International Journal of Computing and Digital Systems
2025, VOL. 17, NO. 1, 1–9

http://dx.doi.org/10.12785/ijcds/1571016767

Encryption Technique Using a Mixture of Hill Cipher and Modified DNA for Secure Data Transmission

Kameran Ali Ameen[1], **Walled khalid Abdulwahab**[1] **and Yalmaz Najm Aldeen Taher**[1]

[1]*Computer Science Department, University of Kirkuk, Kirkuk, Iraq*

Received 6 April 2024, Revised 19 October 2024, Accepted 25 October 2024

Abstract: The 21st century has experienced an information surge due to rapid technological advancement, rendering knowledge a much more vital strategic asset. Due to the lack of security for information transmitted and received over the communications network, hackers can steal information with all their might and intelligence. Therefore, the task of information field security is becoming increasingly important. Unfortunately, current classical encryption methods have become vulnerable to attacks in various ways. Consequently, we must improve existing processes and learning features for communication in the presence of introducer hacking technologies to protect data. Cryptography is the most important part of telecommunication and computer security infrastructure. Using steganography and cryptographic techniques for data security is gaining popularity and widespread adoption. A considerable amount of research has been conducted on DNA-based data encryption techniques. The DNA-based cryptography approach is an innovative paradigm in the world of cryptography, safeguarding data during transmission by transforming original text into an incomprehensible format. This work proposes a novel cryptographic approach integrating Modified DNA sequences with the Hill cipher. The suggested methodology comprises four stages: The Hill cipher algorithm encodes plaintext into n-bit binary values during the first phase. Subsequently, XOR operations are executed on the result, followed by adding a 32-bit key value to the XOR output. Third, Modified DNA cryptography is utilized to create uncertainty and facilitate steganography. The decryption procedure, the final phase, is employed to retrieve the original message on the recipient's side. The suggested approach met the security requirements and showed the capability to counter several security threats. Moreover, the suggested approach offers superior data security compared to current systems. The suggested technology may conceal digital data and ensure the secure transmission of critical information.

Keywords: Hill Cipher, Modified DNA, Cryptography, Steganography

1. Introduction

With the development of technology in the modern era, data security plays a supreme part in securing information. Thus, keeping the confidentiality and integrity of data and the security of individual information becomes one of the biggest concerns [1][2]. Due to threats to data transmitted over networks, improving current approaches and strategies for identifying communication elements that repel hacking techniques is essential [2]. Cryptography and steganography are the most common and widely used data and network security methods [3]. Cryptology technology is not new; it has been explored for more than 2000 years. The name of the cryptology is a mix of the Greek cryptos (hidden) with (study, science) [4]. Furthermore, new methods and techniques in data and network security, such as steganography and watermarking, have been explored [2].

In cryptography methods, an encryption key changes the text to an unreadable form. After data arrives at its intended destination, the decryption key returns the text to its original form [5][6]. It renders the messages unintelligible to outsiders through various text transformations [4]. Steganography aims to hide messages in different media, such as images, video, and audio, to prevent attracting attention to the data that is there [4][5][6]. Cryptography and steganography are independent, interrelated processes that share mutual aims and services for maintaining the confidentiality and integrity of data [7]. These processes are combined to realize high-security requirements [2][6].

Therefore, data cannot be protected from alteration and tampering without applying these technologies. Deoxyribonucleic acid or DNA is discovered in the literature as a new carrier for critical data hiding to achieve the farthest protection, powerful security, high capacity, and low modification rate. Data hiding in DNA sequences is a developing scientific field [2][7]. According to recent studies, DNA offers three benefits that make it a useful environment for

E-mail address: kameran.ameen@uokirkuk.edu.iq, walled.khalid@uokirkuk.edu.iq, yalmaz.science@uokirkuk.edu.iq

data hiding. First, it can hold a lot of data. Second, data can be easily transformed into a DNA sequence. Third, compared to other media, DNA is a better cover media for data hiding due to its complexity and randomness, which create much uncertainty [7][8]. Additionally, steganography is a process that converts data into a DNA sequence so that it can be kept secret from adversaries who try to read and decode the signals [6][9].

This paper develops a system combining cryptography and steganography to achieve high security for transferring sensitive data. The technique utilizes Hill cipher as a cryptography approach with modified DNA sequences to achieve steganography. Initially, the original data is encrypted using Hill cipher, and then an XOR operation is applied to combine the resulting ciphertext with a secret key. Finally, the data is hidden based on Modified DNA cryptography. An efficient and strong encryption scheme has been obtained. This method makes it difficult to understand or decipher the plaintext. Moreover, it seeks to generate a vague message and prevent unauthorized access or modification of the secured data. The results showed an outstanding performance of the proposed technique in terms of capacity and security compared with other existing methods.

The rest of this paper is organized as follows: Section 2 discusses a literature review of the related works. The background of the Biological DNA and Modified DNA sequences and the Hill Cipherare are presented in sections 3 and 4, respectively. Section 5 presents the proposed technique. In section 6, the execution of the proposed technique is discussed and compared with several related works. The security robustness of the proposed approach is analyzed and discussed in Section 6. Finally, the conclusion and the future work are noted in the last section.

2. Literature Survey

This section briefly overviews related works concerned with DNA cryptography and steganography. In [10], a hybrid technique was proposed by combining encryption and steganography. DNA and an advanced encryption standard are applied to encrypt a message. The encrypted message is then hidden within a different DNA sequence, giving the message triple-layer security.

A novel cryptographic security method was put forth in [11] to protect data from unauthorized access. The suggested method, which depends on DNA encryption, uses a 128-bit key to implement the cryptology encryption technique. In addition to this key, there are special ways of substitution that come after the round key selection technique. Compared to traditional DNA and non-DNA-based methods, the suggested technique increases the ciphertext size by 33 percent. In [12], a new DNA sequence-based cryptography method is proposed dependent on a lookup table. Each DNA consists of a lookup table of 64 condos arranged in a matrix of 8 by 8 with replaceable characters in place of the 26 keys alphabet of the play fair cipher algorithm. The results showed that the proposed outperformed some existing methods in terms of providing better security for data during its transmission over the network, in addition to enhancements in terms of encryption and decryption time.

In [13], several security algorithms, DNA, GZIP, AES, and image steganography, were combined. A factor was offered to be multiplied with the last stage of DNA encryption. The results of this operation were pressed utilizing the GZIP technique. Next, to boost security, the AES technique encrypts the message. Finally, LSB image Steganography was used along with a high-quality image to hide the encrypted message. This paper presented a model for the confidential transmission of sensitive data. In [14], a secure communication channel was constructed by combining the strengths of steganography and encryption. An XOR encryption process that depends on DNA encoding was developed. The suggested approach employs DNA sequence as a curtain to conceal the confidential data. The experimental findings demonstrated that the suggested strategy outperformed existing methods regarding blind extraction, capacity, and security.

A method combining lossless compression and DNA cryptography with enhanced data storage was put out in [15]. Using the DNA OTP method, this approach converts regular text into a DNA cipher text. Each DNA nucleotide is given a binary code based on the occurrence of DNA codons. The encrypted text produced by this method is smaller than the comparable plain text. In [16], a multi-layer steganography method was presented and photos and DNA sequences were exploited as sensitive data carriers. The discrete cosine transform (DCT) approach embeds the fictitious DNA in a picture, and the substation algorithm conceals confidential data in the DNA. The findings demonstrate the suggested mechanism's resilience to chi-square and histogram attacks.

The security architecture in [17] utilizes a DNA-based method for encrypting data broadcast by sensor nodes in a wireless sensor network (WSN). The framework comprises many phases, including the encryption and decryption processes between two nodes. The cryptographic process is analogous to the structure and functions of DNA. Data hybridization involves amalgamating fabricated data with an authentic cipher to bolster security. In contrast, data compression has been included in the framework to address the constraints connected with Wireless Sensor Networks (WSNs). A secure method in [18] that integrates steganography and cryptography to safeguard fingerprint pictures during transmission while ensuring secrecy. The method transforms fingerprint photos into binary data, encrypts this data, and integrates it into the DNA sequence. The suggested solution presents a minimal likelihood of compromise, several concealment options, and quick execution durations. This approach is restricted to concealing tiny pictures within DNA sequences and cannot accommodate

video, audio, or huge images. In [19], a study proposes advancements in DNA computing to enhance cloud security by implementing biological authentication procedures. This method integrates biochemically safe DNA signatures with current cloud infrastructures to facilitate multi-factor authentication (MFA), encrypting access to sensitive user information and transactions. The established DNA cryptography techniques provide robustness against prevalent threats.

The above methods achieved good security for the sent data using DNA with one or more encryption methods. Still, they mostly relied on a single key, restricted to a specific type of data or, in some cases, increased the ciphertext length, which reduced the efficiency of using the bandwidth allocated for data transfer. The proposed method mimics these methods in terms of combining encryption and concealment. Still, it relies on modified DNA instead of the traditional one. It relies on the presence of two keys in addition to several operations and transformations, which adds more security to the ciphertext.

3. Background of The Modified and Sequences

The practice of transforming the original message into a comparable substitute using a particular encoding method is known as data hiding. Data concealing in network systems has become a compelling challenge [20][21]. The encoding scheme can work by integrating the important chemical properties of the biological DNA sequences (Deoxyribonucleic Acid) for hiding and transferring the original data. So, the data will be very secure, and nobody can break it easily [20]. Lately, DNA has been utilized in everything in human life as a carrier instead of other cover media (text, video, audio, etc.). Two strands of nucleotides, each coded with four DNA bases, make up biological DNA. As seen in Figure 1, these bases are (A) adenine, (G) guanine, (C) cytosine, and (T) thymine [6][21].

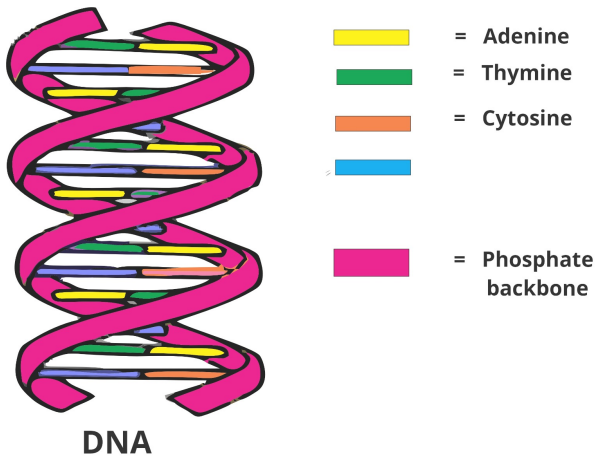

Figure 1. DNA Structure

The hydrogen bonds binding each DNA base to its neighbour: A to T and C to G—are known as complementary pairings of DNA strands. As shown in Table I, the four nucleotide bases (A, T, C, and G) can be encoded using the most basic type of DNA coding [21]. It applies four digital codes like 0(00), 1(01), 2(10), and 3(11). The classical encryption techniques used to encrypt messages based on mathematical equations may not be highly secure and do not meet the required ambition [21] [22].

Thus, many researchers interested in data security are working on applying or integrating the concept of DNA directly or indirectly into their proposed algorithms. They use DNA or modified DNA sequences to encrypt the data by integrating the message into the DNA [20][21]. Further, based on hexadecimal data, the modified DNA sequence can encrypt messages with higher security than other encryption techniques. The modified DNA is described in Table I [22].

4. Background of The HILL Cipher

In 1929, Hill Cipher (HC) was invented by the mathematician Lester S. It is a poly-graphic substitution cipher dependent on a linear algebraic method [23][24]. HC hides the frequencies of a single letter via encrypting pairs of plain text. Thus, it is protected from various encryption text attacks. This technique provides a good spread, where an alteration in one letter of the original text affects all letters in the ciphertext [23][24]. To substitute m ciphertext characters instead of m plain text characters, we need to m linear equations. So, HC is a linear algebra technique based on modular arithmetic. For m = 2, the method can be described in equations 1 and 2 [24][25].

$$C_1 = (K_{11}P_1 + K_{12}P_2) mode 26 \tag{1}$$

$$C_2 = (K_{21}P_1 + K_{22}P_2) mode 26 \tag{2}$$

This case can be expressed in column vectors and matrices as in equation 3 [26][27].

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} mod 26 \tag{3}$$

The relation between plain text and ciphertext characters can be described simply in equation 4 [26][27].

$$C = KP \tag{4}$$

P and C are column vectors of length m, representing the plain text and the ciphertext, respectively, and K is the encryption key represented as a m × m matrix [25][28]. To decrypt a ciphertext, we need to use (K-1), which is the inverse of a matrix (K) as shown in equation 5.

$$KK^{-1} = K^{-1}K = I \tag{5}$$

TABLE I. Modified DNA based on hexadecimal

Modified DNA sequence	Hexadecimal Value	Modified DNA sequence	Hexadecimal Value	Modified DNA sequence	Hexadecimal Value	Modified DNA sequence	Hexadecimal Value
AA	0	TA	4	CA	8	GA	C
AT	1	TT	5	CT	9	GT	D
AC	2	TC	6	CC	A	GC	E
AG	3	TG	7	CG	B	GG	F

Where (I) represents the identity matrix. K^{-1} can be applied to recover the plaintext from the ciphertext. Thus, we can represent the encryption and decryption processes in equation 6 and 7 [26][27]. If the block length is m, there are 26 m possible different letter blocks; all can be deemed as letters in a 26 m-letter alphabet.

$$C = E_k(P) = K.P \tag{6}$$

$$P = D_k(C) = K^{-1}C = K^{-1}KP = P \tag{7}$$

5. Proposed Technique

Biological cryptography systems, such as DNA, are becoming increasingly popular. Many applications utilize them to provide high security and reliability for user messages. This literature proposes an efficient scheme consisting of a mixture of DNA with Hill cipher. Implementing our proposal involves several main steps.

According to Table II, each message character is converted to a number in the first step. Later, these numbers are encrypted using Hill cipher and converted to a binary value. In the second step, the Modified DNA sequence encrypts the message. The result is inverted, and key bits are added to it. Finally, the resulting message is converted into a DNA sequence and then transformed into binary values. On the receiving side, the authorized receiver performs decryption by reversing the above steps to recover the original message. The following subsections clarify more details about the encryption and decryption processes. Figure 2 presents a flowchart that describes the complete encryption and decryption processes.

A. *Encryption Steps by Hill Cipher (Sender side)*

In this subsection, the first stage of the proposed approach, which includes encryption using the Hill cipher, is described briefly.

TABLE II. Character values

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	-
18	19	20	21	22	23	24	25	26

- Step 1: The communication parties specify block length (n), a 32-bit key value (k), key matrix values (K), which are used in Hill cipher encryption and decryption, and the number of messages exchanged with these specifications.
- Step 2: Specify the message to be sent over the network.
- Step 3: According to Table II, each character is converted into a number between 0 and 25.
- Step 4: The number sequences obtained in Step 3 are broken into blocks with a length (n).
- Step 5: Hill cipher, defined in equation (3), is applied to each block number of length n obtained in Step 4 using the key matrix (K). The numbers in the ciphertext must be in two-digit number form.
- Step 6: Each digit in the ciphertext is converted into an equivalent 4-bit binary number. The binary numbers of the same block are concatenated into a single binary block.
- Step 7: The sequence of binary numbers in the binary block is reversed.
- Step 8: Perform an XOR operation between the original and reversed binary block.
- Step 9: The output of the XOR process and the 32-bit key are broken into 4-bit binary blocks. Afterwards, a binary addition operation is applied between each 4-bit message block and a 4-bit key block, increasing the length of the resulting blocks from 4 bits to 5 bits.
- Step 10: Finally, the binary blocks resulting from the addition process are concatenated into one block.

Using a longer encryption key makes the code more secure but also increases its complexity. Since the proposed method contains several transformations, which add some complexity, a 32-bit encryption key was adopted. It provides sufficient security, especially with a second encryption key related to the Hill cipher. Also, using a short-length key makes the available bandwidth more efficient when sending

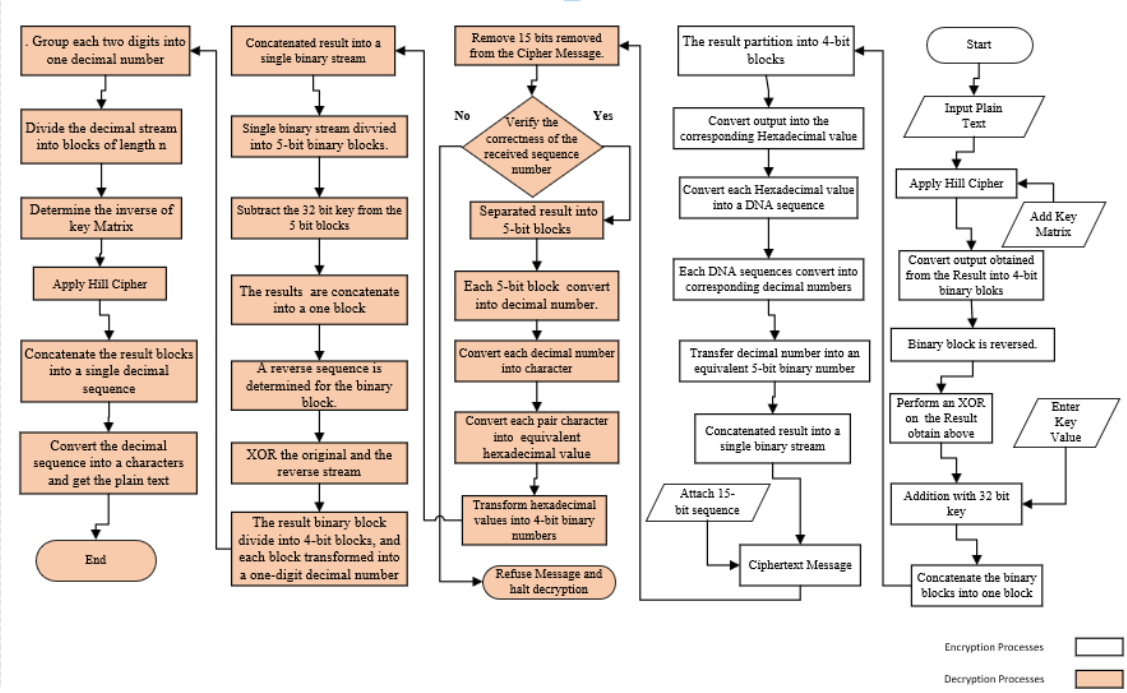

Figure 2. Process of encryption and decryption method

short messages, as we do not need to add padding bits to the message to match the key length.

B. Encryption by Modified DNA (Sender side)

The output of Hill cipher is handled by the modified DNA cryptography according to the following steps.

- Step 1: The output bit stream of Hill cipher is partitioned into 4-bit blocks.
- Step 2: Convert each 4-bit binary block into the corresponding Hexadecimal value.
- Step 3: Based on Table I, each hexadecimal value is converted into a DNA sequence.
- Step 4: Based on Table II, each character in the DNA sequences is converted to the corresponding decimal numbers.
- Step 5: Each decimal number is transformed into an equivalent 5-bit binary number.
- Step 6: The 5-bit decimal numbers are concatenated into a single binary stream to create the final ciphertext message.
- Step 7: A 15-bit sequence number is attached to the final ciphertext before sending it over the network. These 15 bits are arranged as the first five bits as a random number, while the remainder is a message sequence number of 10 bits in length. This 15-bit is shifted one bit to the right using a circular shift register after each message transmission.

C. Decryption Steps of DNA and Hill Cipher (Receiver Side)

In this subsection, the processes that are applied to the received ciphertext to get back the original dispatch are described.

- Step 1: The first 15 bits are removed from the stream. Verify the correctness of the received sequence number and check whether the number of messages exchanged corresponds to the predefined number. If something is wrong, the appropriate actions should be taken, and the decryption process should be halted; otherwise, go to step 2.
- Step 2: The ciphertext binary message is separated into 5-bit blocks.
- Step 3: Each 5-bit block is converted to the corresponding decimal number.
- Step 4: Based on Table II, convert each decimal number to the corresponding character.
- Step 5: The characters are transformed to the capital form; according to Table I, each pair of characters is transformed to the equivalent hexadecimal value.
- Step 6: The hexadecimal values are transformed into 4-bit binary numbers.
- Step 7: A single binary stream is created by concate-

nating the 4-bit binary block.

- Step 8: The binary stream is broken into 5-bit blocks.
- Step 9: A subtraction occurs between the 5-bit binary blocks and the 32-bit key, divided into 4-bit blocks.
- Step 10: The binary blocks resulting from subtraction are concatenated into a single block.
- Step 11: A reverse sequence is determined for the binary block.
- Step 12: An XOR process is executed between the reversed and the original binary blocks.
- Step 13: The result binary block is divided into 4-bit blocks, each transformed into a one-digit integer number.
- Step 14: The sequence of decimal numbers is broken into blocks of length n. Each element in the block includes decimal numbers that consist of two digits.
- Step 15: For the key matrix (K), an inverse key matrix (K-1) is determined.
- Step 16: According to equation 7, the Hill cipher decryption process is applied to each decimal block using K^{-1}.
- Step 17: The blocks of the decimal number are concatenated into a single sequence.
- Step 18: Each decimal number is converted into a character based on TableII to get the original message.

6. Simulation Results

The algorithm described in section 5 is simulated using the bio-informatics toolbox in C-sharp (C#). A personal computer with an Intel(R) Core (TM) i5-3230M CPU running at 2.60 GHz and with RAM of 16 GB is used for the research. We examine our method's security behaviour in light of other DNA cryptography techniques. A plaintext message "GOAL", a key matrix $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$, a block length of value 2, and a 32-bit key are considered to be executed by the proposed technique. Figure 3 shows the simulation result for the considered case using the proposed approach.

The proposed technique's performance is compared with three encryption approaches [8][29][30]. Figure 4 shows further simulations. The same plaintext message is executed, and all required parameters for these approaches are considered.

In [8], steganography and encryption were performed by combining DNA with the Ceaser cipher. Using a 6-bit key, the addition process was applied to the Ceaser encryption output before DNA encryption was used. In [29], the plaintext was encrypted using DNA encoding, a binary complement, and decimal indexing. This work uses no keys.

In [30], the encryption process was initiated and terminated with the DNA. After the initial use of DNA, the suggested key and the DNA result are subjected to a complement procedure. Later, the supplemented streams were subjected to an XOR procedure. Ultimately, steganography was accomplished using the DNA. Compared to these works, the proposed approach can provide more security to the encrypted plaintext. The key used in the proposed approach is more powerful, consisting of an (n×n) key matrix and a 32-bit key.

Furthermore, the proposed approach involves more modifications. This leads to a slight increase in computing complexity, but on the other side, it also increases its power. Table III compares the proposed and other approaches.

7. Security Requirements and Performance Analysis

This section demonstrates the suggested method's compatibility with security specifications and resistance to security breaches.

A. Security Requirements Analysis

In this subsection, we list some of the security concerns raised in the literature and how well the suggested approach fulfils them.

1) Authentication and Integrity: authentication refers to confirming the identification of an entity or user. Moreover, Integrity guarantees that information is not changed or tampered with while transmitted or stored [31][32]. In the case of using a secure approach for key distribution among the communicating parties, along with a combination of two keys, a matrix key and a 32-bit key, the proposed system can fulfil these security requirements.
2) Confidentiality prevents sensitive information from being accessed, disclosed, or used without authorization [31][32]. It is challenging for an adversary to decipher the ciphertext message without knowing the key matrix and the 32-bit key.
3) Data freshness: It shows how current or pertinent the data is. Data freshness proposes that the data is recent such that no adversary can replay an old message [31]. Key updating over time and using a sequence number attached to each encrypted message guarantee that the proposed technique realizes this requirement.

B. Security attack analysis

1) Man-in-middle attack and Eavesdropping: Man-in-middle attack occurs when an attacker secretly intercepts and potentially modifies communications between two parties. The act of surreptitiously listening to a communication without that person's knowledge or consent is known as eavesdropping [33][34][35]. The proposed technique can withstand these attacks,

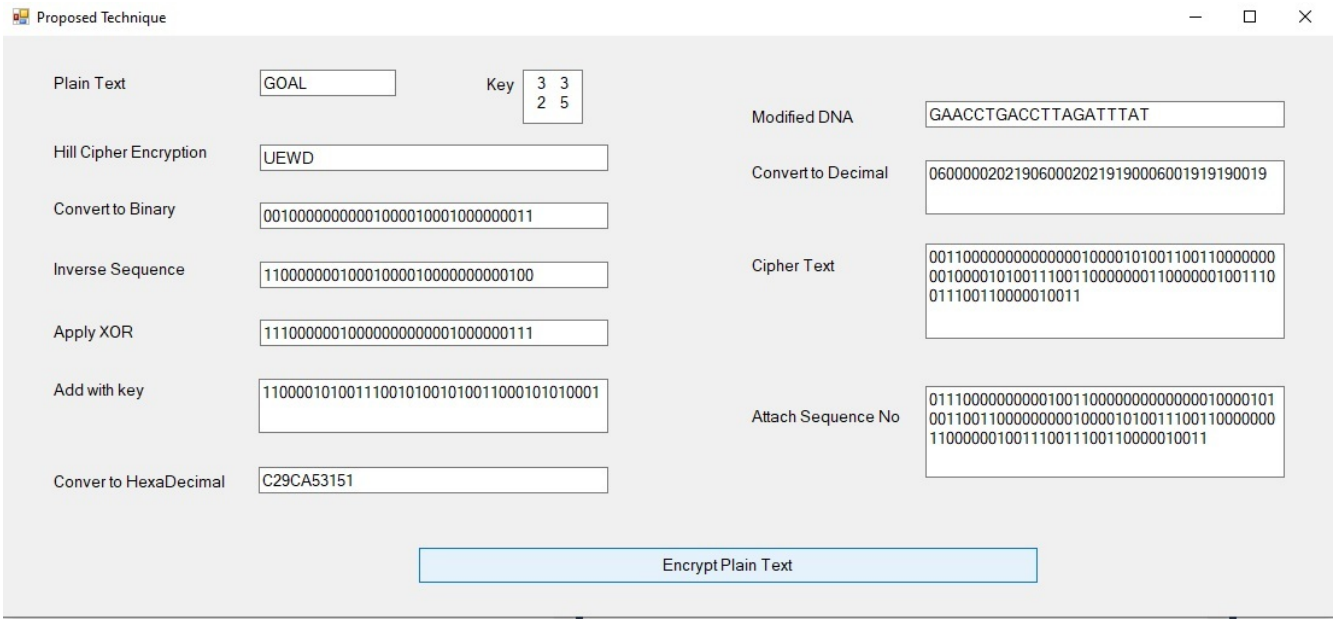

Figure 3. Simulation of the proposed encryption process

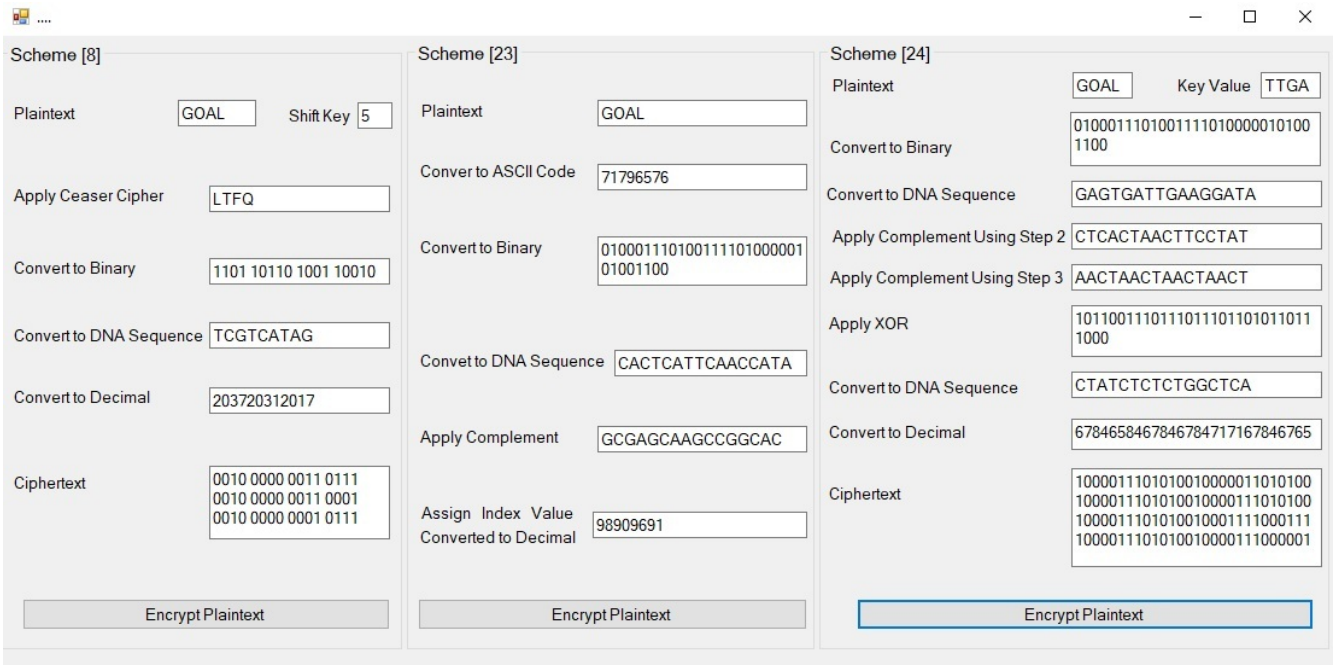

Figure 4. Simulation of other encryption processes

where all transmitted messages are encrypted, and no useful data about the plaintext or the keys is revealed from the ciphertext.

2) Masquerade: the masquerade is described as pretending to be someone else [34][35]. Using a secret approach in key distribution among the communication parties and the difficulty in determining the secret keys from the ciphertext are the tools used by this proposed approach to withstand this attack.
3) Replay: It is a type of cyberattack in which the attacker gains access to legitimately transferred data between parties and maliciously retransmits it later [33][34][35]. This sort of attack is withstood by attaching a sequence number to each transmitted message.

TABLE III. Comparing proposed approach with other literary schemes

Scheme	Comparison Evaluation	Cryptographic method used	Key Number	Steganography method	Type of Encryption
Scheme [30]	Middle	XOR operation and DNA sequence	One Key	No steganography	Symmetric
Scheme [29]	Low	Based on the concept of DNA sequence	No Key	Data hiding	Symmetric
Scheme [12]	Middle	DNA sequence with 64 codons	No Key	No steganography	Symmetric
Scheme [8]	High	Combines DNA sequence with Caesar Cipher	One Key	DNA steganography and cryptography	Symmetric
Proposed approach	High	Combines Modified DNA, Hill Cipher, XOR, and addition with 32-bit key	Two Keys	DNA steganography and cryptography	Symmetric

The algorithm has some weaknesses in the context of high complexity because it includes several transformations, which are used to increase the algorithm's security. Each transformation contributes to the overall complexity, which often refers to time and space complexity. It involves steps that increase the execution time and the memory required.

It is possible to improve the proposed approach in the future either by specifying the most costly transformation and optimizing it to enhance algorithm efficiency or by developing alternative algorithms or techniques that achieve similar results with lower complexity. In addition, it may be possible to develop a mechanism that reduces the number of conversions and replaces them with simplified mathematical operations.

8. Conclusions

Data can be transmitted securely over the network by combining cryptography and steganography. Combining these techniques is one of the modern cryptography methods, and it is a strong guarantor of secure data transmission over the network. This paper applies a hybrid technique by mixing between encryption and steganography methods. A sequence of modifications is applied to the plaintext message, including Hill cipher, reversing, and addition with a key, before applying the Modified DNA to the encrypted message. The proposed technique was compared with other works and analyzed in terms of security requirements and its ability to counter security attacks. The proposed approach matches security requirements well, counters several attacks, and is appropriate for secure data transmission.

References

[1] M. Chanchal, P. Malathi, and G. Kumar, "A comprehensive survey on neural network based image data hiding scheme," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2020, pp. 1245–1249.

[2] Y. Wang, Q. Han, G. Cui, and J. Sun, "Hiding messages based on dna sequence and recombinant dna technique," *IEEE Transactions on Nanotechnology*, vol. 18, pp. 299–307, 2019.

[3] G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba, "Hybrid technique for steganography-based on dna with n-bits binary coding rule," in *2015 7th International Conference of Soft Computing and Pattern Recognition (SoCPaR)*. IEEE, 2015, pp. 95–102.

[4] B. Purnama and A. H. Rohayani, "A new modified caesar cipher cryptography method with legibleciphertext from a message to be encrypted," *Procedia Computer Science*, vol. 59, pp. 195–204, 2015.

[5] A. Majumder, A. Majumdar, T. Podder, N. Kar, and M. Sharma, "Secure data communication and cryptography based on dna based message encoding," in *2014 IEEE international conference on advanced communications, control and computing technologies*. IEEE, 2014, pp. 360–363.

[6] S. Singh and Y. Sharma, "A review on dna based cryptography for data hiding," in *2019 International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 2019, pp. 282–285.

[7] S. Marwan, A. Shawish, and K. Nagaty, "Utilizing dna strands for secured data-hiding with high capacity." *International Journal of Interactive Mobile Technologies*, vol. 11, no. 2, 2017.

[8] Y. N. A. Taher, K. A. Ameen, and A. M. Fakhrudeen, "An efficient hybrid technique for message encryption using caesar cipher and deoxyribonucleic acid steganography," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 2, pp. 1096–1104, 2022.

[9] O. A. Al-Harbi, W. E. Alahmadi, and A. O. Aljahdali, "Security analysis of dna based steganography techniques," *SN Applied Sciences*, vol. 2, no. 2, p. 172, 2020.

[10] K. Sajisha and S. Mathew, "An encryption based on dna cryptography and steganography," in *2017 international conference of electronics, communication and aerospace technology (ICECA)*, vol. 2. IEEE, 2017, pp. 162–167.

[11] L. M. Gupta, H. Garg, and A. Samad, "An improved dna based security model using reduced cipher text technique," *International Journal of Computer Network and Information Security*, vol. 11,

no. 7, pp. 13–20, 2019.

[12] D. Ratna Kishore, D. Suneetha, and G. Praddep, "Enhancement in data security using dna cryptography," in *Soft Computing and Signal Processing: Proceedings of 2nd ICSCSP 2019 2*. Springer, 2020, pp. 63–70.

[13] Q. S. Alsaffar, H. N. Mohaisen, and F. N. Almashhdini, "An encryption based on dna and aes algorithms for hiding a compressed text in colored image," in *IOP Conference Series: Materials Science and Engineering*, vol. 1058, no. 1. IOP Publishing, 2021, p. 012048.

[14] A. Khalifa, "A secure steganographic channel using dna sequence data and a bio-inspired xor cipher," *Information*, vol. 12, no. 6, p. 253, 2021.

[15] M. Padmapriya and P. V. Eric, "A technique of data security using dna cryptography with optimized data storage," *Journal of System and Management Sciences*, vol. 12, no. 4, pp. 412–438, 2022.

[16] A. O. Aljahdali and O. A. Al-Harbi, "Double layer steganography technique using dna sequences and images," *PeerJ Computer Science*, vol. 9, p. e1379, 2023.

[17] M. Poriye and S. Upadhyaya, "A dna based framework for securing information using asymmetric encryption," *Wireless Personal Communications*, vol. 129, no. 3, pp. 1717–1733, 2023.

[18] A. O. Aljahdali, F. Thabit, A. Munshi *et al.*, "A secure fingerprint hiding technique based on dna sequence and mathematical function," *PeerJ Computer Science*, vol. 10, p. e1847, 2024.

[19] T. Kumar, P. Kumar, and S. Namasudra, "A dna-based authentication system for securing cloud data storage and transactions," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2024, pp. 1692–1698.

[20] K. Menaka, "Message encryption using dna sequences," in *2014 World Congress on Computing and Communication Technologies*. IEEE, 2014, pp. 182–184.

[21] B. M. Kumar, B. R. S. Sri, G. Katamaraju, P. Rani, N. Harinadh, and C. Saibabu, "File encryption and decryption using dna technology," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, 2020, pp. 382–385.

[22] P. N. Srinivasu and S. Rao, "A multilevel image encryption based on duffing map and modified dna hybridization for transfer over an unsecured channel," *International Journal of Computer Applications*, vol. 120, no. 4, 2015.

[23] Z. Qowi and N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," in *Journal of Physics: Conference Series*, vol. 1918, no. 4. IOP Publishing, 2021, p. 042009.

[24] Y. S. Santoso, "Message security using a combination of hill cipher and rsa algorithms," *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA)*, vol. 1, no. 1, pp. 20–28, 2021.

[25] S. Achriadi, M. S. Hanafi *et al.*, "Encryption and description of rgb values in images using the hill chiper algorithm," *Jurnal Inotera*, vol. 9, no. 1, pp. 48–52, 2024.

[26] S. Mandowen *et al.*, "Advanced hill cipher algorithm for security image data with the involutory key matrix," in *Journal of Physics: Conference Series*, vol. 1899, no. 1. IOP Publishing, 2021, p. 012116.

[27] A. Hassan, A. Garko, S. Sani, U. Abdullahi, and S. Sahalu, "Combined techniques of hill cipher and transposition cipher," *Journal of Mathematics Letters*, pp. 57–64, 2022.

[28] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, "Enhancing image encryption with the kronecker xor product, the hill cipher, and the sigmoid logistic map," *Applied Sciences*, vol. 13, no. 6, p. 4034, 2023.

[29] B. Pushpa, "A new technique for data encryption using dna sequence," in *2017 International conference on intelligent computing and control (I2C2)*. IEEE, 2017, pp. 1–4.

[30] V. Siddaramappa and K. Ramesh, "Cryptography and bioinformatics techniques for secure information transmission over insecure channels," in *2015 international conference on applied and theoretical computing and communication technology (iCATccT)*. IEEE, 2015, pp. 137–139.

[31] O. R. Arogundade, "Network security concepts, dangers, and defense best practical," *Computer Engineering and Intelligent Systems*, vol. 14, no. 2, 2023.

[32] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 250–10 276, 2020.

[33] K. A. Ameen, B. A. Mahmood, and Y. N. A. Taher, "Secure message transmission scheme in wireless sensor networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1514–1523, 2021.

[34] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, and M. Liyanage, "A survey on network slicing security: Attacks, challenges, solutions and research directions," *IEEE Communications Surveys & Tutorials*, 2023.

[35] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You, and X. Xu, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44 219–44 227, 2020.