Significant features for steganography techniques using deoxyribonucleic acid: a review

Nichirvan Asaad Zebari[1], Dilovan Asaad Zebari[2], Diyar Qader Zeebaree[3], Jwan Najeeb Saeed[4]
[1]Department of Computer Engineering, Harran University, Sanliurfa, Turkey
[2,3]Research Center of Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq
[4]IT Department, Duhok Technical Institute, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq

Article Info

Article history:

Received Apr 14, 2020
Revised Jul 5, 2020
Accepted Jul 28, 2020

Keywords:

Cryptography
Data hiding
Data security
DNA

ABSTRACT

Information security and confidentiality are the prime concern of any type of communication. Rapidly evolution of technology recently, leads to increase the intruder's ability and a main challenge to information security. Therefore, utilizing the non-traditional basics for information security is required, such as DNA which is focused as a new aspect to achieve better security. In this paper, a survey of more recent DNA based on data hiding algorithms are covered. With particular emphasis of different parameters several data hiding algorithms based on DNA has been reviewed. To present a more secure an efficient data hiding algorithms based on DNA for future works, this willbe helpful.

Corresponding Author:

Nichirvan Asaad Zebari
Department of Computer Engineering
Harran University, Sanliurfa, Turkey
Email: kurdid08@gmail.com

1. INTRODUCTION

In the recent past, trends in internet applications have necessitated transmission security. The exposure of information during transmission has given rise to the requirement of encryption when transmitting confidential data [1, 2]. Security is a major concern of any type of communication thereby making security and confidentiality necessary for thriving networks. This is due to the unreliable and unsecure nature of the underlying communication network over which the transfer of sensitive information is carried out [3].

The most widely implemented methods in the communication and computer security fields are cryptography and data hiding. Encryption and data hiding approaches are used to investigate and improve individual privacy [4, 5]. The main goal of cryptography is to protect the message from attackers by replacing the original plaintext message with an unintelligible format called a cipher message. In cryptography, if the system is broken, the intruder can find out the real meaning of the message through the process of cryptanalysis. Therefore, the use of cryptography disguises the message thereby keeping it secure from intruders even though the cipher message is made public after encryption [6-8]. Cryptography techniques are divided into two major categories: substitution and transposition. The substitution ciphers encrypt the confidential data by substituting the data one piece at a time. While in the transposition cipher, the positions held by units of confidential data are shifted according to a regular system, so that the cipher data constitutes a permutation of the confidential data [9].

In contrast, data hiding is used in order to avoid rousing the suspicion of attackers. Data hiding is a science that involves communicating secret data using an appropriate carrier. Data hiding gets a role on the stage of information security. Data hiding refers to the technique of hiding information in digital media in order to conceal the existence of the information [10]. Usually, secure communication is achieved through the application of encryption. But nowadays, the day-by-day rise in the demand for security have led to the use of data hiding for information security [11].

The data hiding technique should cause minimal change in the characteristics of the original media once the data is covered in order to conceal its existence. The main objective behind data hiding is to hide data with minimal differences between the original carrier and the modified one (concealing the message) that can be observed by the naked eye. As a consequence, this reduces suspicion on the existence of a concealed message and is characterized by improved algorithm security. As a result, the hacker cannot easily uncover the underlying confidential information [2]. Data hiding is more secure and often preferred to cryptography for two reasons: cryptology is not sufficient in isolation, for the transmission of data over an insecure, public channel; it is the science of covered writing. On the other hand, data hiding is hidden writing which aims at hiding the existence of the message [9, 12, 13].

A general data hiding system usually consists of two algorithms: embedding and extraction. An embedding algorithm outlines the details for the combination of two files to obtain a stego file made up of the secret data and the carrier. The extraction algorithm, on the other hand, outlines the details of how to subtract a file from another file. Moreover, some schemes use an additional key to increase the security level [13, 14]. Based on these, key data hiding algorithms can be divided into three main categories as shown in Figure1: pure data hiding, secret key and public key algorithms. Firstly, pure data hiding does not use any key; its security is based on the privacy of the algorithm [15, 16]. Secondly, the secret key algorithm uses a single key for both embedding and extraction processes. One of the greatest benefits of secret key algorithms is the fast speed of embedding and extraction processes [17, 18]. Finally, the public key algorithm uses a pair of keys: one for embedding and another one for the extraction process. Robustness is the main attribute of public key algorithms; the knowledge of one key by a third party does not guarantee the discovery of the other key [17, 19]. However, this algorithm has lower speed compared to the private key algorithm by a factor of 100-1000 [20].

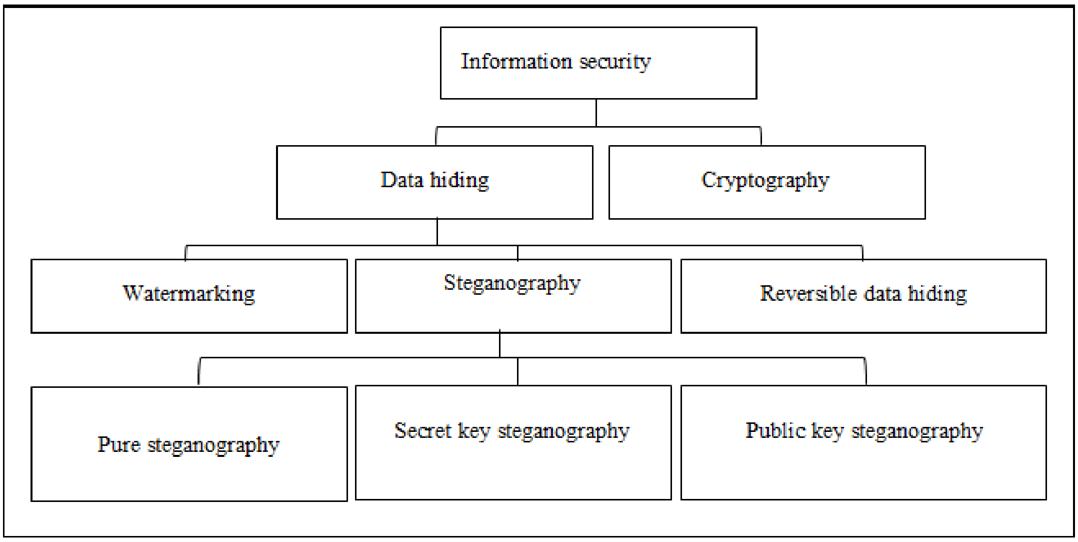

Figure1. Steganography types

Figure 2 shows several multimedia which can serve as data hiding carriers include text, video, audio, and image. Every carrier has its own characteristics and its availability in a certain region which determines the amount of secret information that can be concealed by each carrier [11, 21]. Deoxyribonucleic acid (DNA) is a recent carrier have been used in data hiding area [22, 23]. In this paper, we focus only on data hiding in DNA. The rest of the paper is organized as follow. Section II briefly introduces the background of DNA. Section 2 explained using DNA sequences as a carrier in data hiding technique. Comparative study of recent algorithms is given in Section 3. Finally, the conclusion and future work are given in Section 4.

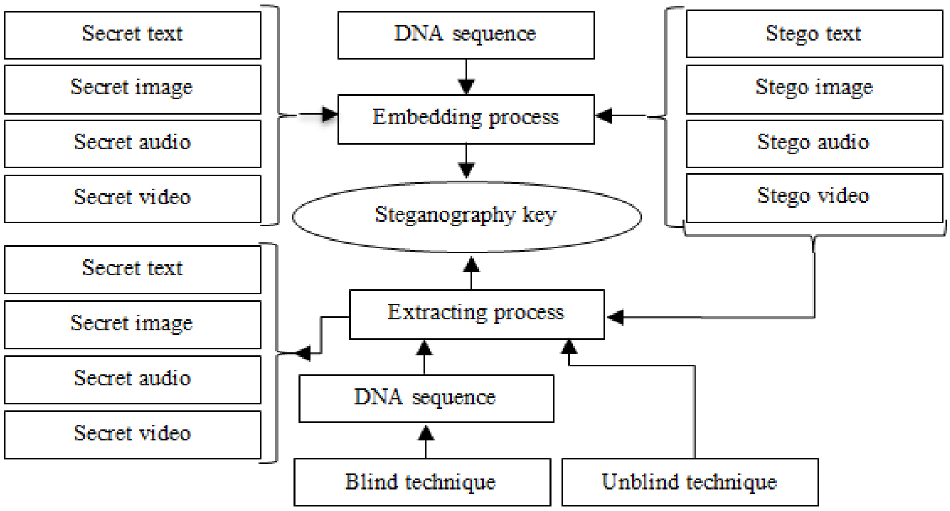

Figure 2. Block diagram of DNA steganography technique

2. DNA

In molecular biology, genetic information and features are stored in DNA. These genetic materials characterize all the behavioral and physical aspects of an organism as it encodes the genetic instructions used in to facilitate the functions of all known living organisms. DNA is a nucleic acid that contains the genetic instructions used in the development and functioning of all known living organisms and viruses [24, 25].

Genetic material known as DNA structure has been found out by Watson and Crick in (1953). DNA is a long molecule located in all living organism's body cells; it is formed by two backbone strands twisted around each other, called a Double helix as shown in Figure 3. Each DNA strand composed of many of tiny subunits called nucleotide. Adenine (A), thymine (T), guanine (G), and cytosine (C) are the four different bases located in DNA sequence which are stick out with sugar and phosphate backbone to complete the nucleotide. Biologically there are two different pairs of DNA bases which are Purine (A and G) and Pyrimidine (T and C). Constantly (A) linked to (T) within two hydrogen bonds and (C) linked to (G) within three hydrogen bonds [26, 27]. Every three adjacent nucleotides constitute a unit known as a codon. With four possible bases, the three nucleotides can give 43 = 64 different possibilities, and these combinations are used to specify 20 different amino acids used by living organisms. The arrangement of the amino acids dictates the structure and function of the resultant protein [17].

DNA can be encoded into a binary form through the use of a binary coding rule. Researchers are free to choose any equivalent binary form for each base (A) can be '00', '01', '10', or '11', and so on. This coding, in addition to the randomness properties makes DNA a suitable candidate for application in both computing and cryptography. Thus, coding DNA to binary form can give 4! = 24 encoding ways [28]. DNA is being proposed for use in many computational applications in a bid to solve many NP-complete and other hard problems [9]. The first experimental of data hiding technique in DNA had done successfully by Clelland using DNA microdots, for concealing secret data [29]. Figure 4 shows a polymer comprised of monomers referred to as deoxyribose nucleotides made up of three components [30].

Recently, protecting confidential data in DNA is born as a new data hiding field. A confidential data instead of chains of zeros and ones can be expressed as a chain of DNA bases. Nowadays a rapid development occurred in the field of data protection; hence a new data hiding approach been depended by protecting data in DNA. Through implementing many researchers on this area data hiding in DNA demonstrated by many researchers as an efficient medium [31]. Data hiding of DNA sequence considered as a branch of cryptography despite of using no encryption [19, 32].

The long-term storage medium of data and an ultra-compact made the DNA to be utilized for concealing, storing, and transmitting information’s is similar to, multimedia carriers. Comparing with other mediums, the area of data hiding in DNA behind several advantages is becoming popular extensively. By combining two DNA sequences with each other, protecting data in DNA can be done just like other medium where used traditional algorithms for concealing information inside them [33-35]. The very high storage capacity feature is one of the most significant benefits of using DNA sequences as a carrier for concealing confidential data. It has ability to store tremendous amount of data, and only one cm (one gram) of DNA has potential to store 455 Exabyte’s of data. Adding to that, more security in term of cryptography and data hiding can be provided for converting any secret data into DNA sequences with more simplicity. Because of that DNA maybe consists of more than 3 billion nucleotides and due to complexity and randomness, it can be considered as a highly efficient carrier for storing information [30, 36].

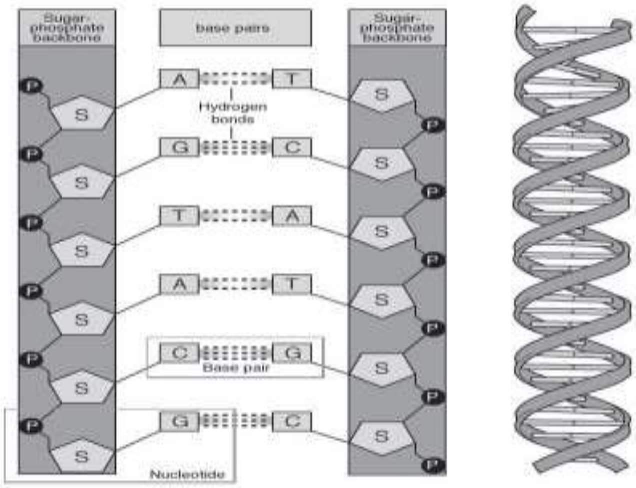

Figure 3. DNA structure [9]

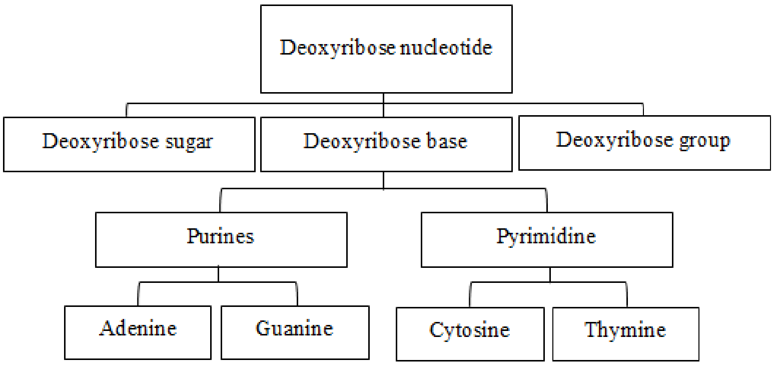

Figure 4. The structure of deoxyribose nucleic DNA[30]

Online databases such as european bioinformatics institute (EBI) and national centre for biotechnology information (NCBI) store vast number of DNA sequences. Thus, for message retrieving the intruders face hard effort to select the exact DNA sequence. The utilization of biological characteristics for embedding data within DNA sequences can be observed as great future of them. The utilization of appropriate methods of data compression provide concealing big amount of information within title DNA, while the same method can be depended with other media that will be used for concealing less data. However, one of the most crucial DNA sequence characteristics is visibility. The real and fake DNA sequence can be distinguished by unauthorized users because the very low visibility. Hence, it is extremely hard or unachievable for the intruders to break the data hiding system of DNA sequences because of the complexity of operations and convert nature of DNA [30, 37]. So, these DNA's benefits and characteristics exploited to conceal confidential data within it.

Several advantages achieved by comparing protecting data in DNA with hiding data in image. First, one of the drawbacks of image is that the opportunity of intruders to extract the message and the distortion will be increased with increasing the embedding capacity and concealing more data. In the other hand, because of that DNA sequence consists of four distinct letters A, C, G, and T which are unmeaning by most people, there is no worry about distortion in it. Second, because of that each base of DNA requires two bits of memory while each pixel of image requires eight bits of memory for storing, the embedding capacity of DNA is extremely bigger than image. Therefore, one bit per nucleotide (bpn) in DNA is equal to four bits per pixel (bpp) in image. Third, computational efficiency in DNA sequence is much better than image because it is quite hard to embed and easy to extract the data applying data hiding algorithms on image while the procedure in DNA is vice versa exactly [1, 35].

3. COMPARATIVE STUDY

Based on different parameters in Table I recent DNA algorithms based on data hiding are compared. The first parameter is the method which is used to hide secret data within DNA reference. In [38] insertion, complementary pair, and substitution techniques proposed which are considered the main techniques for most proposed DNA based on data hiding algorithms. The second parameter is the type of data hiding algorithm, there are three types which are pure data hiding we denoted as (PR), secret key data hiding denoted as (ST), and public key data hiding denoted as (PC). The third parameter shows the blindness property of the proposed algorithm, if the algorithm is blind, we showed by (Y) if the algorithm is un-blind, we showed by (N). The fourth parameter shows if the algorithm combined with an encryption technique, (Y) means combined while (N) means does not combined with any encryption technique. The fifth parameter, this shows if the proposed algorithm is a single layer data hiding by (S) or a double layer data hiding by (D). The sixth parameter, this tells the algorithm conserved the original functionality of the DNA after hiding by (Y) and (N) means does not conserved. The seventh parameter, which shows if the algorithm expands the DNA reference length after hiding by (Y) and (N) means does not expand the length of DNA reference. The eighth parameter shows that if the proposed algorithm considered as a high modification rate (H) or (L) as a low modification rate. DNA is a ninth parameter which shows that how the proposed algorithm selected the DNA reference. Finally, the last parameter shows that the algorithm is based on what is proposed. As a result, the mentioned parameters can be described as a main parameter in DNA based on data hiding.

The conclusion of the previous algorithms has been concluded in Table I. The limitation has been showed in the proposed table based on several parameters as mentioned before. The main objective behind this comparison is to present that how to exploit these parameters to propose a more secure, efficient, and reliable data hiding algorithm based on DNA.

The strengthen of the first parameter which represented by hiding method is substitution which considered as a more efficient of the three main methods because the payload is always keeping as zero. Another parameter which should be supported by hiding data in DNA is key to makes much more difficult to attack the algorithm. Because key is considered as a one of the most crucial parameters in security, it is preferred to use a key as well as to produce not a pure algorithm. The most important parameter which should be focused during hiding data in DNA is blindness property. As long as does not sending the original carrier to the receiver is considered as a more secure algorithm. Thus, to avoid sending original carrier the algorithm should be blind. Un-blind means the original carrier should be send to the receiver which considered as a less secure technique. To provide a double layer data hiding technique into two aspects. First, confidential data should be encrypted before hiding to provide double secured layer technique. Hiding cipher data within DNA reference instead of the original data is considered as a strengthen feature of the proposed technique. Second, hiding data in more depth than the original data hiding techniques to provide double hiding layer. This property will be achieved by integrating a multimedia carrier with DNA reference. Biologically to provide more security is conserving original functionality of the DNA reference after embedding confidential data is considered as a main parameter, this means functionality of producing proteins is not affected by exploiting some DNA properties such as silent mutation and codon redundancy this does not make the attention of attackers. Finally, the quality of stego carrier is considered as a crucial parameter in data hiding field. Producing some distortions in multimedia carriers after embedding data makes more attention for attackers. Thus, minimizing this distortion is considered as a very important parameter. In DNA sequences, the length of DNA as well as the modification rate are used as two measures of stego DNA quality. No expansion in DNA length (payload is equal zero) with low modification rate will result as a superior quality of DNA after embedding confidential data. As a result, the main target behind addressed parameters is to increase the degree of security as possible and to prevent intruders to retrieve the confidential data by any way. Therefore, we can conclude that the main objective for the proposed data hiding algorithms based on DNA is to be not pure system, blind, double secured layers, double hided layers, biologically conserved, and with superior quality. Hiding data in DNA will provide more security by achieving more of these parameters. Three of these parameters have been done in [20, 26, 39-46], most of them focused on not to be a pure system, blind property, and double secured layer. Four of these parameters have been done in [36, 47-49], all of them provided not to be pure system as well as double secured layer. Five parameters have been done in [50-55], most of them focused on not to be a pure system, blind property, double secured layer, and double hided layer. Finally, most of parameters have been done in [18, 56, 57], they achieved that not to be a pure system, blind property, conserving biological functionality, and producing better quality.

Table 1. comparative study of DNA based on data hiding

Ref.	Method	Data hiding type	Blind or not	Encrypted or not	Single/ Double layer	DNA original Function conservation	DNA reference length expansion	Modification rate	DNA reference	Based on	Limitation
[1]	Table lookup substitution method (TLSM)	PR	N	N	S	N	--	H	NCBI	Substitution method	Biological DNA functionality does not maintain
[26]	Complementary	PR	N	N	S	Y	N	L	NCBI	Features of DNA	Unblind technique also the size of massage has been increased
[28]	Least significant base substitution (LSBase)	ST	Y	N	S	Y	N	L	NCBI	Codon degeneracy	Low security based on the probability cracking
[35]	Dictionary based substitution method (DBSM)	PR	Y	N	S	N	Y	--	NCBI	Original substitution and complementary rule	Security is low due to expanding the length of stego DNA and increasing the size of the binary message in some cases
[36]	Substitution	ST	N	Y	S	N	N	H	NCBI	Technique used in [47]	Security is low due to high modification rate and changing the functionality of amino acid also its unblind technique
[38]	Insertion Complementary Substitution	PR	N	N	S	N	Y	L	NCBI	Properties of DNA sequences	Unblind algorithm and the rate of modification is quite high as well as the functionality of amino acid is changed
[39]	Insertion	ST	Y	Y	S	N	Y	--	NCBI	Biological properties of DNA as amino acids	Payload not equal to zero also it needs more data during the extraction process
[41]	Histogram	ST	Y	N	S	--	N	--	----	Histogram technique	Hiding secret data only in nucleotides which their marks are equal to zeros after converting to binary
[42]	Insertion	PC	N	Y	S	N	Y	H	NCBI	DNA sequence and structure of amino acid	Its payload not equal to zero, unblind method, and high modification rate. During the hiding process, the amino acid functionality has been modified
[43]	Two by two generic complementary rules and LSB	ST	N	Y	D	--	--	--	randomly	LSB technique, amino acids, and codons	The receiver needs multiple data to extract the secret data as well as it is considered as an unblind algorithm
[44]	Swiping message bases	ST	Y	Y	S	N	--	H	NCBI	2D chaotic, XOR, and hamming code approach	The functionality of biological DNA has been maintained also it has high modification rate
[45]	GCBS and insertion	ST	Y	Y	S	N	Y	H	NCBI	Some features of DNA sequence	The redundancy process has been used highly in the process of embedding and the modification rate is high. Also, its payload not equal zero
[46]	LSB or module function	ST	Y	N	D	--	--	--	secret data	Secret sharing scheme with the DNA-XOR operator for color images	Consuming time during the process of data extraction.
[47]	Substitution	ST	N	Y	S	N	N	--	NCBI	Amino acid and generic two-by-two complementary rule	The functionality of biological DNA has been changed and its security depends on the reference of DNA
[48]	Complementary	ST	Y	Y	D	--	--	--	text	Image gridding method, LSB, and MSB	It has low capacity
[49]	Substitution	ST	N	Y	S	N	N	H	NCBI	The technique used in [47]	Unsecured technique because the probability cracking is very low

Ref.	Method	Data hiding type	Blind or not	Encrypted or not	Single/ Double layer	DNA original Function conservation	DNA reference length expansion	Modifi cation rate	DNA reference	Based on	Limitation
[50]	Substituting the least significant 2-bit	ST	Y	Y	D	--	--	--	Cheby shev maps	Chebyshev maps, addition and subtraction operations	Receiver needs DNA reference during the extraction as well as its calculation is complex
[51]	Replacing third bases of degenerative codons	ST	Y	Y	D	N	--	--	image	2D chaotic map, degenerative codon, addition, subtraction rules, and LSB	There is two parts of the method header of extraction and the data extractions
[52]	Replacing degenerative genetic code	ST	Y	Y	D	N	--	--	image	2D chaotic map, degenerative genetic code, 2D logistic map,	For secret data extraction, the receiver needs multiple secret key
[53]	Base substitution	ST	Y	Y	D	--	--	--	image	2D logistic map, LSB, and codon property	The process of hiding and extracting require multiple data which makes the security rate of the extracting secret data is high against attackers
[54]	Randomized LSBase substitution	PC	Y	Y	D	--	--	--	NCBI	LSB, amino acids, and codon degeneracy	The functionality of biological DNA has been modified during the embedding process
[55]	Substitution of [1] method	ST	N	Y	S	Y	N	H	NCBI	Microdot, non-coding region of DNA sequence, and prime sequence	In non-coding region the modification rate is high also receiver require multiple data for secret data extraction
[56]	Used rules in table I	PR	Y	Y	S	Y	N	L	NCBI	Repeated nucleotides in DNA and XOR operation	It cannot convert any punctuation marks of secret text to secret DNA, also the rule which used to replace text to DNA should be known by both sender and receiver
[57]	Substitution	ST	Y	Y	S	Y	N	L	NCBI	Amino acids, n-bits coding, LSBase, some DNA properties	In the case of highly repeated bases in the selected DNA reference, the modification rate will be high
[58]	Complement ary	ST	N	Y	S	N	N	--	EBI	Substitution method	Unblind technique
[59]	Complement ary defined as substitution	PR	N	N	S	N	N	L	NCBI	Injective mapping mechanism and repeated nucleotides	Multiple data should be known by the sender and receiver such as hiding rule and injective mapping which makes the security is low. Also, the modification rate is quite high, and it is considered as an unblind technique
[60]	Complement ary	PT	Y	N	D	--	--	--	image	Magic number	
[61]	Complement ary	PC	N	Y	S	N	N	L	NCBI	Prime numbers and substitution method	Unblind method with sending the position of the DNA nucleotide which holds the secret data which makes the probability cracking is very low. Also, during the process, the size of the secret data has been increased
[62]	Complement ary	PR	N	N	S	--	--	--	rando mly	Some of chemical structure of DNA	The selected random DNA reference with complementary rule must send to the receiver for the extraction process

Ref.	Method	Data hiding type	Blind or not	Encrypted or not	Single/ Double layer	DNA original Function conservation	DNA reference length expansion	Modification rate	DNA reference	Based on	Limitation
[63]	LSB insertion	ST	N	N	D	--	--	--	randomly	gray Scale Image	The security rate of hiding process is very low due to the hiding process
[64]	Complementary	PR	N	N	D	--	--	--	randomly	LSB and MSB	Steganography key is not enough secure
[65]	Complementary	ST	N	N	S	N	N	H	randomly	Traditional vigenère cipher and DNA features	Modifying the functionality of the amino acid during embedding process
[66]	Improved insertion	ST	N	N	S	N	Y	--	NCBI	XOR operation	The payload not equal to zero as well as the functionality of original DNA has been changed
[67]	Modified insertion	PR	N	N	S	N	Y	--	randomly	General table of DNA codons	Changing the information of the organism's life and expanding the length of the reference of DNA during hiding process
[68]	Complementary	PR	N	Y	D	--	--	--	randomly	MSB and R, G, B component of image	Using only one component of the cover image for embedding secret DNA bases. Also, its capacity is very low.

PR= pure data hiding; ST= secret key data hiding; PC= public key data hiding Y=yes; N=no; S=single D=double; H=high; L=low

4. CONCLUSION AND FEATURE WORK

Nowadays, in security area the most famous techniques to be used for securing data are cryptography and data hiding. A massive evolution of modern and robust data hiding techniques has required due to surging data storage requirements. Presently, an efficient and reliable biological carrier has been discovered for hiding data which known as DNA. DNA bio-molecular computational abilities are exploited to be use in both techniques' cryptography and data hiding. In this paper we have focused on new aspect to achieve better security depending on DNA to enable secure transmit of the confidential data over the unsecure network. Different DNA-based algorithms for data hiding are addressed and analyzed with an evaluation comparison highlighting their security issues. Different parameters are compared such as: which method is used in hiding data, type of technique, blindness property, secured layer, hided layer, biologically conserved, quality of stego DNA. The main purpose of this comparative study is to equip the future researchers with the knowledge to conduct future research in the field of data hiding to introduce or improve more secure, efficient, and reliable data hiding approaches-based DNA. Therefore, the future researchers need to propose a robust data hiding techniques based on DNA by integrating all or most of the introduced parameters to achieve a secure, efficient, and reliable data hiding technique. By achieving all of these parameters in a technique, retrieving the confidential data by attackers will be near to zero.

REFERENCES

[1] J.-S. Taur, H.-Y. Lin, H.-L. Lee, and C.-W. Tao, "Data hiding in DNA sequences based on table lookup substitution," *International Journal of Innovative Computing, Information and Control,* vol. 8, no. 10, pp. 6585-6598, 2012.

[2] D. A. Zebari, H. Haron, D. Q. Zeebaree, and A. M. Zain, "A Simultaneous Approach for Compression and Encryption Techniques Using Deoxyribonucleic Acid," in *2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, 2019, pp. 1-6, IEEE.

[3] D. A. Zebari, H. Haron, S. R. Zeebaree, and D. Q. Zeebaree, "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations," in *2018 International Conference on Advanced Science and Engineering (ICOASE)*, pp. 312-317, IEEE, 2018.

[4] A. Cheddad, "Steganoflage: a new image steganography algorithm," University of Ulster, 2009.

[5] A. Aieh, A. Sen, S. R. Dash, and S. Dehuri, "Deoxyribonucleic acid (DNA) for a shared secret key cryptosystem with Diffie hellman key sharing technique," in *Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT)*, pp. 1-6: IEEE, 2015.

[6] V. K. Yadav and S. Batham, "A novel approach of bulk data hiding using text steganography," *Procedia Computer Science,* vol. 57, pp. 1401-1410, 2015.

[7] A. M. A. Brifcani and W. M. A. Brifcani, "Stego-based-crypto technique for high security applications," *International Journal of Computer Theory and Engineering,* vol. 2, no. 6, p. 835, 2010.

[8] A. M. Abdulazeez and A. S. Tahir, "Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA," *Int. J. of Computers & Technology,* vol. 4, no. 9, pp. 1988-1993, 2013.

[9] G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba, "Comparative study for various DNA based steganography techniques with the essential conclusions about the future research," in *2016 11th International Conference on Computer Engineering & Systems (ICCES)*, 2016, pp. 220-225: IEEE.

[10] A. Nickfarjam, H. Ebrahimpour-Komleh, and A. P. Najafabadi, "Image hiding using neighborhood similarity," in *2014 6th Conference on Information and Knowledge Technology (IKT)*, 2014, pp. 79-82, IEEE.

[11] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer science review*, vol. 13, pp. 95-113, 2014.

[12] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Shamsuddin, "Information hiding using steganography," in *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings*, pp. 21-25: IEEE, 2003.

[13] Q. M. Hussein, "New Metrics for Steganography Algorithm Quality". *IJAST*, vol. 29 no. 2, 2020.

[14] P. Kumari and R. Kapoor, "Image Steganography for data embedding & extraction using LSB technique," *International Journal of Computer Applications & Information Technology*, vol. 9, no. 2, p. 192, 2016.

[15] R. G. Goswami and S. Tamrakar, "Evolution of Data Hiding By Neural Network and Retrieval or Encrypted Image, Text, Audio and Video Files," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 5, pp. 153-158, 2013.

[16] A. M. Nickfarjam and Z. Azimifar, "Image steganography based on pixel ranking and particle swarm optimization," in *The 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012)*, pp. 360-363: IEEE, 2012.

[17] R. Kaur and M. Mahajan, "Random Pattern based sequential bit (RaP-SeB) Steganography with Cryptography for Video Embedding," *International Journal of Modern Education and Computer Science*, vol. 8, no. 9, p. 51, 2016.

[18] A. Khalifa, "LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography," in *2013 8th International Conference on Computer Engineering & Systems (ICCES)*, pp. 105-110: IEEE, 2013.

[19] S. Jain and V. Bhatnagar, "Analogy of various DNA based security algorithms using cryptography and steganography," in *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 285-291: IEEE, 2014.

[20] P. A. Manisha, "A Survey on DNA Based Cryptography," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 3, no. 4, pp. 132-134, 2015.

[21] J.-S. Pan, T.-G. Ngo, and T.-K. Dao, "A Data Hiding Approach Based on Reference-Affected Matrix," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*: Springer, pp. 53-64, 2020.

[22] S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, and A. Shanthini, "Towards DNA based data security in the cloud computing environment," *Computer Communications*, 2020.

[23] S. P. Singh and M. E. Naidu, "DNA QR coding for data security using DNA sequence," *International Journal of Information Technology*, pp. 1-6, 2020.

[24] M. Borda and O. Tornea, "DNA secret writing techniques," in *2010 8th International Conference on Communications*, pp. 451-456: IEEE, 2010.

[25] R. Satra12, W. A. Kusuma, and H. Sukoco, "Accelerating Computation of DNA Multiple Sequence Alignment in Distributed Environment," 2014.

[26] M. R. Abbasy, P. Nikfard, A. Ordi, and M. R. N. Torkaman, "DNA base data hiding algorithm," *International Journal of New Computer Architectures and their Applications (IJNCAA)*, vol. 2, no. 1, pp. 183-192, 2012.

[27] N. I. Udzir, "Review of DNA and Pseudo DNA Cryptography."

[28] A. Singh and R. Singh, "Information hiding techniques based on DNA inconsistency: An overview," in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 2068-2072: IEEE, 2015.

[29] J.-S. Chen, Y.-B. Chen, P.-f. Hsu, N. Nguyen-Huu, and Y.-L. Lo, "Cryptographic scheme using genetic algorithm and optical responses of periodic structures," *Optics express*, vol. 19, no. 9, pp. 8187-8199, 2011.

[30] D. Zebari, H. Haron, and S. Zeebaree, "Security Issues in DNA Based on Data Hiding: A Review," *International Journal of Applied Engineering Research, ISSN*, pp. 0973-4562, 2017.

[31] M. B. Beck and R. V. Yampolskiy, "Hiding Color Images in DNA Sequences," in *MAICS*, pp. 25-29, 2015.

[32] C. Sreeja, M. Misbahuddin, and M. H. NP, "DNA for information security: A Survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology," in *International Conference on Computing and Communication Technologies*, pp. 1-6: IEEE, 2014.

[33] T. Mandge and V. Choudhary, "A DNA encryption technique based on matrix manipulation and secure key generation scheme," in *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 47-52: IEEE, 2013.

[34] M. Najaftorkaman and N. S. Kazazi, "A method to encrypt information with DNA-based cryptography," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 4, no. 3, pp. 417-426, 2015.

[35] R. Agrawal, M. Srivastava, A. Sharma, "Data hiding using dictionary based substitution method in DNA sequences," *2014 9th International Conference on Industrial and Information Systems (ICIIS)*, pp. 1-6: IEEE, 2014.

[36] S. Marwan, A. Shawish, and K. Nagaty, "DNA-based cryptographic methods for data hiding in DNA media," *Biosystems*, vol. 150, pp. 110-118, 2016.

[37] M. R. Abbasy and B. Shanmugam, "Enabling data hiding for resource sharing in cloud computing environments based on DNA sequences," in *2011 IEEE World Congress on Services*, pp. 385-390: IEEE, 2011.

[38] H. Shiu, K.-L. Ng, J.-F. Fang, R. C. Lee, and C.-H. Huang, "Data hiding methods based upon DNA sequences," *Information Sciences*, vol. 180, no. 11, pp. 2196-2208, 2010.

[39] A. Atito, A. Khalifa, and S. Rida, "DNA-based data encryption and hiding using playfair and insertion techniques," *Journal of Communications and Computer Engineering,* vol. 2, no. 3, p. 44, 2012.

[40] R. Wazirali, Z. Chaczko, and L. Carrion, "Bio-informatics with genetic steganography technique," in *Computational Intelligence and Efficiency in Engineering Systems*: Springer, pp. 333-345, 2015.

[41] Y.-H. Huang, C.-C. Chang, and C.-Y. Wu, "A DNA-based data hiding technique with low modification rates," *Multimedia Tools and applications,* vol. 70, no. 3, pp. 1439-1451, 2014.

[42] M. Skariya and M. Varghese, "Enhanced double layer security using RSA over DNA based data encryption system," *International Journal of Computer Science& Engineering Technology (IJCSET),* vol. 4, no. 06, pp. 746-750, 2013.

[43] C. Shyamasree and S. Anees, "Highly secure DNA-based audio steganography," in *2013 International Conference on Recent Trends in Information Technology (ICRTIT),* pp. 519-524: IEEE, 2013.

[44] E. I. A. El-Latif and M. I. Moussa, "Chaotic Information-hiding Algorithm based on DNA," *International Journal of Computer Applications,* vol. 122, no. 10, pp. 41-45, 2015.

[45] A. Khalifa, A. Elhadad, and S. Hamad, "Secure blind data hiding into pseudo DNA sequences using playfair ciphering and generic complementary substitution," *Appl Math,* vol. 10, no. 4, pp. 1483-1492, 2016.

[46] T. Tuncer and E. Avci, "A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images," *Displays,* vol. 41, pp. 1-8, 2016.

[47] A. Khalifa and A. Atito, "High-capacity DNA-based steganography," in *2012 8th International Conference on Informatics and Systems (INFOS),* pp. BIO-76-BIO-80: IEEE, 2012.

[48] A. Majumdar, M. Sharma, N. Kar, "An Improved Approach to Steganography using DNA Characteristics" 2014.

[49] S. Marwan, A. Shawish, and K. Nagaty, "An Enhanced DNA-based Steganography Technique with a Higher Hiding Capacity," in *Bioinformatics*, pp. 150-157, 2015.

[50] H. Liu, D. Lin, and A. Kadir, "A novel data hiding method based on deoxyribonucleic acid coding," *Computers & Electrical Engineering,* vol. 39, no. 4, pp. 1164-1173, 2013.

[51] P. Das and N. Kar, "A highly secure DNA based image steganography," in *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE),* pp. 1-5: IEEE, 2014.

[52] P. Das and N. Kar, "A DNA based image steganography using 2D chaotic map," in *2014 International Conference on Electronics and Communication Systems (ICECS),* pp. 1-5: IEEE, 2014.

[53] P. Das, S. Deb, N. Kar, and B. Bhattacharya, "An improved DNA based dual cover steganography," *Procedia Computer Science,* vol. 46, pp. 604-611, 2015.

[54] R. M. Tank, H. D. Vasava, and V. Agrawal, "DNA-based audio steganography," *Oriental journal of Computer Science and Technology,* vol. 8, pp. 43-48, 2015.

[55] S. A. M. Marwan, A. Shawish, and K. Nagaty, "Utilizing DNA Strands for Secured Data-Hiding with High Capacity," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 11, no. 2, pp. 88-98, 2017.

[56] F. E. Ibrahim, M. Moussa, and H. Abdalkader, "Enhancing the security of data hiding using double DNA sequences," in *Industry Academia Collaboration Conference (IAC),* pp. 6-8.

[57] 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),* 2015, pp. 95-102: IEEE.

[58] M. R. N. Torkaman, N. S. Kazazi, and A. Rouddini, "Innovative approach to improve hybrid cryptography by using DNA steganography," *International Journal on New Computer Architectures and Their Applications,* vol. 202, pp. 225-236, 2012.

[59] C. Guo, C.-C. Chang, and Z.-H. Wang, "A new data hiding scheme based on DNA sequence," *Int. J. Innov. Comput. Inf. Control,* vol. 8, no. 1, pp. 139-149, 2012.

[60] S. Chakraborty and S. K. Bandyopadhyay, "Two stages data-image steganography using dna sequence," *International Journal of Engineering Research and Development,* vol. 2, no. 7, pp. 69-72, 2012.

[61] B. A. Mitras and A. Abo, "Proposed steganography approach using DNA properties," *International Journal Of Information Technology and Business Management,* vol. 14, no. 1, pp. 96-102, 2013.

[62] K. Menaka, "Message encryption using DNA sequences," in *2014 World Congress on Computing and Communication Technologies,* pp. 182-184: IEEE, 2014.

[63] M. S. Chakraborty and K. Bandyopadhyay, "Data Hiding by Image Steganography Appling DNA Sequence Arithmetic," *International Journal of Advanced Information Science and Technology (IJAIST),* vol. 44, p. 44, 2015.

[64] S. Indora, "Cascaded DNA cryptography and steganography," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT),* pp. 104-107: IEEE, 2015.

[65] K. Meena, K. Menaka, and R. Subramanian, "Secure Message Transfer Using DNA Sequences," *Journal of Computational Intelligence in Bioinformatics,* vol. 9, no. 1, pp. 1-6, 2016.

[66] P. Malathi, M. Manoaj, R. Manoj, V. Raghavan, and R. Vinodhini, "Highly improved DNA based steganography," *Procedia Computer Science,* vol. 115, pp. 651-659, 2017.

[67] M. Yamuna and A. Elakkiya, "Amino Acids in Data Encryption," *J Anal Pharm Res,* vol. 2, no. 5, p. 00030, 2016.

[68] K. Kaur, "A Double Layer Encryption Algorithm based on DNA and RSA for Security on Cloud," *International Research Journal of Engineering and Technology,* vol. 3, no. 03, pp. 1742-1745, 2016.