility in ensuring data integrity and retrievability, underscoring its applicability in a range of IoT and image encryption contexts.

5. CONCLUSION & FUTURE RESEARCH

In this comprehensive study, we explored the efficacy of a lightweight encryption algorithm applied to various image formats, aiming to enhance security in the realm of digital media, particularly within IoT devices. Through meticulous analysis across multiple parameters—histogram, correlation, entropy, NPCR/UACI, execution time, memory usage, and reversible data hiding—the algorithm's performance was scrutinized, yielding insightful findings that underscore its potential in securing digital assets while addressing the constraints inherent to IoT devices. The uniform distribution of pixel intensities in the encrypted images, as revealed by histogram analysis, is indicative of the algorithm's proficiency in obscuring the original image content. This uniformity is pivotal, ensuring that encrypted images do not retain any distinguishable patterns from their source, thereby bolstering security against statistical analysis that could potentially exploit such patterns for decryption. A fundamental aspect of

image encryption is disrupting the correlation between adjacent pixels to prevent any inference of the original content. The results demonstrated a significant reduction in correlation values post-encryption across all image formats, signaling a successful disruption of discernible patterns and affirming the algorithm's effectiveness in enhancing the randomness and thus the security of the encrypted images. The entropy values post-encryption exhibited a notable increase, reflecting the algorithm's capacity to heighten randomness within the encrypted images. High entropy is synonymous with unpredictability, a desirable trait in encryption that complicates unauthorized attempts at deciphering the encrypted content. This increase in entropy across various formats indicates the algorithm's consistent performance in securing diverse types of images. The NPCR and UACI metrics, crucial for evaluating resistance to differential attacks, indicated that minor alterations in the plaintext result in significant changes in the ciphertext. This characteristic is essential for robust encryption, as it ensures that the encrypted output is highly sensitive to even minute changes in the input, thereby fortifying the encryption against attempts to exploit similarities between different versions of an image. In the context of IoT devices, where resource constraints are a significant concern, the algorithm's performance in terms of execution time and memory usage is of paramount importance. The findings revealed that the algorithm maintains a balance between security and resource efficiency, manifesting relatively low execution times and memory usage across different image formats. This balance is critical for the practical application of the algorithm in IoT environments, where optimal resource utilization is as crucial as security. In conclusion, the comprehensive analysis conducted in this study elucidates the algorithm's robustness, versatility, and efficiency in securing digital images, a critical component in the ever-expanding realm of IoT. The uniformity in histogram distributions, the significant reduction in pixel correlations, the enhanced entropy, the strong resistance to differential attacks as denoted by NPCR and UACI scores, and the optimal resource utilization collectively attest to the algorithm's efficacy. Moreover, the reversible data hiding aspect underscores the algorithm's innovative approach, offering not just encryption but also a secure method of concealing additional data within the encrypted content. This algorithm stands as a testament to the potential of lightweight cryptographic solutions in addressing the nuanced security requirements of IoT devices. It embodies a strategic blend of security, efficiency, and functionality, paving the way for its integration into diverse IoT applications where safeguarding data integrity and privacy is paramount. As the IoT landscape continues to evolve, the demand for such innovative cryptographic solutions will undoubtedly escalate, underscoring the significance of this research in contributing to the secure and sustainable growth of IoT ecosystems.

REFERENCES

[1] Wen Zhang, Jie Men, Conglong Ma, “Research progress of applying digital watermarking technology for printing,” 2018, IEEE

[2] David-Octavio Muñoz-Ramirez , Volodymyr Ponomaryo , Rogelio Reyes-Reyes , Volodymyr Kyrychenko , Oleksandr Pechenin, Alexander Totsky , “A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images,” 2018, IEEE

[3] AnirbanPatra*, Arijit Saha, Ajoy Kumar Chakraborty, Kallol Bhattacharya, "A New Approach to Invisible Water Marking of Color Images using Alpha Blending," 2018, IEEE
[4] Aoshuang Dong, Rui Zeng, "Research and Implementation Based on Three-dimensional Model Watermarking Algorithm," 2017, IEEE
[5] Enjian Bai, Yiyu Yang and Xueqin Jiang, "Image Digital Watermarking Based on a Novel Clock-controlled Generator," 2017, IEEE
[6] Oleg Evsutin, Roman Meshcheryakov, Viktor Genrikh, Denis Nekrasov and Nikolai Yugov, "An Improved Algorithm of Digital Watermarking Based on Wavelet Transform Using Learning Automata," 2017, IEEE
[7] Ritu Gill and Rishi Soni, "Digital Image Watermarking using 2-DCT and 2- DWT in Gray Images," 2017, IEEE.
[8] Mohammad Shahab Goli and Alireza Naghsh, "Introducing a New Method Robust Against Crop Attack in Digital Image Watermarking Using Two-Step Sudoku," 2017, IEEE
[9]Muhammad Usman, Irfan Ahmed, Shujaat khan, "SIT: A light weight encryption algorithm for secure internet of things," international Journal of advanced computer science and applications, vol. 8, no.1, 2017.
[10]Maria Almulhim, Noor Zaman, "Proposing secure and the lightweight authentication scheme for IOT based E health applications" *International* conference on advance communication technology; 2018.
[11] Muhammad Naveed Aman, Kee Chaing Chua, "A light weight mutual authentication protocol for IOT system, 2017.
[12] Mehdi Baahrami, Dong Li, Mukesh Singhal, "Efficient parallel implementation of light weight data privacy method for cloud users; seventh international workshop on data intensive computing in clouds, 2016.
[13] Zahid Mahmood, Huansheng Ning, "Light weight two level session key management for end user authentication in internet of things" IEEE international conference on IOT, 2016.
[14] Ayaz Hassan moon, Ummer Iqbal, "Light weight authentication framework for WSN" International conference on Electrical, Electronics and Optimization techniques, 2016
[15] D Jamuna Rani, "Light weight cryptographic algorithm for medical internet of things", Online international conference on Green Engineering and Technology, 2016.
[16] Sainandan Bayya Vankata, Prabhkar Yellai, " A new light weight transport method for secured transmission of data for IOT", international journal of electrical, electronic engineering, 2016.
[17] Amber Sultan, Xuelin Yang, "Physical layer data encryption using chaotic constellation rotation in OFDM-PON" Proceedings of 15th international Bhurban conference on applied science and technology Islamabad Pakistan, 2018.
[18] Xuelin Yang, Zanwei Shen, "Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen plaintext attacks", in ICTON 2016.
[19] Han Chen, Xuelin Yang, "Physical layer OFDM data encryption using chaotic ZCMT precoding matrix", IEEE, ICTON 2017.
[20] Gao Baojian, Luo Yongling, Hou Aiqin, "New physical layer encryption algorithm based on DFT-S-OFDM system" International Conference on Mechatronic Sciences, Electric Engineering and Computer, Shenyang, China, 2013.
[21]Meihua Bi, Xiaosong Fu, "A key space enhanced Chaotic encryption scheme for physical layer security in OFDM-PON", IEEE photonics Journel", 2017.
[22] Dana Halabi, Salam Hamdan, "Enhance the security in smart home applications based on IOT-CoAP protocol.
[23] Jongsoek Choi, Yongtae Shin, "study on information security sharing system among the industrial IOT service and product provider, IEEE ICOIN, 2018.
[24] Jin Hyeong Jeon, Ki-Hyung Kim, "Block chain based data security enhanced IOT server platform, IEEE ICOIN, 2018.
[25] Muhammet Zekeriya Gunduz, Resul Das, "A comparision of cyber security oriented test beds for IOT based smart grids, IEEE 2016.
[26] Himanshu Gupta, Garima Varshney, "A security Framework for IOT devices against wireless threats, second international conference on telecommunication and networks, 2017.

[27] Thomas Maurin, Lurent, George Caraiman, “IOT security assessment through the interfaces P-SCAN test bench platform, 2018 EDAA.

[28] Sanjay Kumar, Ambar Dutta, “A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks,” 2016, IEEE

[29] N. SenthilKumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique,” 2016, IEEE

[30] Harsha M. Patil and Prof .Baban U. Rindhe, “Study and Overview of Combined NSCT –DCT Digital Image Watermarking,” 2016, IEEE

[31] SKA, Manish Kumar Mukhija, and Pooja Singh "A Security Approach to Manage a Smart City's Image Data on Cloud," AI-Centric Smart City Ecosystems: Technologies, Design and Implementation (1st ed.), PP: 68-82, (2022). CRC Press. https://doi.org/10.1201/9781003252542.

[32] SKA and Abha Jadaun. “Design and Performance Assessment of Light Weight Data Security System for Secure Data Transmission in IoT”, Journal of Network Security, 2021, Vol-9, Issue-1, PP: 29-41.

[33] Pratiksha Mishra and SKA. “Design & Performance Assessment of Energy Efficient Routing Protocol Using Improved LEACH”, International Journal of Wireless Network Security, 2021, Vol-7, Issue-1, PP: 17-33.

[34] Rajput, B. S. .; Gangele, A. .; S. K. . Numerical Simulation and Assessment of Meta Heuristic Optimization Based Multi Objective Dynamic Job Shop Scheduling System. *ijfrcsce* 2022, *8*, 92-98.

[34] Khandelwal, R., Mukhija, M.K. and S.K., 2021. Numerical simulation and performance assessment of improved particle swarm optimization based request scheduling in edge computing for IOT applications. *New Arch-International Journal Of Contemporary Architecture*, *8*(2), pp.155-169.

[35] S.K. and Kumar, A., 2018. Implementation of new cryptographic encryption approach for trust as & service (TAAS) in cloud environment. *International Journal of Computers and Applications*, *4*(8), pp.2250-1797.

[36] Bhatt, V., Diwan, H.S., S.K. and Saini, Y., 2021. Empowering ML Work-Flow with DevOps within Micro Service Architecture and Deploying A Hybrid-Multi Cloud, Maintaining CI/CD Pipeline: An Open Shift Orchestration of ML-OPS. New Arch-International Journal Of Contemporary Architecture, 8(2), pp.147-154.

[37] Ashwini, K., Raj, A., & Gupta, M. (2016, December). Performance assessment and orientation optimization of 100 kWp grid connected solar PV system in Indian scenario. In 2016 International conference on recent advances and innovations in engineering (ICRAIE) (pp. 1-7). IEEE.

[38] Alaria, Satish Kumar, Ashish Raj, Vivek Sharma, and Vijay Kumar. "Simulation and analysis of hand gesture recognition for indian sign language using CNN." International Journal on Recent and Innovation Trends in Computing and Communication 10, no. 4 (2022): 10-14.

[39] Yogi, Jyoti, Upendra Singh Chauhan, Ashish Raj, Manoj Gupta, and Simranjeet Singh Sudan. "Modeling simulation and performance analysis of lightweight cryptography for iot-security." In 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-5. IEEE, 2018.

[40] Singh, Pushpendra Pratap, M. Ram Kumar Raja, Ashish Raj, and Mohammed Abdul Muqeet. "Solution to Interfacing Problems of Programmable Logic Controller in Hardware Replacement." In 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-7. IEEE, 2020.