MULTILAYERED DNA-BASED STEGANOGRAPHY & MODIFIED RSA FRAMEWORK FOR ULTRA-SECURE DATA TRANSMISSION

[1]Kohila R, [2]Selvarani C M, [3]Surya S, [4]Yogayuvaraj L, [5]Sricharan G

[1]Assistant Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[2]Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[3,4,5]Student, Department of CSE(Cyber Security), Muthayammal Engineering College.

[1]kohilamca@gmail.com, [2]selvarani.cm.cs@mec.edu.in, [3]suryasivanesan14@gmail.com, [4]yuvarajlakshmanan@gmail.com, [5]charangunthasri@gmail.com

ABSTRACT - In the modern digital era, the security of sensitive data during transmission and storage has become a major challenge due to the growing number of cyber threats. Traditional cryptographic algorithms are vulnerable to brute-force attacks, while standard steganography can be detected through advanced steganalysis. This paper introduces an innovative hybrid encryption framework that integrates DNA computing, image steganography, and a modified RSA algorithm. The proposed system transforms plaintext into DNA-coded sequences, embeds them into a cover image using Least Significant Bit (LSB) or Discrete Wavelet Transform (DWT), and further encrypts the stego-image using modified RSA. This multi-layered architecture ensures a robust level of confidentiality, integrity, and authentication, making unauthorized decoding nearly impossible.

KEYWORDS - Web Security, DNA Cryptography, Steganography, Modified RSA, Network Security, Data Hiding, Image Encryption, Biological Computing.

1. INTRODUCTION

In today's digital communication era, the need for secure data transmission has become more crucial than ever. The exponential growth of internet-based applications has made sensitive information increasingly vulnerable to unauthorized access. Traditional encryption algorithms such as AES and DES face limitations when attackers employ advanced decryption techniques. Similarly, steganography methods that embed secret messages within images offer protection but may be detected by modern tools.

This research proposes an advanced multi-layered approach that combines the strengths of cryptography and steganography. DNA computing, inspired by biological systems, provides a novel way to represent data using nucleotides (A, C, G, T), offering vast storage

capacity and high randomness. By integrating DNA cryptography with image steganography and modified RSA encryption, this framework builds a highly secure data protection model suitable for defense, healthcare, and financial applications.

1.1 SCOPE OF THIS PROJECT

This project aims to:

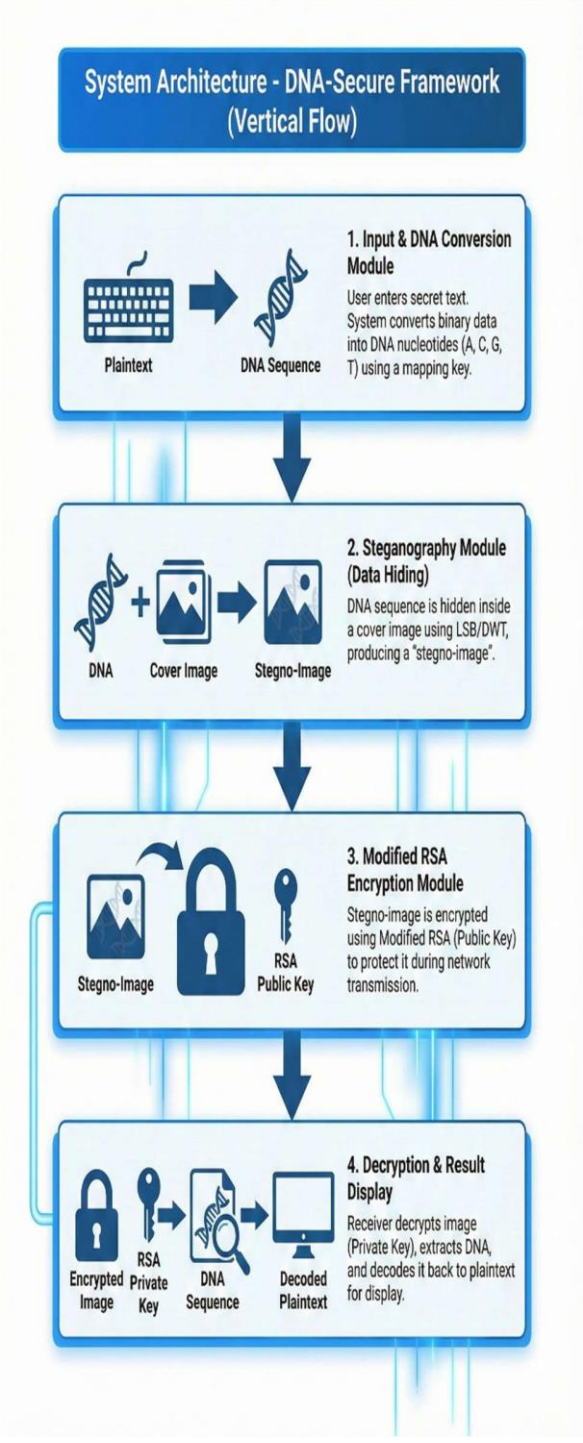
- Develop a hybrid security system integrating DNA computing, Steganography, and Modified RSA.
- Utilize DNA coding to convert plaintext into complex nucleotide sequences (A, C, G, T).
- Embed DNA-coded data into images using LSB/DWT methods for imperceptible hiding.
- Apply modified RSA encryption to the stego-image to secure it against interception.
- Ensure the confidentiality and integrity of data over untrusted networks.

2. PROPOSED WORK

This study proposes an advanced Hybrid Security Framework that integrates multiple detection and protection techniques. The system combines biological encoding (DNA), visual concealment (Steganography), and asymmetric encryption (RSA).

By leveraging the randomness of DNA sequences and the mathematical strength of RSA, the system ensures robust protection. The integration of LSB/DWT for data hiding further strengthens the framework, making it a comprehensive solution for secure data transmission.

2.1 System Architecture



3.1 Data Processing & Preprocessing

To ensure accurate results, the framework incorporates:

- **Message Preprocessing (The "Payload"):** Before the secret message can be hidden or encrypted, it must be converted from human-readable text into a format that the computer and the DNA logic can manipulate.
- **ASCII to Binary Conversion:** Computers cannot process English letters directly. The first step of processing is converting every character of the secret message into an 8-bit binary sequence.
- **Binary to DNA Mapping (Encoding):** The binary stream is broken into pairs (2 bits) and mapped to DNA bases using a specific rule (00=A, 01=T, etc.).
- **Message Processing (Encryption):** Once the data is in "DNA format," the actual encryption logic is applied to secure it.
- **DNA Complementation (The Encryption Algorithm):** The code applies a substitution cipher based on DNA complementarity principles.
- **Image Preprocessing (The "Carrier"):** The image acts as the container for the data. It requires specific preparation to ensure the hiding process (Steganography) works correctly without errors.

3.2 Security Techniques:

3.2.1 DNA Encoding:

Utilizes biological principles to encode binary data into DNA Nucleotides.

- **Mapping:** 00 = A, 01 = C, 10 = G, 11 = T.
- **Benefit:** Increases data complexity and Storage Capacity.

3.2.2 Modified RSA Encryption:

Implements a variation of the standard RSA algorithm.

- **Process:** Encrypts the entire stego-image rather than just the text.
- **Benefit:** Provides a second layer of defense; even if the file is stolen, the image cannot be viewed or analyzed for hidden data.

3.3 TOOLS AND LIBRARIES

This project framework employs the following technologies:

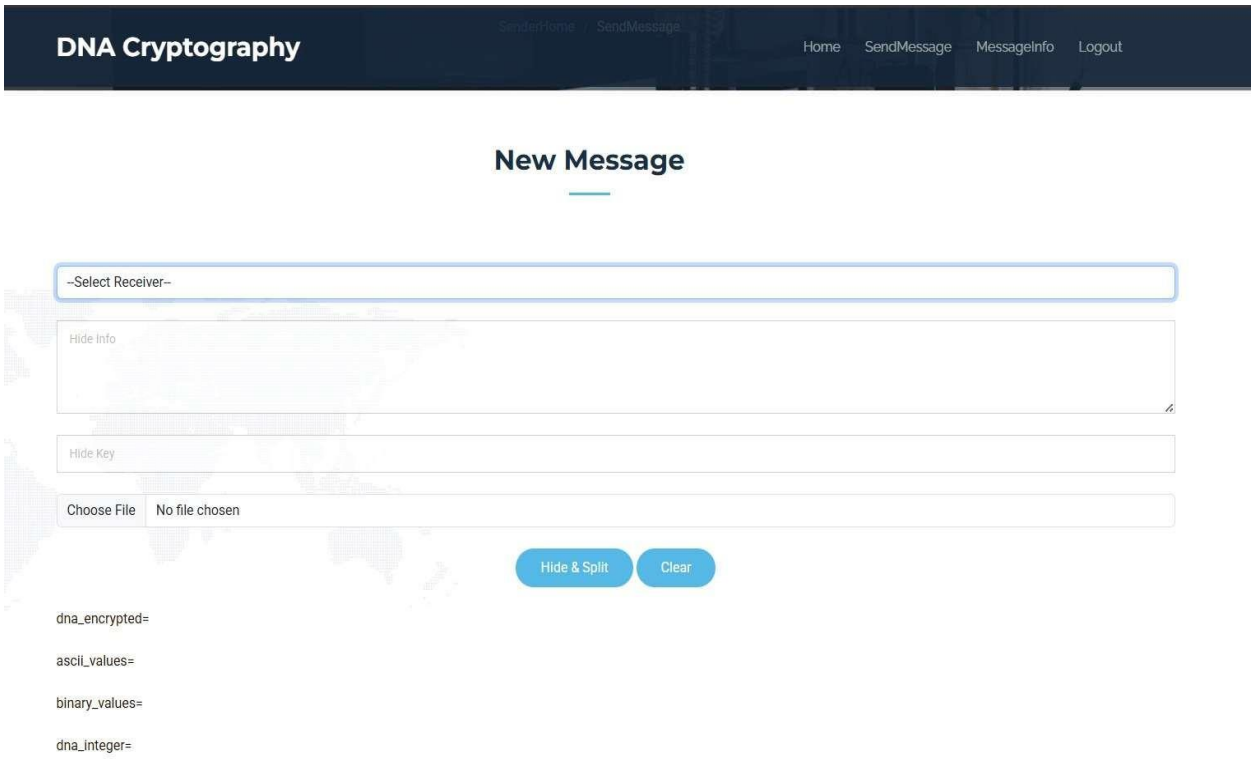
- **Python:** Core programming language for browser algorithm implementation.
- **Visual Studio:** IDE for development.
- **MySQL Server:** Backend for user data management.
- **PIL / OpenCV:** Libraries for image processing and steganography.
- **NumPy:** For efficient array manipulation during DNA encoding.

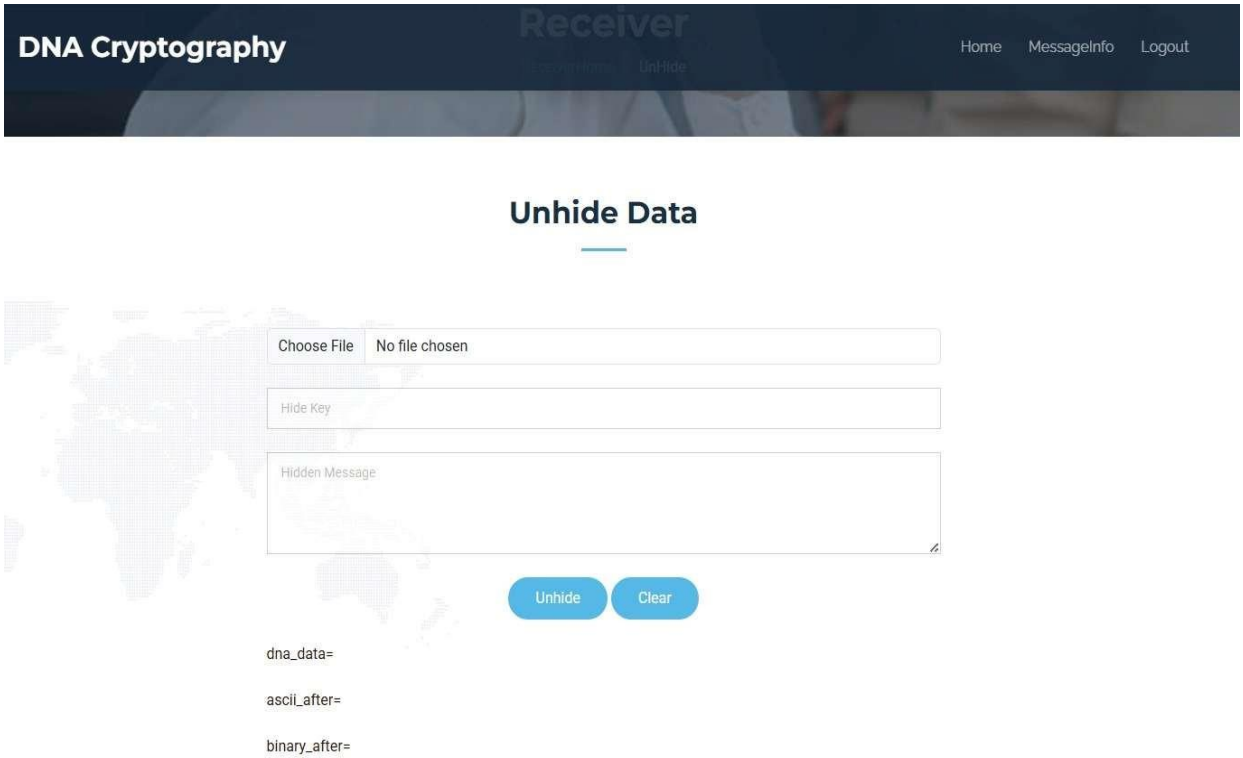
4. PROGRAM

```
from flask import Flask, render_template, request, session, flash
import mysql.connector
app = Flask(__name__)
app.config['SECRET_KEY'] = 'aaa'
@app.route('/')
def home():
    return render_template('index.html')
@app.route('/AdminLogin')
def AdminLogin():
    return render_template('AdminLogin.html')
@app.route('/SenderLogin')
def SenderLogin():
    return render_template('SenderLogin.html')
@app.route('/ReceiverLogin')
def ReceiverLogin():
    return render_template('ReceiverLogin.html')
@app.route('/NewReceiver')
def NewReceiver():
    return render_template('NewReceiver.html')
@app.route('/NewSender')
def NewSender():
    return render_template('NewSender.html')
@app.route("/adminlogin", methods=['GET', 'POST'])
def adminlogin():
    error = None
    if request.method == 'POST':
        if request.form['uname'] == 'admin' and request.form['password'] == 'admin':


            conn = mysql.connector.connect(user='root', password='', host='localhost', database='1dnacryptodb')
            cur = conn.cursor()
            cur.execute("SELECT * FROM sendertb ")
            data = cur.fetchall()
            flash("you are successfully Login")
```

5. RESULTS AND OUTPUT





6. CONCLUSION

This project presents a highly secure and efficient method for data communication by combining DNA computing, image steganography, and modified RSA encryption. The transformation of plaintext into DNA sequences introduces a unique biological approach to encryption, while image steganography effectively conceals the encoded data. The application of modified RSA encryption further strengthens security, ensuring that even if the stego-image is intercepted, it remains inaccessible. Future enhancements may include real-time video steganography and optimizing the algorithm for cloud storage environments to support larger file sizes with lower latency.

REFERENCES

[1] Pavithran, P., et al. "A novel cryptosystem based on DNA cryptography and randomly generated mealy machine." Computers & Security 104 (2021).

[2] Sohal, M., & Sharma, S. "BDNA-A DNA inspired symmetric key cryptographic technique." Journal of King Saud University (2022).

[3] Elamir, M. M., & Mabrouk, M. S. "Secure framework for IoT technology based on RSA and DNA cryptography." Egyptian Journal of Medical Human Genetics (2022).

[4] Chu, L., et al. "A review of DNA cryptography." Intelligent Computing (2025).

[5] Mahjabin, T., et al. "A survey on DNA-based cryptography and steganography." IEEE Access (2023).

[6] Kaur, R., & Kaur, P. (2021). Image steganography using LSB and DWT techniques: A comparative study. International Journal of Computer Applications, 174(14), 1–6.

[7] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.

[8] Swain, G., & Lenka, S. K. (2020). A novel steganography technique using pixel value differencing and RSA encryption.
Journal of Information Security and Applications, 55, 102650.

[9] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752.