

A Study on Steganography using DNA

Fred Ropekkima Darlong, Poulomi Deb, Kumar Amitabh, Indrajit Tripura

Department of CSE, NIELIT, Agartala, India

fropekkima@gmail.com, poulomideb.deb7@gmail.com

amitabh.mcit@gmail.com, itripura217@gmail.com

Abstract. Steganography is the practice of hiding data in plain text or other types of media. It is crucial to protect or make it safe sensitive information from unauthorized access or tampering. Traditional digital storage methods have issues with capacity, security, and traceability. In contrast, DNA-based steganography uses the large storage capacity and complexity of nucleotide sequences. This paper examines the encoding and decoding schemes, security models, synthesis processes, and storage methods of DNA steganography. It also explores trends in encryption patterns, data hiding techniques, and system weaknesses. Conquering the issues of scalability, cost, and standardization remains in spite of tremendous progress in areas such as error correction, biochemical stability, and data security. This review emphasizes the need for multidisciplinary re-search integrating information theory, cryptography, and biotechnology in order to overcome the existing limitations. This paper presents future research directions to achieve secure and optimal data hiding using bio-logical sequences by analyzing the benefit and limitation of DNA-based steganography.

Keywords: DNA Steganography, Data hiding, Cryptography, DNA Encoding, Data Encryption, Data Decryption

(Article history: Selected papers from NIELIT's International Conference on Communication, Electronics and Digital Technologies (NICE-DT'26), 29-30 Jan, 2026, Gorakhpur, India)

1 Introduction

In today's world the important of computer system and the internet becomes a crucial part of our life and it has increased drastically [1]. This huge development of the computer system and internet where we share our data it is important for us. Providing security of our data is very crucial [2]. There are different approaches such as Cryptography and Steganography which main concern is to preserving confidentiality, availability and integrity which are the most important in computer security [3]. The cryptography and steganography are inter connected and shared the common aims to provide security [4]. Cryptography deals with the conversion of text into cipher format making it inaccessible and whereas steganography deals with the with the technique from plain text to secrete message that can be read only by the receiver.

It hide the messages in the sender in which it is hard to detect by the traitor to read it as it is in the plain text [5]. In cryptography although encrypted data can be seen easily it cannot be read by the anyone, it can grab attention using encryption make people suspicions which may reveal the communication pattern and if it is cracked the whole message is being reveal in which steganog-raphy can be a better option. However, Traditional steganography has limited capacity for small space and it is not strong as normal encryption which may result in destroying the hidden message [6]. Many advance detection tools can be used to find anomalies which leave a predictable trace which increase the risk of detection [7]. To overcome those problem DNA based approach has been Introduced [8]. The most important feature of deoxyribonucleic acid (DNA) compared to other traditional technologies are its capacity and concealing medium it can store around hundreds of petabytes in one gram of DNA [9].

Various classic methods are used to hide a secret message inside the cover media in DNA-based steganography, namely insertion, substitution, complemen-tary rule-based algorithms, and hybrid algorithms [10, 11]. Each technique has its respective benefits and drawbacks during an implementation [12, 13]. Thus, the major intention of this paper is

to point out the pros and cons of the newly pro-posed DNA-based steganography algorithm. It also presents ideas to researchers who wish to develop techniques that can work better than the current available DNA-based algorithms. This can be done via three objectives: first, to under-stand the biological details; second, to understand the traditional techniques and modern approaches for data hiding; and third, to analyze the future potential regarding DNA-based information hiding [14, 15].

2 Research Objectives

The objectives of DNA steganography research is to devise secure and efficient methods for concealing information in DNA sequences. This technique utilizes unique properties of DNA for storing and transporting data. This involves the study of various methods that can embed and extract a secret message with minimum variation in biological properties of host DNA and robust against various types of potential attacks. Here's a more detailed breakdown of the research objectives:

- Hiding Data in DNA.
- Ensuring Security and Robustness.
- Applications and Future Directions.

3 Biological background and literature review

The information of Genetic and traits are kept or stored in the DNA, according to molecular biology. This genetic material characterizes all the behavioral and physical traits of an organism because it stores the instructions that allow for the development of the functions in all the known living organisms and viruses.

(Fig. 1). DNA is a nucleic acid that holds the genetic instructions of the biological background for the development and function of all the known living organisms and viruses.

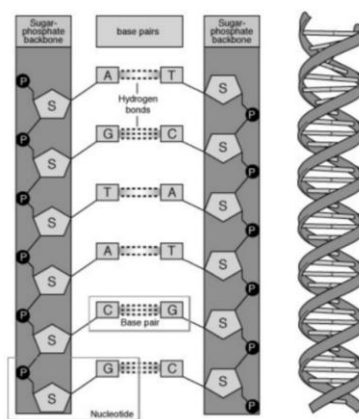


Fig. 1. Structure of DNA.

DNA is composed of two very long strands that twist together into a double helix. Each strand is built from nucleotides. A nucleotide includes three parts: four bases, that is, Adenine as [A], Guanine as [G], Cytosine as [C], and Thymine as [T], a deoxyribose sugar, and a phosphate group. DNA strands have a chemical polarity. It means there are different groups on each end of the molecule.

As shown in Fig. 2, the DNA Nucleotide is not a purine/pyrimidine base. The purines are (A) Adenine and (G) Guanine. The pyrimidines are (T) Thymine and (C) Cytosine. The hydrogen bonds are formed between Adenine and Thymine or Cytosine and Guanine under normal conditions. The rule associated with the complementary bases is called Watson-Crick base pairing rule. The A binds with T through 2 hydrogen bonds and C binds with G through 3 hydrogen bonds. The combination of these nucleotides forms long polymer strands of DNA, allowing for the huge diversity of DNA sequences to exist along with the capability of forming the DNA double helix in organisms.

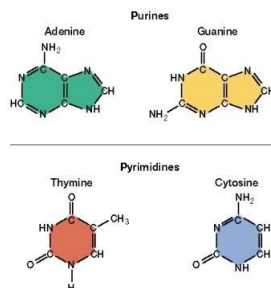


Fig. 2. DNA nucleotide bases.

DNA consists of two long strands that form a double helix, each built from nucleotides. A nucleotide has three parts: four bases (A) Adenine, (G) Guanine, (C) Cytosine and (T) Thymine a deoxyribose sugar, and a phosphate group (see Fig. 1). DNA strands have chemical polarity, meaning that there are different groups at each end of a molecule, that is the bottom end and top end.

As shown in Fig. 2, a DNA nucleotides is neither a purine or a pyrimidine base. The purines are (A) Adenine and (G) Guanine; and the pyrimidines are the (T) Thymine and (C) Cytosine. Under regular conditions Hydrogen bonds form between adenine and thymine, and between cytosine and guanine. This complementary rule, known as Watson-Crick base pairing, states that A pairs with T using 3 hydrogen bonds, while C pairs with G using 3 hydrogen bonds. The variety of these nucleotides provides long polymer strands that compose the DNA double helix, enabling the enormous diversity of DNA sequences found in organisms.

		Second base				
		U	C	A	G	
First base	U	UUU } PHE UUC } UUA } LEU UUG }	UCU } UCC } UCA } UCG }	UAU } TYR UAC } UAA } STOP UAG }	UGU } CYS UGC } UGA } STOP UGG } TRP	U C A G
	C	CUU } CUC } CUA } CUG }	CCU } CCC } CCA } CCG }	CAU } HIS CAC } CAA } CAG }	CGU } CGC } CGA } CGG }	C A G U
	A	AUU } AUC } AUA } AUG }	ACU } ACC } ACA } ACG }	AAU } ASN AAC } AAA } AAG }	AGU } SER AGC } AGA } AGG }	A G C U
	G	GUU } GUC } GUA } GUG }	GCU } GCC } GCA } GCG }	GAU } ASP GAC } GAA } GAG }	GGU } GGC } GGA } GGG }	G C A U

Fig. 3. Standard Amino Acid/DNA Codons.

4 Hidden Techniques of DNA Steganography

DNA steganography uses different coding methods to hide digital information within DNA sequences. This makes it hard to find or understand the hidden data without knowing the specific method used. The main goal of these techniques is to take advantage of the large combinations possible with nucleotide sequences while keeping them plausible in a biological sense. This helps avoid drawing attention during analysis. Several key approaches have come up in the literature.

4.1 High improvement of the DNA based Steganography techniques

The methods or algorithm contains several differences from the others data hid-ing algorithms that have been

used with the DNA sequences. One of the big advantages is the possibility of an adversary of detecting the occurrence of hid-den data in DNA sequences is very low. Moreover, before embedding the information into the DNA sequence, the algorithm encrypts it using a key chosen randomly (F1). Another random key (F2) is utilized to break down the DNA sequence is divided into segments. After that, the parts of the cipher text will be put between these parts, and both keys are secret, which enhances the security of the algorithm. On the other hand, most data-hiding algorithms insert the message as a continuous sequence in the DNA sequence, which is considered less secure. Here, after encrypting the message is converted to binary bits in the ciphertext and each bit of this will be inserted between the DNA segments. Thus, extraction of this ciphertext is hard, as well as differentiating it from a long DNA sequence.

Nevertheless, it has a number of disadvantages. First, the method changes the DNA sequence's length, while the human genome contains about 3×10^9 base pairs. This is because the method does not substitute the encrypted message for DNA segments. Instead of this it does embeds the ciphertext straight for-wardly, which means increasing the length of DNA and thus probably making the changed sequence more recognizable as artificial. Another important point is that the method does not take into consideration keeping the DNA functional.

DNA nucleotide	Decimal	Binary
A	0	00
C	1	01
G	3	10
T	3	11

Fig. 4. DNA Digital Coding

Belows are the steps for encrypting and hiding a message in a DNA sequence in the proposed algorithm are as follows:

The steps of encryption process

– Message Conversion to Binary:

The plaintext message $R = \{r_1, r_2, \dots, r_m\}$ is first broken down into its individual characters. Each character is converted into an 8-bit binary form using the ASCII standard. This ensures consistent binary formatting for later steps.

– Generation of the Primary Key $F1$:

A random integer between 0 and 255 is generated and labeled as the key $F1$. The key is then changed into its 8-bit binary form for direct use in bitwise operations.

– Initialization Through XOR Operation:

The binary value of the last character in the message is XORed with the binary version of the key $F1$. This creates the first layer of cryptographic change.

– Sequential XOR Chaining:

The result of the first XOR is then XORed with the binary value of the character before it. This chained XOR process goes through all characters until every symbol in the message is processed. The series of XOR results creates a new binary sequence AAA.

– Binary-to-Protein Mapping:

The binary sequence AAA is converted into a symbolic, protein-like sequence using a mapping table. This step transforms digital data into a biological-style format to improve concealment.

– Carrier DNA Sequence Preparation:

A random DNA-like sequence SSS is chosen as the cover medium. The nu-cleotide sequence SSS is converted into a binary format using the encoding rules shown in Table-1.

– Segmentation Using Random Parameter $F2$:

A second random number $F2$ is created to define the segmentation size. The binary representation of SSS is divided into segments, each with a length equal to $F2$. This segmentation aids in distributed embedding, making it harder to detect.

– **Embedding of Encoded Data:**

The first binary element from the sequence AAA is placed at the starting of the first binary segment. The second value, taken from the binary key $F1$, is put in the second segment. This process continues until all necessary bits are included in the carrier segments.

– **Formation of the Stego-DNA Sequence:**

Once the embedding is complete, all binary segments are put back together into one binary stream. Using the mapping definitions in Table-1, final binary stream is turned back into a synthetic DNA-like sequence. This sequence creates the stego-DNA, which conceals the encrypted message within a bio-logically realistic structure.

A graphical illustration of the entire encryption workflow is shown in Fig. 5.

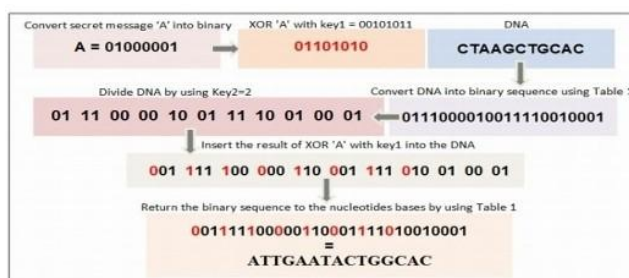


Fig. 5. The encryption process.

The steps of decryption process For decrypting the message, the receiver must have to know the $F1$ and $F2$. And they also need to have the original DNA from the sender. The receiver do the following:

– **Binary Conversion of the Stego-DNA Sequence:**

The synthetic DNA sequence is first converted back into its binary form by using the nucleotide-to-binary mapping outlined in Table-1.

– **Segmentation of the Binary Stream:**

The resulting binary sequence is split into segments. Each segment has a length of $F2 + 1$. This splitting reverses the structure used during the embedding stage.

– **Extraction of Embedded Bits:**

From each segment, the first part is taken. These parts are combined in order to recreate the important binary sequence BBB, which holds the hidden information.

– **Reversal of the Chained XOR Process:**

To get the original message, the first 8 bits of BBB are XORed with the binary key $F1$. Then, the next 8-bit block is XORed with the previous 8-bit block of BBB. This process goes on until the whole sequence is decoded.

– **Recovery of Plaintext:**

The final binary output is then converted into ASCII characters, revealing the original message.

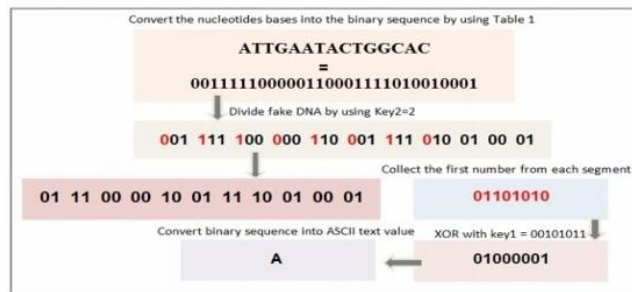


Fig. 6. The decryption process.

5 Security Analysis of DNA Based Steganography

The essence of DNA-based steganography security lies in the complexity and bio-logical diversity of DNA sequences, offering a very large, not-obviously-noticeable method for concealing digital information. Compared with traditional stegano-graphic methods, such as images or audio files, DNA possesses extremely high storage capacity and a huge sequence space, making it rather difficult to detect unauthorized access. Natural DNA sequences have features of randomness and variability, and hidden information could be concealed in biologically normal patterns.

With DNA steganography, the use of biological principles, such as base-pairing rules and methods of sequence encoding, is a key strength. This reliance makes unauthorized decoding difficult unless someone knows the exact encoding method. When applied together with cryptographic techniques such as encryption or key-dependent mapping, DNA steganography adds protection. In such cases, even in cases of interception or scrutiny of the sequence, the hidden information is meaningless without the proper key.

However, the method has its challenges too. The procedures for encoding and storing may introduce vulnerabilities if the mapping rules, primer, or sequence variations are easy to predict or not handled properly. Advanced DNA sequencing tools might enable adversaries to perform statistical or pattern-based analysis to identify anomalies within synthetic sequences. Poor choice of carrier sequences can also raise the chances of detection, especially if the changed DNA drifts too far from expected biological patterns.

In spite of these risks, DNA-based steganography may exhibit a high level of security if strong encoding methods, cryptographic protections, and biologically realistic sequence designs are used. Because it is resistant to some common digital attacks and the analysis of biological data itself is complex, DNA could become a promising medium for embedding information securely. Further improvements in DNA synthesis and sequencing technologies will increase the functionality and security of DNA steganographic systems.

Thus, the basis of the security for this DNA steganographic method depends on the difficulty in identifying the hidden data and reconstructing the required keys. Here is the summary of the probability factors:

- **Binary Mapping Ambiguity:**

This indicates the range of possibilities for binary representations, so the probability of guessing the binary mappings for nucleotides (A, C, G, T) correctly is $1/24$.

- **Message Identification Probability:**

The likelihood of accurately identifying both the message and the reference DNA sequence in the stego-DNA is $1/(n - 1)$, where n represents the total number of bits in the fake sequence.

- **Segmentation Guessing Complexity:**

Since message segments depend on a random key:

- The probability of correctly guessing the message segmentation is $1/2^{(m-1)}$, where m is the number of bits in the secret message.
- The probability of guessing the segmentation of the reference DNA sequence is $1/2^{(s-1)}$, where s is the number of bits in the carrier DNA.

- **XOR-Based Encryption Complexity:**

The XOR chaining used during encryption results in $28m$ possible combinations, making brute-force attempts very unlikely.

6 Working methodology of DNA Steganography in different fields

The previous section discussed some classical or traditional methodologies for the implementation of DNA steganography. These are the methods that use traditional protection techniques in data security to achieve their goals. Recently, new algorithms have emerged. These new trends focus on either exploiting the biological features of DNA or adapting techniques from other areas of computer science. The aim is to provide better solutions and performance than the older methods. In this section, we will critically analyze the recently suggested techniques. We will describe how they work, their advantages and disadvantages, and identify possible improvements.

6.1 Exploiting of the biological features

The particularly interesting property of the DNA is that the presence of a single nucleotide polymorphisms (SNPs). In this situation, a single nucleotide at a specific position of the genome sequence refers among individuals of same species, so two DNA sequences can vary at that exact site. Researchers have recognized that regions containing SNPs can be used to conceal secret information, because an attacker cannot easily tell whether a change in these positions is due to normal genetic variation or to data hiding.

In the proposed method, a DNA steganography methods hides the secret message at SNP locations at the chosen DNA sequence. First, the SNP positions in that sequences are identified. Then, each of the characters of this secret message is convert into a group of three nucleotides using a predefined DNA encoding table. For instance, the letter “H” is encoded as the triplet “TAC” and written into three consecutive SNP positions, as shown in Figs.7 and 8.

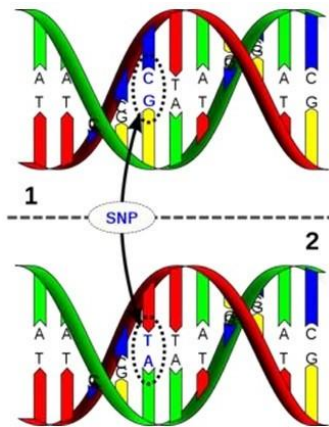


Fig. 7. Single nucleotide polymorphism (SNP).

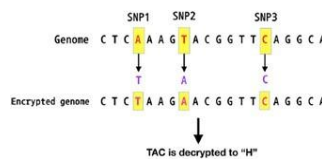


Fig. 8. Encrypting & hiding the character.

6.2 Networking field

For the mutation and modification detection method, we borrowed an idea from networking to identify mistakes in information transfer. To accomplish this, we apply the block checksum method where each nucleotide in the encrypted message is represented numerically as: A=0, T=1, G=2, C=3. The sum of every nine nucleotides is divided by 4. The remainder calculated from the division is then converted to an equivalent DNA representation, which is placed at the end of the message as the tenth nucleotide to make it complete. The process is repeated for every part of the message to encrypt. The following are three cases as depicted in Fig. 9.

Cases	Encrypted message	(A = 0 / T = 1 / G = 2 / C = 3)
Case 1	AGT GCC TAT T	021 233 101 13 MOD 4 = 1 → T
Case 2	GGT GCC TAT T	221 233 101 15 MOD 4 = 3 → C
Case 3	GGT GCC TIG T	221 233 112 17 MOD 4 = 1 → T

Fig. 9. Method of mutation detection.

In first scenario, there is no mutation in the encrypted sequence. This is evidenced by the fact that the last nucleotide conforms to the result derived from the calculation of the checksum. In the second scenario, the mutation occurs at the first position of the sequence. The error can easily be detected since the last nucleotide does not conform to the result of the checksum calculation. Although the proposed approach to mutation detection in this scenario performs well, it has limitations that appear in the third case. In this situation, the appended checksum nucleotide and the calculated checksum result appear identical, giving the impression that the sequence is correct. However, the sequence has actually been altered in multiple positions. Therefore, the proposed approach is reliable only when mutations occur at a single location.

6.3 Data structure field

One of the another computer science concept that supports DNA steganography and helps improve data-hiding capacity is the use of data structures. One suggested method employs a balanced tree to conceal information. This method involves generating a balanced tree from a randomly chosen DNA sequence, with each node of the tree holding a single nucleotide. The height of this tree is proportional to the message to be embedded. Nodes on even-numbered levels can have up to two child nodes, while nodes on odd-numbered levels can have as many as three. By using a Depth First Search (DFS) traversal the structure is explored or navigated.

Then the conversion of every character in the message is started by the encryption process into a group of four nucleotides. Once this conversion is complete, the leaf node nucleotides are replaced—using the encoded characters—in reverse order. The final step is to reconstruct the modified DNA sequence by assembling the nucleotides according to the tree's node references.

For example, to encode the characters A, B, and C, their ASCII values (01000001, 01000010, and 01000011) are first retrieved and then transformed into the nucleotide sets (CAAC, CAAG, and CAAT). Then if the DNA sequence chosen to hide the message (ACGGTTCCAATGCCTAAGCTA), and then it is converted into a balanced tree, as shown in Fig. 10.

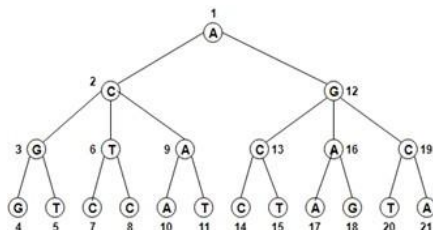


Fig. 10. Random DNA sequence balanced tree.

After it encrypted the data is inserted to the tree's of the leaf nodes, as il-lustrated in Fig. 11. And produced fake DNA sequences from the balanced tree that is (ACGCATATACAGCAGACAC). This framework provides a large data hiding capacity and can manage any kind of input. In addition, the embedding locations are distributed irregularly across the reference sequence rather than in a fixed order. However, the method depends heavily on its structural pat-tern—if the pattern is discovered, the hidden message becomes vulnerable. A potential enhancement to this approach would be replacing the balanced tree with a linked list to store the DNA sequence. Linked lists offer greater flexibility, increased complexity, and smoother transitions between elements compared to tree structures.

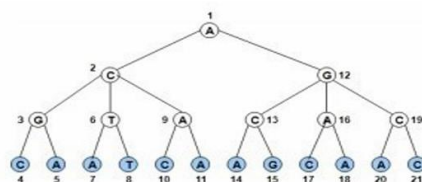


Fig. 11. Balanced tree after the message integration.

6.4 Artificial Intelligence field

In the Artificial intelligence field it can be applied for creation of stronger and more efficient DNA steganography technique. In this approach, a backpropagation-based ANN is used for achieving high and large data-hiding capacity, a low prob-ability of cracking, and the absence of extra payload. The removal of the DNA reference string and the message takes place in the embedding process, and the artificial neuron network produces the set of weights as output. Initially, each character of the hidden message is convert it into its ASCII of binary represen-tation. This binary value is translated into the corresponding DNA nucleotide

according to a predefined of the DNA binary coding scheme. Then each of this nucleotide of this encoded message is assigned a specific position within the DNA reference sequence. The ANN is then utilized to generate a binary positions list, and also the weights obtained during the training time are kept in a set. The set, along with the selected of the DNA reference sequence, is transmitted to the receiver. Figure 12 presents a diagram illustrating the AI-driven encryption and data hiding workflow.

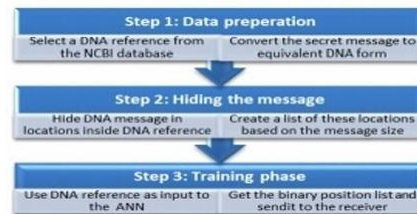


Fig. 12. Data Encryption and Embedding.

At the end of the receiver, the process of extraction is carried out by reversing the process or steps used during embedding. First, the received of the DNA sequence and those set of weights by the sender are input into the ANN. This produces list of a positions indicating where hidden data is located. The DNA letters at these positions are collected to form a set. With the use of the binary coding rule table, the DNA letters are converted back into binary code. Finally, with the conversion of every 8-bit code back into its corresponding ASCII character, the original message is reconstructed. Figure 13 shows a step diagram illustrating the steps of data decryption and message extraction.

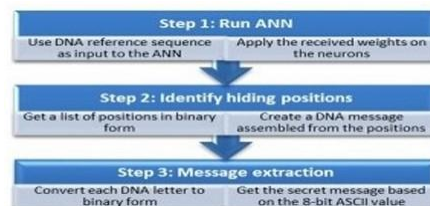


Fig. 13. Data Decryption and Extraction.

7 Comparative Analysis

DNA-based steganography has attracted a lot of interest as a new way to hide data. This is because it offers great storage capacity, is biologically feasible, and provides a high level of secrecy. A review of the current methods shows sharp differences in data encoding, the underlying security model, complexity of computations involved, and practicality of the implementation.

1. **Encoding the strategies:** Different encoding methods can be used in studies on DNA steganography. These can be grouped into three categories: rule-based encoding, cryptographic hybrid encoding, and biological sequence modification.
2. **Security and Robustness:** Security analysis of different studies indicates large differences in the resistance of systems against common attacks.
3. **Capacity and efficiency:** Capacity and efficiency may vary greatly depending upon the method of embedding chosen. It includes such as:
 - i. Direct mapping methods.
 - ii. Hybrid methods.

- iii. Biology-driven embedding.
4. **Practicality and Implementation:** Practical feasibility still is one of the main factors setting studies apart.
5. **Error tolerance and reliability:** Various works propose different approaches to correct errors that may arise during storage or transmission.

The table given below represent a comparative analysis of three major approaches used in DNA based steganography: Rule-Based Encoding, Cryptographic Hybrid and Biological Sequence-Based methods. The comparison table is carried out based on key parameters such as security, stealth, capacity, computational cost, biological feasibility, error tolerance and practical usage.

- Rule-Based Encoding:-Rule based-encoding techniques use predefined map-ping rules to convert digital data into DNA sequences.
- Cryptographic Hybrid Approach:-This approach combines traditional cryptographic techniques with DNA-based encoding to enhance security.
- Biological Sequence-Based Approach:-This method uses real or biologically inspired DNA sequences for data hiding, making it closer to natural DNA behaviour.

Parameter	Rule-Based Encoding	Cryptographic Hybrid	Biological Sequence Based
Security	Low to moderate	High	Very high
Stealth	Moderate	High	Very high
Capacity	High	Moderate	Low to moderate
Computational Cost	Very low	High	Very high
Biological Feasibility	Not required	Not required	Required
Error Tolerance	Low	Moderate	High(depending on method)
Practical Use	Best for digital only system	Good for secure system	Best for advance bio applications

8 Conclusion and Future Work

DNA-based steganography has emerged as a promising technique for information hiding due to the huge storage capacity and complex structure of biological DNA sequences. It can easily be inferred from this work that DNA provides a secure and efficient carrier for embedding secret messages as compared to traditional steganographic and cryptographic approaches. Different techniques analyzed herein for encoding and hiding reveal remarkable achievements in encryption strength, payload capacity, and imperceptibility. Still, challenges such as cost, standardization, and practical implementation require further advances in biochemical synthesis and computation models.

Future research on this should focus on the development of optimized versions of the hybrid algorithms that integrate artificial intelligence, cryptography, and bioinformatics for enhanced security and performance. There is also a need to develop standard frameworks and simulation tools for DNA-based data hiding to guarantee reproducibility and reliability. Furthermore, a strong theoretical basis between molecular biology and information technology can create an avenue for scalable and real-world DNA steganography systems. Conclusion DNA steganography can be considered a futuristic, multidisciplinary field that may redefine secured communication and mechanisms of data storage in coming decades.

References

1. Joshi, Renu, N. Pavithra, and C. K. Singh: Internet an integral part of human life in 21st century: a review. *Current Journal of Applied Science and Technology* **41**(36), 12–18 (2022).
2. Gupta, Ishu, et al.: Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. *IEEE Access* **10**, 71247–71277 (2022).
3. Dhawan, Sachin, and Rashmi Gupta: Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective* **30**(2), 63–87 (2021).
4. Varghese, Fredy, and P. Sasikala: A detailed review based on secure data transmission using cryptography and steganography. *Wireless Personal Communications* **129**(4), 2291–2318 (2023).
5. Purnima, P., Lalitkumar P. Bhैया, and Ghanshyam Sahu: A Review on Reading of Text Hidden in Image Using Steganography. *Research Journal of Engineering and Technology* **14**(1), 41–47 (2023).
6. Wahab, Osama Fouad Abdel, et al.: Hiding data using efficient combination of RSA cryptography, and compression steganography techniques.
7. Li, Zhong, Yuxuan Zhu, and Matthijs Van Leeuwen. "A survey on explainable anomaly detection." *ACM Transactions on Knowledge Discovery from Data*, 18(1), 2023, pp. 1–54.
8. Doricchi, A., Platnich, C.M., Gimpel, A., Horn, F., Earle, M., Lanzavecchia, G., Cortajarena, A.L., Liz-Marzán, L.M., Liu, N., Heckel, R. and Grass, R.N. "Emerging approaches to DNA data storage: challenges and prospects." *ACS Nano*, 16(11), 2022, pp. 17552–17571.
9. Akhtar, Zarif Bin, and Ahmed Tajbiul Rawol. "Unlocking the future for the new data paradigm of DNA data storage: An investigative analysis of advancements, challenges, future directions." *Journal of Information Sciences*, 23(1), 2024, pp. 23–44.
10. Alhabeeb, Omar Haitham, Fariza Fauzi, and Rossilawati Sulaiman. "A review of modern DNA-based steganography approaches." *International Journal of Advanced Computer Science and Applications*, 12(10), 2021.
11. Alhabeeb, Omar Haitham, Fariza Fauzi, and Rossilawati Sulaiman. "Developing a novel DNA-based steganography algorithm using random table generation with segmentation." *Multimedia Tools and Applications*, 83(14), 2024, pp. 40529–40567.
12. Ahmed, Shams Forruque, et al. "Deep learning modelling techniques: current progress, applications, advantages, and challenges." *Artificial Intelligence Review*, 56(11), 2023, pp. 13521–13617.
13. Rozendaal, Kyle, Akalanka Mailewa, and T. Dissanayake Mohottalalage. "Neural network assisted IDS/IPS: An overview of implementations, benefits, and drawbacks." *International Journal of Computer Applications*, 975, 2022, p. 8887.
14. Narayan, M. Shreyansh, Priyanka Biswas, and Nirmalya Kar. "Enhancing Privacy using DNA based Data Hiding." *Proceedings of the 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, IEEE, 2024.
15. Akhtar, Zarif Bin, and Ahmed Tajbiul Rawol. "Unlocking the future for the new data paradigm of DNA data storage: An investigative analysis of advancements, challenges, future directions." *Journal of Information Sciences*, 23(1), 2024, pp. 23–44.