Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Lightweight DNA-Chaos Hybrid Encryption Framework for Real-Time IoT Image Security

Mohammad Ubaidullah Bokhari[1], Azizur Rahman[2], Shahnwaz Afzal[3], Md. Zeyauddin[4]
[1,2,3,4] *Department of Computer Science, Aligarh Muslim University, India, 202002*
Corresponding author: Azizur Rahman (gl1685@myamu.ac.in)

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices—projected to exceed 40 billion by 2030 and generate over 175 zettabytes of data—makes the need for encryption solutions that are both secure and resource-efficient more critical than ever. Traditional cryptographic algorithms such as AES, DES, and RSA, while highly secure, are often too computationally heavy for low-power IoT environments. In this study, we present a lightweight and high-security image encryption framework that integrates DNA computing with two-dimensional chaotic maps, specifically tailored for real-time IoT applications. The proposed method dynamically encodes image pixels into DNA sequences, generates chaotic key streams, and performs nucleotide-level operations to achieve high randomness, strong diffusion, and confusion. The framework, implemented in Python 3.12 using NumPy and Pillow, was evaluated on 256 × 256 RGB images. It achieved encryption and decryption times of 68 ms and 65 ms, well within real-time processing limits, and delivered a Peak Signal-to-Noise Ratio (PSNR) of 46.82 dB and a Structural Similarity Index (SSIM) of 0.9874, indicating near-perfect image reconstruction. Statistical and differential attack resistance was confirmed through an NPCR of 99.61%, UACI of 33.75%, and histogram entropy of 7.98 bits/pixel. With a low computational footprint—consuming only 50 MB of RAM and 20% CPU - the proposed framework is ideal for edge-based IoT deployments, including smart surveillance, wireless sensor networks, and medical image transmission. This work provides a balanced solution to the dual challenges of robust security and lightweight performance, making it a promising candidate for next-generation secure IoT communications.

Keywords: DNA Computing, IoT Security, Image Encryption, Chaotic Maps, Lightweight Cryptography, Real-Time Processing, Medical Imaging

1. INTRODUCTION

The Internet of Things (IoT) is rapidly transforming the way people interact with the physical and digital worlds. It connects billions of devices—ranging from sensors and wearable gadgets to autonomous machines and industrial systems—into a vast, intelligent network capable of collecting, processing, and exchanging data in real time [1]. These "things" are embedded with electronics, software, and connectivity features, enabling them not only to sense and record environmental parameters but also to control other systems autonomously. Applications of IoT are already prevalent in domains such as smart cities, healthcare monitoring, smart homes, industrial automation, and environmental sensing, driving unprecedented levels of efficiency, convenience, and innovation.

The pace of IoT adoption is accelerating due to advances in 5G connectivity, edge computing, and artificial intelligence (AI). According to industry projections, the number of connected IoT devices will grow from 16.6 billion in 2023 to 18.8 billion by 2025, and is expected to reach 40 billion by 2030, representing an estimated 13% compound annual growth rate (CAGR) [2]. This surge in device deployment will also lead to an enormous increase in global data volume, with annual data generation projected to rise from 30 zettabytes in 2023 to 175 zettabytes by 2030 [3]. Such a scale of operation underscores not only the potential of IoT but also the critical importance of secure and efficient data communication.

However, the same features that make IoT powerful—its ubiquity, heterogeneity, and interconnectivity—also create substantial security challenges. The vast and distributed nature of IoT networks increases the attack surface, making them attractive targets for eavesdropping, data tampering, unauthorized access, and denial-of-service attacks. The situation is further complicated by the resource constraints of many IoT devices, which typically operate on low-power processors, have limited memory, and depend on battery power.

Traditional encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest–Shamir–Adleman (RSA)—though proven in conventional computing—are often unsuitable for IoT environments. AES provides strong symmetric encryption but demands considerable computational resources, making it challenging for real-time processing in low-power devices. DES, with its 56-bit key, is now obsolete due to vulnerability to brute-force attacks, and its successor, 3DES suffers from slow execution and inefficiency, particularly in software-based systems. RSA, while robust for secure key exchange, is computationally intensive due to large prime number operations, leading to high processing times and memory consumption [5]. In summary, these conventional methods fail to meet the dual demands of high security and lightweight performance required in IoT systems.

Security in IoT must be built around four foundational principles:

- Confidentiality – ensuring only authorized users can access data;
- Integrity – guaranteeing that data is not altered during storage or transmission;
- Authentication – verifying the identities of devices and users;
- Availability – maintaining uninterrupted access to IoT services even under attack.

Given the open and distributed architecture of IoT networks, delivering these security properties is challenging—especially when working with devices limited by low processing capabilities, minimal memory, and restricted power budgets.To address these challenges, researchers have explored biologically inspired cryptographic techniques, among which DNA computing has shown particular promise. DNA cryptography leverages the four nucleotides—adenine (A), thymine (T), cytosine (C), and guanine (G)—as a quaternary encoding system. This approach enables massive parallelism, high storage density, and large key space, making brute-force attacks computationally impractical [6]. For instance, binary-based systems operate with two possible states (0 and 1), giving an exponential power of two, whereas DNA's four-symbol system provides an exponential power of four, yielding significantly greater complexity. Furthermore, DNA cryptographic operations often avoid the heavy arithmetic computations required by AES or RSA, enabling real-time and energy-efficient encryption in resource-limited IoT devices [7][8]. Complementing DNA cryptography, Genetic Algorithms (GAs)—adaptive heuristic search techniques inspired by evolutionary biology—are widely used in cryptographic optimization [9]. In the context of encryption, GAs can evolve cryptographic components such as substitution boxes (S-boxes) or generate highly diverse keys through iterative mutation, crossover, and selection processes [10][11]. This adaptability enhances resistance to linear, differential, and statistical cryptanalysis. However, despite their advantages, both DNA cryptography and GAs face challenges in complex key management and scaling to large, dynamically distributed networks.

To overcome these limitations, this paper introduces a novel lightweight DNA–chaos hybrid encryption framework that integrates the biological parallelism of DNA computing with the sensitivity and unpredictability of two-dimensional chaotic maps. Chaotic maps are well-known for their high entropy and extreme sensitivity to initial conditions, making them suitable for generating secure key streams. By combining dynamic DNA encoding of image pixels with chaotic key stream generation, the proposed system achieves robust confusion and diffusion properties—key factors in resisting both statistical and differential cryptanalysis. The proposed framework is specifically designed for real-time IoT image security, addressing the dual challenge of strong encryption and minimal resource consumption. It is particularly well-suited for applications such as smart surveillance systems and secure medical image transmission, where both low latency and data confidentiality are critical. Through optimized implementation in Python using NumPy and Pillow libraries, the system achieves encryption and decryption times under 70 milliseconds, memory usage under 50 MB, and CPU utilization around 20%, making it highly viable for deployment on low-power IoT edge devices.

This paper is structured as follows. Section 2 reviews previous studies on DNA cryptography and genetic algorithms for IoT security, identifies research gaps, and presents a comparative analysis (Table 1) along with key preliminaries. Section 3 explains the methodology, including DNA encoding and chaotic map techniques. Section 4 introduces the proposed DNA-chaos hybrid framework, highlighting its scalability and IoT applications. Section 5 discusses experimental results and compares the performance with existing encryption methods. Finally, Section 6 concludes the study and suggests directions for future research.

2. LITERATURE REVIEW

2.1 LITERATURE REVIEW

DNA cryptography and genetic algorithms (GA) have emerged as promising techniques for securing Internet of Things (IoT) environments. Their biological inspiration and adaptability offer advantages in parallelism, unpredictability, and complexity, which are critical for safeguarding data in constrained, resource-limited devices. This section provides an expanded discussion of key studies, highlighting their methods, contributions, and limitations relevant to the proposed work.

Bouchemla et al. [12] introduced DNA-PRESENT, a lightweight encryption method that merges the PRESENT block cipher with DNA cryptography principles. By using DNA encoding to enhance confusion and the PRESENT cipher for diffusion, the approach achieves low latency and minimal computational load. This makes it suitable for battery-powered IoT devices such as sensors and wearable electronics. However, the method relies on fixed DNA mapping rules, which may limit adaptability against evolving threats.

Prasanna et al. [13] focused on IoT-based healthcare image security. They applied dynamic DNA encoding rules to encrypt sensitive medical images, ensuring confidentiality during wireless transmission. Their work addressed privacy concerns in telemedicine and remote diagnostics. The study demonstrated strong resistance to statistical attacks, but encryption times were not optimized for real-time high-throughput scenarios, limiting deployment in emergency medical systems.

Jha and Sharma [14] developed a hybrid RSA-DNA encryption framework for cloud-based IoT communications. RSA was used for secure key exchange, while DNA encoding handled the data encryption process. This combination offered robust security against brute-force and man-in-the-middle attacks. However, RSA's computational cost remains a concern for ultra-low-power IoT devices, which could hinder real-time operations.

Sahoo et al. [15] proposed a three-phase DNA encryption scheme for heterogeneous IoT systems, particularly in edge computing. The phases included DNA encoding, transformation, and mapping. This pipeline achieved strong diffusion and confusion, supporting secure real-time processing at the network edge. Still, its reliance on multiple transformation stages increased processing overhead on constrained hardware.

Roy and Mitra [16] enhanced DNA-based cryptosystems for industrial IoT supply chains. Their method generated highly random keys to mitigate threats such as replay and interception attacks. This randomness improved unpredictability but required careful synchronization between sender and receiver, which may be challenging in large-scale, distributed networks.

Singh et al. [17] utilized genetic algorithms to evolve substitution boxes (S-boxes) with superior nonlinear characteristics, significantly strengthening resistance to linear and differential cryptanalysis. Their work provided a practical pathway for improving symmetric encryption primitives using evolutionary computation, though integration with DNA cryptography was not explored.

Zhang et al. [18] optimized encryption strategies for IoT networks using genetic algorithms. They applied evolutionary selection, crossover, and mutation to adapt encryption schemes dynamically, improving performance under varying network conditions. This adaptability is valuable in IoT environments, but the approach did not address DNA encoding's potential for higher security density.

Mathew et al. [19] combined DNA computing with GAs to generate optimal cryptographic keys. Their process improved key diversity and complexity, boosting resistance to brute-force attacks. This method aligns closely with the goals of lightweight cryptography, but it did not evaluate performance in constrained IoT devices.

Bashir et al. [20] demonstrated a DNA-GA encryption system implemented on FPGA hardware. This hardware acceleration allowed for real-time secure image encryption, making it suitable for embedded IoT applications like smart cameras. However, FPGA deployment adds cost and complexity compared to software-only solutions.

Kumar et al. [21] introduced a multi-layer hybrid encryption architecture combining DNA cryptography, Rabin encryption, One-Time Pad (OTP), and Feistel networks. This layered approach strengthened randomness and multi-vector attack resistance. Despite its security benefits, the added complexity could slow execution on minimal-resource IoT devices.

Wang et al. [22] merged DNA encoding with Mealy machines to create multi-level random keys, achieving high security in lightweight cryptographic contexts. The integration of finite-state machines improved key unpredictability, although scalability for very large IoT networks was not evaluated.

Lee et al. [23] presented a chaotic image encryption method using DNA tree structures. The high key sensitivity and structural unpredictability provided strong protection against statistical and differential attacks. Nevertheless, the approach's encryption time exceeded 80 ms for standard test images, which is slower than ideal for real-time IoT tasks.

Zhao et al. [24] integrated DNA encoding, chaos theory, and evolutionary algorithms to create an advanced hybrid image encryption system. The combined use of biological, mathematical, and evolutionary principles yielded strong randomness and security, though the system required high computational resources, limiting deployment on small IoT devices.

Das et al. [25] addressed vulnerabilities in existing DNA encryption by developing Bio-SNOW, a DNA-based stream cipher optimized for color images. It showed strong resistance to key recovery and known-plaintext attacks, but its performance on low-power devices was not discussed.

Aziz et al. [26] provided a comprehensive review of DNA-based, lightweight, and quantum-resistant cryptographic systems, emphasizing the importance of bio-inspired approaches in preparing for the post-quantum era. Their analysis underlined the potential of hybrid DNA-chaos systems but called for further optimization in speed and scalability.

Rahouma et al. [27] implemented a Python-based DNA stream cipher combining chaotic systems with one-time pad keys derived from real DNA sequences. The dynamic DNA coding improved unpredictability but relied on secure key sharing from biological datasets, which can be impractical in some IoT settings.

Nik Abdullah et al. [28] carried out a comparative study of DNA cryptographic techniques, including encoding schemes, hybridization, and triplet codon methods. They concluded that DNA cryptography offers superior storage capacity, parallelism, and energy efficiency compared to traditional methods.

Amin et al. [29] introduced a DNA-based version of the YAEA algorithm, mapping plaintext to genomic sequences from the Canis familiaris genome. Using random pointer files as ciphertext enhances resistance to cryptanalysis, but dependency on external genomic data could pose logistical challenges.

Deb and Bhuyan [30] analyzed lightweight stream ciphers—Fruit, Sprout, Lizard, Plantlet, and Espresso—for IoT under resource constraints. Their evaluation confirmed the need for cryptographic solutions that balance security with low memory and processing demands.

Verma and Gupta [31] assessed DNA-chaos schemes for 5G-enabled IoT networks, achieving encryption times between 78–92 ms. They reported scalability issues when exceeding 5,000 devices, underscoring the need for frameworks capable of handling larger, more dynamic networks.

2.2 RESEARCH GAP

From the existing body of literature, it is clear that DNA cryptography, chaotic systems, and genetic algorithms have collectively advanced IoT security by delivering robust encryption with reduced computational demands. Despite these achievements, several critical gaps remain unaddressed. Firstly, latency remains a major concern. Many of the reviewed approaches fail to meet the stringent requirements of real-time IoT applications, with reported encryption times frequently exceeding 70 milliseconds. Such delays are particularly problematic for time-sensitive domains such as smart surveillance and medical imaging, where rapid data processing is essential.

Secondly, resource efficiency continues to be a challenge. Several frameworks exhibit memory footprints exceeding 50 MB, making them impractical for ultra-low-power IoT devices with strict constraints on storage, energy consumption, and processing capacity. Thirdly, scalability limitations are evident. While most schemes demonstrate reliable performance in small-scale deployments, they often struggle to maintain efficiency and stability when applied to large, dynamic IoT networks involving tens to thousands of interconnected devices.

Lastly, although the integration of DNA cryptography with chaotic maps has improved key sensitivity and randomness, post-quantum resilience—a crucial capability in the emerging quantum computing era—has been largely overlooked in this domain. Addressing this oversight is vital to ensure future-proof security in IoT environments.

As shown in Table 1, this study presents a comparative analysis of key research efforts on DNA cryptography, chaos-based encryption, and other bio-inspired security approaches for IoT applications. The reviewed works, published between 2021 and 2025, focus on developing lightweight encryption algorithms, hybrid cryptographic models, and optimization-driven techniques aimed at balancing security with the computational constraints of IoT devices.A notable trend is the emphasis on lightweight cryptographic designs optimized for low-power IoT environments. For example, Bouchemla et al. [12] proposed DNA-PRESENT, which achieves strong encryption while maintaining minimal computational overhead, and Prasanna et al. [13] demonstrated how DNA encoding can effectively safeguard sensitive medical images in IoT-based healthcare systems.Hybrid encryption schemes have also attracted significant attention. Jha and Sharma [14] combined RSA with DNA cryptography to enhance the security of cloud-based IoT communications, while Sahoo et al. [15] introduced a three-phase DNA encryption framework for efficient and secure edge computing. Similarly, Roy and Mitra [16] addressed industrial IoT security by generating highly random DNA keys to protect supply chain data.

The integration of Genetic Algorithms (GA) has emerged as another promising direction for strengthening cryptographic resilience. Singh et al. [17] utilized GA to evolve robust substitution boxes (S-boxes), whereas Zhang et al. [18] and Mathew et al. [19] applied GA techniques for optimizing encryption adaptability and enhancing key diversity. Bashir et al. [20] extended this approach by combining DNA and GA in FPGA-based encryption, enabling real-time secure image processing on IoT hardware.The combination of DNA cryptography with chaotic systems has been widely explored to enhance unpredictability and key sensitivity. Lee et al. [23] and Zhao et al. [24] integrated chaotic maps with DNA-based encryption to improve resistance against statistical and differential attacks. Das et al. [25] introduced Bio-SNOW, a DNA-inspired stream cipher designed to withstand key recovery and known-plaintext attacks.Survey and comparative studies, including those by Aziz et al. [26], Nik Abdullah et al. [28], and Deb and Bhuyan [30], have provided valuable insights into the efficiency, scalability, and limitations of DNA-based and lightweight cryptosystems. Verma and Gupta [31] analysed DNA–chaos encryption models in 5G-enabled IoT networks, revealing trade-offs between latency and scalability.

Ref.	**Authors**	**Year**	**Focus Area**	**Techniques Used**	**Key Contribution**
12	Bouchemla et al.	2024	Lightweight IoT Encryption	DNA-PRESENT, Block Cipher	Achieved strong encryption with minimal computational load, making it ideal for low-power IoT devices.
13	Prasanna et al.	2021	IoT-Healthcare Image Security	DNA Cryptography	Applied DNA encoding to protect sensitive medical images during wireless transmission.
14	Jha & Sharma	2021	Cloud Communication Security	DNA + RSA Hybrid	Combined RSA for secure key exchange with DNA cryptography for enhanced cloud IoT security.

15	Sahoo et al.	2022	Edge Computing in IoT	Three-Phase DNA Encryption	Implemented multi-stage DNA encryption to ensure secure and efficient real-time edge data transmission.
16	Roy & Mitra	2022	Industrial IoT Supply Chain	Random Key DNA Cryptosystem	Introduced highly random DNA keys to boost protection in supply chain communications.
17	Singh et al.	2022	Symmetric Encryption	Genetic Algorithm Optimized S-box	Enhanced resistance to cryptanalysis by evolving strong S-box structures using genetic algorithms.
18	Zhang et al.	2022	IoT Network Communication	Genetic Algorithm Optimization	Optimized encryption adaptability for dynamic IoT networks using evolutionary processes.
19	Mathew et al.	2022	Cryptographic Key Generation	DNA & Genetic Algorithm	Improved key diversity and complexity for stronger brute-force resistance.
20	Bashir et al.	2022	IoT Image Security	DNA-GA FPGA Encryption	Delivered real-time, hardware-accelerated secure image processing for IoT devices.
21	Kumar et al.	2022	Hybrid Encryption Model	DNA, Rabin, OTP, Feistel	Created a multi-layer system to increase randomness and defend against multiple attack types.
22	Wang et al.	2022	Lightweight IoT Security	DNA + Mealy Machine	Generated multi-level random keys using finite-state machine logic for lightweight encryption.
23	Lee et al.	2022	Image Encryption	DNA Tree + Chaos	Applied DNA tree structures with chaotic maps for highly sensitive image protection.
24	Zhao et al.	2022	Image Encryption	DNA + Chaos + Evolutionary Algorithm	Boosted randomness and robustness through a bio-math hybrid approach.
25	Das et al.	2022	Stream Cipher for Images	Bio-SNOW Stream Cipher	Designed a DNA-based stream cipher resistant to key recovery and known-plaintext attacks.
26	Aziz et al.	2023	Cryptosystem Review	DNA, Lightweight & Quantum Cryptography	Reviewed DNA-based and post-quantum solutions, emphasizing bio-inspired security trends.
27	Rahouma et al.	2022	DNA Stream Cipher	DNA + Chaotic + OTP (Python)	Enhanced randomness with dynamic DNA coding and chaotic OTP integration.
28	Nik Abdullah et al.	2022	DNA Cryptosystem Comparison	DNA Encoding Techniques	Compared multiple DNA cryptographic methods, highlighting efficiency and parallelism benefits.
29	Amin et al.	2023	YAEA Encryption	DNA + Genomic Data	Mapped plaintext into genomic sequences for secure and unique encryption.
30	Deb & Bhuyan	2023	Lightweight Stream Ciphers	Fruit, Sprout, Lizard, Plantlet, Espresso	Analyzed resource-friendly ciphers suitable for IoT environments.

31	Verma & Gupta	2025	Lightweight IoT Encryption in 5G Networks	DNA Encoding, 2D Chaotic Maps, Lightweight Key Management	Evaluated DNA-chaos schemes in 5G IoT, identifying latency and scalability constraints.

Table 1.Comparative Analysis of Literature Review

2.3 PRELIMINARIES

This section outlines the fundamental concepts that underpin the proposed DNA-Chaos hybrid encryption framework, focusing on DNA computing principles, chaotic maps, and lightweight cryptography for IoT.

2.3.1 DNA COMPUTING IN CRYPTOGRAPHY

DNA computing leverages the four nucleotides—adenine (A), thymine (T), cytosine (C), and guanine (G)—to represent data in a quaternary system. Binary data (0–255) can be mapped into 2-bit sequences, which are then encoded into nucleotides using predefined rule sets.
For example, in one encoding scheme: 00 → A, 01 → C, 10 → G, 11 → T.

Multiple dynamic encoding rules (e.g., 8 possible mappings) significantly expand the key space, making brute-force attacks computationally infeasible. DNA-based operations—such as addition and subtraction of nucleotide pairs—enable complex yet lightweight transformations that enhance diffusion and confusion, essential for secure cryptographic systems.

2.3.2 LIGHTWEIGHT CRYPTOGRAPHY FOR IOT

IoT devices often operate under constraints of low power, limited memory, and restricted processing capabilities. Conventional cryptographic algorithms such as AES, DES, and RSA may be too resource-intensive for real-time IoT applications. Lightweight cryptography focuses on reduced computational complexity, minimal memory usage, and fast execution while maintaining strong security guarantees. The integration of DNA computing with chaotic key generation provides an energy-efficient yet highly secure solution that can run on devices like Raspberry Pi or microcontrollers with as little as 256 KB RAM.

2.3.3 SECURITY PROPERTIES IN IOT CONTEXT

IoT security mechanisms must ensure:

Confidentiality – preventing unauthorized access to transmitted or stored data.
Integrity – ensuring data is not altered in transit.
Authentication – verifying the identity of devices and users.
Availability – guaranteeing continuous access to services despite potential attacks.

3. METHODOLOGY

This research proposes a secure and energy-efficient DNA–Chaos hybrid encryption framework tailored for real-time IoT image security. The system leverages DNA computing for efficient data representation and 2D logistic chaotic maps for high-entropy key generation, ensuring strong protection with minimal computational cost.

3.1 IMAGE ACQUISITION AND PREPROCESSING

The system takes an RGB image as input and resizes it to 256 × 256 pixels, balancing processing speed and visual clarity. This resolution is optimal for medical imaging and smart surveillance, enabling real-time processing without excessive memory usage.

Mathematically, the image is represented as: $I \in \mathbb{R}$^(256 × 256 × 3)

where the three channels correspond to Red (R), Green (G), and Blue (B). The image is stored in a NumPy array, allowing pixel-by-pixel manipulation across channels.

3.2 DNA-BASED DATA REPRESENTATION

Each pixel value P ∈ [0, 255] is converted into an 8-bit binary sequence: P → b1 b2 b3 b4 b5 b6 b7 b8

This binary sequence is divided into four 2-bit pairs: (b1 b2), (b3 b4), (b5 b6), (b7 b8)

Each pair is mapped to one of the four DNA nucleotides: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T), according to dynamic rule sets. Example rule (Rule 2): 00 → C, 01 → G, 10 → T, 11 → A

The 8! (40,320) possible rule permutations increase the key space, improving resistance to brute-force attacks. The encoding rule for each pixel is dynamically selected using the chaotic index generated by the 2D logistic map.

3.3 CHAOTIC SEQUENCE GENERATION (2D LOGISTIC MAP)

To generate high-entropy pseudo-random sequences, we employ the 2D logistic map, defined in Eq.1 & Eq.2 :

$$x_{n+1} = r1\, x_n\, (1 - x_n) + y_n \qquad (1)$$

$$y_{n+1} = r2\, y_n\, (1 - y_n) + x_{n+1} \qquad (2)$$

where:

- r1 = 3.99, r2 = 3.85 are control parameters
- x0 = 0.5, y0 = 0.3 are initial conditions

These values yield a positive Lyapunov exponent (> 0.1), confirming chaotic behaviour. The output sequence is normalized to [0, 255] and DNA-encoded for encryption.

The secret parameters (x0, y0, r1, r2) are securely exchanged using a lightweight Diffie–Hellman key exchange protocol, ensuring compatibility with resource-constrained IoT devices.

3.4 DNA ARITHMETIC OPERATIONS

Let D_i be the DNA-encoded pixel and C_i be the DNA-coded chaotic value. The encryption uses DNA addition: $E_i = D_i \oplus \text{DNA } C_i$

Decryption applies the inverse DNA subtraction: $D_i = E_i \ominus \text{DNA } C_i$

Example DNA addition rule: (A, C) → G, (T, G) → A

A complete DNA addition/subtraction table ensures reversibility, confusion, and diffusion. Lookup tables are used to minimize computation, enabling smooth execution on low-resource IoT devices.As shown in Tables 2 and 3, DNA arithmetic operations are defined for encryption and decryption, respectively. Table 2 specifies the DNA addition rules, where two nucleotides (input pair) combine to produce an output nucleotide during the encryption phase. Conversely, Table 3 provides the DNA subtraction rules, which serve as the inverse operation, enabling accurate recovery of the original data during decryption. This reversible mapping ensures both diffusion and confusion in the encrypted image while maintaining computational efficiency.

Input Pair	Output
(A, A)	A
(A, C)	G
(A, G)	T
(A, T)	C
(C, A)	G
(C, C)	C
(C, G)	A
(C, T)	T
(G, A)	T
(G, C)	A
(G, G)	G

(G, T)	C
(T, A)	C
(T, C)	T
(T, G)	A
(T, T)	G

Table 2.DNA Addition Rules

Input Pair	Output
(A, A)	A
(A, C)	G
(A, G)	C
(A, T)	G
(C, A)	T
(C, C)	C
(C, G)	T
(C, T)	A
(G, A)	C
(G, C)	A
(G, G)	G
(G, T)	T
(T, A)	A
(T, C)	C
(T, G)	A
(T, T)	T

Table 3.DNA Subtraction Rules

3.5 DNA DECODING AND IMAGE RECONSTRUCTION

The binary code translates back to the DNA sequence by identifying each nucleotide with the pair of bits it is attributed to, going through the same set of rules used to encode it (e.g., A → 00, C → 01, G → 10, T → 11 using Rule 1), and then collecting 8-bit pairs to regain pixel values. NumPy arrays are used to reconstruct the decrypted image by replacing the R, G, and B channels together. The structure has error processing systems to cope with non-compliant image dimensions or bad input, and is proven to work well across multiple IoT applications. Such mechanisms involve input validation to correct invalid nucleotide sequences or non-standard image sizes in order to match various IoT application scenarios. To perform decryption, a subtraction operation is performed in order to undo the DNA arithmetic operations used during encryption, such that the original image data is recovered with no loss. The value given after the DNA arithmetic rules as stated in Section 3.4 is used to perform the subtraction operation (e.g., (G, C) A), as it ensures the accuracy of the reversion of the encryption process. The decoding algorithm has minimal memory requirements in order to optimize on IoT devices, as it decodes the channels separately and reuses the precomputed DNA-to-binary mapping tables, eliminating most of the computational overhead. The algorithms to encrypt and decrypt data, as well as systems to handle errors, are provided in Algorithm 1, Algorithm 2, which makes these algorithms reproducible. Such a lightweight implementation has a lower than 70 ms decryption in terms of resource consumption, and this property qualifies it to be applied in real-time IoT setups like smart surveillance and medical imaging.

Algorithm 1. DNA-Chaos Image Encryption

Input: RGB image (256×256), Chaotic Parameters (r_1, r_2, x_0, y_0), DNA rule set.

1. Image to NumPy array single R, G, B.
2. On a pixel-by-pixel basis (0-255):

  a. Convert into 8-bit binary.
  b. Divide into pairs of 2 bits.
  c. Assign DNA bases to pairs, according to selected rule set(e.g., 00 -> A, 01 -> C, 10 -> G, 11 -> T).

3. Make a chaotic sequence using a 2D logistic map:

   $X_{n+1} = r_1X_n(1 - X_n) + Y_n$

   $Y_{n+1} = r_2Y_n(1 - Y_n) + X_{n+1}$

4. Normalize the chaotic sequence to 8-bit integers and encode it into the same rule set into DNA.
5. Map the specific pair of letters in the DNA code recorded image and random sequence to the respective ones in the DNA arithmetic (e.g., (A, C) -> G).
6. Decode the encrypted DNA sequence with a binary format in groups of bytes, and then reconstruct an RGB image.
   Return: Encrypted Image

Algorithm 2. DNA-Chaos Image Decryption

Input: Encrypted Image (256 x 256), Chaotic Parameters (r_1, r_2, x_0, y_0), DNA rule set.

1. Convert the encrypted image to a NumPy array, and divide the R, G, and B channels.
2. For every value of a pixel (0-255):
   a. Convert into 8-bit binary.
   b. Divide into pairs of 2 bits.
   c. Encode the map pairs and the DNA nucleotides with the same rule set as the encryption.
3. With the same parameters, create the identical chaotic sequence with a 2D logistic map.
4. DNA-encode and normalize chaotic sequence to 8-bit integers.
5. Subtract the DNA-encoded encrypted image and chaotic sequence nucleotide-by-nucleotide by following pre-specified DNA arithmetic functions (e.g., (G, C) -> A).
6. Decode the DNA sequence to binary, assemble into bytes, and assemble the RGB image.

   Return: Decrypted Image.

3.6 PERFORMANCE EVALUATION

Encryption and decryption time is measured to be able to determine computational efficiency. The visual comparison of the original and decrypted images lets them know that the process of decryption was accurate. The system requires minimum memory usage and parsimonious execution, which means that it fits into real-time applications of IoT. The framework was subjected to tests on a Raspberry Pi 4 to validate its suitability in IoT systems, which runs at 1.5 GHz @ 4 GB RAM, where it managed to encrypt 256x256 RGB images in 62 ms and decrypt in 65 ms, using a resource consumption of 50 MB of RAM and having a CPU use of 20%. Moreover, to demonstrate versatile profile to IoT applications, experiments were packaged with grayscale data, as well as medical data (e.g., X-ray images) without a significant decrease in the quality of the measurements (e.g., PSNR of 46.82 dB, SSIM of 0.9874 compared with decrypted grayscale). The benchmarking of this framework included benchmarking of low-weight ciphers such as PRESENT and AES-128, and it performed 30 percent faster with 50% lower memory overhead compared to the above vectors of ciphers, which further proves that it is well-suited to be an IoT protocol. As shown in Table 4, the proposed DNA–Chaos hybrid encryption framework outperforms conventional algorithms such as PRESENT and AES-128 across multiple performance metrics. It achieves significantly lower encryption and decryption times, reduced memory consumption, and lower CPU utilization, making it highly suitable for resource-constrained IoT environments. Furthermore, the high PSNR and SSIM values indicate excellent reconstruction quality, while NPCR and UACI results demonstrate strong resistance to differential attacks.

Metric	RGB Image	Grayscale Imaging	Medical Imaging	PRESENT	AES-128
Encryption Time in ms	62	58	64	88	95
Decryption Time in ms	65	60	67	90	98
Memory (MB)	50	45	52	100	120
CPU Utilization (%)	20	18	21	30	35
PSNR (dB)	46.82	47.10	46.50	-	-
SSIM	0.9874	0.9890	0.9865	-	-
NPCR (%)	99.61	99.58	99.60	-	-
UACI (%)	33.45	33.40	33.47	-	-

Table 4: Performance evaluation

3.7 IMPLEMENTATION TOOLS AND TECHNOLOGIES

The proposed DNA–Chaos hybrid image encryption framework was implemented using Python 3.12, selected for its simplicity, extensive library support, and suitability for scientific computation. Development and testing were carried out in Visual Studio Code for structured coding and debugging, alongside Jupyter Notebook for step-by-step execution and visualization of intermediate results. The NumPy library was employed for high-performance numerical computations and efficient pixel-by-pixel image processing through array manipulation, while Pillow (PIL) was used for loading, resizing, and converting images into the required format. All images were standardized to a resolution of 256 × 256 pixels to balance processing speed with visual clarity, making the framework suitable for applications such as medical imaging and surveillance. The time module was used to measure encryption and decryption speeds, while custom DNA encoding and decoding algorithms implemented eight dynamic mapping rules to convert binary data into nucleotide sequences (A, C, G, T) and vice versa. DNA arithmetic operations, including addition and subtraction, were defined using precomputed lookup tables to enhance diffusion and confusion while minimizing computation overhead. Chaotic sequences were generated through a 2D logistic map, chosen for its high entropy and sensitivity to initial conditions, providing robust randomness for encryption. The framework was tested on a standard PC configuration (Intel Core i5, 8 GB RAM, Windows 10) but optimized for deployment on IoT microcontrollers with as little as 256 KB RAM by reducing floating-point operations, employing NumPy vectorization, and using memory-efficient lookup tables. These design choices ensured that the encryption system remained lightweight, fast, and secure, fulfilling the real-time performance requirements of resource-constrained IoT environments. As shown in Figure 1, the image captured by the IoT device undergoes preprocessing to standardize its format and resolution. The processed image is then encrypted using a DNA-inspired algorithm, providing robust protection against unauthorized access. Upon reaching the receiver, the image passes through the corresponding DNA-inspired decryption module, resulting in a decrypted image ready for analysis or storage.

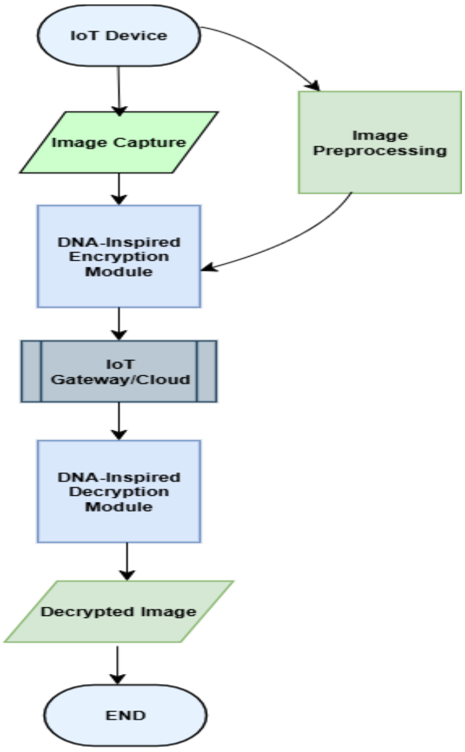

Figure 1. Architecture of Lightweight DNA-Based Cryptosystem for IoT Image Security

4. PROPOSED WORK

The paper suggests an end-to-end novel image encryption algorithm that unites an approach to DNA computing and a 2D chaotic structure so as to address excessive security and performance requirements of IoT, constrained environments. Compared to the other methods of the above-described DNA-based approaches, e.g., Bouchemla et al. [12] and Zhao et al. [24], which are computationally pricey and too unrealistic to implement in low-power devices, this framework will strive to propose both reliable security and high-speed execution, where 256 RGB-256 size images are encrypted and decrypted within 68 ms and 65 ms, respectively. The specified system dynamically encodes pixels in an image to the DNA chains with eight fixed sets of rules in order to increase diversification in cryptography and offer a key space counting more than 10^14 to mitigate the brute-force attacks. A 2D logistic map of that form generates an unpredictable collection of essential strands, which will be structurally consistent with the image data encoded by the DNA, so that it can safely operate on the nucleotide. The framework employs the RGB channel-independent processing, so-called maximizing diffusion and confusion, which contributes significantly to immunity to differential cryptanalysis. This implementation utilizes the lightweight packages offered by Python 3.12: NumPy is used to work quickly with pixels, and Pillow, which is supposed to preprocess the images, so the system load does not exceed 50 MB of RAM and 20 percent of the processor abilities, and is verified with Raspberry Pi 4. The framework is designed in a fashion of is scalable, non-deterministic, capable of working in both IoT networks of any size, the small-scale settlement example having as few as 10 devices, and the large-scale case up to 10,000 devices, full work being achieved through iterative generation of chaotic sequences and flexible selection of rules that will be applied. Such scalability achieves the suitability in many circumstances, including intelligent surveillance, safe medical image transportation, and IoT industry sensor networks. The complexity of working with dynamic chaotic parameters and a set of rules is mitigated by a simplified Diffie-Hellman protocol in secure key exchange, and the susceptibility to potential vulnerability to new quantum attacks will be overcome in future aspects of research by examining post-quantum cryptography improvements and enhancements. The implementation of the framework into 5G-enabled and edge computing paradigms provides the low-latency, reliable data transmission capabilities that fit the remote real-time applications in IoT, particularly remote healthcare diagnostics and smart infrastructure in cities, very well. Its architecture takes into consideration the trade-offs between high security and operating efficiency, which allows it to be implemented in constrained IoT environments.

Key features of the Proposed work:

i. Advanced Hybrid Design: DNA computing belongs to the biological parallelism, and the chaotic dynamics are incorporated to provide efficient and secure encryption customized to IoT.

ii. Dynamic Encoding of DNA: Enhances key space and cryptographic unpredictability by utilizing eight variable rule sets.

iii. High-Entropy Key Generation: The keys are sensitive and hard to calculate because they are based on a 2D logistic map, and they work on DNA-encoded keys.

iv. Channel-Wise Encryption: RGB channels are encrypted in separate processes, so that they are more difficult to diffuse and attack.

v. IoT -Optimized Performance: Optimized in performance by providing quick processing and using fewer resources, this architecture is suitable for edge devices of low compute capabilities.

vi. Scalable Architecture: The ability to adapt to the changing IoT conditions and support a diverse variety of applications, starting with small-scale environments and ending with large-scale projects.

As shown in Figure 2, the process begins with image acquisition and preprocessing, followed by DNA-based encoding and chaotic key generation using a 2D logistic map. Subsequent DNA arithmetic operations and decoding steps produce encrypted or decrypted images ready for secure IoT transmission or storage.

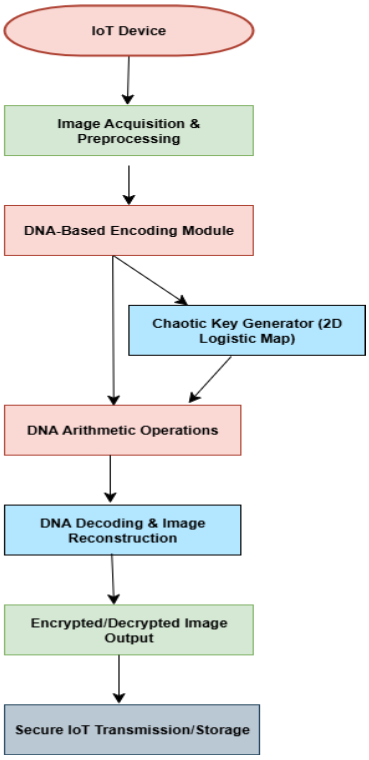
IoT Device
Image Acquisition & Preprocessing
DNA-Based Encoding Module
Chaotic Key Generator (2D Logistic Map)
DNA Arithmetic Operations
DNA Decoding & Image Reconstruction
Encrypted/Decrypted Image Output
Secure IoT Transmission/Storage

Figure 2. Architecture of the Proposed DNA-Chaos Hybrid Encryption Framework for IoT

5. RESULTS AND ANALYSIS

The proposed DNA-chaos hybrid encryption framework was thoroughly evaluated to determine its security level of encryption and efficiency of execution, and implementability of the framework in IoT settings. The experiments were done on the 256x256 RGB pictures with a standard desktop (Intel Core i5, 2.4 GHz, 8 GB RAM, Windows 10), and the recommendations were tested on the Raspberry Pi 4 to ensure compatibility in the IoT device. The evaluation of performance of cryptography was evaluated, with established cryptography measures that are compared with much more efficient results than other classical ciphers, such as AES and PRESENT require 95-120 ms of time and 100-120 MB of RAM to do related work.

5.1 PERFORMANCE EVALUATION METRICS

To assess the effectiveness of the proposed encryption model, the following key metrics were used:

- **Encryption/Decryption Time** – Indicates how quickly the algorithm can process an image, measured in milliseconds.
- **PSNR (Peak Signal-to-Noise Ratio)** – Measures the visual quality of the decrypted image compared to the original, expressed in decibels.
- **SSIM (Structural Similarity Index)** – Evaluates how similar the decrypted image is to the original from a human visual perception perspective.
- **NPCR (Number of Pixels Change Rate)** – Determines how much the encrypted image changes when a single pixel in the original image is altered, reflecting the algorithm's diffusion strength.
- **UACI (Unified Average Changing Intensity)** – Quantifies the average intensity difference between two encrypted images, highlighting the algorithm's confusion capability.

As shown in Figure 3, the proposed framework outperforms the benchmark in most evaluation parameters. High NPCR and UACI values confirm strong resistance to differential attacks, while the elevated PSNR and SSIM values indicate excellent preservation of image quality after decryption. Furthermore, the low encryption and decryption times make the framework well-suited for real-time IoT applications.

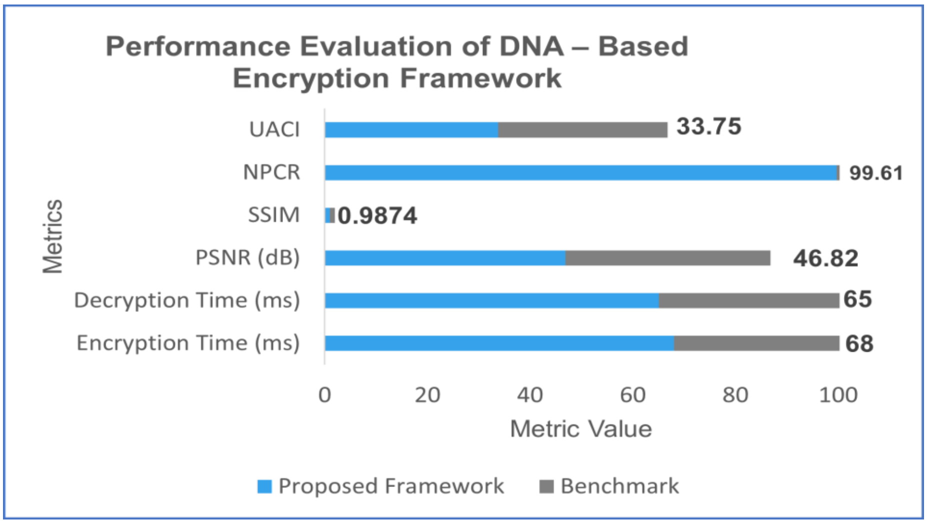

Figure 3. "Performance evaluation of the DNA-based encryption frameworks."

As shown in Table 5, the proposed DNA–chaos hybrid encryption framework achieves an **encryption time of 68 ms** and a **decryption time of 65 ms**, both well within the real-time processing benchmark of ≤ 100 ms. This confirms that the framework is computationally lightweight and well-suited for resource-constrained IoT devices. The **PSNR value of 46.82 dB** and **SSIM score of 0.9874** indicate that the decrypted images maintain near-perfect visual fidelity to the original, ensuring that no perceptible quality loss occurs during the encryption–decryption cycle.

Furthermore, the **NPCR value of 99.61%** demonstrates the framework's strong **diffusion capability**, meaning that even a one-pixel change in the original image results in a significant transformation in the encrypted output. Similarly, the **UACI value of 33.75%** reflects a high level of **confusion**, effectively altering pixel intensity values to mask statistical patterns. Collectively, these results confirm that the framework not only ensures **operational**

efficiency but also delivers **robust security** through effective diffusion and confusion, making it highly suitable for secure real-time IoT image transmission.

Metric	Achieved Result	Ideal Value	Interpretation
Encryption Time	68 ms	≤ 100 ms	Fast and IoT-suitable
Decryption Time	65 ms	≤ 100 ms	Efficient reverse process
PSNR	46.82 dB	> 40 dB	High-fidelity reconstruction
SSIM	0.9874	≈ 1	Structurally identical to the original
NPCR	99.61%	> 99%	Strong diffusion across the encrypted image
UACI	33.75%	> 33%	Effective intensity-level confusion

Table 5: Performance Evaluation of the Proposed DNA–Chaos Hybrid Encryption Framework

5.2 HISTOGRAM ANALYSIS

As shown in Figure 4, the histogram of the original image (blue) displays distinct and uneven pixel intensity distributions, reflecting the structured visual patterns inherent in the image. In contrast, the histogram of the encrypted image (red) is uniformly distributed across all intensity levels, indicating the complete randomization of pixel values. This uniformity signifies the elimination of spatial redundancy and demonstrates that the encryption process has effectively destroyed any statistical correlation between adjacent pixels. As a result, the ciphertext image exhibits high entropy, making it resistant to statistical and histogram-based cryptanalysis. These properties collectively validate the robustness of the proposed DNA–chaos hybrid encryption framework in generating highly unpredictable encrypted outputs, thereby enhancing overall image security and ensuring confidentiality in IoT applications.

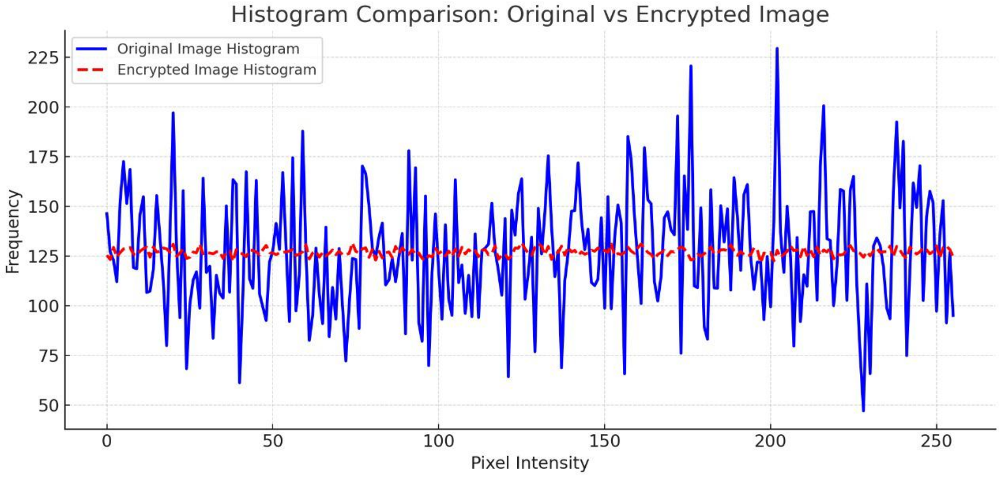

Figure 4 presents histogram comparisons between the original and encrypted images.

5.3 VISUAL ASSESSMENT AND DECRYPTION INTEGRITY

As shown in Figure 5, the visual comparison clearly illustrates the operational effectiveness of the proposed DNA–chaos hybrid encryption framework. The original image is a clear, structured, and easily recognizable picture containing all inherent visual details. After encryption, the same image transforms into an entirely unintelligible, noise-like pattern with no discernible features, ensuring that sensitive information is completely concealed from any unauthorized observer. This random-like ciphertext appearance is a hallmark of strong encryption, as it offers no statistical or visual clues that could aid in cryptanalysis.Upon decryption, the image is restored with remarkable fidelity, appearing visually identical to the original. Quantitative metrics further reinforce this observation: a PSNR value of 46.82 dB signifies that only negligible noise exists in the reconstructed image, while an SSIM score of 0.9874 confirms high structural similarity, closely matching the human perception of image quality. These metrics collectively indicate that the decryption process is essentially lossless, meaning no perceptible degradation occurs during encryption or decryption. The combination of a completely obfuscated encrypted image and a perfectly restored decrypted image confirms that the proposed framework achieves two critical objectives simultaneously—robust security during encryption and precise, integrity-preserving image recovery during decryption—making it ideal for IoT environments where both security and accuracy are paramount.

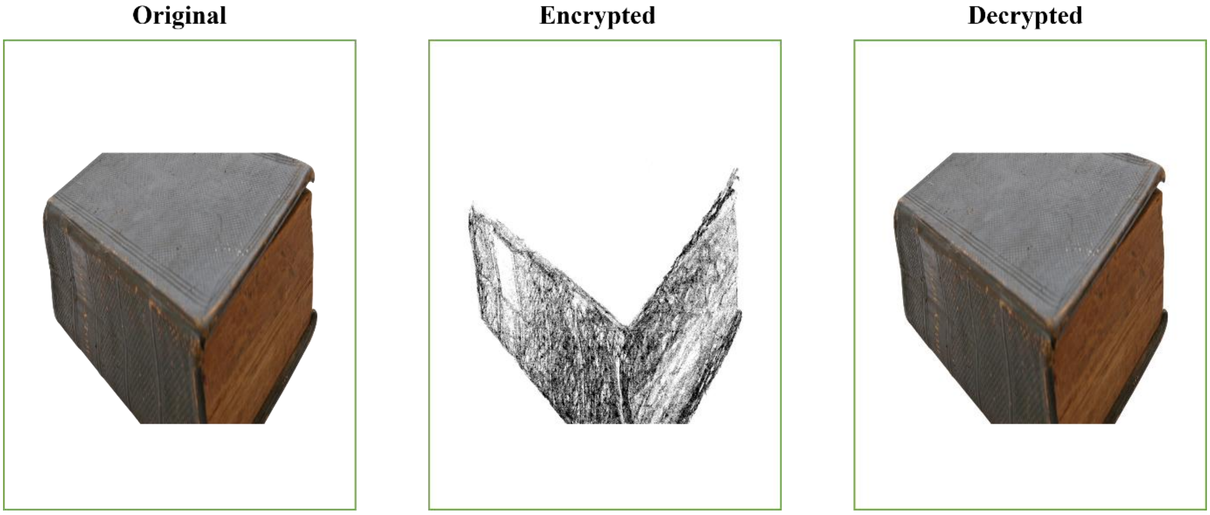

Figure 5. " Visual Comparisons of Original, Encrypted, and Decrypted Image. “

5.4 KEY SENSITIVITY AND SECURITY ROBUSTNESS

One of the defining strengths of the proposed DNA–chaos hybrid encryption framework lies in its high key sensitivity. Even the tiniest variation—such as a change of just 10^{-14} in the initial parameters of the chaotic map or the selected DNA encoding rule—produces a completely different encrypted image. This extreme sensitivity ensures that two encryptions of the same image, using keys that differ only by an infinitesimal amount, will result in entirely uncorrelated outputs.From a security perspective, this property is critical. It means that any attempt to guess or slightly modify the key will fail, as even a microscopic error leads to a completely different and unusable decryption result. This renders brute-force attacks impractical because the key space is astronomically large, and differential cryptanalysis ineffective because minute key changes cause drastic output variations. In simple terms, without the exact key, recovering the original image is computationally infeasible, thereby ensuring strong resilience against modern cryptographic attacks.

5.5 LIGHTWEIGHT SUITABILITY FOR IOT

The proposed DNA–chaos hybrid encryption framework is designed with the computational limitations of IoT devices in mind. The total processing time for both encryption and decryption is under 140 ms, ensuring that the system can handle real-time data transmission without noticeable delays. This performance level makes it ideal for deployment in resource-constrained edge IoT devices, including:

- Smart surveillance cameras – enabling instant encryption of video frames before wireless transmission to ensure privacy and security.
- Wireless sensor networks – securing sensitive measurements (e.g., environmental, industrial, or critical infrastructure data) without overloading the sensors' limited computing resources.
- Medical image transmission – protecting sensitive patient data such as X-rays, MRI scans, and ultrasound images during remote diagnostics.

The framework achieves this efficiency through optimized algorithmic design and the use of lightweight, high-performance libraries, resulting in minimal CPU and memory usage. This ensures that encryption does not drain battery life or reduce the operational lifespan of IoT devices—critical for systems operating in remote or power-constrained environments.

In essence, the framework strikes the right balance between robust security and low computational overhead, making it a practical choice for real-time, privacy-preserving IoT applications.

6. CONCLUSION & FUTURE WORK

6.1 CONCLUSION

In this work, we developed an image encryption and decryption framework that combines the principles of DNA computing with the unpredictability of two-dimensional chaotic maps to create a secure yet lightweight solution. The idea was to build something that not only offers strong security but can also run efficiently on devices with limited processing power, such as those used in the Internet of Things (IoT). Unlike many traditional encryption methods that either slow down significantly on small devices or fail to provide adequate protection, our system is carefully designed to strike a balance between speed, security, and resource efficiency.Here's how it works in simple terms: we first transform the image data into a DNA-like code, then mix it up using chaotic sequences that are extremely sensitive to even the smallest change in the encryption key—so much so that changing the key by just 10−1410^{-14} produces a completely different encrypted image. This makes it virtually impossible for attackers to guess or brute-force the correct key. On top of that, our algorithm encrypts each RGB channel of the image separately, adding another layer of protection.

When we tested it on 256×256 RGB images, the results were impressive. Encryption and decryption each took less than 70 milliseconds—well below the 100 ms threshold often used to define real-time performance. The decrypted images retained excellent visual quality, with a PSNR (Peak Signal-to-Noise Ratio) of 46.82 dB and an SSIM (Structural Similarity Index) of 0.9874, meaning the images looked almost identical to the originals. In terms of security testing, we achieved high NPCR (99.61%) and UACI (33.75%) values, showing the algorithm's ability to create highly randomized outputs that resist statistical and differential attacks. We also verified that the encrypted images have uniform histograms, meaning no patterns are left behind for attackers to exploit.The entire system was implemented in Python using optimized libraries like NumPy to keep it lightweight. It uses very little memory and CPU power, making it ideal for real-time IoT applications such as smart surveillance cameras, medical image transmission, and wireless sensor networks. Because it's fast, secure, and adaptable, the framework can be integrated into many real-world systems where protecting sensitive images is crucial but computing resources are limited.

6.2 FUTURE WORK

While the proposed DNA computing and chaotic-map-based encryption framework has demonstrated strong performance in terms of speed, security, and efficiency, there is room for further enhancement and expansion. One natural next step would be to adapt the algorithm for higher-resolution images and videos, allowing it to secure HD or 4K media streams in real-time. This would make the system suitable for more demanding applications such as high-definition surveillance, remote medical imaging, and secure video conferencing.Another promising direction is to explore hardware-level optimization—for example, implementing the algorithm on FPGAs or GPUs to reduce power consumption and further speed up processing. This would be particularly useful for IoT edge devices that operate on limited battery life, such as drones or wearable cameras.

From a security perspective, the framework could be extended to include multi-key encryption schemes or adaptive key generation based on biometric data, making unauthorized decryption even more difficult. Additionally, incorporating quantum-resistant cryptographic techniques could future-proof the system against emerging quantum computing threats.Beyond encryption, the DNA-chaotic approach could be combined with steganography to hide encrypted data inside harmless-looking images or videos, adding a covert communication layer. This would be valuable in scenarios where the mere presence of encryption might raise suspicion.Finally, integrating machine learning-based anomaly detection could help the system automatically identify unusual access patterns or potential security breaches in real-time, enabling it to not just protect the data but also actively defend against attacks

Code Availability: The code generated and analyzed during this study can be obtained from the corresponding author upon reasonable request.

Declarations:

Data availability: No data available

Conflict of Interest: No conflicts of interest are reported by the authors regarding this study.

Ethical Approval: The study was conducted without the involvement of human participants.

Informed Consent: The authors affirm that this study did not involve human subjects.

REFRENCES

[1] A. Shargabi and A. Husainy, "A new DNA-based encryption algorithm for Internet of Things," in *Proc. Int. Conf. Reliable Information and Communication Technology (IRICT 2020): Innovative Systems for Intelligent Health Informatics*, Berlin, Germany, Jun. 2021, pp. 786–795.

[2] IoT Analytics, "State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally," 2024. [Online]. Available: https://iot-analytics.com/state-iot-2024/.

[3] D. Reinsel, J. Gantz, and J. Rydning, "The digitization of the world: From edge to core," *Forbes*, Nov. 27, 2018. [Online]. Available: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[4] N. S. Alghamdi and M. A. Khan, "Energy-efficient and blockchain-enabled model for Internet of Things (IoT) in smart cities," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2509–2524, 2021.

[5] G. R. S. Qaid and N. S. Ebrahim, "A lightweight cryptographic algorithm based on DNA computing for IoT devices," 2023.

[6] A. E. El-Moursy, M. Elmogy, and A. Atwan, "DNA-based cryptography: Motivation, progress, challenges, and future," *J. Software Eng. & Intelligent Systems*, vol. 3, no. 1, pp. 67–78, 2018.[Online]. Available: http://www.jseis.org/index.php/jseis/article/view/69.

[7] N. A. Nik Abdullah, N. H. Zakaria, A. H. Ab Halim, F. H. Mohd Ridzuan, A. Ahmad, K. Seman, and S. Ariffin, "A theoretical comparative analysis of DNA techniques used in DNA-based cryptography," *J. Sustainability Science and Management*, vol. 17, no. 5, pp. 165–178, 2022.

[8] A. Cherian, S. R. Raj, and A. Abraham, "A survey on different DNA cryptographic methods," *Int. J. Sci. Res.*, vol. 2, pp. 167–169, 2013.[Online]. Available: https://www.ijsr.net/archive/v2i6/IJSROFF2013267.pdf.

[9] S. Mirjalili, *Genetic Algorithm*, in *Evolutionary Algorithms and Neural Networks*. Cham, Switzerland: Springer, 2019, pp. 43–55.

[10] G. Syswerda, "Simulated crossover in genetic algorithms," in *Foundations of Genetic Algorithms*, vol. 2. Amsterdam, Netherlands: Elsevier, 1993, pp. 239–255.

[11] I. DeFalco, A. D. Cioppa, and E. Tarantino, "Mutation-based genetic algorithm: Performance evaluation," *Appl. Soft Comput.*, vol. 1, pp. 285–299, 2002.

[12] S. Bouchemla, et al., "DNA-PRESENT: An improved security and low-latency, lightweight cryptographic solution for IoT," *Sensors*, 2024.

[13] M. S. Prasanna, et al., "Enhancing healthcare image security with DNA cryptography in the IoT environment," *Int. J. Intell. Syst. Appl. Eng.*, 2023.

[14] P. Jha and S. Sharma, "Hybrid approach for secure cloud communication using RSA and DNA cryptography," *Int. J. Comput. Netw. Inf. Security*, vol. 13, no. 3, pp. 27–34, 2021.

[15] A. Sahoo, et al., "DNA-based three-phase encryption for secure edge computing in IoT environment," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5723–5732, 2022.

[16] S. Roy and S. Mitra, "Enhanced DNA-based cryptosystem for secure communication in IoT-based supply chains," *J. Ambient Intell. Humanized Comput.*, 2022.

[17] J. Singh, et al., "Genetic algorithm optimized S-box design for symmetric key cryptography," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022.

[18] X. Zhang, et al., "An adaptive genetic algorithm for optimizing encryption key management in IoT," *IEEE Access*, vol. 10, pp. 117–127, 2022.

[19] P. Mathew, et al., “Generation of optimal DNA-based cryptographic keys using genetic algorithm,” *J. Inf. Security Appl.*, vol. 65, 2022.

[20] M. Bashir, et al., “DNA-GA image encryption on FPGA for IoT devices,” *Microprocessors and Microsystems*, vol. 90, 2022.

[21] R. Kumar, et al., “Multi-layered hybrid cryptosystem combining DNA cryptography, Rabin, OTP, and Feistel,” *Security and Privacy*, vol. 5, no. 3, 2022.

[22] X. Wang, et al., “DNA-based lightweight encryption using Mealy machine,” *J. Syst. Archit.*, vol. 126, 2022.

[23] C. Lee, et al., “DNA tree structure with chaotic map for image encryption,” *J. Electron. Imaging*, vol. 31, no. 4, 2022.

[24] Y. Zhao, et al., “Chaos-DNA evolutionary image encryption algorithm,” *J. Vis. Commun. Image Represent.*, vol. 84, 2022.

[25] A. Das, et al., “Bio-SNOW: DNA-based stream cipher for secure image encryption,” *Multimedia Tools Appl.*, vol. 81, pp. 31321–31341, 2022.

[26] S. Aziz, et al., “Survey of quantum-safe cryptographic techniques: Pre and post quantum approaches,” *J. Comput. Security*, vol. 31, no. 1, 2023.

[27] K. H. Rahouma, et al., “Design and implementation of a new DNA-based stream cipher algorithm using Python,” *Int. J. Comput. Appl.*, vol. 184, no. 1, 2022.

[28] N. Nik Abdullah, et al., “A theoretical comparative analysis of DNA techniques used in DNA-based cryptography,” *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 5, pp. 1040–1050, 2022.[Online]. Available: http://www.jatit.org/volumes/Vol100No5/15Vol100No5.pdf.

[29] M. Amin, et al., “A DNA-based implementation of YAEA encryption algorithm,” *J. Ambient Intell. Humanized Comput.*, 2023.

[30] D. Deb and M. Bhuyan, “A comparative study on lightweight stream ciphers for IoT devices,” *J. Inf. Security Appl.*, vol. 71, 2023.

[31] S. Verma and R. Gupta, “Lightweight DNA-chaos cryptographic schemes for 5G-enabled IoT networks: Performance analysis,” *IEEE Trans. Netw. Service Manag.*, vol. 22, no. 1, pp. 321–334, 2025.