Journal of Harbin Engineering University Vol 44 No. 5
ISSN: 1006-7043 May 2023

Advancing IoT Security: A Hybrid DNA and Chaos-Based Encryption Scheme for Improved Efficiency and Security

Vishwa Mitter[1], Inderpal Singh[2]
[1,2]Department of Computer Science and Engineering
[1,2]CT Institute of Technology and Research, Jalandhar
er.vishwamitter@gmail.com, er.inderpal13@gmail.com

Abstract. With the rapid rise of the Internet of Things (IoT), it is becoming important to ensure the security and privacy of data transmitted by IoT devices. By combining chaotic-based algorithms, DNA-based algorithms, RSA, and HDNARSA algorithms, this study presents a new technique for text encryption in IoT devices. The goal is to provide a robust and secure encryption mechanism for textual data delivered and stored in IoT systems. To create encryption keys, the suggested approach makes use of the features of chaotic maps. These keys are then paired with DNA-based algorithms, which use precise rules to encode the text into DNA sequences then RSA (Rivest-Shamir-Adleman) is used to further change the DNA sequences. The proposed method follows a workflow that includes key generation, encryption, IoT communication, decryption, and original text retrieval. Secure encryption keys are generated using chaotic maps for IoT devices. The text is encoded into DNA sequences, which are then encrypted using the RSA and HDNARSA algorithms. The encrypted data is transmitted over the IoT network, and the recipient device uses the corresponding decryption method to retrieve the original text. Overall, this strategy appears to be a promising solution for safeguarding textual information in IoT devices, as well as preserving the privacy and integrity of data transferred and stored inside IoT networks. It paves the way for more study into harnessing the capabilities of chaotic dynamics, DNA encoding, and well-established cryptographic methods to improve IoT security and enable safe communication in the IoT ecosystem.

Keywords: IoT, Encryption, DNA cryptography, Information security, Chaotic-Encryption Scheme.

1. Introduction

In the cognitive IoT environment, smart devices have evolved processing capabilities that typically allow the connecting node to gather, observe, and analyze the necessary information from their frameworks in adding to answers appropriately [1]. IoT technology growth must focus on the security restrictions of multimedia data, including text, photographs and videos.

The IoT landscape presents unique challenges for encryption due to resource constraints, diverse communication protocols, and the need for efficient yet secure cryptographic operations. Traditional encryption algorithms, such as symmetric and asymmetric key encryption, have been widely used but may not fully address the specific requirements of IoT environments. Hence, there is a need for innovative approaches that leverage emerging technologies and integrate multiple encryption techniques to enhance security. Researchers have created a variety of text and picture-based encryption algorithms that are used to secure data. Due to the significant data requirements, the main methods of the RSA, DES, IDEA, as well as AES are still used to protect the data and image. This study contributes to the subject of IoT security by presenting a complete solution for text encryption in IoT devices that integrates different encryption algorithms. We demonstrate the efficiency and practicality of the suggested technique in providing a high degree of security and confidentiality for textual data in IoT systems through experimental evaluations and performance assessments. The combination of chaotic-based algorithms, DNA-based algorithms, RSA, and HDNARSA algorithms ensures that textual data in IoT systems is secure and secret.

The proposed method capitalizes on the characteristics of chaotic maps, which exhibit deterministic but highly unpredictable behavior. Chaotic maps are utilized for generating encryption keys, introducing randomness and enhancing the security of the encryption process. Additionally, DNA-based algorithms are employed

to encode the textual data into DNA sequences using specific rules. DNA encoding offers benefits such as error correction capabilities and compact representation, making it suitable for securing textual data in resource-constrained IoT devices.

The rest of the paper may be arranged as follows: Section 1 makes reference to the chaotic encryption and also explains the DNA method; Section 2 provides the details of the literature survey and research gaps; and Section 3 contains the suggested work. Section 4 displays the outcomes. The paper's conclusion may be found in section 5.

1.1 Chaos-Based Encryption

The behaviour of non-linear dynamical devices that cannot use a single data connection is the subject of the mathematical study known as the Chaos theory. Wide broadband, ergodicity, as well as sensitivity to beginning circumstances, are just a few of the non-periodic unexpected properties that characterize it [5]. Secure communications methods are just one of the real systems scenarios for which Chaos is an appropriate instrument. Two or more first-order differential equations are used to model chaos-based systems. A theoretical framework creates the chaotic signal, making it simple to replicate. However, despite such a model, reproduction is still difficult. The chaotic feature is also sensitive to the initial values; even a little variation in these variables causes significant variations in the results.

Two stages are required to complete the chaos encryption scheme: For a chaotic map, there are initial conditions consisting of one or more starting values that define the state of the system. It applies the mathematical function to the current state to compute the next state, the process is repeatedly iterative to calculate the next state. Combinations of trigonometric functions, logarithms and exponentiation are nonlinear transformations that introduce irregularity as well as complexity into the system.

Yet, a lot of research has been done recently to create optimization techniques for chaotic systems based on text or image encryption. Even still, the chaos-based approaches are ineffective for fine-tuning the logistic maps to text and image encryption [4].

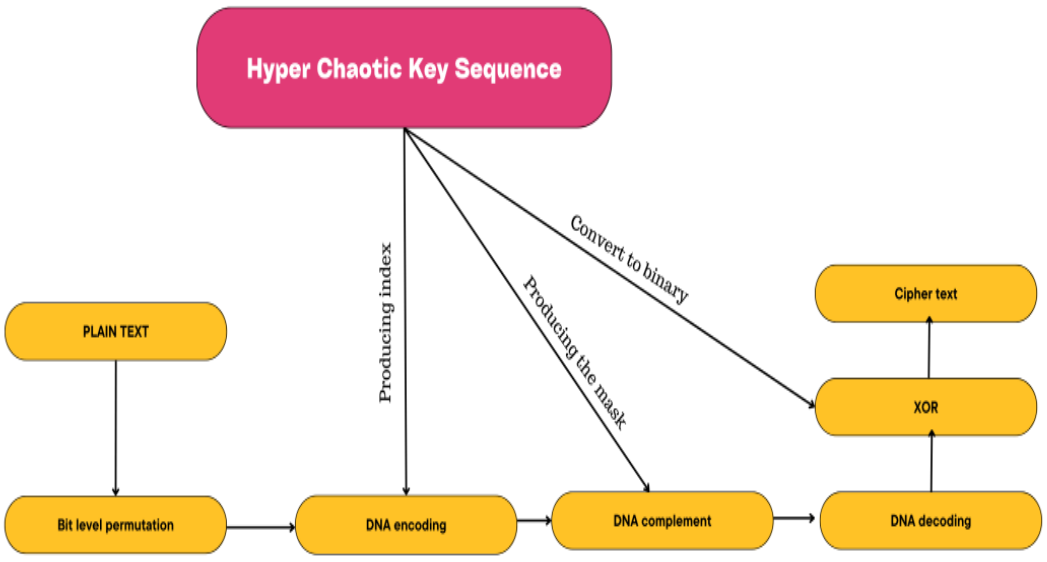

FIGURE 1: Hyper Chaotic key sequence method[6]

1.2 DNA (Deoxyribonucleic Acid)

The biological supermolecule known as DNA (Deoxyribonucleic Acid), which is created when nucleotides merge, is the source plasma of all living things. Deoxyribonucleotides are supposedly thought of as the DNA monomer unit. DNA has 4 distinct kinds of nucleotides bases, including Adenine (A), Cytosine (C), Thymine (T), and Guanine (G).

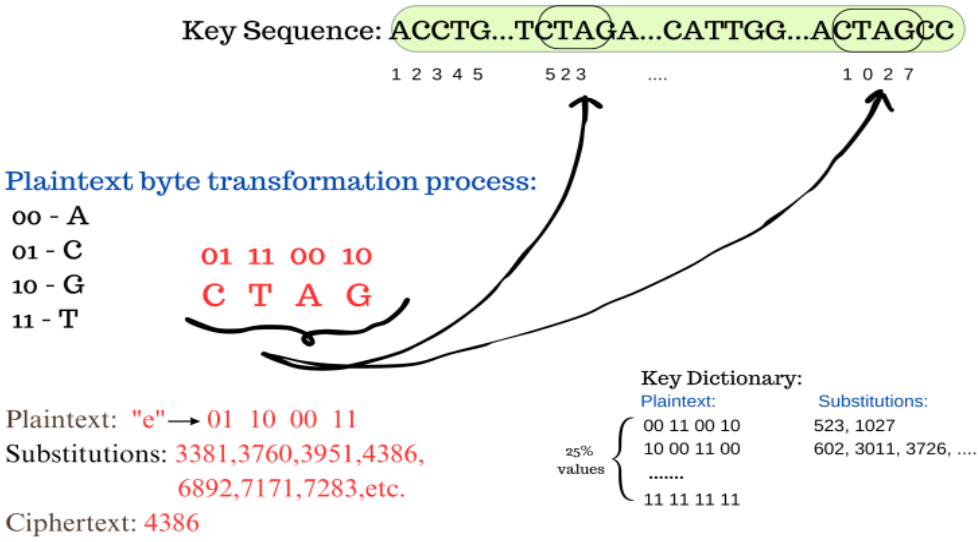

FIGURE 2: DNA Indexing Algorithm's encryption process [8]

The DNA has 2 nitrogen bases: 1. Purines Pyrimidines, second. The single-ring molecules, which have the bases C and T, are referred to as pyrimidines while the double-ring molecules, A & G, are believed to be purines. The vast industries that could be used for image & data encryption, data concealment, steganography, etc. might be discovered using DNA's capabilities.

The encryption process begins with key generation and to generate secure encryption keys the chaotic algorithms are employed. Random and highly secure keys are produced by Chaotic maps. These keys serve as the basis for the encryption and decryption operations. Then encoding with DNA Algorithm process starts, once the encryption keys are generated, the textual data is encoded into DNA sequences using the DNA-based algorithm.

According to predetermined rules, DNA algorithm maps the characters or bits of the text message into specific DNA sequences. The binary data of the text message are represent with the help of DNA sequence design. Compact representation of textual information and error correction capabilities are provided, which are advantageous in IoT environments where data integrity is crucial. Given that the DNA is a sensor module, this can have a variety of outputs depending on the environment. Consequently, it could be said that the environmental factors depicted in Figure 4 completely determine how DNA computations are performed. The term "binary coding scheme" refers to the binary transformation of the DNA sequence.

The DNA elements A, T, C, or G were used in this work to denote the binary values 00, 11, 01, or 10. The binary representation of the DNA sequence "AATCGGAT" in one instance is 0000110110100011. The major bases in RNA (ribonucleic acid) are the same as those in DNA, with the exception that Uracil (U) is used in place of thymine (T).

Base	Complement
A	T
C	G
G	C
T	A

+	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	C	A
T	T	G	A	C

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

TABLE 1 Complementary Tables **TABLE 2** DNA ADDITION **TABLE 3** DNA Sequence Encoding

1.3 Objectives

1. To analyze various security algorithms that can be used for enhancing security in IoT systems, including symmetric and asymmetric encryption methods, and hybrid encryption schemes.

2. To propose an advanced security hybrid approach based on DNA and chaotic-based encryption to overcome the limitations of current models and improve overall efficiency and security.

3. To compare and analyze the performance of the proposed hybrid approach with traditional models, in means of key generation time, encryption/decryption time, data transfer rate, and security level.

2. Literature Survey

In this below section, related work and research gaps in encryption or cryptography techniques have been discussed. Below **TABLE 4** shows the related work in the purposed field.

Author's name	Publishing year	Description
Mona M. Elamir al., [18]	2022	Under this a proposed cryptosystem using the RSA algorithm to encrypt the data especially data used in medical services to make sure data security in network security, which results in the RSA algorithm in cryptography schemes being an efficient algorithm that can be utilized safely
Siham OleiwiTuama al.,[19]	2021	Suggested a chaotic-based bit level scheme using the permutation method that is proposed for securing the cypher text in an efficient manner and also to overcome the drawbacks of conventional permutation of cypher text.
Namasudra et al. [10]	2020	Suggested a method Using the user's secret data, a 1024-bit DNA computing-based random key is

		generated, and the same key is used for information encryption0
M Y T Irsan et al. [11]	2019	The authors demonstrated a method under which an algorithm having chaotic map where MS map used as a keystream generator, resultant cipher-text that is very difficult to be cracked by known plaintext attack and the bruce-force attack.
Vikram et al.,[13]	2019	They suggested a DNA symmetric cryptography that improves data security and the findings demonstrated that the plain-text encryption processes are highly secure.
Nath et al.,[14]	2019	The LCA technique for picture encryption using a chaotic logistic map was suggested and resulting of the suggested method includes investigation via a statistical test, security test, & comparison to other recently created picture encryption algorithms.
Naif et al.,[12]	2019	Used the chaotic gadget with a customized form of lightweight AES, produced the chaos key sequence utilized in the lightweight AES or SHAKE128 & is capable of warding off various attacks.
Hussien et al. [9]	2019	Suggested a method that uses an arbitrary key to muddle the three RGB channels of the image as well as XOR plus-mod as a confusing method.
Jain et al.,[15]	2014	Proposed a various biological as well as arithmetic technicians employed in DNA cryptographic algorithms as these variables also would aid future researchers in designing or improving DNA storage methods for high effective & possible information storage.

2.1 Research Gaps

However, a lot of research has been done recently to develop optimization strategies for chaotic systems based on text encryption. Even still, the chaos-depend approaches are ineffective for fine-tuning the LM to text and image encryption [16]. When implementing different optimization algorithms may be used.

- The encryption technique fulfils the text encryption requirements for all types of data sets, but it does not take into account the usage of newly inspired optimization methods to address the security issues with the text encryption method[14].
- The authors evaluate various DNA cryptography techniques using a few key significant variables. Additionally, these variables would aid future researchers in creating or enhancing DNA storage strategies for safe data storage in a more effective & dependable way. Yet it is not possible to provide a novel method that combines the advantages of both biological and conventional cryptography[15].
- In order to provide safe & effective information access in the CC environment, a unique access control mechanism based on a table and DNA computing is developed. To assess the efficacy of the proposed technique, numerous experiments are carried out, which demonstrate its effectiveness. A cloud environment's identity management strategy can be improved[10]. To demonstrate that the suggested technique offers a superior method for protecting IoT networks, this investigation compares its efficacy with that of conventional models or proposes a hybrid advanced security approach based on DNA and chaotic-based encryption.

3. Proposed Work

The Internet of Things (IoT) has revolutionized the way devices and systems communicate with each other. With the widespread adoption of IoT, there has been a growing concern about the security of the data transmitted over these networks. The increasing set of connected systems & the vast set of information being distributed make it more challenging to establish privacy & confidentiality of information. One of the critical challenges in securing IoT networks is the lack of a suitable cryptography mechanism. Encryption techniques are essential to prevent unauthorized access to data transmission, and they ensure data privacy and confidentiality. While various encryption and cryptographic-based models have been introduced for IoT, there is still a need to enhance the security level& effectiveness of these models.

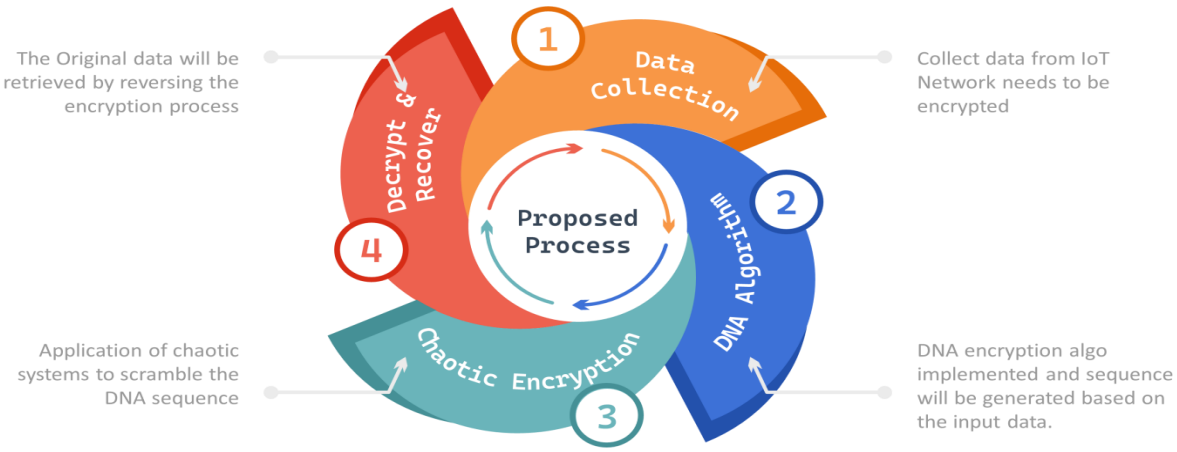

FIGURE 3: Proposed process visual flow

In a recent study, the authors proposed an approach that uses the RSA approach & DNA cryptography to improve the security phase of IoT systems. However, the key generation process of the proposed approach is quite complex, which affects the overall performance of the model. Moreover, RSA is typically utilized to encrypt complete files, making it low effective& high resource-heavy than symmetric-key encryption. This means that the RSA algorithm might occasionally fail since entire encryption needs both symmetric &asymmetric encryption.

Additionally, the large quantity of numbers in RSA leads to a slow data transfer ratio, and it requires a third party to verify the reliability of public keys sometimes. The issue with RSA is also that as these keys grow more time, the required computational capacity for utilizing them grows but the security level does not.

Therefore, there is still a need to analyze various security algorithms that can be used for enhancing security in IoT systems. The proposed solution should overcome the limitations of current models by improving the key generation process and overall efficiency while maintaining a high level of security. This study aims to propose an advanced security hybrid approach based on DNA and chaotic-based encryption and compare its performance with traditional models to ensure that the proposed approach provides a better solution for securing IoT networks.

3.1 Methodology

- Data Collection:

The first step is to collect the data from the IoT network that needs to be encrypted. This data could be any type of information, such as sensor readings, location data, or personal information.

- Apply DNA algorithm:

The DNA algorithm will be utilized to encrypt the collected information. In this process, the DNA sequence will be generated based on the input data using a specific DNA encryption algorithm. The encrypted data will be represented by the DNA sequence.

i. Generate a random key rndKey consisting of 8 binary digits

{
Key = rndKey
}

ii. Convert the Key from binary to decimal and assign it to the Key
iii. Encrypt the text using DNA encryption with Text, Key, and MsgLen and assign it to EncText
iv. Measure the elapsed time for DNA encryption and assign it to dnaET

{
Display 'DNA Encrypted Text :-'
}

v. Display EncText

- Apply chaotic-based encryption:

Chaotic-based encryption will be used as a second layer of encryption. This process involves the application of chaotic systems to scramble the DNA sequence. This additional layer of encryption will enhance the security of the data by making it even more complicated to decipher.

i. Encrypt the EncText using Chaotic encryption and assign the encrypted text to Encrypted and the ChaoticKey
ii. Measure the elapsed time for Chaotic encryption and assign it to chET

{
Display 'Chaotic Encrypted Text :-'
}

iii. Display Encrypted as characters

- Decryption:

To decrypt the data, the chaotic-based encryption layer will be removed first, followed by the DNA algorithm layer. The original data will be retrieved by reversing the encryption process.

Chaotic Decryption

i. Decrypt the Encrypted text using ChaoticKey and assign the result to rcText
ii. Measure the elapsed time for Chaotic decryption and assign it to chDT

DNA Decryption

i. Decrypt the EncText using Key and MsgLen and assign the result to OutputText
ii. Measure the elapsed time for DNA decryption and assign it to dnaDT

{
Display 'Recover Text :-'
}

- Performance Analysis:

The conductance of the suggested approach would be analyzed by comparing it with traditional models. Key performance metrics such as key generation time, encryption/decryption time, data transfer rate, and security level will be used for the analysis. The results will be compared to the traditional models to determine if the proposed approach provides a better solution for securing IoT networks.

Overall, the methodology involves collecting data from the IoT network, applying DNA encryption, applying chaotic-based encryption, decrypting the data, and analyzing the performance of the proposed approach.

3.1 Tool Used

With the use of MATLAB, it is possible to perform complicated operations like technical calculation, graphics, or animation as well as simple numerical calculations like subtracting and adding. The programming language for MATLAB's simplification is C. It provides a user-friendly interface with a wide range of built-in features. Depending on the adaptation, these features change. The fundamental MATLAB building piece is the matrix. Additionally, this platform comes with the built-in image, signal, communications, control, or NN processing capabilities. The network can be simulated using this tool as it supports high graphics. MATLAB is a case- sensitive and implemented in many languages such as JAVA, PYTHON and FORTRAN. In MATLAB, three words are used. These three instructions are as follows:

1. CLC: This option clears the command window & moves the cursor to the top.

2. Clear all: With the use of this authority, the workspace's function and variable names can be completely cleared.

3. Close all: Using this command, all extra windows, including the figure window, can be closed.

4. Results

It is not simple to propose a cryptosystem; it must be reliable, quick, and safe. In order to provide another level of protection to the suggested system, a cryptosystem based on one of the most potent encryption algorithms has been proposed in this study. The chaotic computation theory & the DNA computing theory support this cryptosystem. In this experiment, 100 words of characters were first encoded into DNA format using the chaotic method and public key encryption. Last, but not least, this encrypted text demonstrates the viability of text security in network security. MATLAB 2018 was used to implement this experiment. Beginning with the histogram of the encrypted & initial information, we have used a range of assessment instruments to evaluate our proposed methodology. An unsecured network must appear drastically distinct, as demonstrated below:

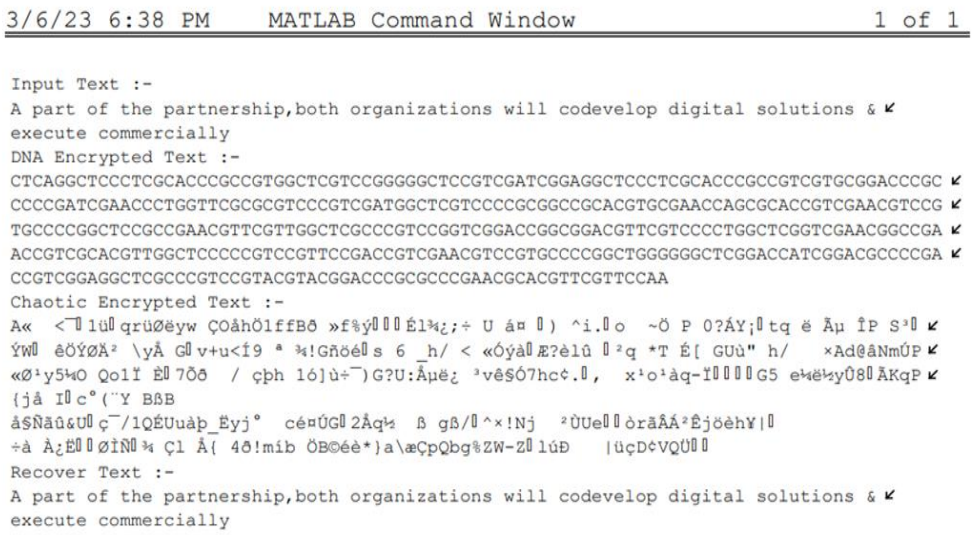

FIGURE 4: MATLAB Command Window

Encryption algorithms are mathematical equations or processes that transform data into ciphertext, which is useless without the key, using keys and occasionally randomness. They are employed in electronic transfers and communications to offer security and stop data fraud. Additionally, they enable the decryption of the data into its unencrypted state with the aid of the keys.

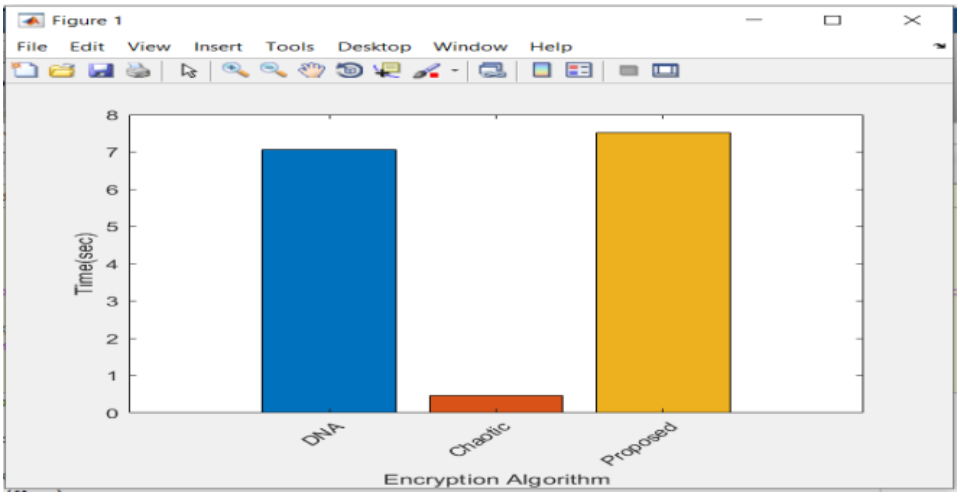

FIGURE 5: Encryption algorithm Vs Time (Sec)

figure 8 shows the graphs of the encryption algorithm versus Time (Sec) which shows that the proposed hybrid approach gives superior results.

TABLE 5: Encryption for DNA, Chaotic, Proposed

Technique	Time(Sec)
DNA	70 Sec
Chaotic	0.5 Sec
Proposed	75 Sec

Decryption is the process of converting a meaningless file into its actual form.

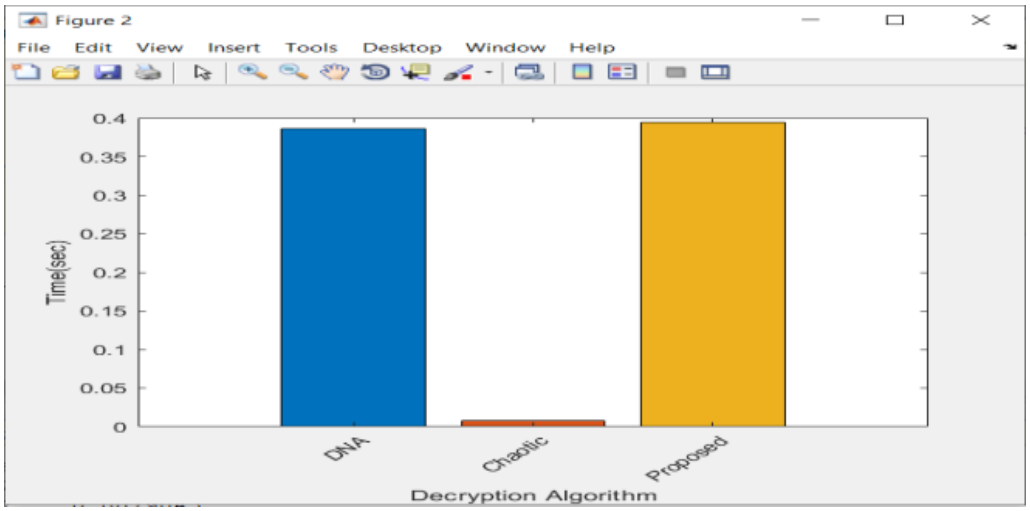

FIGURE 6: Decryption Algorithm Vs Time(Sec)

Figure 9 shows the graphs of the decryption algorithm versus Time(Sec)which shows that the suggested hybrid approach gives superior values for message decryption.

TABLE 6: Decryption for DNA, Chaotic, Proposed

Technique	Time(Sec)
DNA	0.37 Sec
Chaotic	0.2 Sec
Proposed	0.39 Sec

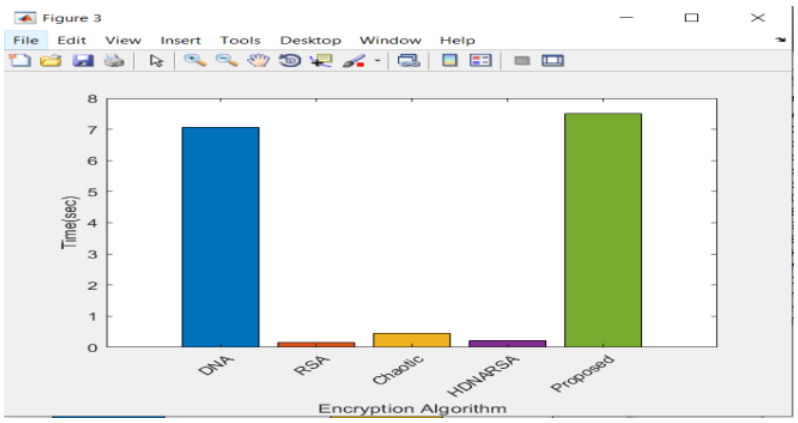

FIGURE 7: Various encryption algorithms vs TIME(Sec)

Figure 10 depicts the encryption process as estimated using several ways, including DNA, Chaotic, RSA, HDNARSA, and the suggested methodology, which yields outstanding results in terms of timing.

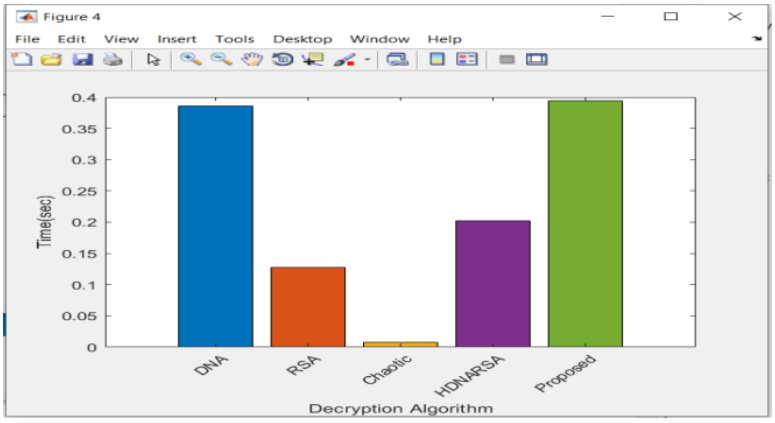

FIGURE 8: Various encryption algorithms vs Time(Sec)

The results show that chaotic maps and DNA encoding rules were employed to boost the proposed system's security level, demonstrating its effectiveness in achieving this goal.

5. Conclusion

Security services based on cryptography can be found in various industries, including those that deal with digital certificates, banking, picture and message encryption, etc. A number of symmetric and asymmetric key cryptography methods, including DES, TDES, AES, and RSA, exist to transform plaintext into ciphertext. The results show that chaotic maps and DNA encoding rules were employed to boost the proposed system's security level, demonstrating its effectiveness in achieving this goal.

References

[1] S. Karthick., "Semi-supervised hierarchy forest clustering and knn based metric learning technique for machine learning system", Journal of Advanced Research in Dynamical and Control Systems. 9(Special Issue 18), pp.2679-2690,2017.

[2] A. Kanso. And M.Gheblehk., "A novel image encryption algorithm based on a 3D chaotic map", An International Journal of Communications in Nonlinear Science and Numerical Simulation. 17(7), pp.2943-2959,2012.

[3] S. Behnia, A. Akhshani, H. Mahmodi and A.Akhavan., " A novel algorithm of image encryption based on the mixture of chaotic maps, In proceedings of Chaos, Solitons and Fractals", 35, pp.408- 419,2008

[4] S. Karthick, S.P. Sankar and T.R. Prathab. (2018) An approach for image encryption/decryption based on quaternion fourier transform. In Proceedings of 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research, ICETIETR, pp. 1-5,2018.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using the external key," Phys. Lett. A, vol. 309, no. 1–2, pp. 75–82, 2003

[6] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou, and M. N. Vrahatis, "Cryptography and cryptanalysis through computational intelligence," Stud. Comput.Intell., vol. 57, pp. 1–49, 2007.

[7] El Assad, Safwan and M. Farajallah., "A new chaos-based image encryption system", An International Journal of Signal Processing: Image Communication. 41, pp.144-157,2016.

[8] Yunpeng Zhang, XianweiZhang, "DNA Cryptography Based On Fragment Assembly", Information Science and Digital Content Technology(ICIDT), 2012.

[9]Hussien, H., "DNA Computing for RGB image Encryption with Genetic Algorithm", 14th International Conference on Computer Engineering and Systems (ICCES),2019.

[10]Namasudra, S., "Fast and Secure Data Accessing by Using DNA Computing for the Cloud Environment", IEEE Transactions on Services Computing, 2020.

[11] Mona M. Elamir, May S. Mabrouk and Samir Y. Marzouk, "Secure framework for IoT

technology based on RSA and DNA cryptography", Egyptian Journal of Medical Human Genetics,23:116,2022.

[12]Naif, J. R., Abdul-Majeed, G. H., & Farhan, A. K., "Secure IOT System Based on Chaos-Modified Lightweight AES", International Conference on Advanced Science and Engineering (ICOASE),2019.

[13]Vikram, A., Kalaivani, S., &Gopinath, G, "A Novel Encryption Algorithm based on DNA Cryptography", International Conference on Communication and Electronics Systems (ICCES),2019.

[14]Nath, S., Som, S., & Negi, M., "LCA approach for Image Encryption Based on Chaos to Secure Multimedia Data in IoT", 4th International Conference on Information Systems and Computer Networks (ISCON),2019.

[15] Jain, S., & Bhatnagar, V., "Analogy of various DNA-based security algorithms using cryptography and steganography", International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),2014.

[16] S. Karthick, S.P. Sankar and T.R. Prathab. (2018) An approach for image encryption/decryption based on quaternion fourier transform. In Proceedings of 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research, ICETIETR,2018.

[17] M Y T Irsan and S C Antoro (2019), "Text Encryption Algorithm based on Chaotic Map". In Proceedings of 2019 The 3rd International Conference on Science, Journal of Physics,2019.

[18] Siham OleiwiTuama and Sahar A. Kadum (2021), "Text Encryption Approach Using DNA Computation and Hyperchaotic System". In Proceedings of 2nd Information Technology to Enhance E-learning and Other Application (IT-ELA) 2021.