An efficient hybrid technique for message encryption using caesar cipher and deoxyribonucleic acid steganography

Yalmaz Najm Aldeen Taher[1], Kameran Ali Ameen[2], Ahmed M. Fakhrudeen[2]
[1]Department of Computer Science, University of Kirkuk, Kirkuk, Iraq
[2]Department of Software, University of Kirkuk, Kirkuk, Iraq

Article Info

Article history:

Received Jul 12, 2021
Revised Aug 6, 2022
Accepted Aug 26, 2022

Keywords:

Caesar cipher
Cryptography
Deoxyribonucleic acid sequence
Encoding
Security

ABSTRACT

Due to security threats on data transmission, a combination of cryptography and steganography techniques are becoming increasingly popular and widely adopted. Correspondingly we have also witnessed most of the literature uses steganography systems development that depends on deoxyribonucleic acid (DNA). However, they are not sufficient to accommodate data security needs nowadays. Therefore, we propose a new cryptographic technique that combines Caesar cipher and DNA cryptography without affecting its functionality or type. In the beginning, a cryptography method encodes the original message and then conceals it into any cover medium by steganography methods. Comparison experiments have been conducted to verify the effectiveness of our proposal. The results demonstrate that our technique outperforms its counterpart in terms of time and complexity.

Corresponding Author:

Kameran Ali Ameen
Department of Computer Science, University of Kirkuk
Kirkuk, Iraq
Email: kameran.ameen@gmail.com

1. INTRODUCTION

Nowadays, data security has become a significant challenge in networks. Data security sent over the network is increasing importance with the fast development of the technology and its integrity and confidentiality [1], [2]. Due to security threats on data transmission, there is a need to enhance the existing methods and techniques to learn communication features in the presence of introducer hacking technologies [3]. Cryptology is existed for more than 2000 years [4], [5]. Briefly, cryptography is the science of hiding data over communications from external threats. Additionally, it is a powerful technique to secure confidentiality, data integrity, and authentication. Therefore, cryptographic techniques are applied to provide security for information such that only authorized persons can decode it [6], [7].

Cryptography has been used in many technologically advanced applications, such as ATM cards, computer passwords, and e-commerce [8], [9]. Secret writing can be achieved by converting plain text into cipher text employing a cryptographic technique. Security is concerned with the protection of data sent/received while transmitting over the networks. For improving data security and maintain confidentiality, there is a need for an effective encryption technique. In cryptography literature, data hiding techniques have been increased continuously due to the necessary demand for data protection [10]. Therefore, achieving complete data security is a challenging issue [7].

Deoxyribonucleic acid (DNA) has been explored as a new carrier for data hiding in the literature. The hereditary material is considered the building block of life in all living organisms [11], [12]. Several methods have been conducted for executing DNA computers (DNA-based) [13], [14]. DNA sequences have some inherent features that can be utilized to hide data. Therefore, it is difficult to distinguish between a real

DNA sequence and a fabricated one [6], [11]. DNA has many advantages; For example, it is capable of storing vast amounts of data. Furthermore, the simplicity of converting data to a DNA sequence leads to its promising effect in Steganography. Moreover, its complexity and randomness enable it to hide any message type and length without noticing [12], [15].

Nevertheless, not all schemes (based on DNA or Caesar cipher) provide robust security than the security requirements exiting [16]. Therefore, this paper proposes a new encryption technique that combines Caesar cipher and DNA cryptography concepts. The benefit of this scheme is that it makes it hard to read and guess about plain text. Finally, the paper aims to combine Caesar's cipher and DNA sequence to prevent unauthorized access to or modification.

The rest of this paper is structured as follows. Section 2 describes the Biological DNA theorem and Caesar cipher. In section 3, we provide essential information about the related works. Section 4 introduces our proposed technique. Section 5 presents an example of implementing the technique. In section 6, we evaluate our technique's security robustness via a series of experiments and comparisons. Finally, in section 7, we conclude by summarizing this paper’s findings.

2. BIOLOGICAL DNA THEOREM AND CAESAR CIPHER

2.1. Biological DNA

Recently, biotechnology has been applied to different fields, where it uses biological information as a carrier to hide data. Hiding data has become an attractive challenge in networks. Biological DNA consists of two strands of nucleotides, each of the strands is coded with four DNA bases, namely [A - adenine], [G - guanine], [C - cytosine], [T - thymine] [17]. The DNA bases are bonded via hydrogen bonds: A with T and C with G. These pairs are complementary DNA strands [7], [18]. The simplest DNA coding patterns encode the four nucleotide bases (A, T, C, and G). As listed in Table 1, it is utilizing four digits like 0(00), 1(01), 2(10), 3(11) [6], [7], [16].

Here is how to display a pop-up window from which to select and apply the AIP Conference Proceedings template paragraph styles. With the advances in DNA cryptography, some researchers work on the DNA directly or indirectly, while others work on incorporating DNA properties into their techniques. For example, ty confirmed that the DNA sequence properties could encrypt data by combining the message into the DNA sequence [16]. The main advantages of DNA that make it efficient for data hiding and transmission are as follows:

a) High storage capacity.
b) The simplicity of encoding data into a DNA sequence makes it a suitable choice for data encryption within it.
c) Complexity and randomness enable it to hide any message type and length without noticing as shown in Table 1.

Table 1. The parameters of the simulation

DNA Base	Binary bits
A	00
C	01
G	10
T	11

2.2. Caesar cipher

Julius Caesar is considered one of the first persons who used encryption to ensure messages while communicating with his generals. Caesar cipher is one of the earliest and most well-known encryption techniques [19], [20]. It is one of the classical substitution type ciphers where each letter in the plaintext is replaced by a letter of some fixed number known as the key of places down the alphabet [4], [21], [22]. For example, with a shift of 3, A would be replaced by D, B would be replaced by E, and C would be replaced by F as shown in Figure 1.

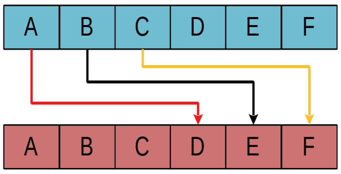


Figure 1. A scheme for codifying messages by replacing each alphabet with an alphabet three places down the line 2

3. RELATED WORKS

In this section, we briefly review some related works are reviewed. The authors in [6] proposed a technique based on DNA patterns to implement data steganography. The technique uses the concept of binary coding to encrypt the source data and apply complementary rules. The DNA sequence is considered a sample to encrypt the message. The technique's stages were designed to work as follows: The plain text converts into an AgI seeding cloud impact investigation (ASCII) code in the first stage. Then, it transforms into a binary-coded form in the DNA sequence where each character is represented using 8 bits. Finally, it implements complementary rules for the DNA sequence.

A new scheme of DNA nucleotides and RNA was proposed in [3]. The scheme aims to generate solutions to hide the message based on the cryptography system over channel communication. The scheme firstly converts data into binary numbers and then to DNA letters. First, the complementary rules of DNA are applied to a DNA-based form of data and the key value. Next, it implements xanthine oxidoreductase (XOR) between the binary form of the key and data. Then, the result converts into a DNA sequence again and then to ASCII code. Lastly, it converts to bits binary.

In Majumder [16] proposed a scheme based on DNA sequence to hiding data. The technique procedure can be summarized as follows: Firstly, it selects a random DNA string. Secondly, the message is converted into its ASCII, and it is then converted into a binary number based on 8 bits. Thirdly, the message index position in the DNA is applied to each letter of the converted sequence. Lastly, each digit in the resultant sequence is replaced with its equivalent three-digit binary value, and the equivalent alphabet value is replaced for the binary value.

In Barmana and Sahab [23], the authors proposed a novel cryptographic scheme that uses a combination between DNA encoding and EC cryptography as a stable security structure of internet of things (IoT). The scheme firstly converts the data into binary data. Then, the DNA sequence is converted into binary DNA. After that, the scheme segments it with k bits in a segment. Next, it inserts each bit of binary data into the beginning of each segment of binary DNA. Then, it concatenates segments of binary DNA and converts them into DNA nucleotides. Lastly, covert ASCII (DN) to EC point, which is an encrypted ciphertext point.

4. THE METHODS

DNA cryptography is challenging to realize in the current time because it can be performed only in labs using chemical processes. Therefore, an efficient scheme (based on Caesar cipher cryptography and DNA cryptography) is proposed here. The scheme aims to ensure robustness and high security to data transmission over the network. The procedures of implementing our scheme consist of three main phases as shown in Figure 1.

Phase 1: The data is encrypted by Caesar cipher.

Phase 2: Encryption using DNA and adding the bits to it.

Phase 3: Decryption process (the reverse process of phases 1 and 2).

4.1. Encryption phases

4.1.1. Caesar cipher

This phase consists of the following steps:

- The sender and receiver select the key value (k) used in the encryption and decryption process and must be secret.
- The sender takes a message that needs to be sent to the receiver over a network.
- Then, each letter of the message is converted into its corresponding sequence according to Table 2.
- Next, in (1) will be applied to encrypt the original message.

$$C = E(k,p) = (p + k) mod\ P \tag{1}$$

Where:

$C\ (p)$ represents the ciphertext that will be sent.

P is a letter of the message.

k refers to the key value.

Table 2. Character value

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

4.1.2. Apply DNA cryptography

Several transmissions are applied to the output of the first phase to get the DNA's encryption. The steps are as follows:

- Every result of the encryption character (represented in the first phase) is converted into a binary number that consists of 6 bits. So, for example, (22) will be (010110), and (0) will be (000000).
- Concatenate the segments of each result (in the step above) into one segment.
- Insert the binary numbers (01), (10), and (11) to the first, second, and third segments, respectively (where the segment consists of 6 bits).
- The last three steps of addition are replayed for the characters sequentially. Similarly, the same process will implement on the remaining letters.
- In the following procedure, concatenate the segments of each result above one part.
- According to Table 1, every two bits (from the one part) formed in the preview step will be converted into a DNA sequence.
- According to Table 2, each DNA sequence is changed with the corresponding sequence value in Table 2 (which is an integer number).
- All values in the preview step's output are converted into binary numbers in 5 bits form. Next, concatenate all the outcomes from the last conversion. Finally, cipher message C is created, as shown in Figure 2.

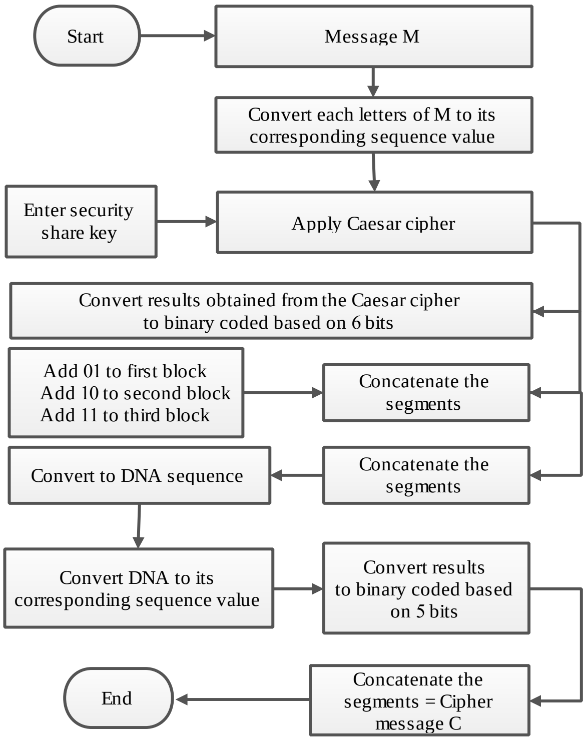

Start
Message M
Convert each letters of M to its corresponding sequence value
Enter security share key
Apply Caesar cipher
Convert results obtained from the Caesar cipher to binary coded based on 6 bits
Add 01 to first block
Add 10 to second block
Add 11 to third block
Concatenate the segments
Convert to DNA sequence
Concatenate the segments
Convert DNA to its corresponding sequence value
Convert results to binary coded based on 5 bits
End
Concatenate the segments = Cipher message C

Figure 2. Flowchart of the encryption proposed technique

4.2. Decryption phase

This phase starts when the recipient receives the cipher message C. Here, several transmissions will be applied to get the plain text by the following steps.

- Separate the cipher message into segments; every segment consists of 5 bits.
- Convert each segment into an integer number.
- According to Table 2, each integer number is changed with the corresponding sequence value in the Table (which is a letter).
- Depending on Table 1, every letter in the preview step's output will be converted into DNA Binary bits.
- In the following process, concatenate all the bits into one part and split the result into segments consisting of 6 bits.

- The binary numbers (01), (10), and (11) are subtracted from the first, second, and third segments, respectively. Later, these three subtractions are replayed for the remaining segments in the same way. Then concatenate all the results in one section.
- The resulting section will be divided into segments based on 6 bits and convert each segment into a letter according to Table 2.
- Each letter in the result (on the last step) is used in (2) to get new results and use the same key value used in encryption. Lastly, the last outcomes are converted into letters according to Table 2, creating the original message as shown in Figure 3.

$$p = D(k, C) = (C - k) mod\ P \qquad (2)$$

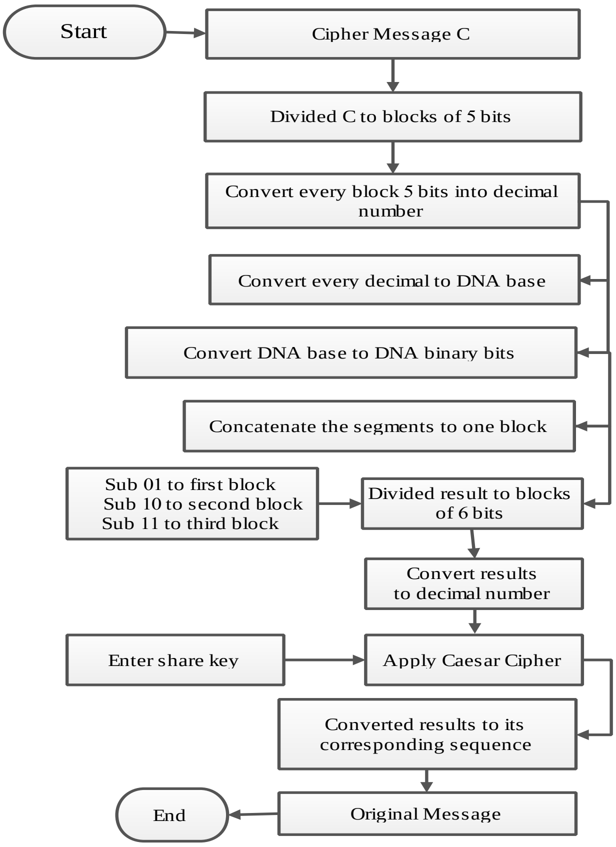

Start
Cipher Message C
Divided C to blocks of 5 bits
Convert every block 5 bits into decimal number
Convert every decimal to DNA base
Convert DNA base to DNA binary bits
Concatenate the segments to one block
Sub 01 to first block
Sub 10 to second block
Sub 11 to third block
Divided result to blocks of 6 bits
Convert results to decimal number
Enter share key
Apply Caesar Cipher
Converted results to its corresponding sequence
End
Original Message

Figure 3. Flowchart of the decryption proposed technique

5. EXAMPLE

This section provides an example of how our proposed technique may work. The methodology mentioned above will be implemented here. The example is divided into eight steps.

a) Consider a message M is “turn”.

b) Each letter of the message is converted to its corresponding sequence according to Table 2 as the following: t = 20, u = 21, r = 18, n = 14.

c) Then, apply Caesar Cipher by (1) to encrypt each message letter when key x= 3, such as Table 3.

Table 3. The parameters of the simulation

Letter	C = (p + K) mod P =	Result
t	(20 + 3) mode 26 =	23
u	(21 + 3) mode 26 =	24
r	(18 + 3) mode 26 =	21
n	(14 + 3) mode 26 =	17

d) Convert all of (23, 24, 21, 17) into a binary-coded form such that each number is represented using 6 bits. 23 = 010111, 24 = 011000, 21 = 010101, 17 = 010001

Then concatenate the segments of each result in this step is “010111011000010101010001”.

e) Add 01 with the first six bits, then add 10 with the second six bits and add 11 with the third six bits. The reply adds 01 with the fourth six bits sequentially as shown in Table 4.

Table 4. The operation add bits

Binary code	Operation +	Result
010111	01	011000
011000	10	011010
010101	11	011000
010001	01	010010

Then concatenate the segments of each result in this step is “011000011010011000010010”.

f) As shown in Table 5, convert the result in step 5 into a DNA nucleotide base, as listed in Table 4.

Table 5. Convert each two-bit to DNA Base

01	10	00	01	10	10	01	10	00	01	00	10
C	G	A	C	G	G	C	G	A	C	A	G

g) As listed in Table 6, we converted the DNA base to its corresponding sequence according to Table 1.

Table 6. Convert each DNA base to digit number

C	G	A	C	G	G	C	G	A	C	A	G
3	7	1	3	7	7	3	7	1	3	1	7

h) Convert all of (3,7,1,3,7,7,3,7,1,3,1,7) into a binary-coded form such that each number is represented using 5 bits, as listed in Table 7.

Table 7. Conversion of the integer number to binary

3	7	1	3	7	7	3	7	1	3	1	7
00011	00111	00001	00011	00111	00111	00011	00111	00001	00011	00001	00111

Concatenate the segments of each result in this step as “000110011100001000110011100111000110011100001000110000100111” which is a cipher message C.

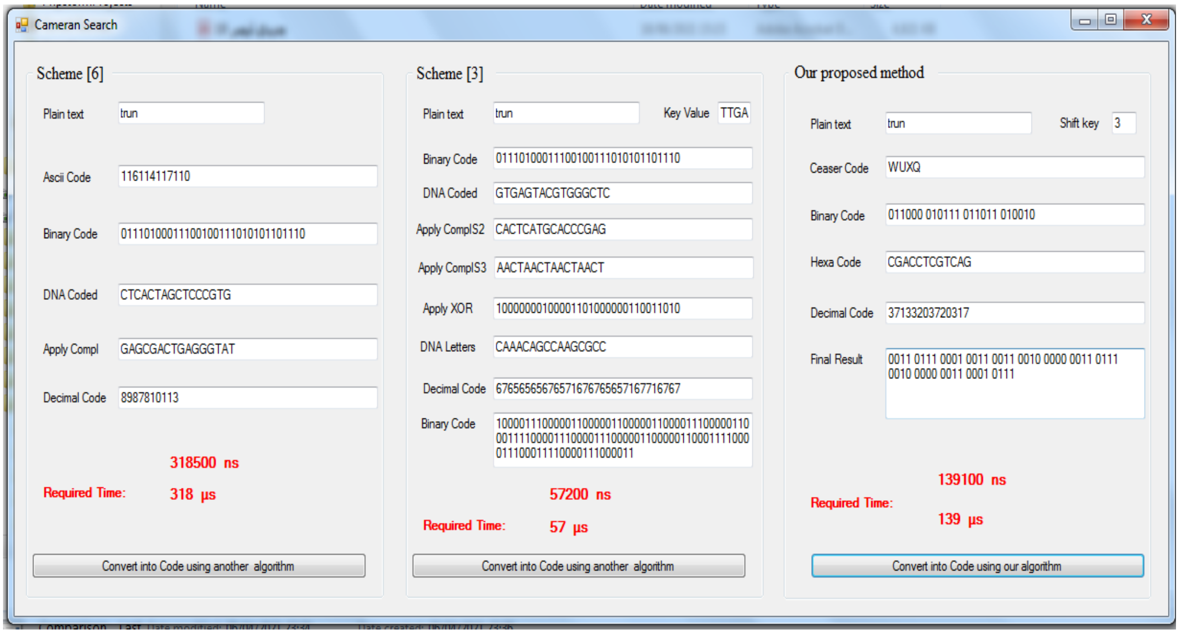
6. SECURITY ANALYSIS

We present experimental results showing the superiority of our technique. The experiments are conducted on Intel(R) Core (TM) i5-3230M CPU @ 2.60 GHz personal computer with 8 GB RAM. The technique is implemented using the C# bio-informatics toolbox. In the second part of this section, we study the security behavior of our technique in comparison with several recent DNA cryptography systems.

6.1. Security analysis

This section evaluates our proposed scheme with some existing counterparts in [3], [6]. In Figures 4 and 5, we calculated the time consumption of encrypting messages. From the figures, we can see that the proposed scheme takes more time from the [3] (which is 57 μsec); however, it takes less than from the [6] (which is 318 μsec). The best explanation of these differences is that the authors in [6] used fewer steps for encryption; however, it lacks to be more secure as our technique does. Additionally, the technique is [3] consumed twice what our technique used because of its complexity. Accordingly, the technique demonstrates that we can balance the strength of the technique. Furthermore, it is possible to get the time required to encrypt the message and the same when applying to decrypt the messages.

Moreover, our proposed scheme's advantage is a low modification, preserving biological functions of the original DNA sequence and simple to be implemented. Moreover, additional bits were added during encrypting to strengthen the scheme. So, the possibility for the attackers to find the original text is very low, and this scheme adds additional security to the message sent.


Cameran Search
Convert into Code using another algorithm
Convert into Code using another algorithm
Convert into Code using our algorithm

Scheme [6]

Plain text: trun

Ascii Code: 116114117110

Binary Code: 01110100011100100111010101101110

DNA Coded: CTCACTAGCTCCCGTG

Apply Compl: GAGCGACTGAGGGTAT

Decimal Code: 8987810113

Required Time: 318500 ns 318 µs

Scheme [3]

Plain text: trun Key Value: TTGA

Binary Code: 01110100011100100111010101101110

DNA Coded: GTGAGTACGTGGGCTC

Apply ComplS2: CACTCATGCACCCGAG

Apply ComplS3: AACTAACTAACTAACT

Apply XOR: 10000000100001101000000110011010

DNA Letters: CAAACAGCCAAGCGCC

Decimal Code: 67656565676571676765657167716767

Binary Code: 100001110000011000001100000110000111000001100011110000011100001110000011000001100011110000111000111100001110000011

Required Time: 57200 ns 57 µs

Our proposed method

Plain text: trun Shift key: 3

Ceaser Code: WUXQ

Binary Code: 011000 010111 011011 010010

Hexa Code: CGACCTCGTCAG

Decimal Code: 37133203720317

Final Result: 0011 0111 0001 0011 0011 0010 0000 0011 0111 0010 0000 0011 0001 0111

Required Time: 139100 ns 139 µs

Figure 4. The details of how the comparison was conducted

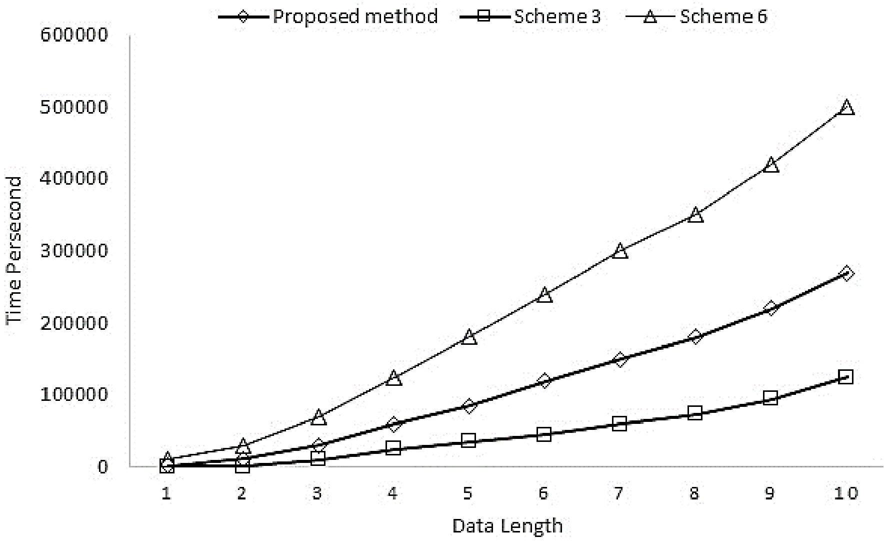


Figure 5. Time consumed to an encryption message

6.2. Performance analysis: A comparison study

Here, the superiority of our technique is rooted in comparing it with several of the DNA-based cryptographic techniques presented in state-of-the-art. The comparisons are conducted in terms of: 1) Data type; 2) Cryptography; 3) The adopted Key-value; 4) The encryption technique used other than DNA encoding; 5) Comparison measures; and 6) Security. The comparisons are listed in Table 8.

Table 8. Comparison between our proposal and some literature schemes

Comparison Measures	Type data	Cryptography used	Key-value used	Encryption Technique used other than DNA encoding	Comparison Measures	Security
Scheme [3]	Any type of data	Symmetric cryptography	The server provided key-value	XOR operation and DNA Complementary rule	Low	The server provided key-value
Scheme [1]	Any type of data	Symmetric cryptography	The user is given key-value	Playfair cipher encryption	Middle	The user is given key-value
Scheme [24]	Any type of data	Symmetric cryptography	The system generates the key value used	DNA-based AES encryption	Middle	The system generates the key value used
Scheme [25]	Any type of data	Symmetric cryptography	The key value is not used	DNA Complementary rule	Low	The key value is not used
Scheme [23]	Any type of data	Symmetric cryptography	The key value is used	Elliptic Curve Cryptography using DNA Encoding	Middle	The key value is used
The proposal	Any type of data	Symmetric cryptography	Key-value is used	DNA based Caesar Cipher	Middle	Key-value is used

7. CONCLUSION

The combination of cryptography and Steganography provides a way for more personal data transfer over a network. Combining DNA-based encryption and Steganography is one of the new systems embedded into the cryptographic field. Here a new hybrid technique is presented by combining the means of cryptography and Steganography as well. In this paper, the secret message that the Ceaser cipher has first encrypted is applied. Then, k bits were added to the messages. Next, the technique encoded the message into DNA bases. The experiments demonstrated that our technique is more secure in comparison with some recently published techniques. Thus, it is not easily accessible for a hacker to crack the encrypted message. The intended receiver can only extract the message by decrypting the cipher information to get the original information. Furthermore, the analysis of the proposed technique shows that this is more powerful against specific attacks. Thus, this technique ensures data integrity and confidentiality over data transmission. Finally, as future work, we plan to extend our work to measure the complexity of our technique compared to the existing techniques in state-of-the-art.

REFERENCES

[1] G. Hamed, M. Marey, S. El-Sayed, and M. 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*, pp. 95-102, 2015, doi: 10.1109/SOCPAR.2015.7492790.

[2] E. Yuan, L. Wang, S. Cheng, N. Ao, and Q. Guo, “A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks,” *Sensors*, vol. 20, no. 6, pp. 1543, 2020, doi: 10.3390/s20061543.

[3] V. Siddaramappa and K. B. 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,* pp. 137-139, 2015, doi: 10.1109/ICATCCT.2015.7456870.

[4] B. Purnamaa 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, doi: 10.1016/j.procs.2015.07.552.

[5] K. Ameen, B. Mahmood, and Y. Taher, “Secure message transmission scheme in wireless sensor networks, ” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1514-1523, 2021, doi: doi.org/10.11591/eei.v10i3.2856.

[6] R. B. Pushpa, “A new technique for data encryption using DNA sequence,” *in 2017 International Conference on Intelligent Computing and Control (I2C2). IEEE*, pp. 1-4, 2017, doi: 10.1109/I2C2.2017.8321834.

[7] K. S. Sajisha and M. Sheena, “An encryption based on DNA cryptography and steganography,” *in 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA) 2017 Apr 20, IEEE*, vol. 2, pp. 162-167, 2017, doi: 10.1109/ICECA.2017.8212786.

[8] O. E. Omolara, A. I. Oludare, and S.E. Abdulahi, “Developing a modified hybrid caesar cipher and vigenere cipher for secure data communication,” *Computer Engineering and Intelligent Systems*, vol. 5, no. 4, pp. 34-46, 2014.

[9] I. Das, S. Singh, S. Gupta, A. Banerjee, Md. Mohiuddin, and S. Tiwary, “Design and implementation of secure ATM system using machine learning and crypto–stego methodology,” *SN Applied Sciences*, vol. 1, no. 9, pp. 1-14, 2019, doi: 10.1007/s42452-019-0988-0.

[10] M. Chanchal, P. Malathi, and T. Kumar, “A comprehensive survey on neural network based image data hiding scheme,” 2020 *Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE,* pp. 1245-1249, 2020, doi: 10.1109/I-SMAC49090.2020.9243579.

[11] G. Cheng, C. Chang, and Z. Wang,“A new data hiding scheme based on dna sequence,” *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 1, pp. 139-149, 2012.

[12] 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, 2017, doi: 10.3991/ijim.v11i2.6565.

[13] D. Naidu, S. Tirpude, K. Kalyani, V. Bongirwar, and T. Sharma,“ Data hiding using meaningful encryption algorithm to enhance data security,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 2, 2020, doi: 10.30534/ijatcse/2020/226922020.

[14] D. Zebari, H. Haron, and S. Zeebaree, “Security issues in DNA based on data hiding: a review,”*International Journal of Applied Engineering Research,* vol.12, no. 24, pp. 15363-15377, 2017.

[15] S. Marwana, A. Shawish, and K. Nagaty, “DNA-based cryptographic methods for data hiding in DNA media,” *Biosystems,* vol. 150, pp. 110-118, 2016, doi: 10.1016/j.biosystems.2016.08.013.

[16] 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 (ICACCCT),* pp. 360-363, 2014, doi: 10.1109/ICACCCT.2014.7019464.

[17] R. M. Indrasena, A.P. Kumar, and K. Reddy, “A secured cryptographic system based on DNA and a hybrid key generation approach,” *Biosystems,* vol. 197, pp. 104207, 2020, doi: org/10.1016/j.biosystems.2020.104207.

[18] M. H. Mohammed, A. I. Taloba, and B. H. Ali, “DNA-based steganography using neural networks,” *2018 International Japan-Africa Conference on Electronics, Communications and Computations,* pp. 79-82, 2018, doi: 10.1109/JEC-ECC.2018.8679564.

[19] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, “A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data,” *IEEE Access*, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739.

[20] K. Singh, R. Johari, K. Singh, and H. Tyagi, “Mercurial cipher: a new cipher technique and comparative analysis with classical cipher techniques,” *in 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE,* pp. 223-228, 2019, doi: 10.1109/ICCCIS48478.2019.8974473.

[21] A. S. Irawan, N. Heryana, and A. Solehudin, “Combination of hill cipher algorithm and caesar cipher algorithm for exam data security,” *Buana Information Technology and Computer Sciences (BIT and CS),* vol. 1, no. 2, pp. 42-45, 2020, doi: doi.org/10.36805/bit-cs.v1i2.1072.

[22] S. N. Gowda, “Innovative enhancement of the caesar cipher algorithm for cryptography,” *in 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA), IEEE,* pp. 1-4, 2016, doi: 10.1109/ICACCAF.2016.7749010.

[23] P. Barmana and B. Sahab, “DNA encoded elliptic curve cryptography system for IoT security*,” International Journal of Computational Intelligence & IoT,* vol. 2, no. 2, 2019.

[24] M. Sabry, M. Hashem, T. Nazmy, and M. E. Khalifa, “Design of DNA-based advanced encryption standard (AES),” *in 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS). IEEE,* pp. 390-397, 2015, doi: 10.1109/IntelCIS.2015.7397250.

[25] K. Menaka, “Message encryption using DNA sequences,” *in 2014 World Congress on Computing and Communication Technologies*, pp. 182-184, 2014, doi: 10.1109/WCCCT.2014.35.

BIOGRAPHIES OF AUTHORS

Yalmaz Najm Aldeen Taher is currently an instructor at the 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 researches in the following areas: Database, Data mining and Cloud Computing. He can be contacted at email: yalmaz.science@uokirkuk.edu.iq.

Kameran Ali Ameen is currently an instructor at the 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 Networks, Authentication in Wireless Sensors Networks, Attacks in Wireless Sensors network, and Encryption/Decryption. He can be contacted at email: kameran.ameen@gmail.com.

Ahmed M. Fakhrudeen is currently the head of the Software department at the College of Computer Science and Information Technology, University of Kirkuk, Iraq. He received Ph.D. in Telecommunication and Data Networks from the University of Salford, Manchester, the United Kingdom, in 2017. Between 2009 and 2013, he was director of the Computer and Internet Centre at the University of Kirkuk's presidency. Between 2017 and 2019, he was head of the Networks department at the College of Computer Science and Information Technology, University of Kirkuk. He researches interest on Cognitive Radio Networks' coexistence issues, Radio Resource Management, and Dynamic Spectrum Access techniques. He can be contacted at email: dr.ahmed.fakhrudeen@uokirkuk.edu.iq.