International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

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

Kameran Ali Ameen[1], Walled khalid Abdulwahab[2] Yalmaz Najm Aldeen Taher[3]

[1,2,3] *Department Computer Science, University of Kirkuk, Kirkuk, Iraq*
E-mail address: kameran.ameen@uokirkuk.edu.iq, walled.khalid@uokirkuk.edu.iq, yalmaz.science@uokirkuk.edu.iq

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: The 21st century has seen an explosion of information due to the quick development of technology, making information a far more crucial strategic resource. In addition, there has been a development in hackers' ability to steal information with all their might and intelligence. Consequently, secretly transmitting information became the main concern of all agencies. Further, as classical cryptographic methods are now exposed to attacks, protecting data by a collection of steganography and cryptography techniques is becoming increasingly popular and widely adopted. Therefore, it has been determined that DNA use in cryptography could lead to new technological advancements by converting original text into an unintelligible format. In this paper, a new cryptographic technique that combines Modified DNA sequence with Hill cipher has been proposed. The proposed technique includes four phases: In the first phase, Hill cipher technology encrypts plain text into n-bit binary numbers. Second, perform XOR operations on the result, and then a key value with a length of 32 bits is added to the output of XOR. Third, Modified DNA cryptography is applied to generate ambiguity and steganography. The decryption process, which is the last phase, applies to recover the original message on the receiver side. The proposed scheme provides higher data security when compared to several existing schemes.

Keywords: Hill Cipher, Modified DNA, Cryptography, Steganography, Secure Data Transmission.

1. INTRODUCTION

This In the modern era, with the development of technology, 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 on 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 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].

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

This work proposes a new technique to combine the Modified DNA concept with the Hill cipher. Initially, the original data is encrypted using Hill cipher cryptography, and the XOR operation is then applied to combine the resulting ciphertext with a secret key. Finally, the data is hidden based on Modified DNA cryptography. This method makes it difficult to understand or decipher the plaintext. Moreover, this paper seeks to generate a vague message and to prevent unauthorized access or modification of the secured data.

The rest of this paper is organized as follows: Section 2 discusses a literature review of the related works. The background of the Hill Cipher and the Biological DNA and Modified DNA sequences 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 Advanced Encryption Standard are applied to encrypt a message. The encrypted message is then hidden within a different DNA sequence. This method gives 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 per cent.

In [12] 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. A model for the confidential transmission of sensitive data was presented in this paper.

In [13] 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 for combining the ideas of lossless compression and DNA cryptography with enhanced data storage was put out in [14]. This approach converts regular text into a DNA cipher text using the DNA OTP method. Each DNA nucleotide is given a binary code based on the occurrence of DNA codons. The encrypted text produced by this method is lower in size than the comparable plain text.

In [15] a method that employed a multi-layer steganography process and exploited photos and DNA sequences as carriers of sensitive data was presented. The discrete cosine transform (DCT) approach embeds the fictitious DNA in a picture, and the substation algorithm is utilized to conceal confidential data in the DNA. The findings demonstrate the suggested mechanism's resilience to chi-square and histogram attacks.

3. 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 [16], [17]. 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 [16], [17]. 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 as in equations 1 and 2 [17] [18].

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

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

This case can be expressed in column vectors and matrices as in equation 3.

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{vmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{vmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \bmod 26 \quad (3)$$

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

$$C = K.P \quad (4)$$

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 [18] [19].
To decrypt a ciphertext, we need to use (K-1), which is the inverse of a matrix (K), where;

$$KK^{-1} = K^{-1}K = I \quad (5)$$

and (I) represents the identity matrix [11, 12, 13]. K^{-1} can be applied to recover the plaintext from the ciphertext. Thus, we can simply represent the encryption and decryption process in equations 6 and 7 respectively. 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.

$$C = E(k, P) = K.P \quad (6)$$

4. Background of the Modified DNA 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].

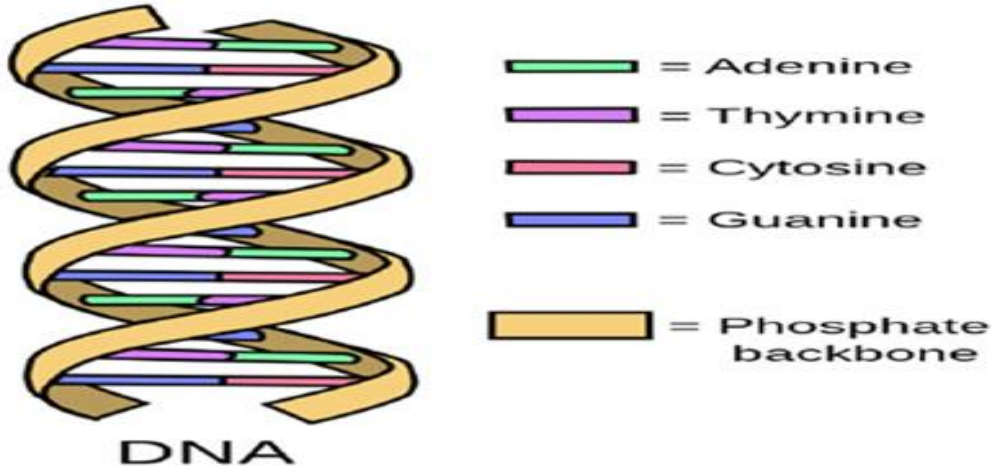

Figure 1. DNA Structure

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 1, 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 coding 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].

TABLE I. Modified DNA based on hexadecimal.

DNA sequence	Hexadecimal Value	DNA sequence	Hexadecimal Value	DNA sequence	Hexadecimal Value	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

5. ROPOSED 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. There are several main steps to implementing our proposal.

Each message character is converted to a number in the first step, according to Table II. 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.

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

A. Encryption Steps by Hill Cipher (Sender side)

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

- 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 2, 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 with a 4-bit key block. The length of the resulting blocks will be increased from 4 bits to 5 bits.
- **Step 10**: Finally, the binary blocks resulting from the addition process are concatenated into one block.

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

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 1, each hexadecimal value is converted into a DNA sequence.
- **Step 4**: Based on Table 2, 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 2, convert each decimal number to the corresponding character.
- **Step 5**: The characters are transformed to the capital form; according to Table 1, 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 concatenating the 4-bit binary block.
- **Step 8**: The binary stream is broken into 5-bit binary blocks.
- **Step 9**: A subtraction occurs between each 5-bit binary block and the 4-bit key 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 block is 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 description 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 Table 2 to get the original message.

6. SIMULATION RESULTS

Before The bio-informatics toolbox in C-sharp (C#) simulates the algorithm described in section 5. A personal computer with an Intel(R) Core (TM) i5-3230M CPU running at 2.60 GHz and 16 GB of RAM is used for the research.

We examine our method's security behaviour in light of other DNA cryptography techniques. Define A plaintext message “GOAL”, a key matrix $\begin{matrix} 3 & 3 \\ 2 & 5 \end{matrix}$, a block length of value 2, and a 32-bit key are considered. The simulation of the encryption process for the considered case using the proposed technique is shown in Figure 2.

The performance of the proposed encryption technique is compared with three encryption approaches

[8],[23],[24]. The simulation of the encryption processes for these approaches is shown in Figure 3. The same plaintext message is executed, and all required parameters for these approaches are considered.

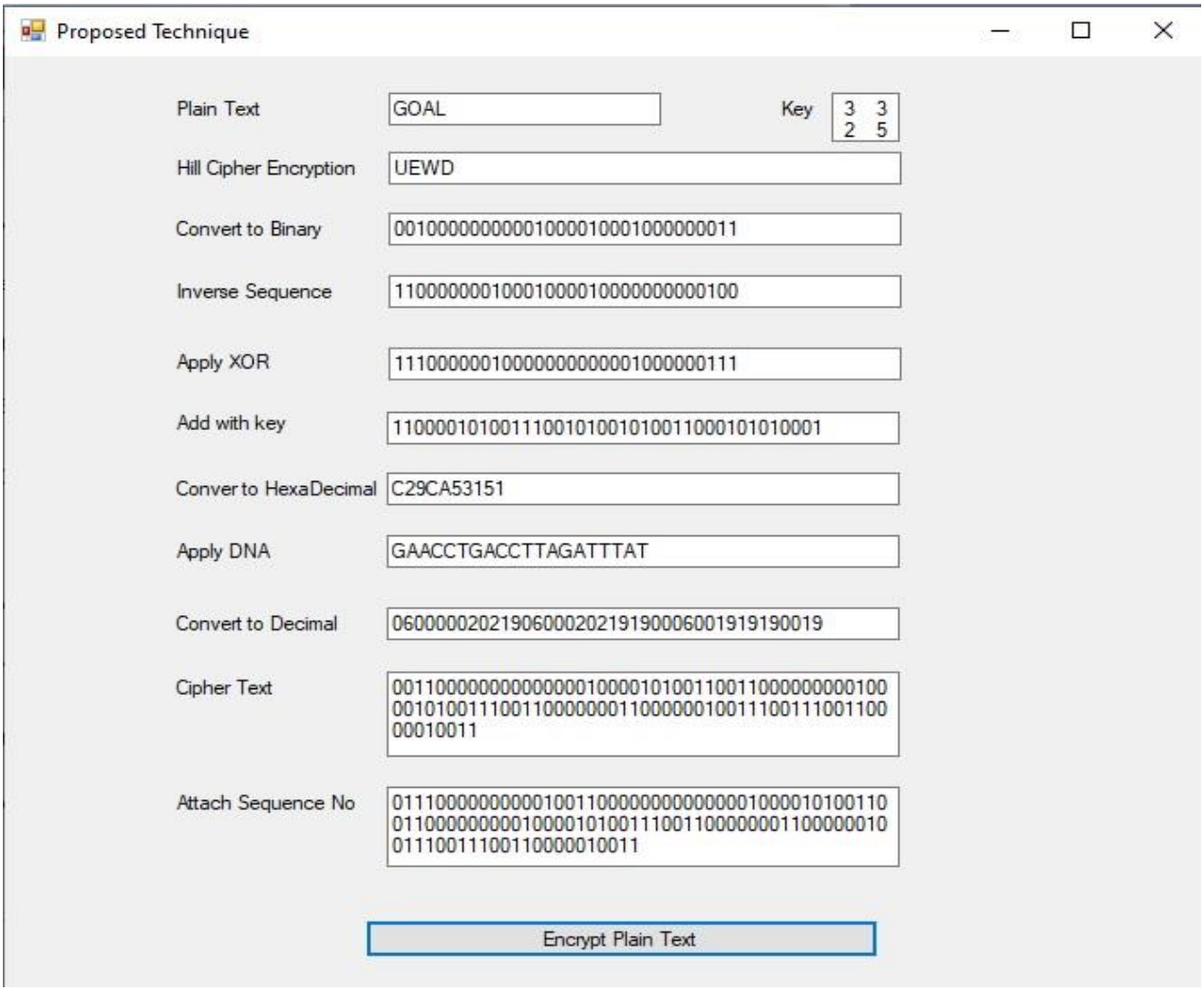

Figure 2. Simulation of the proposed encryption process.

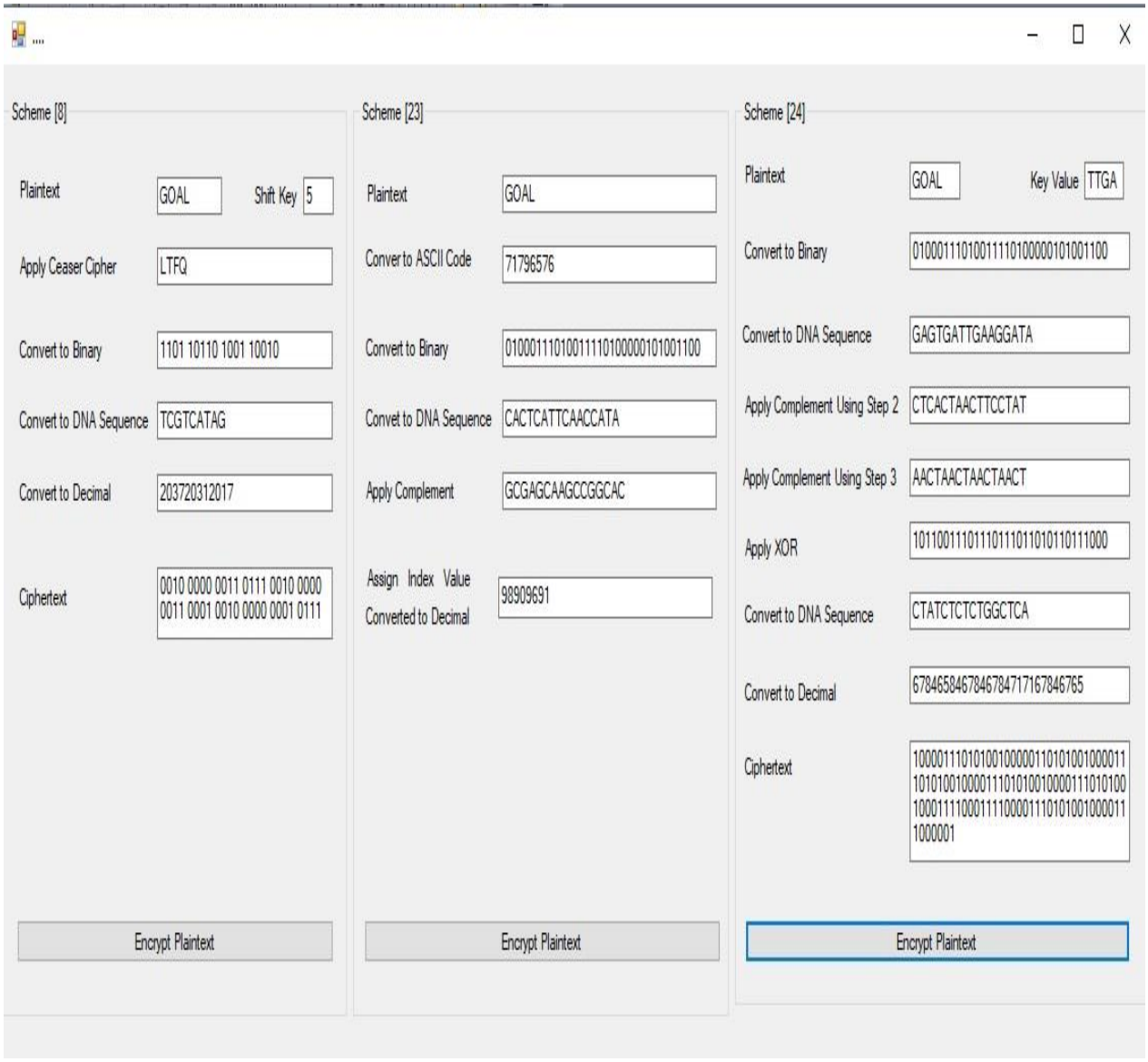

Figure 3. Simulation of other encryption processes.

In [23], the plaintext was encrypted using DNA encoding, a binary complement, and decimal indexing. This work uses no keys. In [24], the encryption process was initiated and terminated with the DNA. Following 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. In [8], steganography and encryption were accomplished 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.

Compared to these works, the proposed approach can provide more security to the encrypted plaintext than other techniques. The key used in the proposed approach is more powerful, consisting of an (n×n) key matrix and a 32-bit key. Furthermore, compared to other procedures, this one involves more modifications. This leads to a slight increase in computing complexity but also increases the power of our strategy. Table III presents further comparisons between the proposed and other approaches.

TABLE III. Comparing our suggestion with a few literary schemes.

Schemes	Comparison Evaluation	Cryptographic method used	Key-value used	Steganography method used	Type of Encryption
Scheme [8]	High	Combines DNA sequence with Caesar Cipher	One Key	DNA steganography and cryptography	Symmetric Encryption
Scheme [23]	Low	Based on the concept of DNA sequence	No Key	Data hiding	Symmetric Encryption
Scheme [24]	Middle	XOR operation and DNA sequence	One Key	No steganography method was used	Symmetric Encryption
Our propose	High	Combines Modified DNA, Hill Cipher, XOR, and addition with 32-bit key	Two Key-values used	DNA steganography and cryptography	Symmetric Encryption

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 fulfills these concerns.

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 [25] [26]. 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 fulfill these security requirements.
2. **Confidentiality**: it prevents sensitive information from being accessed, disclosed, or used without authorization [25],[26]. It is challenging for an adversary to decipher the plaintext message using the ciphertext by employing the Hill cipher, addition with a 32-bit key, and modified DNA.
3. **Data freshness**: It shows how current or pertinent the data is at any particular moment. Data freshness proposes that the data is recent such that no adversary can replay an old message [25]. 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 [27],[28],[29]. The proposed technique can withstand these attacks, where all transmitted messages are encrypted, and no useful data about the plaintext or the keys is revealed from the ciphertext.
2. **Masquerade**: masquerade describes pretending as someone else [28],[29]. Using a secret approach in key distribution among the communication parties, in addition to 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 [27],[28],[29]. This sort of attack is withstood by attaching a sequence number to each transmitted message.

8. CONCLOSIONS

Data can be transmitted securely over the network by combining cryptography and steganography. Combining encryption and steganography is one of the modern methods in the field of cryptography, which is a strong guarantor of secure data transmission over the network. In this paper, a hybrid technique is applied through one of the 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 technique performs better, matches security requirements, counters several attacks, and is appropriate for secure data transmission.

REFERENCES

[1] C. Chanchal, M. Malathi, and G. Kumar, "A Comprehensive Survey on Neural Network ased Image Data Hiding Scheme," *In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India*, IEEE, pp. 1245–1249, Oct. 2020.

[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, Mar. 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), Fukuoka, Japan*, IEEE, pp. 95–102, Nov. 2015.

[4] B. *Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from a Message to Be Encrypted," Procedia Computer Science, Elsevier*, vol. 29, 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, Ramanathapuram, India*: IEEE, pp. 360–363, May 2014.

[6] S. Singh and Y. Sharma, "A Review on DNA Based Cryptography for Data Hiding," *In 2019 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India*: IEEE, pp. 282–285, Feb. 2019.

[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, pp. 88–98, Apr. 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, Nov. 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, pp. 172, Feb. 2020.

[10] K. S. Sajisha and S. Mathew, "An Encryption Based on DNA Cryptography and Steganography," *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India*: IEEE, pp. 162–167, Apr. 2017.

[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, July 2019.

[12] 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, pp. 1-12, Feb. 2021.

[13] A. Khalifa, "A Secure Steganographic Channel Using DNA Sequence Data and a Bio-Inspired XOR Cipher," *Information*, vol. 12, no. 6, pp. 253-267, Jun 2021.

[14] M. K. 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.

[15] A. O. Aljahdali and O. A. Al-Harbi, "Double Layer Steganography Technique Using DNA Sequences and Images*," PeerJ Computer Science*, vol. 9, pp. 1379-1400, May 2023.

[16] Z. Qowi and N. Hudallah, "Combining Caesar Cipher and Hill Cipher in The Generating Encryption Key on The Vigenere Cipher Algorithm," *Journal of Physics: Conference Series*, vol. 1918, no. 4, 2021.

[17] Santoso, Y. S, "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, Mar. 2021.

[18] T. S. Achriadi, Hardisal, Asmaidi, and M. S. Hanafi, "Encryption and Description of RGB Values in Images Using the Hill Chiper Algorithm," *Jurnal Inotera*, vol. 9, no. 1, pp. 48–52, Jan. 2024.

[19] 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, pp. 4034-4057, Mar. 2023.

[20] K. Menaka, "Message Encryption Using DNA Sequences," *In 2014 World Congress on Computing and Communication Technologies, Trichirappalli, India:* IEEE, pp. 182–184, Feb. 2014.

[21] B. M. Kumar, B. R. S. Sri, G. M. S. A. Katamaraju, P. Rani, N. Harinadh, and Ch. Saibabu, "File Encryption and Decryption Using DNA Technology," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India*: IEEE, pp. 382–385, Mar. 2020.

[22] P. NagaSrinivasu and Ch. Seshadri 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, pp. 1–4, June 2015.

[23] B. *R. Pushpa, "A New Technique for Data Encryption Using DNA Sequence," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India: IEEE*, pp. 1–4, June 2017.

[24] V. Siddaramappa and K. B. Ramesh, "Cryptography and Bioinformatics Techniques for Secure Information Transmission over Insecure Channels," *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India*: IEEE, pp. 137–139, Oct. 2015.

[25] O. R. Arogundade "Network Security Concepts, Dangers, and Defense Best Practical," *Computer Engineering and Intelligent Systems*, vol. 14, no. 2, pp. 25-38, July 2023.

[26] 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 Things Journal*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020.

[27] 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.

[28] 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*, vol. 26, no. 1, pp. 534 - 570, 2023.

[29] *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. 44219–44227, Mar. 2020.

Kameran A. Ameen is currently instructor at University of Kirkuk, Kirkuk, Iraq. He received a B.Sc. degree in Computer Science from Kirkuk University/ College of Science, Kirkuk, Iraq in 2008 and an M.Sc degree in Information Technology from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: Computer Networks, Security in Wireless Sensors Network, Authentication in Wireless Sensors Networks, Attacks in Wireless Sensors network and Encryption/Decryption.

Walled K. Abdulwahab was born in Baghdad, Iraq, in 1978. He received a (B.Sc.) degree in Information Engineering from the University of Baghdad in 2001 and (M.Sc.) and (PhD) degrees from Al-Nahrain University, Iraq, in 2012 and 2021, respectively, in Information and Communication Engineering. He published 6 papers in international and national journals and scientific conferences. His research interests cover Modern error correction codes for next-generation networks, low-complexity decoders, and mmWave channel modelling.

Yalmaz N. Taher is currently instructor at University of Kirkuk, Kirkuk, Iraq. He received a B.Sc. in Computer Science from Kirkuk University/ College of Science, Kirkuk, Iraq in 2006 and an M.Sc in Mathematics and Computer Science from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: Database, Data mining and Cloud Computing.