International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Healthcare Image Security with DNA Cryptography in the IOT Environment

Animesh Kairi[1*], Tapas Bhadra[2], Tufan Saha[3], Sayantan Saha[4]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: The integration of DNA cryptography into IoT-based healthcare image systems represents a groundbreaking approach to tackle the pressing issue of data security and patient privacy in the digital healthcare landscape. With the increasing reliance on the Internet of Things in healthcare, the need for robust security measures is paramount to protect sensitive medical information. This research explores the feasibility and efficacy of employing DNA cryptography to encode medical data, adding an additional layer of security to data transmitted over IoT networks while ensuring compatibility with existing healthcare infrastructure. By enhancing data integrity, particularly in the realm of E-healthcare, this innovative cryptosystem has the potential to facilitate secure patient data transfer between healthcare institutions, ultimately advancing patient care and preserving privacy. The promising integration of DNA cryptography underscores its potential as a secure and rapid technique, offering a hopeful solution to the security challenges faced by healthcare image systems within IoT environments.

Keywords*: IoT Security; DNA Computing; DNA cryptography; Image encryption and Decryption;*

1. Introduction

The convergence of IoT and DNA cryptography offers a compelling solution to the escalating security challenges in our increasingly interconnected world. The IoT's vast presence in our daily lives and industries necessitates a robust security imperative, considering the wealth of sensitive data at stake. DNA cryptography's innovative approach brings forth several noteworthy advantages, including heightened data protection, tamper resistance, scalability, and long-term viability. The IoT has become an integral part of our daily lives, as well as various industries and economies. It offers numerous benefits, such as automation, data exchange, and resource optimization. However, the sheer scale and diversity of interconnected devices in the IoT create a complex security landscape. Each device, from smart appliances to industrial sensors, can be a potential entry point for cyberattacks. However, it is essential to acknowledge the potential challenges, such as complexity and cost, associated with its implementation. Moreover, ethical and privacy concerns pertaining to the use of genetic material need to be carefully addressed. As technology evolves, the synergy of IoT and DNA cryptography stands as a promising frontier in fortifying IoT security, promising to safeguard both individuals and organizations while ensuring data privacy and integrity.

DNA, the remarkable molecule of life, boasts an extraordinary set of characteristics that have captivated scientists for years. Its unparalleled data storage capacity, utilizing a four-letter alphabet, provides a density surpassing traditional digital methods, sparking interest in DNA's potential for storing immense volumes of information in minimal space [1-5]. Furthermore, its durability, capable of withstanding environmental extremes and radiation, allows us to extract and explore DNA from ancient organisms, unraveling the mysteries of the past. DNA's resilience, with built-in self-repair mechanisms, ensures the integrity of genetic information, contributing to its long-term stability. Shaped by billions of years of evolution, DNA has become the ultimate vessel for genetic data, finely tuned by natural selection. The concept of DNA as a cryptographic tool opens doors to secure data storage [8-11], harnessing its unique attributes, and heralding a new era in data security, though challenges, such as cost and efficiency, remain [21-23]. This research field promises groundbreaking innovations in data storage and security, potentially revolutionizing various domains where data preservation and security are paramount.

Using DNA cryptography in conjunction with IoT does indeed represent an innovative approach to enhancing security in the digital world. While the concept is intriguing, it's important to consider both the potential benefits and challenges associated with this paradigm shift:

[1*] *Institute of Engineering & Management, Kolkata, India, Email: ani.kairi@gmail.com*
[2] *Aliah University, Kolkata, India,*
Email: tapas.bhadra@aliah.ac.in
[3] *Institute of Engineering & Management, Kolkata, India, Email: tufan.saha@outlook.com*
[4] *Institute of Engineering & Management, Kolkata, India, Email: sayantandas636@gmail.com*
***Corresponding Author:** Animesh Kairi*
Email: ani.kairi@gmail.com

Benefits:

✓ ***Inherent Complexity:*** DNA is incredibly complex, and its use as a cryptographic medium can make it extremely challenging for attackers to decipher encoded data. The vast sequence possibilities offer a level of security that is difficult to achieve through traditional cryptographic methods.

✓ ***Natural Privacy:*** DNA-encoded data is inherently private, requiring a deep understanding of biology and specialized sequencing technologies to access and decrypt. This adds a significant layer of privacy protection to IoT data, making it less susceptible to unauthorized access.

✓ ***Authentication and Authorization:*** DNA-based authentication mechanisms can enhance the security of IoT ecosystems by ensuring that only trusted devices can access the network. This extra layer of security can help protect against unauthorized intrusion.

Challenges:

✓ ***Technical Complexity*****:** Working with DNA-based cryptography is technically complex. It requires specialized equipment and expertise in both genetics and cryptography. Implementing and maintaining such systems may be cost-prohibitive for many organizations.

✓ ***Biological Realities*****:** DNA-based data storage and cryptography may be susceptible to biological degradation or changes, potentially leading to data loss or corruption over time. The stability and longevity of DNA as a data storage medium need to be carefully considered.

✓ ***Scalability*****:** Scaling DNA cryptography for widespread IoT use may be challenging. Encoding, storing, and decoding data in DNA is not as straightforward as conventional digital methods, and it may not be as easily scalable.

✓ ***Regulatory and Ethical Concerns*****:** The use of DNA for data encryption and storage could raise regulatory and ethical issues. There may be concerns about how personal genetic information is used and protected.

✓ ***Access and Recovery*****:** Accessing and recovering data from DNA-encoded storage can be time-consuming and may not be practical for all types of data or in emergency situations.

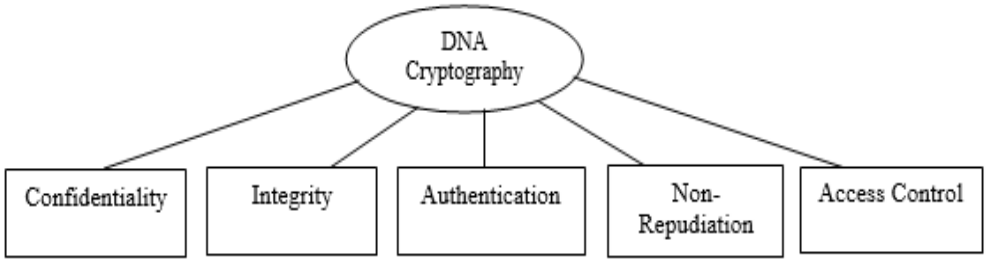


Figure 1: DNA Cryptography Objective

✓ ***Primary Objectives of DNA Cryptography*****:**

- Confidentiality: DNA cryptography aims to ensure the confidentiality of information by encrypting data to make it unreadable without the appropriate decryption key.
- Integrity: It maintains the integrity of data by providing mechanisms to detect tampering or alterations during transmission or storage, using techniques like digital signatures and message authentication codes (MACs).
- Authentication: Cryptography helps establish the authenticity of message senders or data sources through digital signatures and authentication protocols.
- Non-repudiation: It provides non-repudiation, meaning senders cannot deny the authenticity of a message or transaction, thanks to digital signatures.
- Access Control: Cryptography controls access to data or resources, ensuring only authorized users can decrypt and access specific information using encryption and access control mechanisms.

✓ ***Application in Healthcare IoT:***

- The article focuses on using DNA-based cryptographic frameworks to enhance data security in IoT environments, particularly in the context of securing sensitive healthcare information.
- It mentions the potential for remarkable success in image reconstruction while maintaining high-quality results.

✓ ***Challenges and Considerations:***

- Practical implementation of DNA cryptography requires solutions for DNA sequencing, scalability, and integration into existing IoT infrastructure.

- Ethical considerations surrounding the use of DNA for cryptographic purposes are emphasized and require careful examination.

✓ ***Structure of the Article:***

- The article is structured into several sections, including Literature Review, Methodology, Evaluation and Metrics, Results and Analysis, Discussion, and Conclusion, each providing in-depth insights into the topic.

✓ ***Overall Vision:***

- It conveys an optimistic outlook on the potential of DNA cryptography, describing it as a journey into uncharted territory where security has no bounds.
- It envisions a future where the fusion of biology and technology can lead to unbreakable security in the age of IoT.

2. Literature Review

The integration of DNA cryptography into the Internet of Things (IoT) represents a promising avenue to tackle the pressing security and privacy challenges within this rapidly expanding ecosystem. IoT, encompassing a vast array of interconnected devices, often grapples with issues such as diverse security features, data privacy concerns, and the complexities of scaling security measures across numerous distributed devices. By incorporating DNA cryptography, IoT systems can bolster their security by adding an extra layer of protection against cyber threats. The inherent privacy of DNA-encoded data necessitates specialized knowledge and sequencing techniques for decryption, ensuring that sensitive information remains confidential. Additionally, DNA-based authentication mechanisms can restrict access to authorized devices, enhancing overall security. However, it's crucial to acknowledge the practical challenges, cost considerations, and ethical and regulatory issues related to the use of biological materials. While this integration holds great promise, it is a burgeoning field, and further research and development are needed to fully unlock its potential.

The approach described combines the power of Elliptic Galois Cryptography Protocol, private data encryption, steganographic encoding, and the matrix XOR encoding method to safeguard the secure transmission of sensitive medical information over the Internet of Things (IoT). By leveraging elliptic curve cryptography and Galois field theory, the protocol ensures robust security while encrypting the private data received from various medical sources, guaranteeing its confidentiality. Steganography techniques, particularly the matrix XOR encoding method, are used to discreetly embed this encrypted data into a low-complexity image, making it inconspicuous to potential eavesdroppers. The approach's success hinges on the strength of the encryption and steganography methods, robust key management, and compliance with applicable privacy and security regulations, such as HIPAA, to protect sensitive medical data effectively.

Securing a healthcare IoT system is of paramount importance, considering the sensitive nature of patient data and the real-time monitoring involved. The system's security considerations are multifaceted, encompassing encryption, authentication, data integrity, access control, network security, data storage, and regulatory compliance. These measures collectively ensure that patient data is kept confidential, remains unaltered during transmission, and is only accessible to authorized personnel [2-4]. Regular security audits and updates are crucial to adapt to the ever-evolving landscape of IoT-related threats and vulnerabilities, providing patients and healthcare providers with confidence in the system's reliability and data protection. Adhering to healthcare data privacy regulations, such as HIPAA or GDPR, is essential to ensure legal compliance and maintain patient trust in the system's integrity.

Since the advent of RFID technology in IoT back in 1999, it has played a crucial role in identifying and tracking objects and assets across various applications. However, securing IoT devices with limited resources, such as RFID tags, has posed significant challenges due to their inherent constraints. To address these issues, innovative solutions have emerged. One notable advancement is the introduction of the Secure Lightweight Mutual RFID Authentication Protocol (SecLAP), designed for medical IoT scenarios where RFID is employed to transmit patient data to the cloud. Its primary objective is to mitigate vulnerabilities found in the Lightweight RFID Mutual Authentication (LRMI) protocol. Furthermore, enhancements to existing RFID authentication mechanisms have been proposed to bolster security [4-6]. In addition, strategies have been developed to minimize the reliance on RSA public key cryptography, incorporating machine learning and parallel processing for more efficient sensor operation. Finally, the Lightweight Anonymous Authentication Protocol (LAAP) offers an alternative solution, tailored for edge devices with resource constraints. It utilizes exclusive-OR operations and one-way functions, ensuring lightweight and anonymous authentication, making it suitable for both 5G and IoT applications with minimal overhead. These protocols and strategies collectively tackle the security and efficiency challenges inherent in using RFID technology within the context of transmitting sensitive medical data to the cloud,

prioritizing authentication and confidentiality while accommodating the limitations of IoT devices.

Group authentication plays a crucial role in various contexts, and the summaries of different research papers shed light on their distinct characteristics and challenges. In the realm of IoT, a many-to-many authentication approach is outlined, catering to group-oriented applications, but it may not be suitable for resource-constrained devices. Vehicular communication emphasizes decentralized and scalable authentication, though lacking a detailed security analysis. Mobile WiMAX networks propose a group-based handover authentication strategy, introducing some computational overhead [9-10]. Secure mutual authentication for RFID employs hash-based encryption, increasing computational load. Profile-based authentication and authorization are mentioned but without specific implementation details. Peer-to-peer group negotiation systems are discussed, albeit with limited coverage of security aspects and applicability to other ad-hoc networks. In ad-hoc networks, a lightweight, distributed group authentication technique is introduced, yet lacks performance analysis [11-15]. Each of these contexts presents unique challenges and solutions within the realm of group authentication, catering to their specific requirements and constraints.

3. Methodology

The integration of Decimal Bond DNA cryptography [16] with IOT (Internet of Things) a cutting-edge solution to bolster security within the Internet of Things (IoT) landscape by combining Decimal Bond DNA cryptography [16] with IoT technology. The provided approach outlines a novel DNA cryptography methodology, which is detailed in **Table 1** and visually represented in Figure 2.

Table 1:DNA Cryptography Encryption

Step	Description
1. Data Encoding	Convert binary data (0s and 1s) into DNA sequences, often using a mapping of binary digits to DNA bases (e.g., A, C, G, T). Divide data into segments for encoding.
2. Error Correction	Add error correction codes to DNA sequences to detect and correct errors during encoding, storage, or transmission.
3. DNA Synthesis	Use automated DNA synthesizers to create physical DNA strands following the encoded sequences.
4. Storage/Transmission	Store or transmit synthesized DNA as required, which may involve secure storage or transmission channels.
5. DNA Sequencing	Sequence the DNA to retrieve the encoded information using techniques like Sanger sequencing or Next-Generation Sequencing (NGS).
6. Error Detection/Correction	If error correction codes were added, use them to detect and correct errors during decoding.
7. Data Reconstruction	Extract and reverse the mapping from DNA bases to binary digits to reconstruct the original data.
8. Additional Security Measures	Implement security measures such as access controls, encryption before encoding, and data integrity verification.

Algorithm: DNA Cryptography Encryption

Input:
- Original image data file stored or transmitted
Output:
- Retrieved Encoded image data

Steps:
1. Data Encoding:
   a. Convert raw data into Binary Data to DNA Sequences
   b. Divide the Data into Segments for Encoding
2. Error Correction:
   a. Add Error Correction Codes to DNA Sequences
   b. These codes enable error detection and correction
3. DNA Synthesis:
   a. Use Automated DNA Synthesizers to Create DNA Strands
   b. Follow the Encoded Sequences
4. Storage/Transmission:
   a. Store or Transmit Synthesized DNA as Required
   b. Employ Secure Storage or Transmission Channels
5. DNA Sequencing:
   a. Sequence the Synthesized DNA
   b. Utilize Techniques like Sanger Sequencing or Next-Generation Sequencing (NGS)
6. Error Detection/Correction:
   a. If Error Correction Codes were Added:
      i. Use them to Detect Errors
      ii. Correct Errors During Decoding
7. Data Reconstruction:
   a. Extract and Reverse the Mapping from DNA Bases to Binary Digits
   b. Reconstruct the Original Binary Data
8. Additional Security Measures:
   a. Implement Security Measures:
      i. Access Controls
      ii. Encryption Before Encoding
      iii. Data Integrity Verification

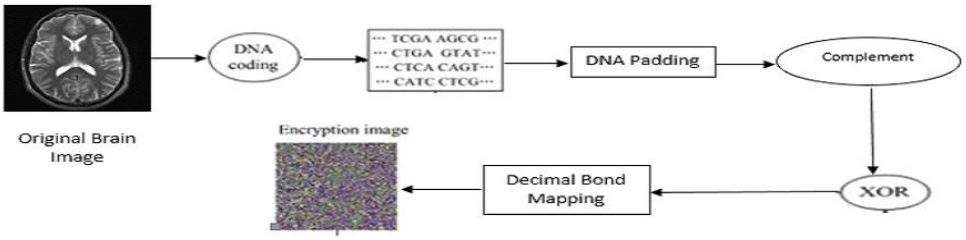


Figure 2: DNA Encryption Process

In DNA cryptography, decryption entails the process of unraveling the encoded information stored in synthetic DNA sequences, ultimately recovering the original binary data, as outlined in Table 2.

Table 2: DNA Cryptography Decryption

Step	Description
1. DNA Sequencing	Sequence the synthesized DNA to obtain the DNA base sequence.
2. Data Extraction	Extract the encoded binary data from the DNA base sequence.
3. Error Detection	Check for errors in the extracted data and identify their locations.
4. Error Correction	If error correction codes were used, apply them to correct errors.
5. Data Reconstruction	Reverse the mapping from DNA bases to binary digits to reconstruct the original data.
6. Additional Processing	Depending on the specific cryptographic method, additional processing may be required, such as decryption if the binary data was encrypted before encoding.
7. Data Verification	Verify the integrity and authenticity of the decrypted data, often using authentication mechanisms like digital signatures.

Algorithm: DNA Cryptography Decryption

Input:
- Sequenced DNA (obtained from the encoded data)
- Encryption keys

Output:
- Decrypted Original Data in terms of Image

Steps:
1. DNA Sequencing:
   a. Sequence the Synthesized DNA to Obtain the DNA Base Sequence.
2. Data Extraction:
   a. Extract the Encoded Binary Data from the DNA Base Sequence.
   b. Reverse the Mapping from DNA Bases to Binary Digits.
3. Error Detection:
   a. Check for Errors in the Extracted Binary Data.
   b. Identify Error Locations (if errors are detected).
4. Error Correction:
   a. If Error Correction Codes Were Used:
      i. Apply Error Correction Codes to Correct Detected Errors.
      ii. Ensure Data Integrity and Accuracy.
5. Data Reconstruction:
   a. Reverse the Mapping from DNA Bases to Binary Digits Again.
   b. Reconstruct the Original Binary Data.
6. Additional Processing:
   a. Depending on the Cryptographic Method:
      i. If Encryption Was Applied Before Encoding:
         - Decrypt the Binary Data Using Appropriate Keys.
      ii. Perform Any Other Required Processing.
7. Data Verification:
   a. Verify the Integrity and Authenticity of the Decrypted Data.
   b. Use Authentication Mechanisms (e.g., Digital Signatures).

The process of creating a prototype for our proposed technique, and we have chosen Python as the programming language for development. This prototype is being designed to run on an Intel(R) Core(TM) i3-9100F hardware platform.

System Configuration Details:

- Processor: Intel(R) Core(TM) i3-9100F CPU @

3.60GHz

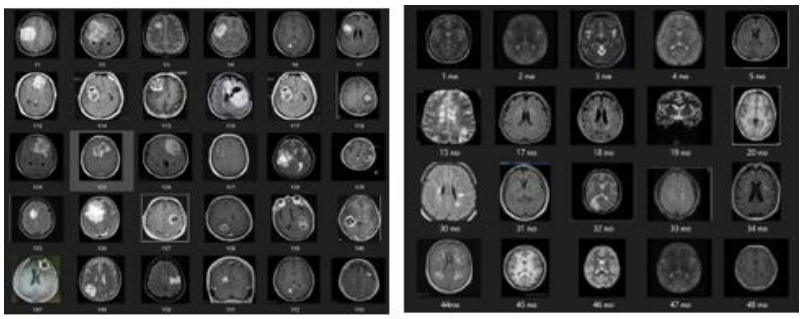
- Installed RAM: 8.00 GB
- Device ID: DDBEBA7F-55AF-4410-A60A-FC338149E86A
- Product ID: XXXXX-71397-24932-AAOEM
- System type: 64-bit operating system, x64-based processor
- Operating System: Windows 10

Key Generation: Both the private and public keys are generated using Python programming. The private key, as depicted in Figure 4, is a fixed size of 25 bytes, following the method described in reference [22].

```
1AGCT00GCTA01CTAG10TAGC11
```

Fig. 4. Private Key

For our IoT image processing project, we have incorporated brain images obtained from Kaggle, Lena, Pepper, and Baboon images to perform comprehensive result analyses. In particular, Figure 5 in our research showcases snapshots of human brain images, differentiating between those with tumors and those without. These brain images play a pivotal role in our encryption techniques, which utilize DNA cryptography for enhanced data security and privacy.



(a) (b)

Fig. 5. Human Brain Images a) with Tumor b) without Tumor

(a) (b) (c)

Fig. 6. a) Lena b) Pepper c) Baboon

4. Evaluation and Metrics

These criteria play a crucial role in the realm of image encryption and cryptography, enabling the evaluation of encryption algorithms to ensure the resilience and effectiveness of data protection. Correlation, histogram analysis, and signal-to-noise ratio measurements are pivotal in determining the dissimilarity between the original and encrypted data, as well as the overall quality of encryption. Peak Signal-to-Noise Ratio and Mean Square Error provide quantifiable metrics for assessing the level of distortion introduced during encryption, with lower values indicating superior encryption quality. Additionally, decryption and encryption times are vital, particularly in real-time applications, where speed is essential. Unified Average Changing Intensity aids in understanding how encryption impacts the average intensity of the data [17]. The choice of these criteria depends on the specific objectives and demands of the cryptographic application, ensuring a comprehensive evaluation of cryptosystem performance.

$$\text{UACI} = \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{F * T} * 100\% \quad (1)$$

The correlation between two adjacent pixels can be calculated using the following formula, which computes the coefficients for the association between the two images based on their neighboring pixel values:

$$C_{X,Y} = \frac{\mathrm{Cov}\ (X, Y)}{\sqrt{D\,(X)\,D\,(Y)}}, \tag{2}$$

Correlation Coefficient = Σ(xi * yi) / (n * σx * σy)

$\mathrm{Cov}\ (X, Y)$ he correlation between the X and Y pixels. The details are as follows:

$$\mathrm{cov}\ (X, Y) = \left(\frac{1}{N}\right) \sum_{i=1}^{N} (X_i - E\,(X))\,(Y_i - E\,(Y)) \tag{3}$$

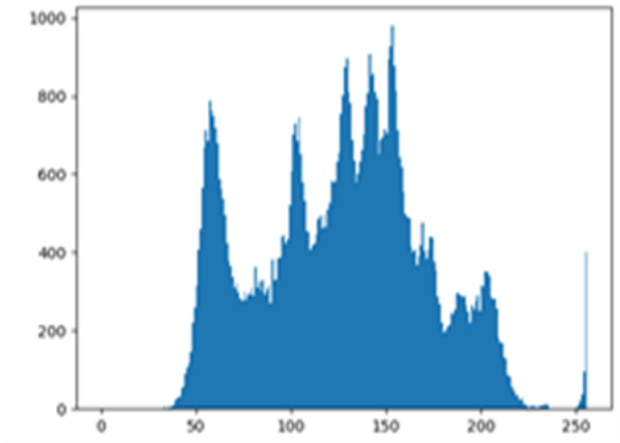
where

$$E(X) = (1/N)\sum_{i=1}^{N} X_i$$

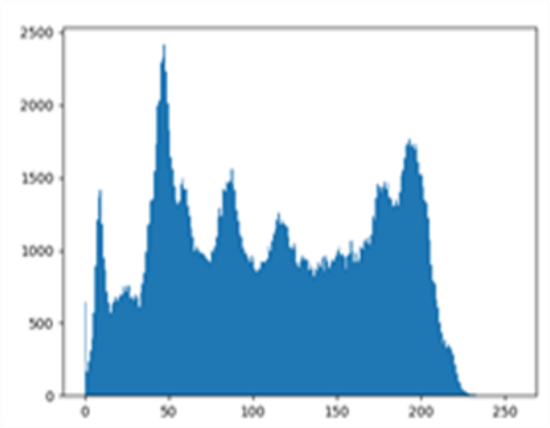
$$D\,(X) = \left(\frac{1}{N}\right) \sum_{i=1}^{N} (X_i - E\,(Y))\,2 \tag{4}$$

5. Results and Analysis

Analyzing DNA cryptography within IoT architecture using histogram analysis offers a powerful approach to assess the quality of encryption methods applied to image data. This method involves comparing the histograms of the original image and the encrypted image, which can reveal critical insights into the encryption process. A uniform histogram in the ciphered picture suggests that the encryption has successfully concealed the original image's characteristics, enhancing its resistance to statistical attacks. This visual and intuitive analysis method is particularly valuable in applications like secure image transmission and medical IoT, where data privacy and integrity are paramount. Nevertheless, it's important to acknowledge the challenges of achieving true histogram uniformity and addressing potential vulnerabilities beyond pixel intensity distribution to ensure a robust and secure IoT ecosystem.



(a)



(b)

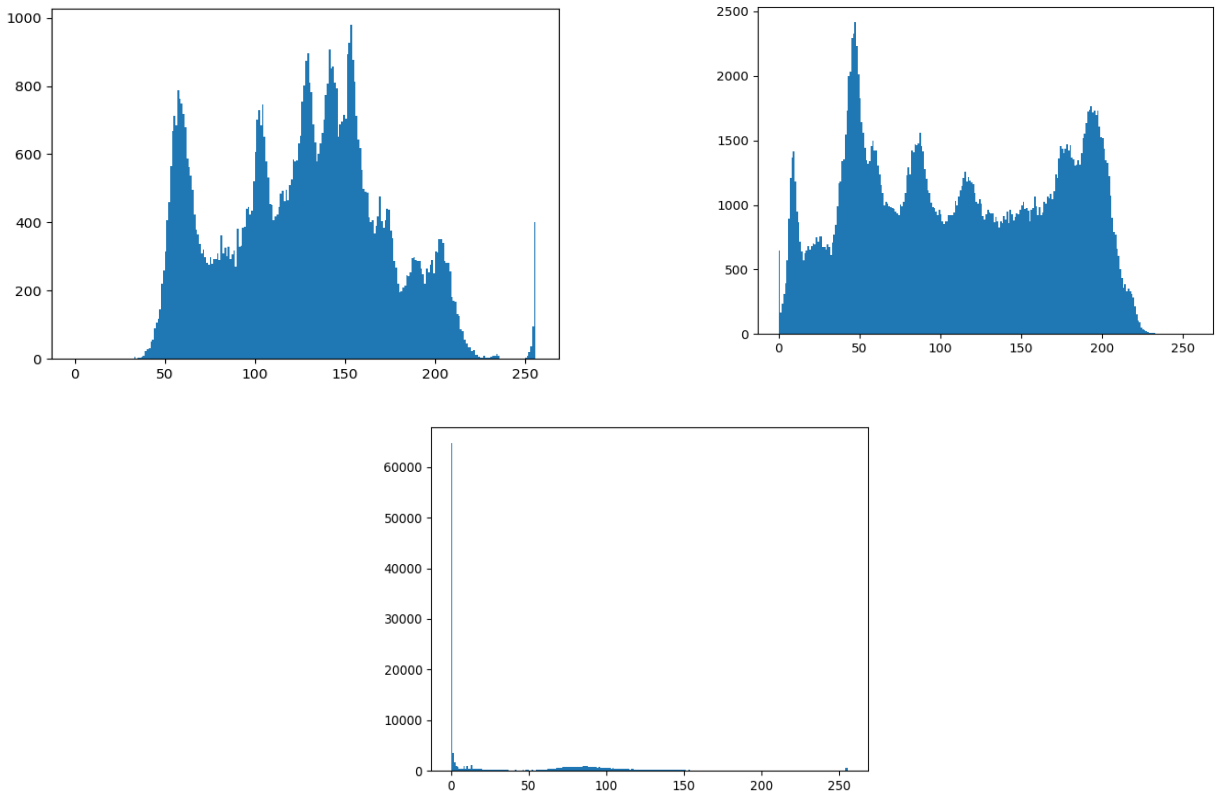


Fig.7. Input Image of Histogram (a) Lena (b) Pepper (c) Baboon (d) Brain with tumor (e) Brain without tumor

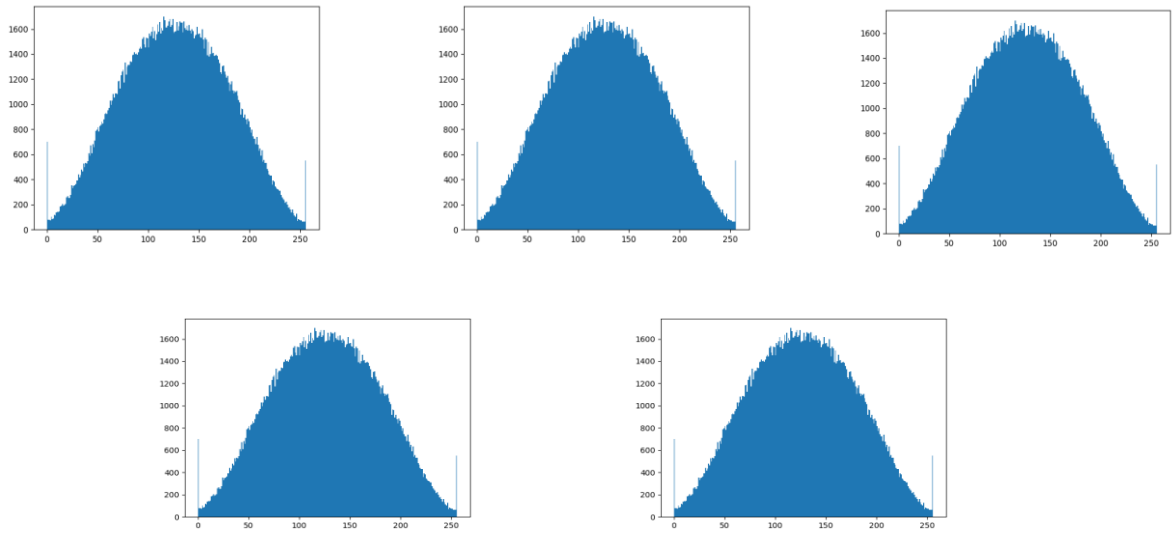


Fig.8. Encrypted Histogram Image of (a) Lena (b) Pepper (c) Baboon (d) Brain with tumor (e) Brain without tumor

(ii) Correlation Coefficient Analysis:

The focus lies in scrutinizing the impact of encryption on the relationships between neighboring pixels within images. To achieve this, a crucial statistical tool, the correlation coefficient, is employed to quantify the strength and direction of linear relationships between adjacent pixel values. This comparison is made between two types of images: encrypted and unencrypted. Encrypted images have undergone some form of transformation to safeguard their content, and their correlation coefficients are measured across sets of three consecutive pixels in various orientations—vertical, horizontal, and diagonal. The striking observation is the pronounced reduction in the significance of neighboring pixel components in the encrypted images, indicating a disruptive effect of the encryption process on the spatial patterns and relationships between adjacent pixels. This

comprehensive analysis serves as a valuable part of a broader investigation into how encryption techniques influence the visual characteristics and structural integrity of images.

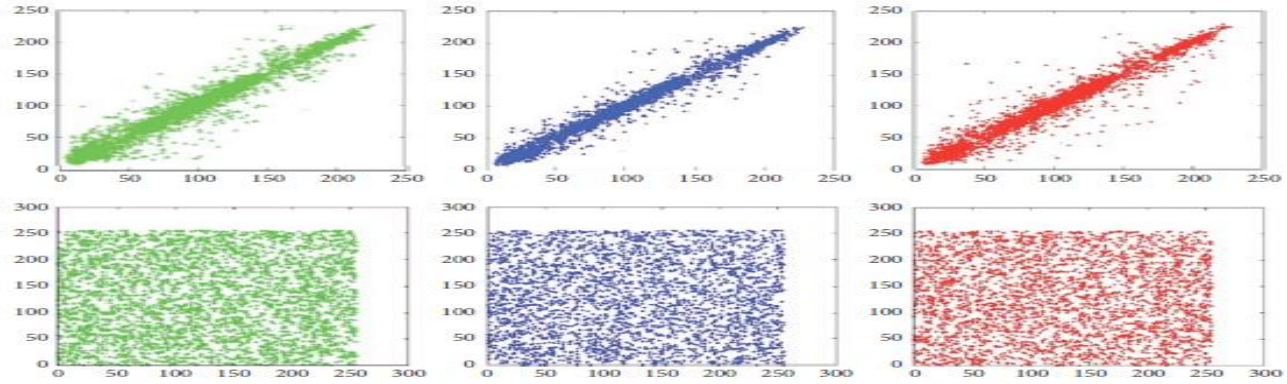


Fig.9. Correlation between two neighboring vertical pixels in Lena's photos, both encrypted and unencrypted

(iii) Different Attacks and Chosen Plaintext Attack: NPCR (Number of Pixel Changes Rate) and UACI (Unified Average Change Intensity) are essential metrics used to assess the effectiveness of DNA-based cryptographic techniques against attacks. These metrics help evaluate how resistant the encryption process is to small changes in the original data, which is crucial for ensuring the security and reliability of the encryption scheme. NPCR measures the percentage of pixel changes between the original and encrypted images when a one-bit difference is introduced, with a higher NPCR indicating a more significant change. On the other hand, UACI assesses the average intensity of these differences and aims for lower values, signifying that the discrepancies are less perceptible. The specific equations and parameters for these metrics may vary depending on the cryptographic system and image format, so it's important to consult the relevant documentation or cryptographic literature for precise details specific to your DNA-based cryptographic technique.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W * H} * 100\%, \tag{5}$$

$$\mathrm{UACI} = \frac{\sum_{i,j} C1(i,j) - C2(i,j)}{255} * 100\%,$$

The performance and characteristics of a novel DNA-based cryptography technique in comparison to other encryption methods. This method demonstrates remarkable results, with NPCR and UACI values reaching 99.72% and 34.45%, respectively, indicating its exceptional ability to retain the original image's characteristics while sensitively responding to even minor alterations. Moreover, the technique exhibits robustness against various attacks, ensuring that any tampering attempts are readily detectable through changes in these metrics. Its efficient processing times, as shown in Table 4, make it practical for real-world applications, which demand swift encryption and decryption processes. Notably, the method generates distinct keys for each session, enhancing security by preventing the reuse of compromised keys from previous sessions. Furthermore, the technique is memory-efficient, as demonstrated in Table 5, which is crucial, particularly in scenarios with limited storage capacity. In summary, the DNA-based cryptography method strikes a harmonious balance between security, efficiency, and resilience against attacks, making it a promising approach in the field of encryption.

Table 3. Comparison of Unified Average Change Intensity (UACI) and Number of Pixel Changes (NPCR)

Algorithms	Techniques Used	Pepper Image	Lena Image	Baboon Image
Proposed DNA-Based Cryptography	UACI	34.45	34.42	33.45
	NPCR	99.72	99.69	99.69
New DNA-coded fuzzy-based (DNAFZ)[18]	UACI	33.32	33.46	33.55
	NPCR	99.58	99.67	99.6
Image encryption scheme based on a hybrid model [19]	UACI	33.46	33.44	33.46
	NPCR	99.61	99.62	99.6
Image encryption scheme based on DNA sequence [20]	UACI	33.52	33.5	33.47
	NPCR	99.6	99.61	99.61
A robust lightweight algorithm in IOT [21]	UACI	33.46	33.44	33.49
	NPCR	99.6	99.62	99.62

Table 4. Time Comparison Depends Upon Number of Word

No of Words	Encryption time (sec)	Decryption time (sec)
1 word	0.0215	0.0327
More than 1 word	0.035	0.0466

Table 5. Memory Requirements Comparison of Encrypted and Decrypted Files

Encrypted File size (byte)	Input File size (byte)	Decrypted File size (byte)
5.08	5	5
37.32	37	37

The promising potential of a DNA-based cryptographic framework for safeguarding healthcare images in IoT environments. This framework has been

shown to be effective and robust, demonstrating its capability to protect sensitive medical data from unauthorized access and cyber threats. Its resistance to attacks underscores its reliability in maintaining data integrity. Moreover, the framework's efficient processing times and consistent memory requirements make it well-suited for IoT devices, where resource constraints are common. As such, this conclusion underscores the importance of DNA cryptography in addressing the critical security needs of healthcare applications within the IoT landscape, offering a strong foundation for securing medical information and images.

6. Discussions

In the era of digital communication and international collaboration among medical institutions, safeguarding the integrity of medical photographs is of paramount importance. These images often contain sensitive patient information, necessitating a robust security solution. Traditional real-time encryption techniques, as alluded to in the passage, may not provide the level of security required for such critical data sharing. To address this challenge, a novel picture encryption technique has been introduced, boasting both effectiveness and high security while minimizing processing demands. Notably, the incorporation of DNA cryptography within this proposed approach is a significant innovation, capitalizing on DNA's inherent efficiency to further fortify the system's security. The passage also underscores the critical role of cryptographic keys, where even slight alterations can have profound implications for decryption, rendering the system exceptionally secure. This integrated approach not only ensures data security but also makes any unauthorized attempts at decryption significantly challenging due to potential alterations in the retrieved data, thereby

advancing the safety of medical image sharing in the digital age.

7. Conclusions

In conclusion, DNA cryptography presents a promising avenue for achieving robust security in IoT applications. However, its widespread adoption in real-world IoT deployments hinges on a comprehensive approach that takes into account various critical factors. These include the practicality and scalability of the encryption method, cost-effectiveness in relation to security benefits, optimization to meet resource constraints of IoT devices, continuous security and efficiency assessments, and tailoring to specific use cases. Ethical considerations and integration challenges must not be overlooked, and interdisciplinary collaboration is pivotal in ensuring the technology's suitability. With a commitment to continuous innovation and a thorough examination of these elements, DNA cryptography could indeed play a pivotal role in safeguarding IoT data in the future.

Funding

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Availability of data and materials

All data generated or analyzed during this study are included in the article (and in its supplementary materials).

Acknowledgments

Not applicable.

Declarations

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

References

[1] Manjit Kaur, Ahmad Ali AlZubi, Dilbag Singh, Vijay Kumar, Heung-No Lee, "Lightweight Biomedical Image Encryption Approach", IEEE Access, vol.11, pp.74048-74057, 2023.

[2] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big data security intelligence for healthcare industry 4.0" in Cybersecurity for Industry 4.0, Cham, Switzerland: Springer, pp. 103-126, 2017.

[3] Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: a solution to secure IoT." Wireless Personal Communications 112 (2020): 1947-1980.

[4] Aghili, S. F., Mala, H., Kaliyar, P., & Conti, M. (2019). SecLAP: Secure and lightweight RFID authentication protocol for Medical IOT. Future Generation Computer Systems, 101, 621–634. Doi: https://doi.org/10.1016/j.future.2019.07.004.

[5] Wang, K.-H., Chen, C.-M., Fang, W., & Tsu-Yang, W. (2018). On the security of a new ultra-lightweight authentication protocol in an IOT environment for RFID tags. Journal of Supercomputing, 74, 65–70. https://doi.org/10.1007/s11227-017-2105-8.

[6] Domb, M. (2017). An adaptive lightweight security framework suited for IOT. In J. Sen (Ed.), Internet of Things: Technology, Applications and Standardization, IntechOpen. http://dx.doi.org/ 10.5772/intec hopen.73712.

[7] Gope, P. (2019). LAAP: Lightweight anonymous authentication protocol for D2D-Aided fog computing paradigm. Computers & Security, 86, 223–237. https://doi.org/10.1016/j.cose.2019.06.003.

[8] Mahalle, Parikshit N., Neeli Rashmi Prasad, and Ramjee Prasad. "Threshold cryptography-based group authentication (TCGA) scheme for the Internet of Things (IoT)." In 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), pp. 1-5. IEEE, 2014.

[9] Lein Harn, “Group Authentication,” In IEEE Transactions on Computers, IEEE Computer Society Digital Library, IEEE Computer Society, 16 October 2012.

[10] Lei Zhang, Qianhong Wu, Solanas A., and Domingo-Ferrer J., “A Scalable Robust Authentication Protocol for Secure Vehicular Communications,” In IEEE Transactions on Vehicular Technology, Volume: 59, no. 4, pp:1606-1617, May 2010.

[11] Anmin Fu, Shaohua Lan, Bo Huang, Zhenchao Zhu, and Yuqing Zhang, “A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks,” In IEEE Communications Letters, Volume:16, no:11, pp:1744-1747, November 2012.

[12] Morshed M.M., Atkins A., and Yu H., “Efficient Mutual Authentication Protocol for Radiofrequency Identification Systems,”

Communications, IET, Volume: 6, no: 16, pp: 2715- 2724, November 6, 2012.

[13] [13] Pfleeger Shari Lawrence, Rogers Marc, Bashir Masooda, Caine K., Caputo Deanna, Losavio Michael, and Stolfo Sal, "Does Profiling Make Us More Secure?" In IEEE Journal of security and privacy, Volume:10, Issue:4, 2012.

[14] Squicciarini A.C., Paci F., Bertino E., Trombetta A., and Braghin S., "Group-Based Negotiations in P2P Systems," In IEEE Transactions on Parallel, and Distributed Systems, Volume: 21, no:10, pp:1473-1486, October 2010.

[15] L. A. Martucci, T. C. M. B. Carvalho and W. V. Ruggiero, "A Lightweight Distributed Group Authentication Mechanism," In Proc. of 4th International Network Conference, Plymouth, UK.

[16] Kairi A, Gagan S, Bera T and Chakraborty M. 2019 DNA Cryptography-Based Secured Weather Prediction Model in High-Performance Computing. Proceedings of International Ethical Hacking Conference 2018. Pages 103-114.

[17] Elamir, M.M., Al-Albany, W.I. & Mabrouk, M.S. Hybrid image encryption scheme for secure E-health systems. Netw Model Anal Health Inform Bioinforma 10, 35 (2021). https://doi.org/10.1007/s13721-021-00306-6.

[18] G. Mohamed, N. O. Korany, and S. E. El-Khamy, "New DNA coded fuzzy based (DNAFZ) S-boxes: application to robust image encryption using hyperchaotic maps," IEEE Access, vol. 9, pp. 14284–14305, 2021.

[19] E. Zarei Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems, and hash functions," Multimedia Tools and Applications, vol. 79, 2020.

[20] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," Neural Computing & Applications, vol. 31,no. 1, pp. 219–237, 2019.

[21] H. A. Al-Ahdal, G. A. Al-Rummana, and N. K. Deshmukh, "A robust lightweight algorithm for securing data in the Internet of things networks," in Sustainable Communication Networks and Application, P. Karuppusamy, I. Perikos, F. Shi, and T. N. Nguyen, Eds., Springer, Singapore, 2021.

[22] Kairi, T. Bhadra, "Decoding The Future Using A Novel DNA-Based Cryptosystem", in Journal of European Chemical Bulletin, Volume -12, Special Issue-10: Page: 3597 –3609 2023.